

УДК 004.056(075.8)

ББК 32.81я73

М48

Рецензенты:

д-р физ.-мат. наук, проф. кафедры «Информационная безопасность»
факультета «Информатика и системы управления»

МГТУ им. Н.Э. Баумана *В.А. Орлов*;

доц., канд. техн. наук, зав. кафедрой «Автоматизированные системы
обработки информации и управления» института компьютерных
технологий МГУЭСИ *А.А. Микрюков*;

заслуженный деятель науки РФ, д-р техн. наук,
действительный член Международной академии информатизации,
проф. кафедры № 43 «Стратегические информационные
исследования» факультета КИБ НИЯУ МИФИ *А.В. Петраков*

Мельников Д.А.

М48 Информационная безопасность открытых систем : учебник /
Д.А. Мельников. — М. : ФЛИНТА : Наука, 2013. — 448 с.

ISBN 978-5-9765-1613-7 (ФЛИНТА)

ISBN 978-5-02-037923-7 (Наука)

Учебник посвящен теоретическим основам обеспечения ИБ: архитектура ИБ, концептуальные основы (концептуальные понятия) обеспечения ИБ, основы аутентификации, управления доступом, обеспечения неотказуемости, конфиденциальности, целостности, аудита безопасности, оповещения об опасности и обеспечения ключами.

Для студентов государственных образовательных учреждений высшего профессионального образования, обучающихся по направлениям 230700 «Прикладная информатика», 090900 «Информационная безопасность» (ИБ) и 230100 «Информатика и вычислительная техника», а также специальностям 090301 «Компьютерная безопасность», 090303 «Информационная безопасность автоматизированных систем» и 090305 «Информационно-аналитические системы безопасности»; аспирантов и практических работников, занимающихся вопросами синтеза и оптимизации систем обеспечения безопасности открытых (прикладных) информационно-технологических сетей и систем.

УДК 004.056(075.8)

ББК 32.81я73

ISBN 978-5-9765-1613-7 (ФЛИНТА) © Мельников Д.А., 2013

ISBN 978-5-02-037923-7 (Наука) © Издательство «ФЛИНТА», 2013

ОГЛАВЛЕНИЕ

Предисловие	11
Введение	14
Глава 1. Архитектура безопасности ИТС	20
1.1. Почему необходимо защищаться?	20
1.2. Источники и последствия реализации угроз ИБ	21
1.3. Функция, способы и средства обеспечения ИБ	31
1.4. Архитектура безопасности ЭМВОС	33
1.4.1. Термины и определения	34
1.4.2. Услуги и способы обеспечения безопасности	38
1.4.3. Принципы архитектуры безопасности ЭМВОС	47
1.5. Принципы архитектуры безопасности сети Интернет	52
Глава 2. Концепции обеспечения информационной безопасности	53
2.1. Общие концепции обеспечения ИБ	55
2.1.1. Информация, необходимая для обеспечения ИБ	55
2.1.2. Сетевой сегмент безопасности	56
2.1.3. Предположения относительно ПЛБ для определенных СЛБ	61
2.1.4. Надежные (доверенные) объекты/субъекты	62
2.1.5. Доверие	63
2.1.6. Третьи доверенные стороны	64
2.2. Общая информация для обеспечения безопасности	64
2.2.1. Метки безопасности	65
2.2.2. Криптографические проверочные суммы	70
2.2.3. Сертификаты безопасности	72
2.2.4. Способы защиты сертификатов безопасности	76
2.2.5. Маркеры безопасности	83
2.3. Общие средства обеспечения безопасности	84
2.3.1. Вспомогательные средства	85
2.3.2. Функциональные средства	86
2.4. Взаимосвязи между СПБ	88
2.5. Отказ в обслуживании и доступность	90
Глава 3. Теоретические основы аутентификации	92
3.1. Общие положения	92
3.1.1. Основные концепции аутентификации	92
3.1.2. Практические аспекты функционирования СЛАУ	97
3.1.3. Принципы, используемые при аутентификации	102
3.1.4. Фазы (этапы) аутентификации	103
3.1.5. Привлечение ДТС	105

УДК 004.056(075.8)

ББК 32.81я73

М48

Рецензенты:

д-р физ.-мат. наук, проф. кафедры «Информационная безопасность»
факультета «Информатика и системы управления»

МГТУ им. Н.Э. Баумана *В.А. Орлов*;

доц., канд. техн. наук, зав. кафедрой «Автоматизированные системы
обработки информации и управления» института компьютерных
технологий МГУЭСИ *А.А. Микрюков*;

заслуженный деятель науки РФ, д-р техн. наук,
действительный член Международной академии информатизации,
проф. кафедры № 43 «Стратегические информационные
исследования» факультета КИБ НИЯУ МИФИ *А.В. Петраков*

Мельников Д.А.

М48 Информационная безопасность открытых систем : учебник /
Д.А. Мельников. — М. : ФЛИНТА : Наука, 2013. — 448 с.

ISBN 978-5-9765-1613-7 (ФЛИНТА)

ISBN 978-5-02-037923-7 (Наука)

Учебник посвящен теоретическим основам обеспечения ИБ: архитектура ИБ, концептуальные основы (концептуальные понятия) обеспечения ИБ, основы аутентификации, управления доступом, обеспечения неотказуемости, конфиденциальности, целостности, аудита безопасности, оповещения об опасности и обеспечения ключами.

Для студентов государственных образовательных учреждений высшего профессионального образования, обучающихся по направлениям 230700 «Прикладная информатика», 090900 «Информационная безопасность» (ИБ) и 230100 «Информатика и вычислительная техника», а также специальностям 090301 «Компьютерная безопасность», 090303 «Информационная безопасность автоматизированных систем» и 090305 «Информационно-аналитические системы безопасности»; аспирантов и практических работников, занимающихся вопросами синтеза и оптимизации систем обеспечения безопасности открытых (прикладных) информационно-технологических сетей и систем.

УДК 004.056(075.8)

ББК 32.81я73

ISBN 978-5-9765-1613-7 (ФЛИНТА) © Мельников Д.А., 2013

ISBN 978-5-02-037923-7 (Наука) © Издательство «ФЛИНТА», 2013

ОГЛАВЛЕНИЕ

Предисловие	11
Введение	14
Глава 1. Архитектура безопасности ИТС	20
1.1. Почему необходимо защищаться?	20
1.2. Источники и последствия реализации угроз ИБ	21
1.3. Функция, способы и средства обеспечения ИБ	31
1.4. Архитектура безопасности ЭМВОС	33
1.4.1. Термины и определения	34
1.4.2. Услуги и способы обеспечения безопасности	38
1.4.3. Принципы архитектуры безопасности ЭМВОС	47
1.5. Принципы архитектуры безопасности сети Интернет	52
Глава 2. Концепции обеспечения информационной безопасности	53
2.1. Общие концепции обеспечения ИБ	55
2.1.1. Информация, необходимая для обеспечения ИБ	55
2.1.2. Сетевой сегмент безопасности	56
2.1.3. Предположения относительно ПЛБ для определенных СЛБ	61
2.1.4. Надежные (доверенные) объекты/субъекты	62
2.1.5. Доверие	63
2.1.6. Третьи доверенные стороны	64
2.2. Общая информация для обеспечения безопасности	64
2.2.1. Метки безопасности	65
2.2.2. Криптографические проверочные суммы	70
2.2.3. Сертификаты безопасности	72
2.2.4. Способы защиты сертификатов безопасности	76
2.2.5. Маркеры безопасности	83
2.3. Общие средства обеспечения безопасности	84
2.3.1. Вспомогательные средства	85
2.3.2. Функциональные средства	86
2.4. Взаимосвязи между СПБ	88
2.5. Отказ в обслуживании и доступность	90
Глава 3. Теоретические основы аутентификации	92
3.1. Общие положения	92
3.1.1. Основные концепции аутентификации	92
3.1.2. Практические аспекты функционирования СЛАУ	97
3.1.3. Принципы, используемые при аутентификации	102
3.1.4. Фазы (этапы) аутентификации	103
3.1.5. Привлечение ДТС	105

3.1.6. Типы участников информационного взаимодействия	111
3.1.7. Аутентификация физического лица (гражданина, пользователя), или персонификация	112
3.1.8. Типы атак на процедуру аутентификации	112
3.2. Вспомогательная информация и средства аутентификации	116
3.2.1. Вспомогательная информация для аутентификации	116
3.2.2. Средства аутентификации	123
3.3. Свойства способов аутентификации	131
3.3.1. Симметричные/асимметричные методы аутентификации	131
3.3.2. Использование криптографических/некриптографических методов	132
3.3.3. Типы аутентификации	132
3.4. Способы аутентификации	134
3.4.1. Классификация по критерию уязвимости	134
3.4.2. Инициирование доставки	147
3.4.3. Использование СЕРТ АУ	148
3.4.4. Обоюдная аутентификация	148
3.4.5. Характеристики классов способов аутентификации	149
3.4.6. Классификация на основе конфигурации	151
3.5. Взаимодействие с другими службами и способами обеспечения безопасности	156
3.5.1. Управление доступом	156
3.5.2. Целостность данных	156
3.5.3. Конфиденциальность данных	157
3.5.4. Неотказуемость	157
3.5.5. Аудит	158
3.6. Персонификация (аутентификация пользователей)	158
3.6.1. Общие положения	158
3.6.2. Процессы, действующие от имени пользователя	162
3.7. Аутентификация в ЭМВОС и Интернет-архитектуре	162
3.7.1. Аутентификация объекта	162
3.7.2. Аутентификация источника данных	163
3.7.3. Использование аутентификации уровнями ЭМВОС и Интернет-архитектуры	163
3.8. Практические аспекты парирования атак типа «повторная передача» на основе применения уникальных чисел или встречных запросов	165
3.8.1. Уникальные числа	165
3.8.2. Встречные запросы	166
3.9. Защита процедуры аутентификации	167
3.9.1. Атаки типа «прослушивание/повторная передача»	167
3.9.2. Атаки типа «повторная передача одной и той же проверяющей стороне»	167

3.9.3. Атаки типа «повторная передача разным проверяющим сторонам»	168
3.9.4. Атаки типа «перехват/повторная передача»	168
3.9.5. Использование индикатора «приглашение/запрос» для защиты от атак нарушителя	170
3.9.6. Протокол на основе встречных вызовов	170
3.9.7. Протокол на основе уникальных чисел	172
3.10. Примеры способов аутентификации	172
3.10.1. Способ аутентификации с использованием уникального числа и интерактивного СЕРТ АУ	173
3.10.2. Способ аутентификации с использованием встречного запроса и интерактивного СЕРТ АУ	175
Глава 4. Теоретические основы управления доступом	180
4.1. Общие положения	180
4.1.1. Цель управления доступом	180
4.1.2. Основные аспекты УД	181
4.1.3. Распределение компонентов УД	193
4.1.4. Распределение компонентов УД в нескольких ССБ	195
4.1.5. Угрозы УД	196
4.2. Политики УД	196
4.2.1. Отображение политики УД	197
4.2.2. Управление политиками	199
4.2.3. Детализация и локализация	200
4.2.4. Унаследованные правила	201
4.2.5. Приоритет среди правил ПЛУД	202
4.2.6. Правила ПЛУД в режиме «по умолчанию»	203
4.2.7. Отображение политики среди взаимодействующих ССБ	203
4.3. Вспомогательная информация и средства УД	204
4.3.1. ВИ для УД	204
4.3.2. Защита ВИУД	208
4.3.3. Средства УД	210
4.4. Классификация способов УД	216
4.4.1. Введение	216
4.4.2. Схема УД на основе списков доступа	219
4.4.3. Мандатная схема	223
4.4.4. Схема на основе меток безопасности	226
4.4.5. Контекстная схема	230
4.5. Взаимодействие с другими СЛБ и СПБ	232
4.5.1. Аутентификация	232
4.5.2. Обеспечение целостности данных	233
4.5.3. Обеспечение конфиденциальности данных	233

4.5.4. Аудит	233
4.5.5. Другие СЛБ, связанные с УД	235
4.6. Обмен СЕРТ УД между компонентами	236
4.6.1. Ретрансляция нескольких СЕРТ УД	236
4.7. Управление доступом в ЭМВОС и Интернет-архитектуре	238
4.7.1. Общие положения	238
4.7.2. Использование УД в рамках уровней ЭМВОС и Интернет-архитектуры	238
4.8. Проблема уникальности (неединственность) параметров подлинности для УД	239
4.9. Распределение компонентов УД	241
4.9.1. Реализационные аспекты	242
4.9.2. Размещение ФПРИ- и ФПРР-модулей	243
4.9.3. Информационное взаимодействие между компонентами УД	244
4.10. Сравнительный анализ УДПР и УДПП	246
4.11. Способ обеспечения ретрансляции ВИУД через инициатора	247
Глава 5. Теоретические основы обеспечения неотказуемости	251
5.1. Общие положения	252
5.1.1. Основные концепции обеспечения неотказуемости	252
5.1.2. Роль и участие ДТС	253
5.1.3. Фазы процедуры обеспечения неотказуемости	255
5.1.4. Некоторые формы служб обеспечения неотказуемости	258
5.1.5. Примеры доказательств при обеспечении неотказуемости в рамках ЭМВОС и Интернет-архитектуры	260
5.2. Политики обеспечения неотказуемости	261
5.3. Вспомогательная информация и средства обеспечения неотказуемости	263
5.3.1. Вспомогательная информация	263
5.3.2. Средства обеспечения неотказуемости	264
5.4. Способы обеспечения неотказуемости	269
5.4.1. СЛНТ, использующая маркеры безопасности (защитные конверты) ДТС	269
5.4.2. СЛНТ, использующая маркеры безопасности и модули, защищающие от несанкционированного вмешательства	270
5.4.3. СЛНТ, использующая ЭЦП	271
5.4.4. СЛНТ, использующая метки времени	273
5.4.5. СЛНТ, использующая промежуточную ДТС	274

5.4.6. СЛНТ, использующая нотариальное заверение	274
5.4.7. Угрозы СЛНТ	275
5.5. Взаимосвязи с другими СЛБ и СПБ	281
5.5.1. Аутентификация	281
5.5.2. Управление доступом	281
5.5.3. Обеспечение конфиденциальности	281
5.5.4. Обеспечение целостности	281
5.5.5. Аудит	282
5.5.6. Обеспечение ключами	282
5.6. СЛНТ в системах ЭМВОС и Интернет-архитектуры	282
5.6.1. СЛНТ с подтверждением источника данных	282
5.6.2. СЛНТ с подтверждением доставки данных	283
5.7. СЛНТ в системах хранения и ретрансляции	284
5.8. Восстановление в СЛНТ	286
5.9. Взаимодействие со Службой единого каталога	289
Глава 6. Теоретические основы обеспечения конфиденциальности	295
6.1. Общие положения	296
6.1.1. Основные концепции обеспечения конфиденциальности	296
6.1.2. Классы СЛКН	301
6.1.3. Типы СПКН	302
6.1.4. Угрозы конфиденциальности	303
6.1.5. Типы атак на конфиденциальность	305
6.2. Политики обеспечения конфиденциальности	306
6.2.1. Отображение (описание) политики	306
6.3. Вспомогательная информация и средства обеспечения конфиденциальности	307
6.3.1. Вспомогательная информация	307
6.3.2. Средства обеспечения конфиденциальности	308
6.4. Способы обеспечения конфиденциальности	310
6.4.1. Обеспечение конфиденциальности на основе предотвращения доступа	311
6.4.2. Обеспечение конфиденциальности на основе шифрования	311
6.4.3. Обеспечение конфиденциальности на основе контекстно-зависимого размещения	315
6.5. Взаимодействие с другими СЛБ и СПБ	316
6.5.1. Управление доступом	316
6.6. Обеспечение конфиденциальности в ЭМВОС и Интернет-архитектуре	316
6.6.1. Услуга по обеспечению конфиденциальности информационного обмена с установлением соединения	317

6.6.2. Услуга по обеспечению конфиденциальности информационного обмена без установления соединения (дейтаграммный режим)	317
6.6.3. Услуга по обеспечению конфиденциальности отдельных полей	317
6.6.4. Услуга по обеспечению конфиденциальности потока трафика	318
6.6.5. Использование услуг по обеспечению конфиденциальности на уровнях ЭМВОС и Интернет-архитектуры	318
6.7. Форматы представления информации	321
6.8. Скрытые каналы передачи	323
Глава 7. Теоретические основы обеспечения целостности	328
7.1. Общие положения	329
7.1.1. Основные концепции обеспечения целостности	332
7.1.2. Типы СЛЦЛ	332
7.1.3. Типы СПЦЛ	333
7.1.4. Угрозы целостности	334
7.1.5. Типы атак на целостность	335
7.2. Политики обеспечения целостности	336
7.2.1. Описание политики	336
7.3. Вспомогательная информация и средства обеспечения целостности	338
7.3.1. ВИ, необходимая для обеспечения целостности	338
7.3.2. Средства обеспечения целостности	340
7.4. Классификация способов обеспечения целостности	341
7.4.1. Обеспечение целостности на основе криптографии	341
7.4.2. Обеспечение целостности на основе контекста сообщения	345
7.4.3. Обеспечение целостности на основе обнаружения нарушений и передачи ответных квитанций	347
7.4.4. Обеспечение целостности путем препятствования (предотвращения)	348
7.5. Взаимосвязи с другими СЛБ и СПБ	349
7.5.1. Управление доступом	349
7.5.2. Аутентификация источника данных	349
7.5.3. Конфиденциальность	349
7.6. Обеспечение целостности в ЭМВОС и Интернет-архитектуре	350
7.6.1. Целостность соединения с восстановлением	350
7.6.2. Целостность соединения без восстановления	350

7.6.3. Целостность отдельных полей при виртуальном соединении	351
7.6.4. Целостность соединения в дейтаграммном режиме	351
7.6.5. Целостность отдельных полей при соединении в дейтаграммном режиме	351
7.6.6. Применение СЛЦЛ в рамках уровней ЭМВОС и Интернет-архитектуры	351
7.7. Целостность внешних данных	353

Глава 8. Теоретические основы аудита безопасности

и оповещения об опасности	358
8.1. Общие положения	360
8.1.1. Модель и функции	361
8.1.2. Фазы процедур АДБ и оповещения об опасности	365
8.1.3. Корреляция аудиторской информации	368
8.2. Политики и другие аспекты аудита безопасности и оповещения об опасности	369
8.2.1. Политика	369
8.2.2. Законодательные аспекты	369
8.2.3. Требования к защите	370
8.3. Вспомогательная информация и средства для аудита безопасности и оповещения об опасности	371
8.3.1. ВИ в интересах СЛАО	372
8.3.2. Средства для СЛАО	373
8.4. Способы проведения АДБ и применения СОП	377
8.5. Взаимосвязи с другими СЛБ и СПБ	377
8.5.1. Аутентификация объекта/субъекта	377
8.5.2. Аутентификация источника данных	378
8.5.3. Управление доступом	378
8.5.4. Обеспечение конфиденциальности	378
8.5.5. Обеспечение целостности	378
8.5.6. Обеспечение неотказуемости	379
8.6. Общие принципы АДБ и СОП в ЭМВОС и Интернет-архитектуре	379
8.7. Реализация модели АДБ и СОП	381
8.8. Регистрация времени возникновения событий, подлежащих аудиторскому контролю	384

Глава 9. Теоретические основы обеспечения ключами

9.1. Общая модель обеспечения ключами	390
9.1.1. Общие положения	390
9.1.2. Защита ключей	390
9.1.3. Общая модель жизненного цикла ключа	393

9.2. Основные концепции обеспечения ключами	398
9.2.1. Службы (услуги по) обеспечения(ю) ключами	398
9.2.2. Обеспечивающие службы (услуги)	405
9.3. Концептуальные модели распределения ключей между двумя взаимодействующими сторонами	406
9.3.1. Общие положения	406
9.3.2. Распределение ключей между связанными объектами	407
9.3.3. Распределение ключей в рамках одного ССБ	407
9.3.4. Распределение ключей между двумя ССБ	411
9.4. Провайдеры специализированных услуг	414
9.5. Угрозы системе обеспечения ключами	414
9.6. Информационные объекты в службе обеспечения ключами	415
9.7. Классы прикладных криптографических систем	416
9.7.1. Единая классификация криптографических систем	416
9.7.2. СЛАУ и СЛЦЛ и ключи	417
9.7.3. СЛКН и ключи	419
9.7.4. Совмещенные службы	420
9.8. Обеспечение жизненного цикла СЕРТ ОК	420
9.8.1. Общие положения	420
9.8.2. Удостоверяющий центр	420
9.8.3. Процедура сертификации	422
9.8.4. Распределение и использование СЕРТ ОК	429
9.8.5. Маршруты сертификации	430
9.8.6. Аннулирование сертификатов	430
Список используемых сокращений	434
Литература	436

Предисловие

Настоящий учебник предназначен для студентов государственных образовательных учреждений высшего профессионального образования, обучающихся по направлениям 230700 «Прикладная информатика», 090900 «Информационная безопасность» (ИБ) и 230100 «Информатика и вычислительная техника», а также специальностям 090301 «Компьютерная безопасность», 090303 «Информационная безопасность автоматизированных систем» и 090305 «Информационно-аналитические системы безопасности». Учебник будет полезен аспирантам и практическим работникам, занимающимся вопросами синтеза и оптимизации систем обеспечения безопасности открытых (прикладных) информационно-технологических сетей и систем (ИТС). Он состоит из девяти глав.

В первой главе представлены модель возможных источников угроз ИБ и последствия их реализации, архитектуры безопасности ЭМВОС и пятиуровневой Интернет-архитектуры, основные термины и определения, способы и средства защиты информации, услуги и службы обеспечения ИБ.

Вторая глава посвящена основным концепциям (концептуальным понятиям), которые непосредственно связаны с политиками, правилами политик и участниками процедур обеспечения ИБ, способами и средствами защиты открытых (прикладных) ИТС, подсистем и объектов, расположенных внутри таких систем, а также с взаимодействием ИТС между собой.

В третьей главе определен общий подход к реализации служб аутентификации. В главе рассматриваются способы и средства обеспечения аутентификации, которые нацелены на парирование угроз, связанных с проведением атак типа «маскарад» и «повторная передача сообщений». Особое внимание уделено персонализации и схемам аутентификации.

В четвертой главе рассмотрен общий подход к реализации службы управления доступом, а также определены базовые концепции УД и описаны наиболее известные службы и способы УД.

Современное развитие информационных технологий (ИТ) затронуло практически все сферы жизнедеятельности человека — экономику, финансы, военную и социальную сферы, науку, образование и др. В настоящее время речь идет уже об информационно-технологических сетях и системах (ИТС), которые стали логическим результатом развития вычислительных и информационно-телекоммуникационных сетей и систем. Это также обусловлено тем, что:

- 1) ИТС основаны на применении современных ИТ, под которыми понимается совокупность процессов и методов поиска, сбора, хранения, обработки, предоставления, распространения информации и способов осуществления (реализации) таких процессов и методов;
- 2) по своему предназначению ИТС делятся на *информационные*, которые обеспечивают электронный информационный обмен между пользователями или прикладными процессами, инициированными пользователями, и *технологические*, которые обеспечивают работоспособность информационных систем, или обеспечивают решение специализированных задач (например глобальной навигации и местопределения и др.);
- 3) даже в рамках одной ИТС функционируют две группы процессов: *информационные*, которые реализуются в соответствии с протоколами информационного обмена (например, в Интернет-архитектуре — протоколы IP, TCP, FTP, HTTP и др.), и *технологические*, которые обеспечивают работоспособность, надежность и эффективность самой ИТС (например, в Интернет-архитектуре — протоколы NTP, SNMP, DNS-система и др.).

Абстрактно ИТС можно представить как совокупность систем, связанных между собой некоторой передающей средой. В качестве систем выступают главные¹ (серверы), терминаль-

¹ Главная вычислительная машина (GBM) или главный компьютер («a host computer», RFC—1122).

ные (концентраторы, мультиплексоры) и персональные ЭВМ (компьютеры) и узлы связи (коммутаторы, маршрутизаторы и др.). Передающая среда может иметь любую физическую природу и представлять собой совокупность проводных, волоконно-оптических, радиорелейных, тропосферных и спутниковых линий (каналов) связи. В каждой из систем сети существует некоторая совокупность процессов¹. Процессы, распределенные по разным системам, взаимодействуют через передающую среду путем обмена сообщениями².

Для обеспечения открытости, гибкости и эффективности ИТС управление процессами организуется по многоуровневой схеме, приведенной на рис. В.1. В каждой из систем прямоугольниками обозначены программные и аппаратные модули, реализующие определенные функции обработки и передачи данных. Модули иерархически распределены по уровням 1...7.

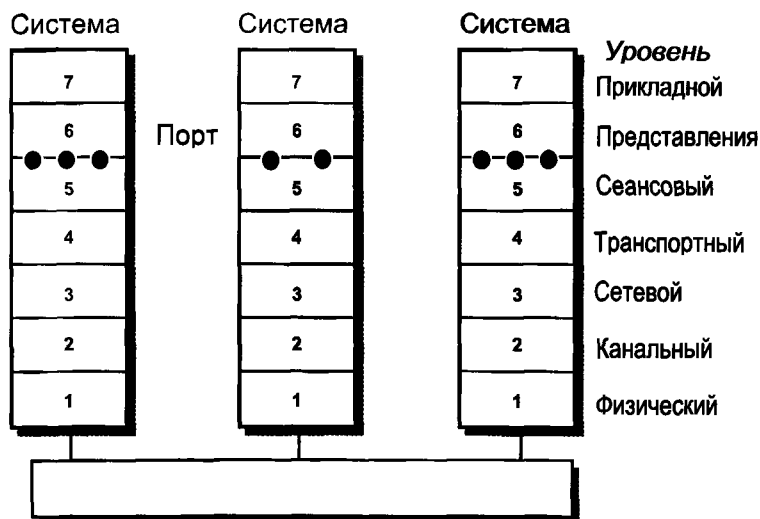


Рис. В.1. Многоуровневая организация управления (архитектура) ИТС (Эталонная модель взаимодействия открытых систем)

¹ Процесс — это динамический объект, реализующий собой целенаправленный акт обработки данных.

² Сообщение — последовательность данных, имеющая законченное смысловое значение.

Представленная выше семиуровневая модель (Эталонная модель взаимодействия открытых систем — ЭМВОС, Reference Model for Open Systems Interconnecting), именуемая *архитектурой открытых систем*, принята в качестве стандарта Международным союзом электросвязи (МСЭ, ITU-T Rec. X.200, 1994) и Международной организацией по стандартизации (МОС, International Organization for Standardization, ISO/IEC¹ 7498-1) и используется как основа при разработке ИТС.

Количество уровней архитектуры и распределение функций между ними существенно влияют на сложность программного обеспечения ЭВМ, входящих в ИТС, и на эффективность самой ИТС. Формальной процедуры выбора количества уровней архитектуры не существует. Выбор производится эмпирическим путем на основе анализа различных вариантов организации ИТС и опыта разработки и эксплуатации ранее созданных сетей и систем. Это относится в первую очередь к архитектуре Интернет-сети (RFC-1122), представленной на рис. В.2.

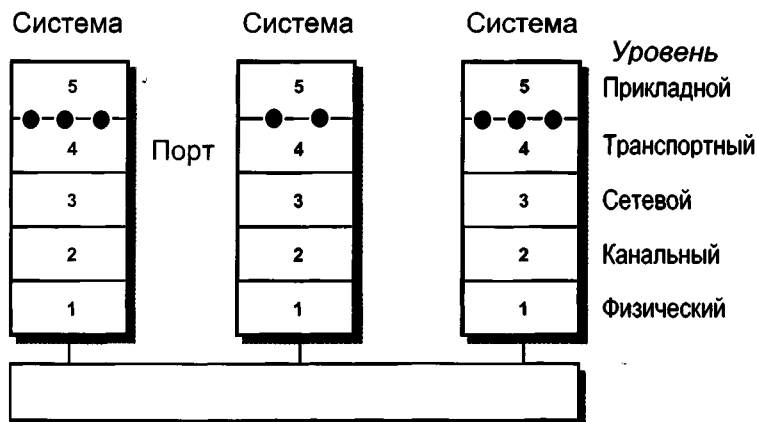


Рис. В.2. Интернет-архитектура

¹ Международная электротехническая комиссия (МЭК, International Electrotechnical Commission) — международная некоммерческая организация по стандартизации в области электрических, электронных и смежных технологий.

Различие ЭМВОС и Интернет-архитектуры состоит в том, что:

- функции сеансового (4) уровня ЭМВОС объединены с функциями транспортного (3) уровня. В частности, Интернет-протокол управления передачей (Transmission control protocol — TCP) является протоколом транспортного уровня и на него возложены дополнительные функции организации сеансов связи на период взаимодействия процессов. TCP-протокол по запросам процессов создает *порты* для приема и передачи сообщений и организует виртуальные соединения — *логические каналы* (associations);
- функции уровня представления (6) ЭМВОС объединены с функциями прикладного (7) уровня. В частности, Интернет-протокол TELNET реализует трансляцию различных языков, форматов данных и кодов для взаимодействия разнотипных ЭВМ (компьютеров) и устанавливает стандартный способ взаимодействия для каждой программы (процесса) с терминалами любого типа, а также для взаимодействия «терминал-терминал» и «процесс-процесс». TELNET-протокол вводит единый для всей Интернет-сети интерфейс, называемый сетевой виртуальный терминал (Network Virtual Terminal — NVT). В то же время в рамках Интернет-архитектуры TELNET-протокол относится к прикладному (7) уровню (RFC-1123).

Отображение ЭМВОС в Интернет-архитектуру представлено на рис. В.3.

ИТС, соответствующие ЭМВОС и Интернет-архитектуре, являются открытыми системами, под которыми понимаются базы данных (БД), распределенные прикладные системы разного назначения, системы с открытой распределенной обработкой и собственно взаимодействие самих ИТС.

Происходящие сегодня мировые процессы глобализации и тотальной информатизации привели к появлению

«киберпространства»¹. Фактически киберпространство представляет собой глобальную информационно-технологическую инфраструктуру (ИТИ). Киберпространство наряду с положительными и эффективными факторами воздействия на развитие и гармонизацию мировой цивилизации принесло и новые виды угроз личности, обществу, государству и всему человечеству.

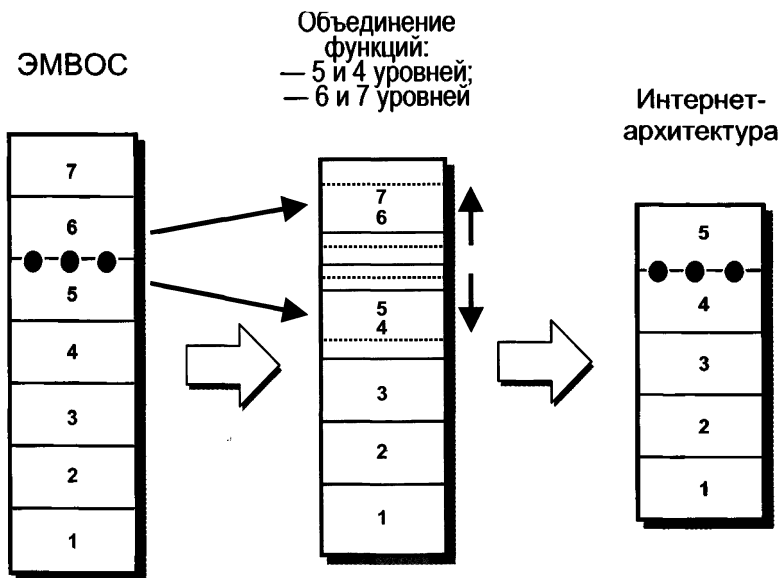


Рис. В.3. Отображение ЭМВОС в Интернет-архитектуру

Парирование таких киберугроз, обеспечение ИБ национальных ИТИ, выявление и предотвращение киберпреступлений стали стратегическими задачами практически всех экономически развитых государств мира. Международные (МСЭ, МОС, МЭК

¹ Киберпространство (cyber space) — пришедшее из американской жизни понятие, введенное писателем Уильямом Гибсоном в книге «Neuromancer (Remembering Tomorrow)». Оно описывает виртуальное пространство, в котором циркулируют электронные данные всех компьютеров мира.

и др.) и национальные организации (NIST¹, ANSI² и др.) по стандартизации проводят активную работу по выработке соответствующих рекомендаций и стандартов по защите не только информации, циркулирующей в ИТС, но и самих ИТС.

Основополагающим международным стандартом, положившим начало развитию всей международной системы стандартизации в области ИБ, стала *Архитектура безопасности взаимодействия открытых систем* (Security Architecture for Open Systems Interconnection; ITU-T Rec. X.800, 1991; ISO/IEC 7498-2: 1989).

Позже были приняты международные стандарты, определяющие основные концепции и концептуальные понятия обеспечения ИБ открытых систем (ITU-T Rec. X.810, 1995; ISO/IEC 10181-1: 1996). В рамках этих концепций обеспечения ИБ открытых систем были выделены основные составляющие (направления) обеспечения ИБ, к которым относятся:

- аутентификация (ITU-T Rec. X.811, 1995; ISO/IEC 10181-2: 1996);
- управление доступом (ITU-T Rec. X.812, 1995; ISO/IEC 10181-3: 1996);
- обеспечение неотказуемости (ITU-T Rec. X.813, 1995; ISO/IEC 10181-4: 1996);
- обеспечение конфиденциальности (ITU-T Rec. X.814, 1995; ISO/IEC 10181-5: 1996);
- обеспечение целостности (ITU-T Rec. X.815, 1995; ISO/IEC 10181-6: 1996);
- аудит ИБ и оповещение об опасности (ITU-T Rec. X.815, 1995; ISO/IEC 10181-7: 1996);
- обеспечение ключами (ISO/IEC 11770-1: 2010).

Все перечисленные выше стандарты и легли в основу данного учебника.

¹ Национальный институт стандартов и технологий (National Institute of Standards and Technology) Министерства торговли США.

² Американский национальный институт стандартов (American National Standards Institute) — объединение американских промышленных и деловых групп, разрабатывающее торговые и коммуникационные стандарты.

АРХИТЕКТУРА БЕЗОПАСНОСТИ ИТС

Современное развитие ИТС характеризуется в первую очередь их глобализацией и проникновением во все сферы жизнедеятельности человека. Сети Интернет — яркий тому пример. Однако, сети Интернет, являясь уникальным новшеством и «носителем всемирной информатизации», преподнесли своим пользователям (потребителям информационных услуг) новый набор весьма своеобразных и специфических угроз личности, государству и обществу. Такое развитие событий обострило проблемы защиты информации в ИТС и, в частности, в сетях Интернет. Более того, огромное количество предложений и средств по обеспечению ИБ в ИТС привело их разработчиков к созданию *архитектуры* ИБ.

1.1. Почему необходимо защищаться?

Разработчики ИТС при создании сетей закладывают в них весь необходимый набор функций, обеспечивающих высококачественный информационный обмен с помощью различных абонентских терминалов и использованием различных сред передачи (первичных систем электросвязи). Очевидно, что ошибки при организации и ведении информационного обмена вероятны и их появление обусловлено эффективностью функционирования отдельных сетевых программно-аппаратных комплексов и всей сети в целом, а также помеховой обстановкой в тех или иных каналах (линиях) связи. Защита от такого рода ошибок не является предметом рассмотрения данной книги. Хотя в настоящее время существуют методы активных атак, замаскированные под функциональные ошибки ИТС.

Вся мировая история показывает, что шпионская (разведывательная) деятельность по добыванию различного рода информации является «основой основ» политики любого государства (включая экономический шпионаж). Человек непредсказуем:

окружающие обстоятельства могут повлечь его к поиску информации, доступ к которой ограничен определенным кругом лиц, — это с одной стороны. А с другой, — любой владелец конфиденциальной информации желает обезопасить ее от посторонних. Именно наличие человеческого фактора при эксплуатации и функционировании ИТС обуславливает необходимость дополнения стандартного набора функций для открытых систем, т.е. ЭМВОС или Интернет-архитектуры, еще одной функцией обеспечения безопасности ИТС.

Электронные коммуникации сближают людей: время и расстояния исчезают. Глобальная Интернет-сеть объединяет миллионы жителей Земли и обрабатывает огромное количество информации. Поэтому сеть Интернет является «широким полем деятельности» для специалистов в области компьютерного шпионажа (компьютерной разведки).

Очень часто можно слышать, что сеть Интернет предоставляет широчайший спектр услуг по защите информации и т.д. Возникает вопрос: «А так ли это на самом деле?» Пользователям сети Интернет необходимо знать, что в США существует директива президента страны «Об управлении шифрованием в обществе» («Public Encryption Management»), которая однозначно устанавливает, что вывозимые (за пределы государства, т.е. США) криптографические средства защиты информации не должны служить препятствием для органов электронной разведки США при добытии ими информации. Другими словами, любые программные и аппаратные средства защиты информации (в том числе и криптографические), используемые в сети Интернет, являются «прозрачными» для специальных служб США¹.

1.2. Источники и последствия реализации угроз ИБ

Необходимо сразу отметить, что именно противоправная деятельность человека (или группы людей) является источником угроз информационной безопасности (ИБ) ИТС.

¹ По данным некоторых зарубежных экспертов, орбитальная группировка разведывательных спутников системы «Эшелон» (ECHELON) США контролирует до 90% мирового интернет-трафика.

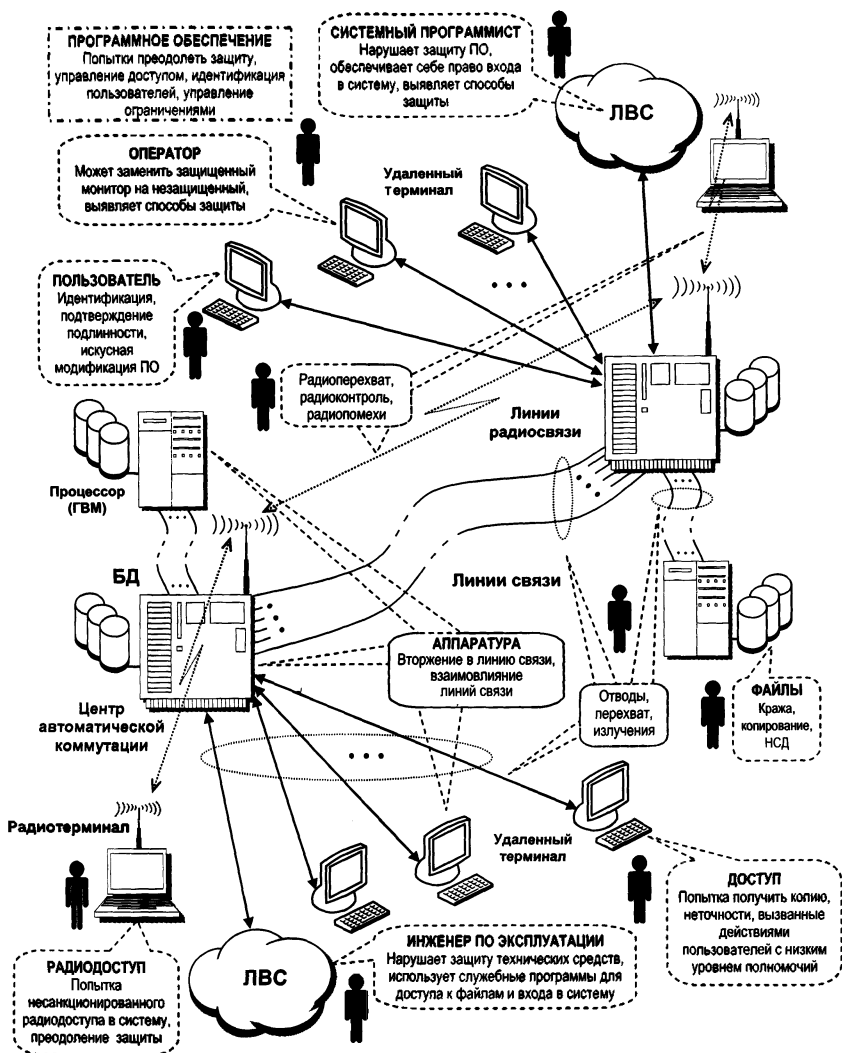


Рис. 1.1. Источники возможных угроз безопасности ИТС

Современные модели угроз ИБ ИТС, предлагаемые и рекомендуемые большинством официальных структур, включая отечественные, построены на основе моделирования поведения

нарушителя и поэтому весьма громоздки, и что самое главное — неадекватны. В погоне за чрезмерной детализацией угроз и поведения нарушителя (модель нарушителя) можно вообще «уйти в сторону» от решаемой задачи. Дело в том, что никогда нельзя спрогнозировать поступки и действия того или иного возможного нарушителя. Более того, часто бывает так, что нарушителем становится человек, от которого вообще не ожидали каких-либо противоправных действий.

Очевидно, что сами угрозы могут варьироваться, изменяться и обновляться, так как в основе таких угроз лежит поведение человека, которое непредсказуемо, но с точки зрения их реализации (претворения в жизнь) и достижения результата, они все приводят к последствиям, которые могут быть объединены в группы (виды).

Специалисты, занимающиеся проблемой информационной безопасности в сети Интернет, определили четыре вида последствий угроз: вскрытие, обман, разрушение, захват (узурпация). Последствием воздействия угроз является нарушение безопасности ИТС (рис. 1.1). Рассмотрим эти последствия, а также перечень и сущность различных видов угрожающих воздействий, которые являются причинами дискредитации системы безопасности ИТС. (Угрожающие действия, являющиеся следствием случайных событий (природных явлений), обозначены «*».)

А. «(Несанкционированное) Вскрытие» (unauthorized disclosure): Обстоятельство или событие, посредством которого субъект получил доступ к охраняемым данным (например конфиденциальным), не имея на самом деле прав доступа к ним. Следующие угрожающие действия могут стать причиной несанкционированного вскрытия:

А.1. «Разоблачение» (exposure): Угрожающее действие, посредством которого охраняемые данные стали доступны непосредственно субъекту, не имеющему на это право. Оно включает:

А.1.1. «Преднамеренное разоблачение» (deliberate exposure): Умышленный допуск к охраняемым данным субъекта, не имеющему на это право.

А.1.2. «Просмотр остатка данных» (scavenging): Исследование доступных данных, оставшихся в системе, с целью получения несанкционированного знания охраняемых данных.

А.1.3.* «Ошибка человека» (human error): Действие или бездействие человека, которое неумышленно повлекло за собой несанкционированное знание субъектом охраняемых данных.

А.1.4.* «Аппаратно-программная ошибка» (hardware or software error): Ошибка системы, которая повлекла за собой несанкционированное знание субъектом охраняемых данных.

А.2. «Перехват» (interception): Угрожающее действие, посредством которого субъект имеет непосредственный несанкционированный доступ к охраняемым данным, циркулирующим между полномочными источниками и получателями. Оно включает:

А.2.1. «Кража» (theft): Получение доступа к охраняемым данным путем воровства различных накопителей информации независимо от их физической сущности (например кассеты с магнитной лентой или магнитные диски и др.).

А.2.2. «Прослушивание» (пассивное, wiretapping/passive): Обнаружение и запись данных, циркулирующих между двумя терминалами в системе связи.

А.2.3. «Анализ излучений» (emanations analysis): Непосредственное получение содержания передаваемых в системе связи сообщений путем обнаружения и обработки сигнала, излучаемого системой и «переносящего» данные, но не предназначенного для передачи сообщений.

А.3. «Умозаключение» (inference): Угрожающее действие, посредством которого субъект получает несанкционированный, но не прямой, доступ к охраняемым данным (но не обязательно к данным, содержащимся в передаваемых сообщениях) путем осмысления характеристик или «побочных продуктов» систем связи. Оно включает:

А.3.1. «Анализ трафика» (traffic analysis): Получение знания охраняемых данных путем наблюдения за изменением характеристик системы связи, которая транспортирует данные.

А.3.2. «Анализ сигналов» (signals analysis): Непрямое получение знания охраняемых данных, передаваемых в системе связи, путем обнаружения и анализа сигнала, излучаемого системой и «переносящего» данные, но не предназначенного для передачи сообщений.

А.4. «Вторжение» (intrusion): Угрожающее действие, посредством которого субъект обеспечивает несанкционированный доступ к охраняемым данным путем обмана средств обеспечения безопасности системы. Оно включает:

А.4.1. «Посязгательство» (trespass): Получение несанкционированного физического доступа к охраняемым данным путем обмана системных средств защиты информации.

А.4.2. «Проникновение» (penetration): Получение несанкционированного логического доступа к охраняемым данным путем обмана системных средств защиты информации.

А.4.3. «Реконструкция» (reverse engineering): Добыча охраняемых данных путем декомпозиции и анализа конструкции системного компонента.

А.4.4. «Криптоанализ» (cryptanalysis): Преобразование зашифрованных данных в открытый текст (дешифрование) без априорных знаний о параметрах и алгоритме процедуры зашифрования.

В. «Обман» (deception): Обстоятельство или событие, которое может повлечь за собой получение полномочным субъектом искаженных данных, воспринимаемых им как верные. Следующие угрожающие действия могут повлечь за собой обман:

В.1. «Маскарад» (masquerade): Угрожающее действие, посредством которого субъект получает несанкционированный доступ к системе или осуществляет злонамеренное действие, выступая в роли полномочного субъекта:

В.1.1. «Мистификация» (spoof): Попытка субъекта осуществить несанкционированный доступ в систему под видом полномочного пользователя.

В.1.2. «Устройство для злонамеренных действий» (malicious logic): С точки зрения «маскарада», любое аппаратно-программное устройство или программное обеспечение (например «троянский конь»), которое якобы предназначено для поддержания эффективного и устойчивого функционирования системы, но на самом деле обеспечивает несанкционированный доступ к системным ресурсам или обманывает пользователя путем выполнения другого злонамеренного акта.

В.2. «Фальсификация» (falsification): Угрожающее действие, посредством которого искаженные данные вводят в заблуждения полномочного субъекта:

В.2.1. «Подмена» (substitution): Внесение изменений или замена истинных данных на искаженные, которые служат для обмана полномочного субъекта.

В.2.2. «Вставка» (insertion): Добавление искаженных данных, которые служат для обмана полномочного субъекта.

В.3. «Отказ» (repudiation): Угрожающее действие, посредством которого субъект обманывает другого путем ложного отрицания ответственности за какое-либо собственное действие:

В.3.1. «Ложный отказ источника» (false denial of origin): Действие, посредством которого автор («держатель») данных отрицает свою ответственность за авторство (генерирование) этих данных.

В.3.2. «Ложный отказ получателя» (false denial of receipt): Действие, посредством которого получатель данных отказывается от получения этих данных и обладания ими.

С. «Разрушение» (disruption): Обстоятельство или событие, которое препятствует или прерывает корректное функционирование системных служб и реализацию необходимых действий. Следующие угрожающие действия могут вызвать разрушение:

С.1. «Вредительство» (*incapacitation*): Угрожающее действие, которое препятствует или прерывает функционирование системы путем вывода из строя ее компонентов:

С.1.1. «Устройство для злонамеренных действий» (*malicious logic*): С точки зрения «вредительства», любое аппаратно-программное устройство или программное обеспечение (например «логическая бомба»), умышленно встраиваемое в систему для нарушения ее работоспособности или уничтожения ее ресурсов.

С.1.2. «Физическое разрушение» (*physical destruction*): Умышленной разрушение системного компонента с целью препятствия нормальному функционированию системы или его прерывание.

С.1.3.* «Ошибка человека» (*human error*): Действие или бездействие человека, которое неумышленно повлекло за собой выход из строя компонента системы.

С.1.3.* «Аппаратно-программная ошибка» (*hardware or software error*): Ошибка, которая либо повлекла за собой повреждение системного компонента, либо привела к прекращению нормального (или полному прекращению) функционирования системы.

С.1.4.* «Природный катаклизм» (*natural disaster*): Любое природное явление (например пожар, наводнение, землетрясение, молния или смерч), повлекшее за собой выход из строя компонента системы.

С.2. «Порча» (*corruption*): Угрожающее действие, которое вносит нежелательное изменение в функционирование системы путем вредительского изменения алгоритмов функционирования или данных системы:

С.2.1. «Подделка» (*tamper*): С точки зрения «порчи», умышленное искажение программного обеспечения, данных или управляющей информации системы с целью прерывания или препятствования корректному выполнению системных функций.

С.2.2. «Устройство для злонамеренных действий» (*malicious logic*): С точки зрения «порчи», любое аппаратно-программное устройство или программное обеспечение

(например «компьютерный вирус»), преднамеренно встроенное в систему с целью изменения алгоритмов и процедур функционирования системы или ее данных.

С.2.3.* «Ошибка человека» (*human error*): Действие или бездействие человека, которое неумышленно повлекло за собой искажение алгоритмов и процедур функционирования системы или ее данных.

С.2.4.* «Аппаратно-программная ошибка» (*hardware or software error*): Ошибка, которая повлекла за собой изменение алгоритмов и процедур функционирования системы или ее данных.

С.2.5.* «Природный катаклизм» (*natural disaster*): Любое природное явление (например мощный электромагнитный импульс, вызванный молнией), повлекшее за собой искажение алгоритмов и процедур функционирования системы или ее данных.

С.3. «Препятствие» (*obstruction*): Угрожающее действие, которое прерывает предоставление системных услуг путем воздействия на системные процессы с целью их замедления или блокировки:

С.3.1. «Помеха» (*interference*): Прерывание системных процессов и процедур путем блокировки соединений, данных пользователей и управляющей информации.

С.3.2. «Перегрузка» (*overload*): Прерывание системных процессов и процедур путем размещения чрезмерно большого объема «бесполезной» информации (передача вредоносного трафика) в системных компонентах с целью снижения их функциональной эффективности или их блокировки.

Д. «Захват/узурпация» (*usurpation*): Обстоятельство или событие, в результате которого управление службами системы и ее функционирование перешло к незаконному субъекту. Следующие угрожающие действия могут повлечь за собой «захват»:

Д.1. «Незаконное присвоение» (*misappropriation*): Угрожающее действие, посредством которого субъект при-

сваивает себе функции несанкционированного логического или физического управления системным ресурсом:

D.1.1. «Кража службы» (*theft of service*): Несанкционированное использование службы субъектом.

D.1.2. «Кража функциональных возможностей» (*theft of functionality*): Незаконное приобретение действующих аппаратно-программных средств и программного обеспечения компонентов сети.

D.1.3. «Кража данных» (*theft of data*): Незаконное приобретение и использование данных.

D.2. «Злоупотребление» (*misuse*): Угрожающее действие, которое повлекло за собой выполнение системным компонентом каких-либо функций или процедур обслуживания, подрывающих безопасность системы:

D.2.1. «Подделка» (*tamper*): С точки зрения «злоупотребления», умышленное искажение программного обеспечения, данных или управляющей информации системы с целью принуждения системы выполнять несанкционированные функции или процедуры обслуживания.

D.2.2. «Устройство для злонамеренных действий» (*malicious logic*): С точки зрения «злоупотребления», любое аппаратно-программное устройство или программное обеспечение, преднамеренно встроенное в систему с целью выполнения или управления несанкционированными функцией или процедурой обслуживания.

D.2.3. «Нарушение дозволенности» (*violation of permissions*): Действие субъекта, которое обеспечивает для него превышение дозволенных системных полномочий путем выполнения несанкционированной функции.

Анализ представленных угроз и последствий их воздействия показывает, что конечными их целями являются (рис. 1.2):

- 1) информация пользователей, циркулирующая в ИТС, — чтение и искажение (разрушение) информации и/или нарушение процедур информационного обмена;

- 2) работоспособность самой ИТС — чтение и искажение (разрушение) управляющей информации и/или нарушение процедур управления сетевыми (системными) компонентами или всей сетью (системой).

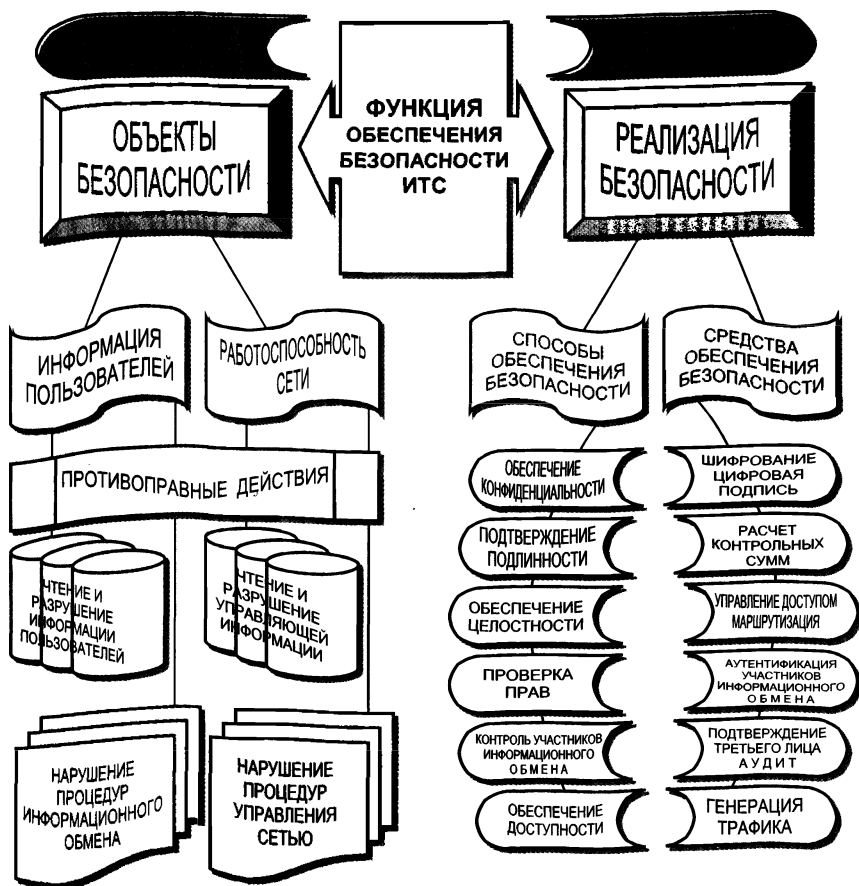


Рис. 1.2. Объекты и реализационные аспекты функции обеспечения ИБ ИТС

1.3. Функция, способы и средства обеспечения ИБ

На сегодняшний день существует несколько точек зрения на обеспечение безопасности информации в ИТС. Это относится к моделям безопасности Международного союза электросвязи (ITU-T, X.800), Международной организации по стандартизации (ISO), министерства обороны США (Department of defense — DOD) и рабочей группы по безопасности IETF (IRTF) сети Интернет. Анализ этих моделей показывает, что любая сеть должна обеспечивать дополнительную(ые) функцию(ии) безопасности (помимо стандартного набора функций для любой открытой системы), которая(ые) в свою очередь определяет(ют) объекты сетевой безопасности и ее реализационные аспекты (см. рис. 1.2). Этот рисунок показывает, что функция безопасности «разбивается» на подфункции и реализуется через определенный набор способов и средств обеспечения защиты сети. Каждая подфункция относится к определенному уровню архитектуры ЭМВОС и включает соответствующую группу способов и средств обеспечения безопасности. При этом одни и те же способы и средства могут применяться на различных уровнях архитектуры ИТС.

Под *способом обеспечения информационной безопасности* (СПБ) понимается совокупность приемов или операций, при реализации которых достигается какая-либо цель или решается определенная задача по защите данных.

Под *средством обеспечения информационной безопасности* (СРБ) понимается комплекс технических устройств (аппаратно-программных, программных и др.), обладающих определенными свойствами и реализующими один или несколько способов защиты информации. При этом несколько различных средств могут реализовать один способ обеспечения информационной безопасности.

В соответствии с существующими моделями обеспечения ИБ ИТС, каждый уровень ЭМВОС или Интернет-архитектуры включает дополнительную(ые) функцию(ии) по обеспечению не только защиты данных пользователей, но и защиту самих управляющих функций, которые поддерживают «нор-

мальную» работоспособность сети. Эта(и) дополнительная(ые) функция(ии) разбита(ы) на соответствующие подфункции (со своими группами способов и средств безопасности), а последние «распределены и встроены» в соответствующие протоколы информационного обмена на каждом уровне управления.

На рис. 1.3 представлены средства защиты информации в ИТС.



Рис. 1.3. Средства защиты информации

Под *архитектурой безопасности* будем понимать распределение дополнительной(ых) функции(ий) обеспечения безопасности по уровням архитектуры управления ИТС с целью обеспечения защиты от угроз ИБ, причем средства каждого уровня обеспечивают защиту только от конкретного вида угроз, к которому наиболее уязвим данный уровень, или создание защиты на этом уровне позволяет избежать дублирования функций обеспечения безопасности от этого вида угроз на других уровнях (хотя дублирование таких функций на каждом уровне не исключается).

1.4. Архитектура безопасности ЭМВОС

Одним из первых международных стандартов, определяющих архитектуру безопасности открытых систем, была Рекомендация ИТУ-Т (МККТТ) X.800. Этот стандарт дал общее описание функции обеспечения безопасности ИТС ЭМВОС. Эта функция реализуется системой обеспечения ИБ ИТС (СОИБ). Другими словами, СОИБ решает комплексную задачу обеспечения ИБ ИТС.

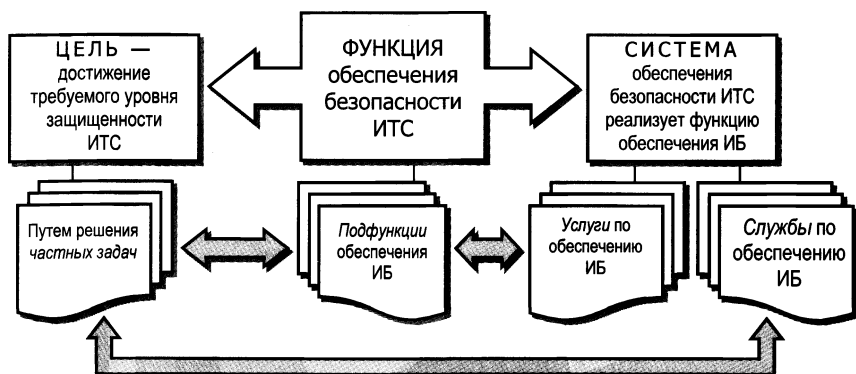


Рис. 1.4. Задача и состав системы обеспечения безопасности ИТС

Функция обеспечения безопасности является дополнительной (не обязательной), а ее реализация зависит от «желания» пользователя и/или владельца ИТС, поэтому СОИБ обеспечивает достижение поставленной перед ней цели путем предоставления услуг по обеспечению безопасности. Подсистемы обеспечения безопасности в рамках СОИБ именуются службами, которые и решают частные задачи путем реализации подфункций и предоставления услуг по обеспечению безопасности (рис. 1.4).

1.4.1. Термины и определения

Рекомендация ITU-T X.800 вводит следующие термины и определения:

- *управление доступом (access control)* — предотвращение неавторизованного использования ресурса, включая предотвращение использования ресурса нерегламентированным способом;
- *перечень управления доступом (access control list)* — список субъектов¹ (включающий их права доступа), которые авторизованы для предоставления им доступа к ресурсу;
- *идентифицируемость (accountability)* — свойство, которое гарантирует, что все действия субъекта могут быть зафиксированы в целях последующего подтверждения их однозначной принадлежности субъекту;
- *активная угроза (active threat)* — угроза преднамеренного неавторизованного изменения состояния системы;
- *аутентификационная информация (authentication information)* — информация, используемая для подтверждения подлинности объекта;
- *аутентификационный обмен (authentication exchange)* — способ подтверждения подлинности объекта с помощью средств информационного обмена;
- *авторизация (authorization)* — удовлетворение прав, которое включает предоставление доступа на основе прав доступа;
- *доступность (availability)* — свойство, обеспечивающее открытый и технически приемлемый доступ по запросу авторизованного субъекта;
- *мандат доступа (capability)* — метка, используемая как идентификатор при доступе к ресурсу, причем обладание такой меткой дает право доступа к ресурсу;
- *конфиденциальность (confidentiality)* — свойство, обеспечивающее недоступность или нераскрываемость информации неавторизованными пользователями, субъектами или процессами;

¹ В данном случае под термином «объект» понимается тот или иной сетевой ресурс, а «субъект» — тот, кто обращается к ресурсу (пользователь, процесс и т.п.).

- *верительные данные (credentials)* — данные, которые предоставляются субъекту для формирования предъявляемой им аутентификационной информации;

- *криптографическая проверочная сумма (cryptographic checkvalue)* — информация, которая была получена путем осуществления криптографического преобразования некоторой последовательности символов;

- *целостность данных (data integrity)* — свойство, обеспечивающее защиту данных от их изменения или разрушения каким-либо неавторизованным способом;

- *аутентификация источника данных (data origin authentication)* — подтверждение того, что источник полученных данных в действительности является тем, за кого себя выдает;

- *отказ в обслуживании (denial of service)* — воспрепятствование авторизованному доступу к ресурсу или прерывание процедур, которые являются критичными во времени;

- *цифровая (электронная цифровая) подпись (digital signature)* — присоединенные в исходной последовательности символов данные или криптографически преобразованная исходная последовательность символов, которые позволяют получателю этой исходной последовательности символов удостовериться относительно отправителя этой последовательности и ее целостности, а также защитить их от подделки, например, тем же самым получателем;

- *политика безопасности, основанная на проверке подлинности (identity-based security policy)* — политика безопасности (ПЛБ), основанная на проверке подлинности пользователей и/или атрибутов пользователей, групп пользователей или субъектов, действующих от имени и по поручению пользователей и ресурсов/объектов, к которым осуществляется доступ;

- *ключ, или криптоключ (key)* — последовательность символов, которая принимает непосредственное участие в управлении процедурами шифрования и расшифрования;

- *обеспечение ключами (key management)* — генерация, хранение, распределение, удаление, архивация и применение ключей в соответствии с политикой безопасности;

- *обнаружение манипуляций (manipulation detection)* — способ, который используется для выявления факта модификации данных (либо случайной, либо умышленной);
- *«маскарад» (masquerade)* — ситуация, при которой один субъект выдает себя за другого;
- *нотариальное заверение (notarization)* — регистрация данных доверенной третьей стороной (ДТС), которая в последующем позволяет гарантировать точность их параметров и характеристик, например содержание, источник, время и доставку;
- *пассивная угроза (passive threat)* — угроза неавторизованного вскрытия информации без изменения состояния системы;
- *пароль (password)* — конфиденциальная аутентификационная информация, которая, как правило, представляет собой последовательность символов;
- *аутентификация взаимодействующего субъекта (peer-entity authentication)* — подтверждение того, что субъект на противоположенной стороне соединения является тем, с кем необходимо провести процедуру информационного обмена (ПИНО);
- *физическая безопасность (physical security)* — комплекс мероприятий, используемых для обеспечения физической защиты ресурсов от последствий реализации умышленных и случайных угроз ИБ;
- *секретность/неприкосновенность частной жизни (privacy)* — право пользователей контролировать или влиять на то, какая информация, связанная с их жизнедеятельностью (например персональные данные), может накапливаться и храниться, а также кем и кому она может быть раскрыта;
- *отрицание (repudiation)* — отказ одного из взаимодействующих субъектов при проведении ПИНО от участия в этой процедуре или в отдельных ее фазах;
- *управление маршрутизацией (routing control)* — применение правил при выполнении процедуры маршрутизации, таких как выбор или отказ от определенных сетей, каналов связи или ретрансляционных участков;
- *политика безопасности, основанная на применении правил (rule-based security policy)* — ПЛБ, основанная на использовании единых правил, предназначенных для всех пользователей.

Эти правила обычно являются компромиссом между критичностью предназначенных для доступа ресурсов и обладателями соответствующих атрибутов пользователей, групп пользователей или субъектов, действующих от имени пользователей;

- *аудит безопасности (security audit)* — независимая проверка и ревизия системных записей и основных направлений деятельности с целью оценки адекватности системных средств управления и обеспечения гарантий их соответствия принятой политике безопасности и применяемым функциональным процедурам, а также для выявления уязвимых мест в системе обеспечения ИБ и выработки рекомендаций по внесению изменений в систему управления, политику безопасности и соответствующие процедуры;

- *исходные данные для аудита безопасности (security audit trail)* — накопленная и реально используемая для более успешного проведения аудита безопасности информация;

- *метка безопасности (security label)* — символ или набор символов (вставка символа или набора символов), непосредственно («жестко») связанный с ресурсом (который может быть последовательностью символов), означающий или предполагающий использование атрибутов безопасности этого ресурса;

- *политика безопасности (security policy)* — совокупность критериев или правил для оценки корректности функционирования служб безопасности;

- *услуга по обеспечению безопасности (security service)* — услуга, предоставляемая одним из уровней архитектуры ЭМ-ВОС (дополнительная подфункция), которая гарантирует адекватную защиту систем или доставки данных;

- *защита отдельных полей (selective field protection)* — защита определенных полей сообщения, подлежащего передаче;

- *критичность (sensitivity)* — свойство ресурса, которое означает его ценность или важность, а также может включать его уязвимость;

- *угроза (threat)* — потенциальное нарушение безопасности;

- *конфиденциальность потока трафика (traffic flow confidentiality)* — услуга по обеспечению конфиденциальности, предназначенная для нейтрализации угрозы анализа трафика;

- *заполнение трафика (traffic padding)* — генерация ложных запросов на соединение, ложных сообщений и/или ложных последовательностей символов в сообщениях;
- *надежное функционирование (trusted functionality)* — функциональный процесс (процедура), относительно которого существует предположение, что он протекает (выполняется) корректно в соответствии с некоторым(и) критерием(ями), например, в точном соответствии с политикой безопасности.

1.4.2. Услуги и способы обеспечения безопасности

Архитектура безопасности ЭМВОС включает следующие услуги по обеспечению безопасности.

1. *Аутентификация (authentication)*. Эта услуга может быть двух видов:

- 1) *аутентификация взаимодействующего субъекта (peer-entity authentication)*. Эта услуга обеспечивается N -ым уровнем архитектуры ЭМВОС и тем самым подтверждает субъекту $(N+1)$ -го уровня, что субъект на противоположной стороне соединения является тем субъектом $(N+1)$ -го уровня, с которым необходимо провести ПИНО;
- 2) *аутентификация источника данных (data origin authentication)*. Эта услуга обеспечивается N -ым уровнем архитектуры ЭМВОС и тем самым подтверждает субъекту $(N+1)$ -го уровня, что источником поступивших данных является запрашиваемый субъект $(N+1)$ -го уровня.

2. *Управление доступом (УД)*. Эта услуга обеспечивает защиту от несанкционированного использования ресурсов, которые доступны через ЭМВОС-сети/системы.

3. *Конфиденциальность данных (data confidentiality)*. Эта услуга может быть четырех видов:

- 1) *конфиденциальность виртуального соединения (connection confidentiality)*. Эта услуга обеспечивает конфиден-

циальность всех данных пользователя на N -ом уровне архитектуры ЭМВОС после установления соединения на этом уровне;

- 2) *конфиденциальность информационного обмена без установления соединения (connectionless confidentiality)*. Эта услуга обеспечивает конфиденциальность для всех данных пользователя на N -ом уровне архитектуры ЭМВОС при отправке одиночной дейтаграммы (дейтаграммный режим доставки сообщений) на этом уровне;
- 3) *конфиденциальность отдельных полей (selective field confidentiality)*. Эта услуга обеспечивает конфиденциальность отдельных полей в последовательности символов, отправленной пользователем на N -ом уровне архитектуры ЭМВОС в режиме с установлением соединения или дейтаграммном режиме;
- 4) *конфиденциальность потока трафика (traffic flow confidentiality)*. Эта услуга обеспечивает защиту информации, которая может быть извлечена при ведении наблюдения потоков трафика.

4. *Целостность данных (data integrity)*. Эта услуга может быть пяти видов:

- 1) *целостность соединения с его последующим восстановлением (connection integrity with recovery)*. Эта услуга обеспечивает целостность всех данных пользователя на N -ом уровне архитектуры ЭМВОС после установления соединения на этом уровне, а также выявление любой модификации, ложной вставки, ложного удаления или повтора любых данных в пределах всей последовательности дейтаграмм (с попыткой восстановления всей последовательности);
- 2) *целостность соединения без его последующего восстановления (connection integrity without recovery)*. Эта услуга обеспечивает целостность всех данных пользователя на N -ом уровне архитектуры ЭМВОС после установления соединения на этом уровне, а также выявление любой мо-

дификации, ложной вставки, ложного удаления или повторной передачи любых данных в пределах всей последовательности дейтаграмм (без попытки восстановления все последовательности);

3) *целостность отдельных полей при организации виртуального соединения (selective field connection integrity)*. Эта услуга обеспечивает целостность отдельных полей сообщения пользователя на N -ом уровне архитектуры ЭМВОС в рамках протокольного сообщения этого уровня, передаваемого по виртуальному соединению, а также выбирает способ обнаружения «поврежденных» отдельных полей вследствие их модификации, ложной вставки, ложного удаления или повторной передачи;

4) *целостность информационного обмена без установления соединения (connectionless integrity)*. Если эта услуга предоставляется на N -ом уровне архитектуры ЭМВОС, то она обеспечивает гарантированную целостность при запросе субъекта $(N+1)$ -го уровня. Кроме того, данная услуга обеспечивает целостность одиночной дейтаграммы (дейтаграммный режим доставки сообщений), а также может выбирать способ обнаружения модификации принятой дейтаграммы. Более того, она может выбрать способ (но не любой среди всех возможных) обнаружения повторной передачи дейтаграммы;

5) *целостность отдельных полей при организации информационного обмена без установления соединения (selective field connectionless integrity)*. Эта услуга обеспечивает целостность отдельных полей одиночной дейтаграммы (дейтаграммный режим доставки сообщений), а также может выбирать способ обнаружения модификации отдельных полей.

5. *Неотказуемость (non-repudiation)*. Эта услуга может быть двух видов:

1) *защита от ложного отказа источника (non-repudiation with proof of origin)*. Эта услуга защищает получателя

данных от любой попытки отправителя умышленно отказаться от передачи этих данных или их компонентов;

- 2) *защита от ложного отказа получателя (non-repudiation with proof delivery)*. Эта услуга защищает отправителя данных от любой попытки получателя умышленно отказаться от получения этих данных или их компонентов.

Архитектура безопасности ЭМВОС включает следующие способы обеспечения безопасности (СПБ).

1. *Шифрование (encipherment)*. С помощью шифрования можно обеспечить конфиденциальность данных или информации о потоке трафика. Кроме этого шифрование может использоваться и в других СПБ.

2. *Электронная цифровая подпись (ЭЦП)*. Применение ЭЦП предусматривает реализацию двух процедур:

- 1) собственно процедура формирования ЭЦП (подписывание электронного сообщения). В этой процедуре используется информация, которая секретна (т.е. уникальна или конфиденциальна) с точки зрения субъекта — автора подписи. Формирование ЭЦП предусматривает либо шифрование сообщения, либо вычисление криптографической проверочной суммы сообщения; для этого секретная информация автора подписи используется в качестве секретного ключа;
- 2) процедура проверки подписанного электронного сообщения. В этой процедуре используются дополнительные процедуры и информация, которые являются общеизвестными, но из которых нельзя получить секретную информацию автора подписи.

Основным свойством ЭЦП является то, что подпись может быть сформирована только на основе использования секретной информации автора ЭЦП. Таким образом, после проверки ЭЦП она в последующем (причем в любой момент времени) может быть удостоверена доверенной третьей стороной (ДТС, напри-

мер, судьей или третейским судьей), т.е. последняя может доказать то, что только владелец уникальной секретной информации мог сформировать (быть автором) ЭЦП.

3. *Управление доступом.* При УД могут использоваться, либо аутентификация личности субъекта, либо информация о субъекте (например, принадлежность к известной группе субъектов), либо мандат доступа с целью определения и реализации прав доступа субъекта. Если же субъект пытается использовать неавторизованный ресурс или авторизованный ресурс недозволённым способом, то функция УД будет блокировать попытку и дополнительно может оповещать об инциденте с целью включения сигнала тревоги и/или записи об инциденте в исходные данные для проведения аудита СОИБ. При передаче данных в дейтаграммном режиме любое оповещение передающей стороны об отказе ей в доступе может быть объяснено только как обман средств УД источником данных.

Способы УД могут быть реализованы с помощью соответствующих средств защиты (средств УД), размещаемых на одной (или обеих) стороне виртуального соединения и/или в любой промежуточной точке.

4. *Целостность данных.* Существуют два вида услуг по обеспечению целостности данных:

- 1) целостность одного сообщения или поля данных;
- 2) целостность потока сообщений или полей данных. Для реализации этих двух видов услуг используются разные способы обеспечения целостности, хотя реализация второй без реализации первой бессмысленна. Обеспечение целостности одиночного сообщения или поля предполагает два процесса, один из которых осуществляется отправителем, а другой — получателем;
- 3) отправитель присоединяет к сообщению параметр, который является функцией самого сообщения. Этот параметр может быть дополнительной информацией (например блочный проверочный код или криптографическая проверочная сумма), которая сама может быть зашифрована;

- 4) получатель формирует соответствующий параметр и сравнивает его с полученным параметром с целью установления факта модификации сообщения в процессе передачи.

При использовании только одного такого способа невозможно обеспечить защиту от атак типа «Повторная передача сообщения». На соответствующих уровнях архитектуры ЭМВОС обнаружение манипуляции с данными может привести к процедуре восстановления (например с помощью повторной передачи или исправления ошибки) на этом или более высоком уровне.

При доставке данных в режиме виртуального соединения обеспечение целостности последовательности сообщений (т.е. защита против нарушения порядка следования, потери, повторной передачи и вставки или модификации сообщений) требует применения дополнительного способа точного соблюдения порядка следования сообщений, например, последовательной нумерации сообщений, включения в них меток времени или их криптографической «связки» (или «привязки»).

В дейтаграммном режиме доставки сообщений для защиты от некоторых подвидов атак типа «Повторная передача сообщения» может использоваться процедура включения в сообщения меток времени.

5. Обмен аутентификационной информацией. Средства защиты, реализующие данный способ, могут встраиваться на *N*-ом уровне архитектуры ЭМВОС с целью обеспечения аутентификации взаимодействующего субъекта. Если средство аутентификации субъекта не аутентифицировало последнего, то это приводит к удалению или прерыванию соединения и может повлечь за собой оповещение администрации СОИБ об инциденте и/или дополнение исходных данных для проведения аудита СОИБ записью о произошедшем инциденте.

Этот способ обеспечения ИБ может основываться на использовании:

- 1) аутентификационной информации (например пароли), которая передается отправителем и проверяется получателем;

- 2) криптографических алгоритмов;
- 3) особенностей и/или собственности субъекта.

6. *Заполнение трафика.* Средства защиты, реализующие заполнение трафика, могут использоваться для обеспечения различных уровней защиты от анализа трафика. Этот способ может быть эффективным только тогда, когда заполнение трафика защищено с помощью услуги конфиденциальности.

7. *Управление маршрутизацией.* Маршруты доставки либо могут выбираться динамически, либо могут быть заранее спланированы с учетом использования только защищенных подсетей, ретрансляционных участков или каналов/линий связи.

Оконечные (прикладные) системы в целях выявления постоянных атак, связанных с манипуляцией данными, могут потребовать от провайдера сетевых услуг формирование соединения с использованием различных маршрутов.

Для обеспечения надежной доставки данных метки безопасности могут быть запрещены в соответствии с политикой безопасности при передаче таких данных через надежные подсети, ретрансляционные участки или каналы/линии связи. Кроме этого, инициатор соединения (или отправитель, в случае дейтаграммного режима доставки) может заявить протест относительно предоставляемых маршрутов доставки и при этом запросить, чтобы определенные подсети, ретрансляционные участки или каналы/линии связи были исключены из маршрутов доставки.

8. *Нотаризация (нотариальное заверение).* Свойства (такие как целостность, авторство, время и получатель) данных, которые циркулируют между двумя или более субъектами, могут быть гарантированы с помощью нотариального заверения. Гарантии предоставляются нотариусом, выступающим в роли ДТС, которому доверяют взаимодействующие субъекты и который хранит необходимую информацию для подтверждения

востребованной гарантии путем свидетельствования. Каждая сторона информационного обмена может использовать средства ЭЦП, шифрования и защиты целостности как соответствующие услуги, предоставляемые нотариусом. При запросе нотариального заверения данные циркулируют между взаимодействующими субъектами, с использованием защищенного соединения, и нотариусом.

К *общесистемным СПБ* (т.е. независимым от архитектуры ЭМВОС) относятся:

- 1) *надежность (гарантированность) функционирования.* Обеспечение надежности функционирования используется в первую очередь для корректной реализации других способов обеспечения ИБ в средствах защиты. Любая процедура, напрямую обеспечивающая реализацию способа безопасности или доступ к услуге по обеспечению безопасности, должна заслуживать доверия;
- 2) *использование меток безопасности.* Ресурсы, включая собственно данные, могут иметь маркеры безопасности, непосредственно связанные с ними, например, для указания критичности уровня. Метки безопасности могут представлять собой дополнительные данные, которые связаны с транслируемыми данными. Соответствующие маркеры безопасности должны быть четко идентифицируемыми, чтобы они могли быть корректно проверены. Кроме того, они должны быть отделены (иметь границу) от данных, с которыми они связаны;
- 3) *обнаружение событий*, влияющих на безопасность;
- 4) *накопление и использование исходных данных для аудита безопасности;*
- 5) *восстановление безопасности.* Этот способ связан с запросами средств защиты, реализующих другие способы безопасности, на выполнение процедур восстановления на основе принятых правил.

Далее представлена табл. 1.1, иллюстрирующая связи между услугами и способами обеспечения безопасности.

Связи между услугами и способами обеспечения ИБ ИТС

Услуга \ Способ								
	Шифрование	ЭЦП	Управление доступом	Целостность данных	Обмен аутентификационной информацией	Заполнение трафика	Управление маршрутизацией	Нотариальное заверение
1	2	3	4	5	6	7	8	9
Аутентификация взаимодействующего субъекта	✓	✓			✓			
Аутентификация источника данных	✓	✓						
Управление доступом			✓					
Конфиденциальность виртуального соединения	✓						✓	
Конфиденциальность информационного обмена без установления соединения	✓						✓	
Конфиденциальность отдельных полей	✓							
Конфиденциальность потока трафика	✓					✓	✓	
Целостность соединения с последующим восстановлением	✓			✓				

Таблица 1.1 (окончание)

1	2	3	4	5	6	7	8	9
Целостность соединения без последующего восстановления	✓			✓				
Целостность отдельных полей при организации виртуального соединения	✓			✓				
Целостность информационного обмена без установления соединения	✓	✓		✓				
Целостность отдельных полей при организации информационного обмена без установления соединения	✓	✓		✓				
Защита от ложного отказа источника		✓		✓				✓
Защита от ложного отказа получателя		✓		✓				✓

1.4.3. Принципы архитектуры безопасности ЭМВОС

Архитектура безопасности ЭМВОС¹ содержит следующие *принципы распределения услуг и способов обеспечения ИБ по уровням*:

- 1) количество альтернативных вариантов реализации услуги должно быть минимальным;

¹ Рекомендация ITU-T X.800 предусматривает, что все открытые системы имеют оконечные системы, включающие семь уровней архитектуры, и промежуточные системы (например узлы коммутации).

- 2) допускается создание защищенных систем путем встраивания услуг по обеспечению безопасности в архитектуру ЭМВОС на нескольких уровнях;
- 3) целесообразно, чтобы дополнительные функции, востребованные СОИБ, без необходимости не дублировали существующие функции ЭМВОС;
- 4) любые возможные нарушения функциональной независимости уровня ЭМВОС должны быть исключены;
- 5) количество реализуемых надежных функций должно быть минимальным;
- 6) в тех случаях, когда субъект зависит от способа обеспечения ИБ, реализуемого средством защиты, которое встроено субъектом на нижнем уровне архитектуры, любые промежуточные уровни должны функционировать таким образом, чтобы всякое нарушение безопасности исключалось;
- 7) там, где это возможно, дополнительные функции безопасности, реализуемые на конкретном уровне архитектуры, должны быть определены (описаны) таким образом, чтобы это не помешало их внедрению в форме независимых и самостоятельных модулей.

Кроме того, архитектура ЭМВОС включает модель запроса, управления и использования защищенных услуг информационного взаимодействия, которая состоит из описания:

- 1) особенностей защиты взаимодействующих процессов;
- 2) условий применения услуг безопасности;
- 3) функционирования защищенного информационного обмена в режиме с установлением соединения;
- 4) функционирования защищенного информационного обмена в режиме без установления соединения.

В табл. 1.2 и 1.3 представлено распределение услуг и способов безопасности по уровням архитектуры ЭМВОС (архитектура безопасности ЭМВОС).

Распределение услуг безопасности по уровням архитектуры ЭМВОС (архитектура безопасности ЭМВОС)

Услуга \ Уровень архитектуры ЭМВОС	1	2	3	4	5	6	7 ¹
Аутентификация взаимодействующего субъекта			✓	✓			✓
Аутентификация источника данных			✓	✓			✓
Управление доступом			✓	✓			✓
Конфиденциальность виртуального соединения	✓	✓	✓	✓		✓	✓
Конфиденциальность информационного обмена без установления соединения		✓	✓	✓		✓	✓
Конфиденциальность отдельных полей						✓	✓
Конфиденциальность потока трафика	✓		✓				✓
Целостность соединения с последующим восстановлением				✓			✓
Целостность соединения без последующего восстановления			✓	✓			✓
Целостность отдельных полей при организации виртуального соединения							✓

¹ Необходимо отметить, что прикладные процессы седьмого уровня архитектуры могут сами предоставлять услуги безопасности.

Таблица 1.2 (окончание)

Уровень архитектуры ЭМВОС \ Услуга	1	2	3	4	5	6	7
Целостность информационного обмена без установления соединения			✓	✓			✓
Целостность отдельных полей при организации информационного обмена без установления соединения							✓
Защита от ложного отказа источника							✓
Защита от ложного отказа получателя							✓

Таблица 1.3

Распределение способов обеспечения безопасности по уровням ЭМВОС

Способ \ Уровень ЭМВОС	Шифрование	ЭЦП	Управление доступом	Целостность данных	Обмен аутентификационной информацией	Заполнение трафика	Управление маршрутизацией	Нотариальное заверение
1	2	3	4	5	6	7	8	9
1	✓							
2	✓							

Таблица 1.3 (окончание)

1	2	3	4	5	6	7	8	9
3	✓	✓	✓	✓	✓	✓	✓	
4	✓	✓	✓	✓	✓			
5								
6	✓	✓		✓				✓
7	✓	✓	✓	✓	✓	✓		✓

Таблица 1.4

Распределение услуг по обеспечению безопасности по уровням Интернет-архитектуры (архитектура безопасности сети Интернет)

Услуга \ Уровень архитектуры сети Интернет	1	2	3	4	5
Аутентификация и авторизация взаимодействующего субъекта			✓	✓	✓
Аутентификация источника данных			✓	✓	✓
Управление доступом			✓		✓
Конфиденциальность виртуального соединения		✓	✓	✓	✓
Конфиденциальность информационного обмена без установления соединения		✓	✓	✓	✓
Конфиденциальность отдельных полей					✓
Конфиденциальность потока трафика	✓		✓		✓

Уровень архитектуры сети Интернет	1	2	3	4	5
Услуга					
Целостность виртуального соединения			✓	✓	✓
Целостность информационного обмена без установления соединения			✓	✓	✓
Целостность отдельных полей при организации информационного обмена					✓
Защита от ложного отказа источника					✓
Защита от ложного отказа получателя					✓

1.5. Принципы архитектуры безопасности сети Интернет

На сегодняшний день архитектура безопасности сети Интернет до конца не определена и тем более не стандартизирована. Существует ряд моделей безопасности в ИТС. Однако модель безопасности ЭМВОС не приемлема для Интернет-сетей (RFC—791, RFC—1122, RFC—1123, RFC—1349, RFC—1958), так как их архитектуры отличаются количеством уровней (ЭМВОС — 7, а Интернет — 5), тем не менее услуги и способы обеспечения безопасности, определенные для ЭМВОС, аналогичны тем, которые используются в Интернет-архитектуре. Поэтому для сети Интернет наиболее приемлемыми моделями безопасности являются модели МОС, министерства обороны США и собственно рабочей группы по безопасности IETF (IRTF) Интернет.

В табл. 1.4 показано распределение услуг по обеспечению безопасности по уровням Интернет-архитектуры в соответствии с идеологией сетевой безопасности в сети Интернет.

КОНЦЕПЦИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Большинство открытых (прикладных) ИТС, архитектура которых соответствует ЭМВОС или Интернет-архитектуре, предъявляют жесткие требования по обеспечению ИБ с целью защиты от угроз, возникающих при информационном взаимодействии как внутри самих систем, так и между собой. Под термином *открытые системы* понимаются БД, распределенные прикладные системы, системы с открытой распределенной обработкой и собственно взаимодействие самих ИТС. Концептуальные основы обеспечения ИБ связаны со способами и средствами защиты подсистем и объектов, расположенных внутри таких систем, а также с взаимодействием систем между собой. Однако основы ИБ не затрагивают методологию проектирования самих систем и способов.

Обеспечение ИБ охватывает элементы данных (информационные элементы) и последовательности процедур (но не протокольные элементы данных), которые используются при предоставлении определенных услуг по обеспечению ИБ. Услуги по обеспечению ИБ могут предоставляться соответствующими службами обеспечения безопасности (СЛБ) при информационном взаимодействии объектов/субъектов ИТС, а также при обмене данными между ИТС и при управлении самими ИТС.

Концептуальные основы обеспечения ИБ могут использоваться в качестве основы для стандартизации, применения единой терминологии и описания общих абстрактных служебных интерфейсов при выполнении определенных требований к обеспечению ИБ.

Одна СЛБ очень часто зависит от других СЛБ, что затрудняет самостоятельное функционирование одного направления обеспечения ИБ от других. Основы обеспечения ИБ включают рассмотрение соответствующих СЛБ, описывают совокупность

способов, которые могут использоваться при предоставлении услуг по обеспечению ИБ, и определяют взаимозависимость услуг и способов обеспечения ИБ (СПБ). Следствием детального описания этих способов может стать доверие к различным СЛБ, а также доверие одной СЛБ к другой.

В данной главе рассматриваются:

- концепции (концептуальные компоненты, понятия и определения) обеспечения ИБ, которые используются в большинстве СЛБ;
- взаимозависимость СЛБ и СПБ.

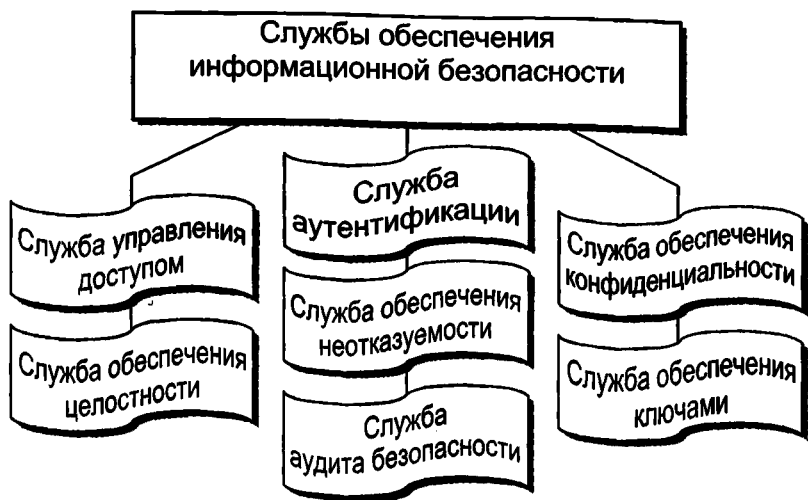


Рис. 2.1. Службы обеспечения ИБ

Концептуальные основы обеспечения ИБ включают несколько частей, каждая из которых представляет собой отдельную главу данной книги, посвященную конкретной СЛБ, а именно (рис. 2.1):

- служба аутентификации (СЛАУ);
- служба управления доступом (СЛУД);
- служба обеспечения неотказуемости (СЛНТ);
- служба обеспечения конфиденциальности (СЛКН);

- служба обеспечения целостности (СЛЦЛ);
- служба аудита безопасности и оповещения об опасности (СЛАО);
- служба обеспечения ключами (СЛКЛ).

2.1. Общие концепции обеспечения ИБ

Большинство концептуальных понятий и определений обеспечения ИБ необходимы для описания самих СЛБ и раскрывают функции (функциональность) этих служб. На рис. 2.2 представлены основные концептуальные компоненты, понятия и определения обеспечения ИБ.

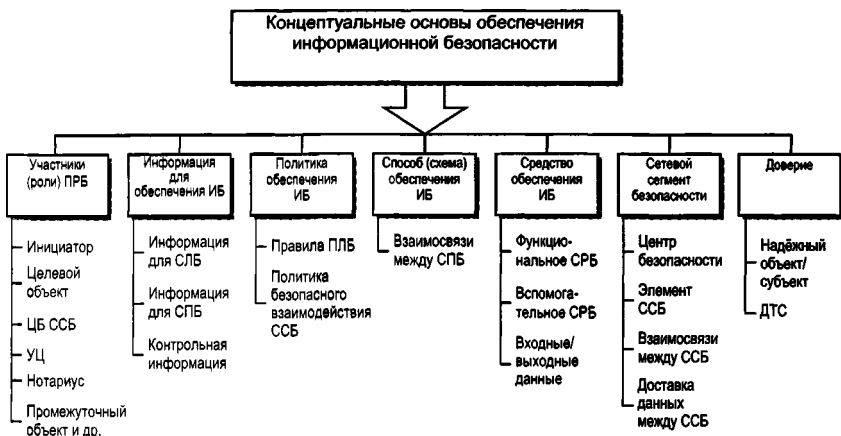


Рис. 2.2. Концепции обеспечения информационной безопасности

2.1.1. Информация, необходимая для обеспечения ИБ

Информация, необходимая для обеспечения ИБ, представляет собой вспомогательную информацию (ВИ), которая востребована СЛБ и используется ею. К ВИ относятся:

- правила политики обеспечения безопасности (ПЛБ);
- информация, необходимая для функционирования определенных СЛБ, например ВИ для процедуры аутентифи-

кации (аутентификационная информация, authentication information) и ВИ для процедуры управления доступом (access control information);

- информация, необходимая для реализации СПБ, например метки безопасности (security labels), криптографические проверочные суммы (КПС), сертификаты безопасности (СЕРТ|ИБ) и маркеры безопасности (security tokens).

2.1.2. Сетевой сегмент безопасности

Сетевой сегмент безопасности (ССБ) представляет собой совокупность информационных (информационно-технологических) элементов, определяемых ПЛБ и находящихся под управлением единого центра безопасности (ЦБ), который осуществляет целенаправленную деятельность по обеспечению ИБ. Функциональная деятельность ССБ основана на привлечении одного или нескольких элементов из самого ССБ и, возможно, элементов других ССБ.

Примерами такой деятельности являются:

- обеспечение доступа к элементам;
- установление или использование соединений N -го уровня ЭМВОС или Интернет-архитектуры;
- процедуры, относящиеся к специфическим функциям обеспечения и управления;
- процедуры обеспечения неотказуемости (ПРНТ) с привлечением нотариуса.

Любой процесс может быть связан с обеспечением ИБ даже тогда, когда он на текущий момент времени не является объектом тех СПБ, которые могли бы его «заставить» выполнять требования любой ПЛБ, хоть как-то касающейся их применения. Соответственно, процессы, выполнение которых может быть прервано (или вообще прекращено) из-за любых перестановок групп элементов, могут сами зависеть от процедур обеспечения ИБ (ПРБ), а в дальнейшем могут стать контролируруемыми объектами со стороны СПБ.

В открытых системах элементами ССБ являются логические или физические элементы, например существующие открытые системы, прикладные процессы, объекты *N*-го уровня ЭМВОС или Интернет-архитектуры, элементы протокольных данных *N*-го уровня ЭМВОС или Интернет-архитектуры, ретрансляторы и пользователи существующих открытых систем. Очень часто возникает необходимость отделения пользователей от других элементов в ССБ. В таких случаях для обозначения всех элементов, не относящихся к пользователям, используется термин *объекты (элементы) данных* (data objects).

2.1.2.1. ПЛБ и правила ПЛБ

ПЛБ отражает требования к обеспечению ИБ в ССБ в целом. Например, ПЛБ может определять требования, которые устанавливаются, либо для всех участников ССБ при функционировании в определенных условиях, либо для всей информации, циркулирующей в ССБ. В итоге ПЛБ будет применяться (реализовываться) СЛБ, которые в свою очередь будут определены в соответствии с требованиями ПЛБ, а СПБ будут выбираться исходя из применяемых СЛБ. Решение относительно применения того или иного СПБ будет приниматься исходя из последствий реализации возможных угроз и объема ресурсов, необходимых для парирования таких угроз.

ПЛБ формально представляется как совокупность наиболее общих принципов, зафиксированных на естественном (читабельном) языке. Эти принципы отражают требования по обеспечению ИБ соответствующей организации или участников ССБ. Перед тем как эти требования могут быть отражены в реальных открытых системах, ПЛБ должна быть скорректирована, причем так, чтобы из нее можно было выделить набор правил ПЛБ. Представление таких требований в форме правил ПЛБ является чисто технической задачей. ПЛБ накладывает ограничения на деятельность элементов, являющихся ее объектами, либо путем требования точного выполнения определенного действия, либо путем наложения запрета на выполнение определенных действий. Кроме того, ПЛБ может предоставлять элементам право

на выполнение (осуществление) некоторой части определенных действий.

Правила ПЛБ для ССБ бывают двух типов: 1) затрагивающие вопросы функционирования в рамках одного ССБ; 2) затрагивающие вопросы функционального взаимодействия двух и более ССБ. Правила ПЛБ второго типа называются *правилами безопасного взаимодействия* (ПБВ). ПЛБ, кроме того, может устанавливать правила взаимодействия между всеми ССБ, а также правила взаимодействия определенной группы ССБ.

Правила ПЛБ для ССБ должны всегда быть актуальными, так как изменяется сама система, могут изменяться ее функциональные аспекты и соответственно ПЛБ ССБ тоже может корректироваться.

2.1.2.2. Центр ССБ

Центр ССБ представляет собой исполнительный орган ССБ, который несет ответственность за внедрение и выполнение ПЛБ в ССБ.

Центр ССБ:

- может быть составным объектом. Такой объект должен быть идентифицируемым;
- может, в зависимости от применяемой ПЛБ, субъектом которой может быть сам этот центр ССБ, делегировать ответственность за внедрение и выполнение ПЛБ одному или нескольким объектам;
- иметь центр ССБ над всеми элементами ССБ.

ПРИМЕЧАНИЕ. ПЛБ может отсутствовать, если центр ССБ решил не вводить каких-либо ограничений.

Два ССБ считаются связанными, если их функционирование ограничивается только согласованием собственных ПЛБ.

2.1.2.3. Взаимосвязи между ССБ

Концептуальное понятие ССБ считается основополагающим по двум причинам:

- оно может использоваться для описания процедур обеспечения и администрирования ИБ;
- оно может использоваться как «строительный блок» при моделировании основных направлений деятельности по обеспечению ИБ, которые затрагивают элементы, находящиеся под управлением различных ЦБ.

ССБ могут быть связаны между собой различными способами. Взаимосвязи между ССБ должны быть зафиксированы в ПЛБ ССБ и предварительно согласованы их ЦБ. Эти взаимосвязи описываются с использованием терминов¹ «элементы и основные направления деятельности ССБ» и отображаются в ПБВ каждого взаимодействующего ССБ.

Говорят, что два ССБ являются *изолированными* друг от друга, если они не имеют ни общих элементов данных, ни общих направлений деятельности и, более того, не могут взаимодействовать.

Говорят, что два ССБ являются *независимыми* друг от друга если:

- они не имеют общих элементов данных;
- основные направления деятельности в рамках каждого ССБ основаны только на его собственных ПЛБ (и соответствующих группах правил ПЛБ);
- центры ССБ не осуществляют координацию своих ПЛБ.

Два и более независимых ССБ могут заключить между собой соглашение о скоординированном обмене информацией между ними.

Говорят, что ССБ *A* является *сетевым субсегментом безопасности* другого ССБ *B* тогда и только тогда, когда:

- множество элементов *A* является подмножеством множества элементов *B* или совпадает с ними;
- совокупность основных направлений деятельности *A* является частью совокупности основных направлений деятельности *B* или совпадает с ними;

¹ Использование рассматриваемых в этой главе терминов не является строго обязательным.

- юрисдикция над *A* делегирована центром безопасности *B* центру безопасности *A*;
- ПЛБ *A* не противоречит ПЛБ *B*. При необходимости, *A* может вводить дополнительную ПЛБ, если это допускается ПЛБ *B*.

Говорят, что ССБ *A* является *сетевым суперсегментом безопасности* по отношению к другому ССБ *B* тогда и только тогда, когда *B* является *сетевым субсегментом безопасности* по отношению к *A*.

2.1.2.4. Формирование ПБВ

Информационное взаимодействие между ССБ должно быть отражено в ПБВ. Они составляют определенную часть общих правил ПЛБ каждого ССБ. ПБВ устанавливают общие:

- СЛБ и СПБ, которые могут варьироваться при каждом информационном взаимодействии, как правило, путем согласования;
- элементы ВИ в каждом ССБ, взаимодействующего по принципу «каждый с каждым», как правило, путем взаимно-однозначного отображения.

Для обеспечения возможного обмена правилами ПЛБ между ССБ необходима ВИ. ПБВ могут определяться различными способами в зависимости от реального взаимодействия между ССБ.

Для обеспечения безопасного взаимодействия между независимыми ССБ, ПБВ должны быть согласованы центрами безопасности взаимодействующих ССБ.

Для обеспечения безопасного взаимодействия между сетевыми субсегментами безопасности ПБВ могут формироваться ЦБ сетевого суперсегмента безопасности. Если это допускает ПЛБ сетевого суперсегмента безопасности, то сетевые субсегменты безопасности могут формировать свои собственные ПБВ.

2.1.2.5. Доставка ВИ между ССБ

ПБВ могут сами содержать ВИ, и может возникнуть необходимость в доставке такой ВИ между ССБ. В этой связи возможны следующие случаи:

- семантика и формат представления ВИ в каждом ССБ идентичны. Это означает, что отображение не требуется;
- семантика представления ВИ в каждом ССБ идентична, но форматы ее представления отличаются. Это означает, что методы описания ВИ различны, и, следовательно, необходимо отображение синтаксиса;
- семантика и формат представления ВИ в каждом ССБ различны. Это означает, что ПБВ должны определять способ отображения ВИ одного ССБ в ВИ другого ССБ. Кроме этого, может понадобиться отображение синтаксиса.

2.1.3. Предположения относительно ПЛБ для определенных СЛБ

Способы УД (СПУД) могут использоваться в некоторых реальных СЛЦЛ или СЛКН. В таких случаях правила ПЛБ, определяющие функционирование СЛЦЛ или СЛКН, должны устанавливать порядок использования СПУД. Способы УД рассматриваются в терминах «инициатор» и «целевой объект». Правила ПЛБ определяют как объекты/субъекты, информация и элементы данных в политиках обеспечения целостности (ПЛЦЛ) и конфиденциальности (ПЛКН) связаны с инициаторами и целевыми объектами, указанными в способах УД.

ПЛКН устанавливают, что объекты/субъекты могут контролировать информационные элементы. Существуют два способа, в соответствии с которыми процедура, осуществляемая инициатором по отношению к целевому объекту, может раскрыть информацию о взаимодействующей стороне. Во-первых, в результате проведенной инициатором процедуры ему может стать известна некоторая информация о целевом объекте. Во-вторых, запрос процедуры, направленный целевым объектом, может обе-

спечить его некоторой информацией об инициаторе. Когда для обеспечения СЛКН применяются способы управления доступом, тогда объекты/субъекты, пытающиеся получить информацию, считаются инициаторами, а информационные элементы — целевыми объектами.

ПЛЦЛ устанавливают, что объекты/субъекты могут модифицировать элементы данных. Существуют два способа, в соответствии с которыми процедура, осуществляемая инициатором по отношению к целевому объекту, может повлечь модификацию данных. Во-первых, процедура может напрямую повлечь модификацию данных, расположенных внутри целевого объекта. Во-вторых, в результате процедуры может последовать модификация данных, расположенных внутри инициатора. Когда для обеспечения СЛЦЛ применяются СПУД, тогда объекты/субъекты, пытающиеся модифицировать данные, считаются инициаторами, а элементы данных — целевыми объектами.

2.1.4. Надежные (доверенные) объекты/субъекты

Говорят, что объект/субъект является *надежным* (доверенным) для некоторых видов основной деятельности в соответствии с ПЛБ, если объект/субъект может нарушить ПЛБ либо путем осуществления процедур, которые не предусмотрены для выполнения, либо путем прерывания процедур, которые предусмотрены для выполнения. ПЛБ устанавливает, какие объекты/субъекты являются надежными, и для каждого надежного объекта/субъекта устанавливает совокупность видов основной деятельности, при осуществлении которых объект/субъект считается надежным. Объект/субъект, который считается надежным при осуществлении соответствующей совокупности видов основной деятельности, не обязательно является надежным при осуществлении всех видов основной деятельности в пределах ССБ.

Содержащаяся в ПЛБ декларация о том, что объект/субъект должен вести себя соответствующим образом, не обязательно гарантирует, что объект/субъект будет вести себя именно таким образом. Соответственно, ПЛБ может требовать наличия средств выявления нарушений ПЛБ, являющихся следствием некоррект-

ного поведения надежного объекта/субъекта. Надежный объект/субъект, который может вести себя некорректно и при этом его некорректное поведение не будет обнаружено, называется *безусловно надежным объектом/субъектом*. Надежный объект/субъект, который может нарушить ПЛБ и при этом не может воспрепятствовать обнаружению его некорректного поведения, называется *условно надежным объектом/субъектом*.

Надежный объект/субъект может быть безусловно надежным объектом/субъектом при реализации некоторого подмножества направлений своей основной деятельности, а также быть условно надежным объектом/субъектом при реализации другого подмножества направлений своей основной деятельности. Такой объект/субъект может нарушать ПЛБ по некоторым аспектам без обнаружения таких нарушений, но не может нарушать ПЛБ по другим аспектам без обнаружения таких нарушений.

ПЛБ ССБ может содержать декларацию о том, что элемент, не входящий в этот ССБ, является надежным при реализации некоторого подмножества направлений своей основной деятельности в пределах данного ССБ. ПЛБ могут устанавливать, как в пределах ССБ объекты/субъекты должны взаимодействовать с надежным объектом/субъектом, расположенным за пределами данного ССБ.

2.1.5. Доверие

Говорят, что объект/субъект *X доверяет* объекту/субъекту *Y* (при реализации некоторого подмножества направлений своей основной деятельности) тогда и только тогда, когда *X* верит в то (уверен в том), что *Y* функционирует соответствующим образом и в соответствии с направлениями своей основной деятельности.

Доверие не обязательно является *обоюдным*. Объект/субъект, который не доверяет объекту/субъекту, может воспользоваться услугами обеспечения безопасности, предоставляемыми надежным объектом/субъектом. Примером ситуации, в которой доверие является обоюдным, может быть случай, когда два надежных объекта/субъекта взаимодействуют при реализации

данных на группы, которые в рамках одной группы должны быть защищены и обрабатываться одним и тем же способом. Кроме того, ПЛБ описывает сам способ защиты, который должен быть реализован по отношению к каждой группе элементов данных.

Все аспекты обеспечения безопасности, отраженные в ПЛБ, указываются в метке безопасности, которая включает:

- уровень защиты данных, хранящихся в системе;
- полномочия доступа к данным, процессам или ресурсам;
- требуемые отметки обеспечения безопасности, которые должны отображаться на любом дисплее или быть опубликованы;
- требования маршрутизации и шифрования данных, транслируемых между системами;
- требования по защите от несанкционированного (неавторизованного) копирования;
- методы хранения данных;
- алгоритмы шифрования, которые должны быть использованы;
- методы аутентификации объектов/субъектов;
- должны ли операции над объектом/субъектом подвергаться аудиторской проверке;
- требуется ли обеспечение неотказуемости получателей при получении ими квитанции от объекта/субъекта;
- требуются ли (если да, то чьи) ЭЦП для аутентификации данных.

Если данные хранятся в ИТС или транслируются по каналам/линиям связи (виртуальным соединениям) между системами, то данные помечаются для указания защищенного сегмента (группы), которому они принадлежат, и, следовательно, как эти данные должны обрабатываться с целью обеспечения безопасности. Метка может быть опознаваема вне зависимости от защищаемой информации, но, тем не менее, она остается логически привязанной к ней.

Целостность меток и целостность их привязок к информации должны быть гарантированными. Для этого ИТС должна при-

нимать соответствующие решения по обеспечению безопасности, например УД и маршрутизация, причем без необходимости обращения к защищаемой информации. Метка безопасности может быть связана с каждым информационным объектом в ИТС, например документами, сообщениями электронной почтовой службы, окнами экранных интерфейсов, записями в БД, записями в БДК и электронными формами. Метки предназначены для использования в тех случаях, когда информационные объекты хранятся и циркулируют между соответствующими системами, либо внутри них, и когда они обрабатываются прикладными системами, которые функционируют на основе меток, включая прикладные системы, которые формируют новые информационные объекты на основе существующих.

Когда помеченные данные должны передаваться между различными ССБ, последние должны согласовать единую ПЛБ, которая будет применяться к таким данным. Если метки, описанные политикой, применяемой внутри ССБ, отличаются от меток, описанных политикой для распространяемых данных, то политика для распространяемых данных должна определять правила отображения одной группы меток в другую и наоборот.

Само по себе наличие меток еще не дает каких-либо гарантий по защите информации. ПЛБ, применяемая по отношению к информации, должна «принудительно навязываться» для исполнения каждой организацией, несмотря на то, что помеченная информация является предметом ее контроля. Все организации, пользователи и ИТС, которые обрабатывают какой-либо элемент информации, должны заранее знать (быть ознакомлены с) ПЛБ, применяемую(ой) к такой информации. Организациям, обменивающимся информацией, необходимо установить между собой взаимное доверие, которое бы означало, что информация будет обрабатываться в соответствии с согласованными ПЛБ. Такое доверие, как правило, устанавливается на основе формального соглашения (договора).

2.2.1.1. Описание метки в ASN.1-коде

Рассмотрим пример метки конфиденциальности для СЛУД, которая имеет следующее ASN.1-кодирование:

```

id-ConfidentialityLabel OBJECT IDENTIFIER ::= {
    joint-iso-itu-t sios(24) specification(0) securityLabels(1) confidentiality(0)}

ConfidentialityLabel ::= SET {
    security-policy-identifier SecurityPolicyIdentifier OPTIONAL,
    security-classification INTEGER(0..MAX) OPTIONAL,
    privacy-mark PrivacyMark OPTIONAL,
    security-categories SecurityCategories OPTIONAL }
(ALL EXCEPT({-- none; at least one component shall be present --}))

SecurityPolicyIdentifier ::= OBJECT IDENTIFIER

PrivacyMark ::= CHOICE {
    pString PrintableString (SIZE(1..ub-privacy-mark-length)),
    utf8String UTF8String (SIZE(1..ub-privacy-mark-length))
}

ub-privacy-mark-length INTEGER ::= 128 — ITU-T Rec. X.411 | ISO / IEC 10021—4

SecurityCategories ::= SET SIZE (1..MAX) OF SecurityCategory

SecurityCategory ::= SEQUENCE {
    type [0] SECURITY-CATEGORY.&id ({SecurityCategoriesTable}),
    value [1] SECURITY-CATEGORY.&Type ({SecurityCategoriesTable}
    {@type})
}

SECURITY-CATEGORY ::= TYPE-IDENTIFIER
SecurityCategoriesTable SECURITY-CATEGORY ::= {...}

```

Пример расширения класса информационного объекта «TYPE-IDENTIFIER» представлен в международном стандарте ISO/IEC 15816.

2.2.1.2. Методы привязки меток конфиденциальности

Первый метод. Копия данных (*D*) и копия метки безопасности (*L*) хранятся вместе (в форме записи данных) в пределах границ системы безопасности. Предположим, что система способна защитить целостность метки безопасности, а также целостность (и по возможности конфиденциальность) самих данных. Защита должна быть такой, чтобы неавторизованный пользователь или прикладной процесс не были способны модифицировать данные или их соответствующую метку безопасности. Этот метод привязки не предполагает использования

криптографических функций для «связки» данных и метки безопасности.

Второй метод. Несекретная ЭЦП вычисляется по D и L , используя алгоритм формирования ЭЦП ($SigAlg$) и секретный ключ (X) из алгоритма шифрования с открытым ключом. То есть,

$$S = SigAlg(X, f(D), L).$$

ЭЦП хранится вместе с D и L в записи данных. Сформированная таким способом ЭЦП привязывает L к D . В этом выражении символ « f » обозначает открытую функцию, такую, что $f(D)$ не раскрывает информацию о D .

Если используется этот метод привязки, то нет необходимости хранения L и S в пределах границ системы безопасности. При обращении к криптографической службе и предоставлении ей некорректного значения либо L , либо D , либо S будет обнаружено соответствующее противоречие. Это противоречие вскрывается путем использования открытого ключа из алгоритма шифрования с открытым ключом в качестве проверочного ключа для проверки ЭЦП.

Третий метод. Несекретный аутентификационный код сообщения (message authentication code, MAC-код) вычисляется по D и L , используя алгоритм зашифрования ($MacAlg$) в режиме формирования MAC-кода и секретный ключ ($K-MAC$) из алгоритма формирования MAC-код. То есть,

$$MAC = MacAlg(K-MAC, f(D), L).$$

MAC-код хранится вместе с D и L в записи данных. Сформированный таким способом MAC-код привязывает L к D . В этом выражении символ « f » обозначает открытую функцию, такую, что $f(D)$ не раскрывает информацию о D .

Если используется этот метод привязки, то нет необходимости хранения L и MAC-код в пределах границ системы безопасности. При обращении к криптографической службе и предоставлении ей некорректного значения либо L , либо D , либо MAC-кода будет обнаружено соответствующее противоречие. Это противоречие вскрывается путем вычисления эталонного

значения МАС-кода с использованием предоставленных значений L и D , а также копии K -МАС, и последующим сравнением вычисленного эталонного значения МАС-кода с предоставленным значением МАС-кода.

2.2.2. Криптографические проверочные суммы

КПС представляет собой информацию, которая формируется из элемента данных путем выполнения криптографического преобразования. КПС на основе симметричной криптографии (seal, криптоконверт), ЭЦП и цифровые отпечатки (digital fingerprint) являются примерами криптографических проверочных сумм.

Криптоконверт является формой КПС, вычисленной с использованием симметричного криптографического алгоритма и секретного ключа, известного взаимодействующим сторонам. Криптоконверты используются для выявления модификаций во время доставки данных.

ЭЦП является КПС, которая защищает от незаконного копирования получателем и вычисляется с использованием закрытого ключа и асимметричного криптографического алгоритма. Поверка подлинности ЭЦП требует знания того же самого криптографического алгоритма и соответствующего открытого ключа.

ПРИМЕЧАНИЕ. Несмотря на то, что существуют другие средства предотвращения попыток получателя фальсифицировать (подделать) КПС (например использование аппаратных криптографических модулей для защиты от фальсификаций), в данной главе используется термин «ЭЦП», который означает, что КПС вычисляется с использованием асимметричного криптографического алгоритма.

ПРИМЕЧАНИЕ. В некоторых асимметричных криптографических алгоритмах процедура вычисления ЭЦП требует использования более одного закрытого ключа. Если такие алгоритмы используются, то различным объектам/субъектам может быть за-

прещено обладание несколькими закрытыми ключами. Это гарантирует, что объекты/субъекты будут взаимодействовать при формировании ЭЦП.

Цифровой отпечаток является характеристикой элемента данных, который максимально отражает (соответствует) элемент(у) данных, а с вычислительной точки зрения невозможно найти какой-либо другой элемент данных с таким же цифровым отпечатком. Для формирования цифрового отпечатка могут использоваться некоторые типы КПС (например полученные в результате применения *однонаправленной функции* (ОНФ) по всей последовательности данных). Цифровые отпечатки могут быть сформированы посредством и других криптографических алгоритмов. Например, копия элемента данных является цифровым отпечатком.

ПРИМЕЧАНИЕ. ОНФ не эквивалентны цифровым отпечаткам. Некоторые ОНФ не приемлемы для формирования цифровых отпечатков, а некоторые цифровые отпечатки не формируются с использованием ОНФ.

ПРИМЕЧАНИЕ. Вычисление ЭЦП с использованием асимметричного алгоритма может занять слишком много времени, так как в целом асимметричные алгоритмы, с вычислительной точки зрения, являются весьма затратными. Скорее всего, ЭЦП лучше сформировать по цифровому отпечатку данных, чем по всей совокупности самих данных. Это может быть результатом уменьшения времени, затрачиваемого на вычисления, так как можно гораздо быстрее вычислить ЭЦП по короткому цифровому отпечатку, чем по всему длинному сообщению.

КПС не приемлемы для защиты одиночного элемента данных от атак типа «повторная передача». Защита от атак такого рода может быть обеспечена за счет включения в данные определенной информации, которая может быть использована для обнаружения повторов, например *последовательный номер* или *метка времени*, а также использование «*криптографической связки*». Для защиты от повторной передачи такая информация должна быть проверена получателем защищенного элемента данных.

2.2.3. Сертификаты безопасности

2.2.3.1. Общие положения

СЕРТ|ИБ представляет собой совокупность связанных с обеспечением безопасности данных, который выдается ЦБ или ДТС (УЦ) вместе ВИ и используется при предоставлении услуг обеспечения целостности и аутентификации источника данных. СЕРТ|ИБ содержит указатель периода времени, в течение которого он является действительным.

СЕРТ|ИБ используются при доставке ВИ от ЦБ (или ДТС) тем объектам/субъектам, которым необходима такая информация при реализации функций обеспечения безопасности. СЕРТ|ИБ может содержать ВИ для одной или нескольких СЛБ.

СЕРТ|ИБ могут содержать ВИ в целях:

- УД (СЕРТ|УД);
- аутентификации (СЕРТ|АУ);
- обеспечения целостности (СЕРТ|ЦЛ);
- обеспечения конфиденциальности (СЕРТ|КН);
- обеспечения неотказуемости (СЕРТ|НТ);
- проведения аудита (СЕРТ|АО);
- обеспечения ключами (СЕРТ|КЛ).

2.2.3.2. Проверка последовательности (цепочки) связанных сертификатов

Проверка сертификата включает проверку его целостности и подтверждение представленного параметра подлинности организации, выдавшей (выпустившей) СЕРТ|ИБ, а также проверку того, что организация, выдавшая СЕРТ|ИБ, является авторизованной (уполномоченной) для выпуска сертификатов. Эти процедуры могут потребовать наличия дополнительной ВИ.

Если сторона, проверяющая сертификат, не имеет ВИ, необходимой для его проверки, то может воспользоваться сертификатом другого УЦ для получения необходимой ВИ. Этот процесс может повторяться с целью формирования *последовательности (цепочки) связанных СЕРТ|ИБ*. Последняя содержит ВИ, кото-

рая определяет безопасный маршрут от известного УЦ (т.е. УЦ, для которого ВИ уже была сформирована) до объекта/субъекта, которому необходима сертифицированная ВИ.

Цепочка сертификатов должна использоваться только тогда, когда ее появление обусловлено ограничениями, наложенными всеми соответствующими ПЛБ. Наличие только одной цепочки является недостаточным. Цепочка должна использоваться только тогда, когда такое использование допускается доверенными взаимосвязями между стороной, проверяющей цепочку, и УЦ, которые сформировали СЕРТ|ИБ в цепочке, а также допускается доверенными взаимосвязями между этими УЦ. Такие взаимосвязи устанавливаются ПЛБ стороны, проверяющей цепочку, и ПЛБ УЦ. Соответственно, некоторые УЦ являются надежными относительно выпуска ими сертификатов для некоторых других УЦ, в то время как некоторые другие являются надежными относительно выпуска ими сертификатов только для объектов/субъектов, находящихся под их административным управлением.

2.2.3.3. Аннулирование (отзыв) сертификатов

ВИ, содержащаяся в сертификате, может стать не действительной. Например, если закрытый ключ был скомпрометирован, то соответствующий открытый ключ не должен больше использоваться, и, следовательно, сертификаты, которые содержат этот открытый ключ, должны быть аннулированы (отозваны).

Способы, которые могут использоваться для аннулирования СЕРТ|ИБ, предусматривают применение *сертификата отзыва* (СЕРТ|ОТ) и *сертификата списка отзыва* (СЕРТ|СО). СЕРТ|ОТ представляет собой СЕРТ|ИБ, который указывает на то, что соответствующий сертификат был аннулирован. СЕРТ|СО представляет собой сертификат, который определяет список аннулированных сертификатов.

2.2.3.4. Повторное использование сертификатов

Некоторые сертификаты предназначены для многократного использования, например при продолжительном информационном взаимодействии, в то время как другие предназначены для

однократного использования. Сертификаты, используемые в процедурах аутентификации (СЕРТ|АУ), являются примером сертификатов, используемых многократно (ITU-T Rec. X.509 | ISO/IEC 9594—8). Примером СЕРТ|ИБ для одноразового использования являются сертификаты для УД (СЕРТ|УД), которые обеспечивают однократный доступ. Сертификаты для одноразового использования могут содержать информацию, предотвращающую их повторное использование (например уникальный номер).

2.2.3.5. Структура сертификата

Единая форма сертификатов включает три следующих компонента (рис. 2.3):

- информация, которая обязательна во всех сертификатах;
- ВИ, необходимая для одной или нескольких СЛБ;
- информация для управления или ограничения использования ВИ.

Информация, которая обязательна во всех сертификатах, разделена на две категории:

- a) информация, которая используется в процедурах обеспечения целостности и аутентификации источника данных (например КПС и указатели на информацию, используемую для ее проверки). До того, как будет предоставлена услуга по аутентификации источника данных, дополнительно должен быть указан проверяемый параметр подлинности источника сертификата (т.е. выпускающего УЦ);
- b) информация, по которой может быть определен (например явно указанный срок действия) или извлечен (например время издания сертификата и продолжительность его действия) период действия сертификата. Такая информация предотвращает не предусмотренное повторное использование сертификата, несмотря на то, что сертификат может использоваться повторно много раз в пределах своего срока действия.



Рис. 2.3. Структура сертификата

Информация для управления или ограничения использования ВИ разделена на три категории:

- а) информация, используемая для защиты сертификата от неавторизованного (несанкционированного) применения. Например:
- информация (например уникальный идентификатор, УИД), устанавливающая объект/субъект или объекты/субъекты, информация о которых включена в сертификат;
 - информация, устанавливающая объекты/субъекты, которым разрешено пользоваться ВИ, содержащейся в сертификате;

- информация, которая контролирует, сколько раз может использоваться сертификат;
 - информация, определяющая ПЛБ, в соответствие с которой должен использоваться сертификат;
 - методы защиты и соответствующие параметры защиты сертификата от кражи;
 - информация, используемая для защиты от атак типа «повторная передача» (например уникальный номер или запрос);
- b) информация, которая может использоваться в процедуре аудита безопасности. Например:
- контрольный идентификатор СЕРТ|ИБ (например последовательный (серийный) номер), который является уникальным для сертификата по отношению ко всем другим сертификатам, выданным одним и тем же УЦ или его представителем;
 - параметр подлинности (предназначенный для аудита) объекта/субъекта, которому был выдан сертификат;
- c) информация, которая может использоваться в процедуре восстановления безопасности. Например:
- контрольный идентификатор сертификата, который может использоваться для аннулирования определенного сертификата;
 - групповой идентификатор сертификата, который может использоваться для аннулирования группы сертификатов.

2.2.4. Способы защиты сертификатов безопасности

Рассмотрим некоторые примеры способов защиты СЕРТ|ИБ.

Потенциальной угрозой для безопасности самого сертификата является угроза, при которой нарушитель выдает себя за истинного владельца сертификата, который указан в этом СЕРТ|ИБ. Такое неавторизованное (несанкционированное) использование сертификата называется *кражей сертификата*.

Угроза может быть внешней или внутренней. Внешняя угроза заключается в том, что нарушитель может получить сертификат путем прослушивания линий (каналов) связи, которые используются только по своему прямому назначению. Внутренняя угроза заключается в том, что объект/субъект, имеющий легитимное право на получение сертификата (например с целью формирования ВИ взаимодействующей стороны), может ложно выдавать себя за объект/субъект (владельца), указанный в сертификате.

Сертификат можно защитить от кражи путем непосредственного использования СЛБ, обеспечивающих защиту линий (каналов) связи при взаимодействии открытых систем, или путем использования альтернативного метода защиты, требующего дополнительных параметров, которые являются внутренними и внешними по отношению к защищаемому сертификату.

Говорят, что способ защиты сертификата обеспечивает *функцию делегирования*, если объект/субъект, имеющий право пользоваться сертификатом, может передать свое право другому объекту/субъекту.

2.2.4.1. Защита путем использования СЛБ, обеспечивающих защиту линий (каналов) связи при взаимодействии открытых систем

Угроза кражи внешним нарушителем может быть предотвращена путем использования СЛКН при доставке сертификатов между взаимодействующими сторонами.

2.2.4.2. Защита путем использования параметра, размещенного внутри сертификата

Существует несколько альтернативных методов защиты СЕРТ|ИБ от кражи. Каждый из этих методов использует внутренние параметры, размещенные внутри сертификата, и соответствующие внешние параметры. Некоторые методы могут указываться в самом сертификате. Такие методы включают:

- метод на основе аутентификации;
- метод на основе использования секретного ключа;

- метод на основе использования открытого ключа;
- метод на основе использования ОНФ.

Сертификаты могут использовать несколько таких методов в различных сочетаниях.

Метод на основе аутентификации. В этом методе внутренним параметром являются УИД объектов/субъектов, которым разрешено использовать сертификат. Внешним параметром является УИД объекта/субъекта, который предполагает использовать сертификат. Этот внешний параметр предоставляется службой аутентификации. Кроме того, сертификат может включать дополнительные внутренние параметры, например серийный номер СЕРТ|ИБ.

Метод на основе аутентификации обеспечивает защиту сертификата следующим образом:

- он ограничивает использование СЕРТ|ИБ только теми объектами/субъектами, чьи идентификаторы содержатся в сертификате.

Этот метод не позволяет авторизованному (уполномоченному) пользователю сертификатом передавать свои права другому объекту/субъекту, так как объекты/субъекты, которым разрешено пользоваться сертификатом, были зафиксированы в момент выпуска сертификата. Таким образом, этот метод не обеспечивает функцию делегирования.

Метод на основе использования секретного ключа. В этом методе весь сертификат зашифровывается с использованием симметричного криптографического алгоритма. В данном случае внешним параметром является секретный ключ, используемый для зашифрования сертификата.

Метод на основе использования секретного ключа обеспечивает защиту сертификата следующим образом:

- он ограничивает использование СЕРТ|ИБ только теми объектами/субъектами, которым известно значение секретного ключа (т.е. они могут расшифровать зашифрованный сертификат).

Этот метод обеспечивает функцию делегирования, так как авторизованный (уполномоченный) пользователь сертификатом может передать свои права другому объекту/субъекту путем передачи ему либо секретного ключа, либо расшифрованного сертификата.

Метод на основе использования открытого ключа. В этом методе внутренним параметром являются открытый ключ, а внешним параметром является соответствующий закрытый ключ.

Метод на основе использования открытого ключа обеспечивает защиту сертификата следующим образом:

- он ограничивает использование сертификата только теми объектами/субъектами, которым известно значение закрытого ключа (т.е. они могут сформировать ЭЦП с использованием закрытого ключа).

Этот метод обеспечивает функцию делегирования, так как авторизованный (уполномоченный) пользователь сертификатом может передать свои права другому объекту/субъекту путем передачи ему закрытого ключа.

Метод на основе использования ОНФ. В этом методе внутренним параметром является результат применения ОНФ к внешнему параметру. Внутренний параметр называется *ключом защиты*, а внешний параметр — *контрольным ключом*.

Метод на основе использования ОНФ обеспечивает защиту СЕРТ|ИБ следующим образом:

- он ограничивает использование сертификата только теми объектами/субъектами, которым известно значение контрольного ключа (т.е. они могут доказать, что знают контрольный ключ, путем демонстрации его значения).

Этот метод обеспечивает функцию делегирования, так как авторизованный (уполномоченный) пользователь сертификатом может передать свои права другому объекту/субъекту путем передачи ему контрольного ключа.

2.2.4.3. Защита внутренних и внешних параметров в течение их доставки

Существуют четыре наиболее важных случая:

- доставка внутреннего параметра в ЦБ до выпуска им сертификата. Этот тип доставки необходим только тогда, когда внутренние и внешние параметры не формируются ЦБ;
- доставка внешнего параметра из ЦБ после выпуска им сертификата. Этот тип доставки необходим только тогда, когда внутренние и внешние параметры формируются ЦБ;
- доставка внешнего параметра между взаимодействующими сторонами, когда право использования сертификата подтверждено;
- доставка внешнего параметра между взаимодействующими сторонами, когда право использования сертификата делегировано.

Доставка внутренних параметров в выпускающий ЦБ. В методах на основе аутентификации, использования открытого ключа и ОНФ внутренний параметр может быть доставлен в ЦБ еще до его размещения в сертификате. В течение доставки в ЦБ внутреннего параметра его целостность должна быть защищена.

В методе на основе использовании секретного ключа внешний параметр (т.е. секретный ключ) может быть доставлен в ЦБ до выпуска сертификата. При доставке необходимо обеспечить защиту целостности и конфиденциальности.

Доставка внешних параметров между взаимодействующими сторонами. В методе на основе аутентификации внешний параметр (параметр подлинности пользователя сертификатом) предоставляется способом аутентификации.

В методах на основе использования секретного ключа и ОНФ внешний параметр должен доставляться между взаимодействующими сторонами, когда сертификат уже используется. Использование сертификата ограничивается теми, кто знает

правильное значение секретного или контрольного ключа. В течение доставки внешнего параметра между взаимодействующими сторонами его конфиденциальность должна быть защищена.

Различие между этим двумя методами заключается в том, что когда используется метод на основе секретного ключа необходимо установить значение внешнего параметра еще до того, когда может быть проверена КПС сертификата, а при использовании метода на основе ОНФ, КПС сертификата может быть проверена еще до того, как будет установлен внешний параметр.

В методе на основе использования закрытого ключа нет необходимости доставлять внешний параметр между взаимодействующими сторонами, когда КПС сертификата уже используется, так как одна из сторон может доказать, что она знает закрытый ключ и что его не нужно устанавливать (путем формирования ЭЦП). При использовании этого метода внешний параметр (закрытый ключ) нужен только при делегировании права на пользование сертификатом. В течение доставки закрытого ключа между взаимодействующими сторонами его конфиденциальность должна быть защищена.

2.2.4.4. Использование сертификата одиночными объектами/субъектами или группами объектов/субъектов

Рассмотренные выше методы защиты могут применяться для ограничения пользования сертификатов либо одиночными поименованными объектами/субъектами, либо поименованными группами объектов/субъектов:

- сертификат может быть привязан к определенному объекту/субъекту. Секретный, закрытый или контрольный ключ в зашифрованном виде доставляется одиночному объекту/субъекту, а УИД или атрибут безопасности объекта/субъекта помещается в сертификат;
- сертификат может быть привязан к поименованной группе объектов/субъектов. Секретный, закрытый или контрольный ключ в зашифрованном виде доставляется членам группы, а УИД или атрибуты безопасности груп-

пы помещаются в сертификате. В этом случае любой член группы может воспользоваться сертификатом.

2.2.4.5. Использование сертификата при УД

Сертификаты могут использоваться при УД. В этом случае очень важно установить защищенную связь между сертификатами и запросами доступа, которые он обслуживает. Если такой защищенной связи не существует, то СЕРТ|УД становятся уязвимы к атакам типа «повторная передача», при осуществлении которых нарушитель вслед за ложным запросом доступа передает копию настоящего сертификата.

Такие атаки могут быть парированы с помощью СЛЦЛ, которая обеспечивает «связку» СЕРТ|УД, внешнего параметра и запроса доступа.

При использовании метода на основе аутентификации такая связка может быть установлена путем соединения процедуры аутентификационного обмена со способом обеспечения целостности (СПЦЛ)¹.

При использовании метода на основе секретного ключа такая связка может быть установлена путем включения ключа для СПЦЛ в «тело» СЕРТ|УД и путем использования этого ключа при формировании КПС запроса доступа. С другой стороны, секретный ключ (или его разновидность) может использоваться в качестве ключа для СПЦЛ.

ПРИМЕЧАНИЕ. Использование одного и того же криптоключа в СПЦЛ и способе обеспечения конфиденциальности (СПКН) может повлечь за собой появление некоторых типов атак. Для защиты от такой угрозы можно использовать *разновидности ключа*. Разновидность криптоключа представляет собой другой криптоключ, который вычислен из оригинального криптоключа, но не такой же, как последний.

При использовании метода на основе ОНФ такая связка может быть установлена путем использования контрольного ключа в качестве ключа для СПЦЛ, основанного на ОНФ.

¹ Этот способ рассматривается в главе 3.

При использовании метода на основе открытого ключа такая связка может быть установлена путем использования закрытого ключа при формировании ЭЦП запросов доступа.

Помимо всех этих методов, связка между СЕРТ|УД, внешнего параметра и запроса доступа может быть установлена путем использования СЛЦЛ, которая является частью службы установления соединений при взаимодействии открытых систем.

2.2.5. Маркеры безопасности

Маркер безопасности представляет собой совокупность данных, защищенных одной или несколькими СЛБ, вместе с ВИ, используемой для обеспечения функционирования этих СЛБ, которая доставляется между взаимодействующими сторонами (объектами/субъектами). Маркеры безопасности могут классифицироваться в соответствие с тем, кто их сформировал, и с тем, какие СЛБ использовались для защиты их содержания.

Маркер безопасности, который выпущен УЦ и защищен с использованием служб обеспечения целостности и аутентификации источника данных, называется сертификатом обеспечения безопасности (см. § 2.2.3).

Для реализации большинства СПБ необходим обмен ВИ, целостность которой должна быть защищена в течение информационного взаимодействия двух сторон (объектов/субъектов), причем ни одна из них не является УЦ. Для обеспечения целостности информационного обмена используются маркеры безопасности, а не СЕРТ|ИБ, так как взаимодействующие объекты/субъекты, которые их сформировали, не являются УЦ. Такие маркеры безопасности называются *маркерами безопасности, целостность которых защищена*.

Все маркеры безопасности, целостность которых защищена, содержат:

- информацию, которая обеспечивает защиту целостности и аутентификацию источника данных (например КПС и указатель на информацию, используемую для ее проверки).

Маркер безопасности, целостность которого защищена, может содержать следующие дополнительные элементы информации:

- информацию, из которой может быть установлен срок действия маркера безопасности;
- информацию, используемую для защиты от атак типа «повторная передача» (например уникальный номер).

2.3. Общие средства обеспечения безопасности

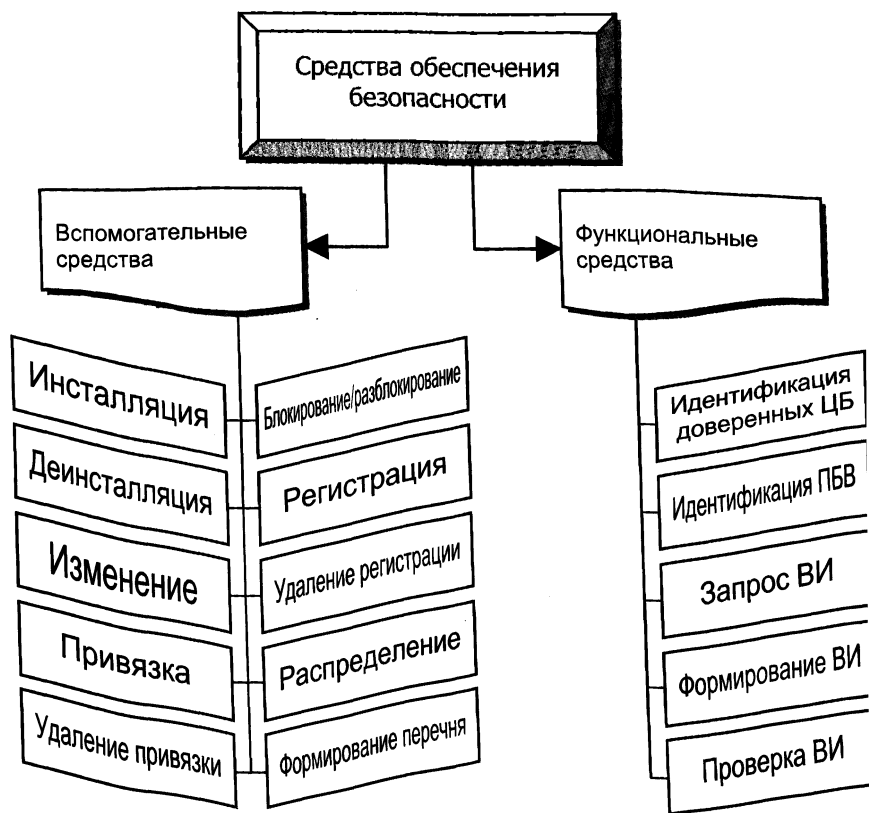


Рис. 2.4. Концептуальные средства обеспечения безопасности

Средства обеспечения безопасности делятся на два основных класса (рис. 2.4):

- a) вспомогательные (обеспечивающие) СРБ;
- b) функциональные СРБ.

2.3.1. Вспомогательные средства

К вспомогательным (обеспечивающим) СРБ относятся те средства, которые непосредственно в ПРБ не участвуют:

1. *Средство инсталляции ВИ (install)*. Это средство обеспечивает начальную загрузку ВИ, которая «привязана» к элементу¹.
2. *Средство деинсталляции ВИ (deinstall)*. Это средство используется для удаления объекта/субъекта из ССБ путем аннулирования ВИ, которая «объявляла» (указывала на то, что) этот объект/субъект участником ССБ.
3. *Средство изменения ВИ (change)*. Это средство используется при модификации ВИ, связанной с элементом.
4. *Средство привязки ВИ (validate)*. Это средство устанавливает привязку некоторой совокупности ВИ к элементу. Средство привязки ВИ используется УЦ или его представителем.
5. *Средство удаления привязки ВИ (invalidate)*. Это средство блокирует любое использование ВИ, связанной с элементом. Средство удаления привязки ВИ используется УЦ или его представителем. ВИ, заблокированная с помощью средства удаления привязки, может храниться внутри системы с целью проведения последующей процедуры аудита безопасности и для обеспечения гарантии того, что ВИ остается заблокированной.

¹ Под элементом понимается информационный (информационно-технологический) элемент (совокупность данных).

6. *Средство блокирования/разблокирования СЛБ (disable/re-enable security service)*. Эти средства блокируют и разблокируют определенные компоненты СЛБ.
7. *Средство регистрации (enrol)*. Это средство побуждает ЦБ зафиксировать некоторую ВИ, связанную с объектом/субъектом. Средство регистрации может использоваться любым объектом/субъектом, кроме ЦБ. Например, объект/субъект, желающий присоединиться к ССБ, может использовать средство регистрации для оповещения ЦБ о своем желании присоединиться к ССБ.
8. *Средство удаления регистрации (un-enrol)*. Это средство используется для удаления элемента из ССБ и аннулирования связанной с этим элементом ВИ. Средство удаления регистрации используется ЦБ или его представителем.
9. *Средство распределения ВИ (distribute)*. Это средство используется ЦБ или его представителем для обеспечения доступности компонентов ВИ для других объектов/субъектов.
10. *Средство формирования перечня (list)*. Это средство формирует перечень ВИ, которая прикреплена к определенному элементу.

2.3.2. Функциональные средства

К функциональным СРБ относятся те средства, которые непосредственно участвуют в ПРБ:

1. *Средство идентификации доверенных (надежных) ЦБ*. Это средство идентифицирует те ЦБ, которые являются доверенными (надежными) в контексте ПЛБ по отношению к определенным элементам и по отношению к основным направлениям их деятельности, связанной с обеспечением безопасности (например обеспечение ключами шифрования, СЕРТ|УД или СЕРТ|АУ).
2. *Средство идентификации правил безопасного взаимодействия*. Это средство идентифицирует используемые ПБВ. Функционирование этого средства может сопрово-

ждаться предварительным формированием информации или ее согласованием между элементами связанных друг с другом ССБ.

ПРИМЕЧАНИЕ. ПБВ формируются путем соглашения между ССБ, а не путем использования этого средства. Это средство идентифицирует те ПБВ, которые уже сформированы и приемлемы для соответствующего направления деятельности.

3. *Средство запроса ВИ.* Это средство запрашивает необходимую ВИ перед началом определенной процедуры (деятельности). Примерами разновидностей такого средства являются:
 - при управлении доступом: средство запроса на получение ВИ для УД, привязанной к инициатору; средство запроса получение ВИ для УД, привязанной к целевому объекту;
 - при аутентификации: средство запроса на получение необходимой ВИ для процедуры аутентификации.
4. *Средство формирование ВИ.* Это средство формирует ВИ для определенной процедуры (деятельности), связанной с обеспечением безопасности. Примерами разновидностей такого средства являются:
 - при управлении доступом: средство формирования ВИ для УД с целью ее последующей привязки;
 - при аутентификации: средство формирование необходимой ВИ для процедуры аутентификации;
 - при обеспечении неотказуемости: средство формирования доказательства.
5. *Средство проверки ВИ.* Это средство осуществляет проверку подлинности ВИ, полученной путем применения средства формирования ВИ. Средство проверки ВИ может само формировать ВИ, которая будет передана другому используемому средству проверки ВИ. Примерами разновидностей такого средства являются:
 - при управлении доступом: средство проверки ВИ для УД;

- при аутентификации: средство проверки ВИ для процедуры аутентификации;
- при обеспечении неотказуемости: средство проверки подлинности доказательства.

Пример ситуации, при которой данные, полученные на выходе средства проверки ВИ, передаются обратно для последующей процедуры проверки, представляет собой *протокол обоюдной аутентификации*. Предположим, что стороны *A* и *B* желают аутентифицировать друг друга, и *A* инициирует информационный обмен в соответствии с некоторым протоколом. *A* использует средство формирования для генерирования аутентификационной информации, содержащей защиту параметра подлинности *A* и запрос, на который должна ответить *B*. *B* использует средство проверки с целью проверки того, что запрос поступил от *A*, и кроме этого формирует новый элемент аутентификационной информации, содержащей защиту параметра подлинности *B* и ответ на запрос *A*. Затем *A* использует средство проверки для обработки ответа *B*. Средство проверки устанавливает, что ответ поступил от *B* и что он совпадает с переданным запросом.

На практике могут понадобиться *дополнительные средства обеспечения безопасности*, которые не были рассмотрены ранее (например средства обеспечения физической и персональной безопасности). Однако такие средства в дальнейшем не рассматриваются. Тем не менее использование таких дополнительных средств обеспечения безопасности может даже исключить необходимость использования некоторых рассмотренных ранее СЛБ.

2.4. Взаимосвязи между СПБ

Очень часто для одной взаимодействующей стороны необходимо обращаться к нескольким различным СЛБ. Такое требование может быть удовлетворено либо за счет использования одного СПБ, который основан на нескольких СЛБ, либо за счет одновременного использования нескольких различных СПБ.

Если различные СПБ используются одновременно, то иногда возникает ситуация, в которой СПБ взаимодействуют не лучшим образом, чем может воспользоваться нарушитель. То есть, способы, обеспечивающие приемлемый уровень защищенности, которые при их изолированном использовании могут стать более уязвимыми, применяются в сочетании с другими способами. Очень часто бывает так, что два СПБ могут комбинироваться несколькими различными способами. Уязвимости совместно используемых способов могут отличаться друг от друга в зависимости от способа совместного использования СПБ.

Наиболее важным случаем взаимодействия СПБ является совместное использование криптографических способов (например СПЦЛ со СПКН, или способ обеспечения неотказуемости (СПНТ) со СПКН). Уровень защищенности, обеспечиваемый двумя совместно используемыми способами, зависит от порядка, в соответствии с которым осуществляются криптографические преобразования (криптопреобразования).

В целом, когда используются асимметричные криптографические алгоритмы, целесообразно сначала осуществлять криптопреобразования для обеспечения целостности или неотказуемости, и только потом зашифровывать подписанные данные или данные, защищенные с помощью КПС.

Противоположным примером, когда необходимо использовать две СЛБ в обратном порядке (т.е. СЛКН первой), является случай, в котором службы используются между различными взаимодействующими сторонами, а одной стороне необходимо проверить целостность шифртекста при условии, что ей запрещено знать открытый текст. Такая ситуация характерна для систем обмена сообщениями, в которых ретрансляционному узлу может понадобиться проверка целостности и источника сообщения, но вместе с тем ему запрещено знать текст сообщения.

Использование СЛЦЛ и СЛКН в рассмотренном противоположном порядке несет определенные риски, связанные с тем, что СЛЦЛ не сможет обеспечивать СЛНТ. Если все-таки необходимо использовать все три службы и требуется обратный порядок применения СЛЦЛ и СЛКН, то можно использовать

два СПЦЛ, причем первый до применения СПКН, а второй — после. Примером такой ситуации является система обмена сообщениями. Если защита конфиденциальности обеспечена, то в сообщении могут быть помещены две различные ЭЦП (первая ЭЦП формируется по шифртексту для защиты от вскрытия сообщения при его обработке в ретрансляционном узле, а вторая ЭЦП формируется по открытому тексту для предоставления получателю доказательства неотказуемости источника).

2.5. Отказ в обслуживании и доступность

Отказ в обслуживании (denial of service, DoS-атака) наступает всякий раз тогда, когда качество обслуживания падает ниже требуемого уровня, включая событие, когда служба (услуга) становится вообще недоступной. Такой отказ в обслуживании может быть следствием внешней атаки нарушителя или нештатных (катастрофических) событий (например шторм или землетрясение). *Доступность* представляет собой условие, при котором отказ в обслуживании или резкое снижение качество связи (соединения) невозможны.

Условия для отказа в обслуживании не всегда возможно предотвратить. Для выявления отказа в обслуживании могут использоваться СЛБ, чтобы в последующем провести необходимые корректирующие процедуры (настройки). Однако факт выявления такого отказа не способен определить, было ли это обусловлено проведенной атакой нарушителя или нештатным (катастрофическим) событием. В соответствии с ПЛБ, при обнаружении условий для отказа в обслуживании, возможно, потребуется регистрация этого события (для последующего проведения аудиторской проверки) и передача сигнала оповещения об опасности средству обработки таких сигналов.

После того, как условие отказа в обслуживании было установлено, могут использоваться СЛБ для своих собственных корректировок и для возвращения к приемлемому уровню качества обслуживания. Для обнаружения условий отказа и для проведения корректирующих процедур (настроек) могут использоваться СЛБ, а также другие обеспечивающие службы, не связанные с

безопасностью (например перенаправление трафика по другим каналам и линиям связи, включение средств резервного копирования и хранения или перевод резервных средств обработки в интерактивный режим).

Различные службы являются объектами DoS-атак, а способы, используемые для их предотвращения, могут варьироваться в зависимости от вида защищаемой прикладной системы. Это означает, что невозможно с помощью какого-либо стандартного метода классифицировать способы защиты от DoS-атак.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ АУТЕНТИФИКАЦИИ

Во многих реальных прикладных системах предъявляются требования по обеспечению безопасности, основанные на корректности идентификации привлекаемых участников информационного взаимодействия. Такие требования могут включать защиту имущества и ресурсов от несанкционированного (неавторизованного) доступа (НСД). Для реализации такой защиты могут использоваться процедуры и способы управления доступом, основанные на параметре подлинности (*identity*), а также/или принуждения к прохождению процедуры идентификации с помощью проведения проверки регистрационных записей соответствующих событий, и с целью учета и выставления счета на оплату.

Процедура подтверждения подлинности называется *аутентификацией*. В данной главе определен общий подход к реализации служб аутентификации.

3.1. Общие положения

3.1.1. Основные концепции аутентификации

Аутентификация дает гарантию того (подтверждает), что объект действительно является тем, за кого себя выдает. Аутентификация имеет значение только в условиях информационного взаимодействия объекта (кого проверяют) и субъекта (кто проверяет) аутентификации. В ИТС рассматриваются две наиболее важных формы аутентификации:

- объект выступает в роли претендента, устанавливающего информационное взаимодействие с субъектом (аутентификация объекта);
- объект является источником совокупности данных, которые доступны субъекту (аутентификация источника данных).

Эти две формы аутентификации имеют между собой различия, заключающиеся в следующем:

- аутентификация объекта обеспечивает подтверждение (доказательство) подлинности объекта в рамках информационного взаимодействия. Подлинность аутентифицированного объекта может быть гарантирована только тогда, когда функционирует соответствующая служба аутентификации;
- аутентификация источника данных обеспечивает подтверждение (доказательство) подлинности объекта, который несет ответственность за некоторую совокупность данных.

Когда используется аутентификация источника данных, тогда необходимо иметь соответствующую дополнительную гарантию того, что данные не были модифицированы. Это может быть достигнуто за счет использования службы обеспечения целостности. Например:

- за счет использования систем, в которых данные не могут быть модифицированы;
- путем проверки того, что принятые данные полностью совпадают с цифровой копией (цифровым отпечатком) переданных данных;
- путем использования ЭЦП;
- путем использования алгоритмов симметричной криптографии.

Термин информационное взаимодействие (соединение, информационный обмен), используемый в определении аутентификации объекта, может интерпретироваться весьма широко и может относиться, например, к взаимодействию открытых систем, связи между процессами или взаимодействию между пользователем и терминалом.

3.1.1.1. Идентификация и аутентификация

Взаимодействующая сторона информационного соединения является объектом, чья подлинность может быть аутентифи-

цирована (подтверждена). Объект может иметь один или более отличительных идентификаторов, непосредственно связанных с этим объектом. Для проверки действительной подлинности объектов субъект может воспользоваться услугами службы аутентификации. Проверенная подлинность объекта именуется аутентифицированной (подтвержденной) подлинностью.

Примеры взаимодействующих сторон информационного соединения, которые могут быть идентифицированы и в последующем аутентифицированы, следующие:

- пользователи (граждане, физические лица, персоны);
- процессы;
- реальные открытые системы;
- логические объекты каждого из уровней ЭМВОС или Интернет-архитектуры;
- организации (юридические лица).

УИД должны быть однозначными в границах конкретного ССБ. УИД позволяют отличить взаимодействующую сторону информационного соединения от других возможных сторон в границах одного и того же ССБ одним из следующих способов:

- в случае низкого уровня кластеризации, благодаря принадлежности к группе объектов, учитывая их равнозначность при решении задачи аутентификации; в этом случае вся группа объектов рассматривается как одна взаимодействующая сторона информационного соединения, имеющая один УИД;
- в случае высокого уровня кластеризации идентифицируется один и только один объект.

Когда между различными ССБ осуществляется процедура аутентификации, тогда УИД может быть неприемлемым для однозначной идентификации объекта, так как различные администрации, управляющие этими ССБ, могут использовать те же самые УИД. В этом случае УИД должен использоваться совместно с идентификаторами ССБ с целью присвоения каждому сетевому объекту своего уникального идентификатора.

Типичными примерами УИД являются:

- имена в рамках распределенных прикладных служб;
- сетевые адреса;
- названия прикладных процессов и прикладных объектов;
- идентификаторы объектов;
- персональные имена (уникальные в рамках конкретного ССБ);
- номера паспортов или электронных средств социальной защиты.

3.1.1.2. Объекты и субъекты аутентификации

Термин *претендент* (объект аутентификации, предъявляющий права, *claimant*) используется для определения объекта, который является или представляет взаимодействующую сторону информационного обмена для проведения в отношении него процедуры аутентификации. Претендент обладает функциями, которые необходимо инициализировать от имени взаимодействующей стороны в течение процедуры аутентификации.

Термин *проверяющая сторона* (субъект аутентификации, *verifier*) используется для определения субъекта, который является или представляет взаимодействующую сторону информационного обмена, запрашивающую подтверждение подлинности. Субъект аутентификации обладает функциями, которые необходимо инициализировать в течение процедуры аутентификации.

Взаимодействующая сторона информационного обмена, участвующая в обоюдной аутентификации, будет выступать в двух ролях одновременно, а именно как *претендент* (объект аутентификации) и как *проверяющая сторона* (субъект аутентификации).

Термин *доверенная третья сторона* (ДТС, *trusted third party*) используется для определения ЦБ или его представителя, которому доверяют обе взаимодействующие стороны, относительно его деятельности по обеспечению безопасности. В данном случае ДТС обеспечивает проведение процедуры аутентификации.

из одной или нескольких частных процедур обмена ВИАУ в целях проведения процедуры аутентификации.

На рис. 3.1 показаны взаимосвязи между претендентом, проверяющей стороной и ДТС, а также три типа ВИАУ.

В некоторых случаях с целью проведения процедуры обмена ВИАУ претенденту может понадобиться обращение в ДТС. Аналогично, и проверяющая сторона может обратиться к ДТС с целью проведения процедуры обмена ВИАУ. В таких случаях ДТС может хранить проверочную ВИАУ, относящуюся к взаимодействующей стороне.

Возможен случай, когда ДТС используется для доставки ВИАУ, предназначенной для обмена в процедуре аутентификации.

Возможно, что взаимодействующим сторонам понадобится хранить ВИАУ для ее последующего использования в процедуре аутентификации самой ДТС.

3.1.2. Практические аспекты функционирования СЛАУ

3.1.2.1. Угрозы аутентификации

Цель аутентификации — обеспечить гарантированное подтверждение подлинности взаимодействующей стороны. Способы и средства обеспечения аутентификации обычно должны парировать угрозы, связанные с проведением атак типа «маскарад» и «повторная передача сообщений».

Атака маскарад относится к обману, при котором нарушитель выступает в роли полномочного объекта, т.е. нарушитель подменяет претендента, который определенным образом устанавливает связь с проверяющей стороной (например выступая в роли источника данных или посредством установления соединения для проведения информационного обмена). Эти типы угроз включают атаки типа «повторная передача», «ретрансляция» и компрометация предъявляемой ВИАУ.

Угроза атаки маскарад связана с деятельностью, которая инициирована либо претендентом, либо проверяющей стороной (например выступая в роли источника данных или посредством

установления соединения для проведения информационного обмена). Защита против атаки маскарад при осуществлении каких-либо действий по установлению и обеспечению информационного взаимодействия требует использование службы обеспечения целостности с целью «привязки» компонентов этих данных к процедуре обмена ВИАУ. Для нейтрализации угроз, относящихся к атакам маскарад, должна использоваться процедура аутентификации, причем во взаимосвязи с некоторой формой службы обеспечения целостности, которая связывает подтверждение подлинности с информационным взаимодействием.

Атака типа «повторная передача» относится к повтору процедуры обмена ВИАУ с целью выполнения неавторизованных (несанкционированных) действий. Атаки такого типа обычно проводятся в сочетании с другими атаками, например модификация данных. Не все способы и средства адекватны с точки зрения нейтрализации атак типа «повторная передача». Такие атаки могут стать угрозой для других служб безопасности. Аутентификация может быть использована для предотвращения атак «повторная передача», так как она предполагает использование средств для установления источника информации при электронном взаимодействии сторон.

3.1.2.2. Ретрансляция процедуры аутентификации

В отдельных случаях взаимодействующая сторона будет вынуждена обмениваться информацией с другой стороной в рамках одной системы не напрямую. В такой ситуации в рамках системы должен быть сформирован ее представитель. Более того, перед тем как в границах системы будет сформирован представитель взаимодействующей стороны, последняя должна пройти процедуру собственной аутентификации.

Когда представитель взаимодействующей стороны действует от ее имени, он пройдет процедуру собственной аутентификации вместо представляемой им стороны. Ввиду того что представитель взаимодействующей стороны действует так, как если бы он являлся этой стороной, действия последней внутри системы могли бы распространяться без необходимого непосредственного ее участия.

Когда взаимодействующей стороной является физическое лицо (пользователь), то для ограничения «времени жизни» его представителя в период времени, в течение которого сам пользователь работает в некотором определенном сегменте системы (сети), могут использоваться специализированные способы и средства.

Претендент, действующий от имени одной взаимодействующей стороны, может получить доступ в другую систему, которая, в свою очередь, сформирует своего собственного представителя взаимодействующей стороны с последующей ее аутентификацией. Формирование такого представителя рассматривается как ретрансляции процедуры аутентификации.

Проведение ретрансляции процедуры аутентификации рассмотренным выше способом может быть запрещено ПЛБ.

3.1.2.3. Односторонняя и обоюдная аутентификация

Процедура аутентификации может быть односторонней или обоюдной (двусторонней). Односторонняя аутентификация обеспечивает гарантированное подтверждение подлинности только одной взаимодействующей стороны. Обоюдная аутентификация обеспечивает гарантированное подтверждение подлинности обеих взаимодействующих сторон.

Процедура аутентификации объекта может быть либо односторонней, либо обоюдной. Вполне очевидно, что аутентификация источника данных всегда является односторонней.

3.1.2.4. Начало процедуры аутентификации (аутентификационного обмена)

Процедура аутентификации может быть инициирована либо претендентом, либо проверяющей стороной. Взаимодействующая сторона, которая начинает обмен ВИАУ, называется инициатором процедуры аутентификации.

3.1.2.5. Отзыв (аннулирование) ВИАУ

Отзыв (аннулирование) ВИАУ означает окончательную недействительность проверочной ВИАУ.

В некоторых конкретных ситуациях отзыв ВИАУ может быть востребован ПЛБ. Решение об аннулировании ВИАУ может основываться на выявлении событий, угрожающих безопасности, изменении политики или может быть вызвано другими причинами. Отзыв ВИАУ может подразумевать прекращение существующего доступа или иметь другие последствия.

Кроме этого, могут произойти следующие действия:

- a) регистрация события с целью его последующего анализа в рамках проведения аудита;
- b) локальный отчет о событии;
- c) удаленный отчет о событии;
- d) разъединение существующего соединения.

Для каждого события выбирается специфическая реакция (ответное действие), которая зависит от действующей ПЛБ и других факторов, связанных с состоянием информационного взаимодействия, например вносились или нет изменения в учетные данные после того, как взаимодействующая сторона была зарегистрирована и начала информационный обмен.

3.1.2.6. Гарантированность непрерывной аутентификации

Аутентификация объекта обеспечивает гарантированное подтверждение его подлинности только на определенный момент времени. Одним из способов обеспечения гарантированной непрерывной аутентификации является «связывание» СЛАУ и СЛЦЛ.

Говорят, что СЛАУ и СЛЦЛ связаны, когда одна взаимодействующая сторона была аутентифицирована с использованием службы аутентификации в начальной фазе установления соединения, а в последующем передача данных от имени этой стороны была связана не только с процедурой обмена ВИАУ, но и с процедурой обеспечения целостности. Такой подход гарантирует, что более поздняя информация не может быть изменена другой стороной соединения, и более того, должна поступать только от той взаимодействующей стороны, которая

была аутентифицирована в начальной фазе установления соединения. Очень важно, что СЛЦЛ используется на протяжении всего выбранного маршрута доставки информации от одной аутентифицированной взаимодействующей стороны до проверяющей стороны. Например, атака «маскарад» возможна только в том случае, если часть информации могла быть сформирована взаимодействующими сторонами, которые не прошли процедуру аутентификации.

Другим способом обеспечения гарантированности того, что взаимодействующий объект остается тем же, что и был в начальной фазе соединения, является периодическое проведение процедуры аутентификации на основе обмена ВИАУ. Однако этот способ не предотвращает вторжения в промежуточных интервалах, и поэтому не обеспечивает гарантии непрерывности аутентификации. Например, возможна следующая атака: нарушитель в момент, когда поступает команда на проведение следующей процедуры аутентификации, «разрешает» полномочному объекту провести все необходимые для аутентификации действия. Затем, по завершении этих действий, нарушитель снова «захватывает» соединение, обеспечивающее информационное взаимодействие.

Если для реализации СПЦЛ необходим ключ, то последний может быть выбран из параметров, которые определяются в течение процедуры аутентификации. Полученный таким образом ключ, связанный с аутентифицированной взаимодействующей стороной, будет использоваться при реализации способа обеспечения целостности, направленного на «связывание» СЛАУ и СЛЦЛ, как было рассмотрено ранее.

Способ вычисления ключа для СЛЦЛ может быть определен как составная часть совокупности параметров, которые определяют, какие методы и алгоритмы целесообразно использовать на протяжении всей процедуры аутентификации.

ПРИМЕЧАНИЕ. Когда используются и другие СЛБ, существует возможность определения служебной информации на основе параметров, которые определяются в течение процедуры аутентификации, например секретный ключ.

3.1.2.7. Распределение компонентов аутентификации среди нескольких ССБ

Если имеет место несколько ССБ, то при установлении информационного взаимодействия возможна ситуация, при которой находящийся в одном сегменте претендент может быть аутентифицирован проверяющей стороной, расположенной в другом сегменте. Следовательно, к процедуре аутентификации может быть привлечено несколько ССБ, среди которых:

- ССБ, в котором расположен инициатор процедуры аутентификации;
- ССБ, в котором расположена проверяющая сторона;
- ССБ, в которых расположены ДТС.

Тем не менее необходимости в наличии всех этих сегментов нет.

Прежде чем проводить процедуру аутентификации между разными ССБ, необходимо сформировать соответствующую ПБВ.

3.1.3. Принципы, используемые при аутентификации

Соответствующий метод аутентификации будет опираться на ряд предположений и гипотез, связанных с одной или несколькими взаимодействующими сторонами.

Принципы, используемые при аутентификации, следующие:

- а) что-нибудь известно, например пароль;
- б) чем-нибудь владеют, например магнитной или смарт-картой;
- с) некоторые неизменные характеристики, например биометрические идентификаторы;
- д) признание такого третьего объекта (ДТС), который бы подтвердил результаты процедуры аутентификации;
- е) контекст, например адрес взаимодействующей стороны.

Целесообразно отметить, что во всех этих принципах есть свои слабости. Например, аутентификация того, чем владеют, т.е. гораздо чаще аутентифицируется объект, которым владеют,

а не его владелец. В некоторых случаях слабости могут быть преодолены за счет одновременной реализации нескольких принципов. Например, при использовании смарт-карты (чем-нибудь владеют) слабость может быть преодолена за счет применения PIN-кода (что-нибудь известно) с целью аутентификации пользователя карты. Более того, принцип *е*) является особенно слабым и фактически всегда используется в «связке» с другим принципом.

Следует отметить, что в принципе *д*) существуют два типа рекурсии:

- с целью собственной идентификации ДТС может потребовать проведения процедуры собственной аутентификации;
- для проведения аутентификации ДТС может использоваться четвертая взаимодействующая сторона.

Анализ существующих методов аутентификации, основанных на этих принципах, будет указывать, какие стороны участвуют в ПИНО, какие принципы используются и какие взаимодействующие стороны аутентифицированы.

3.1.4. Фазы (этапы) аутентификации

При проведении процедуры аутентификации возможны следующие фазы:

- фаза инсталляции;
- фаза изменения ВИАУ;
- фаза распределения;
- фаза получения;
- фаза доставки;
- фаза проверки;
- фаза блокировки;
- фаза отмены блокировки;
- фаза деинсталляции.

Границы этих фаз не обязательно являются четкими по времени, т.е. фазы могут перекрываться между собой.

Не все из этих фаз востребованы конкретной схемой аутентификации. Более того, в некоторых случаях установленная последовательность фаз может отличаться от последовательности, которая представлена ниже.

3.1.4.1. Инсталляция

В этой фазе определяются предъявляемая ВИАУ и проверочная ВИАУ.

3.1.4.2. Фаза изменения ВИАУ

В этой фазе взаимодействующая сторона или администратор добиваются изменения предъявляемой ВИАУ и проверочной ВИАУ (например смена пароля).

3.1.4.3. Фаза распределения

В этой фазе проверочная ВИАУ доводится до взаимодействующей стороны (например претендента или проверяющей стороны) с целью последующего использования этой ВИАУ в процессе ее проверки в течение процедуры обмена ВИАУ. Например, в автономных прикладных системах взаимодействующие стороны могут приобретать сертификаты для аутентификации, списки аннулированных сертификатов и УЦ. Фаза распределения может быть проведена до, в течение или после фазы доставки.

3.1.4.4. Фаза получения

В этой фазе претендент или проверяющая сторона могут получить необходимую информацию для реализации определенной процедуры обмена ВИАУ, например процедуры аутентификации. Различные процедуры могут запросить обмен ВИАУ путем взаимодействия с ДТС или путем обмена сообщениями между аутентифицируемыми сторонами.

Например, когда используется центр распределения ключей (ЦРК) в режиме реального времени, то претендент или проверяющая сторона может получить из ЦРК некоторую информацию, такую как СЕРТ|АУ, с целью проведения процедуры аутентификации с другой стороной.

3.1.4.5. Доставка

В этой фазе ВИАУ для обмена доставляется претенденту и проверяющей стороне.

3.1.4.6. Проверка

В этой фазе предоставленная при обмене ВИАУ сравнивается с проверочной ВИАУ. Кроме этого взаимодействующая сторона, не способная сама проверить предоставленную при обмене ВИАУ, может установить взаимодействие с ДТС, которая и проверит эту ВИАУ. В таком случае ДТС ответит либо положительно, либо отрицательно.

3.1.4.7. Блокировка

В этой фазе состояние, сформированное взаимодействующей стороной, которая могла быть предварительно аутентифицирована, временно блокируется для проведения процедуры аутентификации.

3.1.4.8. Фаза отмены блокировки

В этой фазе заблокированное состояние, сформированное взаимодействующей стороной, разблокируется.

3.1.4.9. Фаза деинсталляции

В этой фазе взаимодействующая сторона выделяется из группы взаимодействующих сторон (персонифицируется).

3.1.5. Привлечение ДТС

Способы и средства аутентификации могут характеризоваться числом привлеченных (привлекаемых) ДТС.

3.1.5.1. Аутентификация без привлечения ДТС

В самой простой ситуации ни претендент, ни проверяющая сторона не привлекают какую-либо третью сторону для формирования и проведения обмена ВИАУ и самой процедуры аутентификации (рис. 3.2). В этом случае проверочная ВИАУ для

взаимодействующей стороны должна быть установлена на проверяющей стороне.

До тех пор пока большинство объектов будут ограничены весьма незначительным числом возможных соединений с партнерами, такой подход в крупномасштабных прикладных системах будет использоваться очень редко. В худшем случае каждая проверяющая сторона должна будет иметь проверочную ВИАУ для каждого из всех объектов ССБ, а рост требуемой общей информации будет пропорционален квадрату общего числа взаимодействующих объектов.



Рис. 3.2. Аутентификация без привлечения ДТС

3.1.5.2. Аутентификация с привлечением ДТС

Проверочная ВИАУ может быть получена на основе информационного взаимодействия с ДТС. Целостность такой информации должна быть гарантирована. Последнее также необходимо и при обеспечении конфиденциальности предъявляемой ДТС ВИАУ и проверочной ВИАУ, если предъявляемая ВИАУ может быть получена из проверочной ВИАУ логическим путем.

Процедура аутентификации может затрагивать одну ДТС или группу ДТС (см. *d*) в § 3.1.3). Введение дополнительных ДТС обеспечивает аутентификацию среди большой группы объектов, при этом потребуются соответствующая информация только об ограниченном числе объектов (не обо всех других объектах). Таким образом, общий объем обрабатываемой ин-

формации будет расти линейно с ростом числа привлекаемых к аутентификации объектов.

Многосторонние связи (информационный обмен) могут характеризоваться в зависимости от требований к соединениям (число используемых активных каналов/линий связи) и в соответствии с наличием необходимого уровня административного управления, например задержка, которая вполне естественна при аннулировании ВИАУ.

Поточная (in-line) аутентификация. В этом случае ДТС (промежуточная система, an intermediary) непосредственно «вклинивается» в аутентификационный обмен между претендентом и проверяющей стороной (расположена на маршруте информационного взаимодействия). Взаимодействующая сторона аутентифицируется промежуточной системой, которая затем гарантированно подтверждает ее подлинность в последующем поточном аутентификационном обмене (рис. 3.3).



Рис. 3.3. Поточная аутентификация

Поточная аутентификация требует, чтобы проверяющая сторона доверяла промежуточной системе с целью обеспечения информационного взаимодействия с прошедшей корректную процедуру аутентификации противоположной стороной и чтобы проверяющая сторона гарантировала подлинность промежуточной системы на протяжении всей процедуры аутентификации.

С целью обеспечения регулярности (этапности и непрерывности) проведения процедуры аутентификации до начала

следующего этапа может налагаться временный запрет на ее проведение. Целесообразно, чтобы претендент обладал своей собственной аннулированной ВИАУ и поддерживал ее в актуальном состоянии, это позволит промежуточной системе (ДТС) незамедлительно обновлять текущее состояние претендента и отклонять какие-либо последующие попытки проведения аутентификации.

Иногда ситуация может измениться так, что гарантия будет получена от последовательной группы (цепочки) ДТС. В зависимости от реально действующей ПЛБ ответственность за определение того, является или нет группа ДТС правомерной и надежной, несет либо проверяющая сторона, либо последняя в цепочке ДТС.

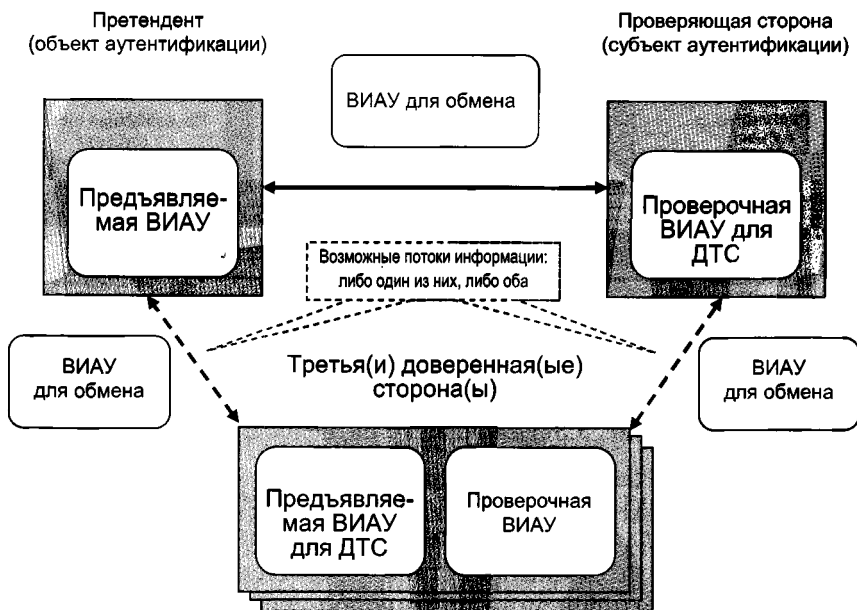


Рис. 3.4. Интерактивная аутентификация¹

¹ Процедуры обмена ВИАУ между тремя объектами, представленными на этом рисунке, различаются между собой.

Интерактивная (on-line) аутентификация. В этом случае при каждом требовании любой из сторон аутентификационного обмена привлекается функционирующая одна или несколько ДТС. Однако, в отличие от поточной аутентификации, интерактивные ДТС не располагаются непосредственно на маршруте аутентификационного обмена между претендентом и проверяющей стороной (рис. 3.4). Интерактивные ДТС могут быть востребованы претендентом с целью формирования ВИАУ для обмена и могут содействовать проверяющей стороне в процедуре проверки ВИАУ для обмена. Интерактивная ДТС может выпускать интерактивные сертификаты для аутентификации.

Интерактивная аутентификация требует, чтобы имелась некоторая последовательность ДТС, привлекаемых к формированию ВИАУ, используемой при обмене между проверяющей стороной и ДТС, которая может подтвердить подлинность предъявляемой объектом ВИАУ. В простейшем случае для прямого взаимодействия между претендентом или проверяющей стороной необходима лишь одна ДТС. Тем не менее такой случай может быть расширен до взаимодействия с последовательной группой ДТС, с которыми претендент или проверяющая сторона устанавливают прямые или опосредованные соединения.

С целью обеспечения регулярности (этапности и непрерывности) проведения процедуры аутентификации до начала следующего этапа может налагаться временный запрет на ее проведение.

Примерами интерактивных ДТС могут быть серверы интерактивной аутентификации или ЦРК.

Независимая (off-line) аутентификация. Независимая (или автономная) аутентификация отличается тем, что для ее проведения необходимо использовать сертифицированные перечни аннулированных сертификатов, списки сертификатов, восстановленных из аннулированных сертификатов, интервалы изъятия сертификатов или другие опосредованные методы аннулирования проверочной ВИАУ (рис. 3.5).

При таком виде аутентификации одна или несколько ДТС обеспечивают процедуру аутентификации без своего непосредственного участия в ней после каждого запроса на ее проведение.

Автономная ДТС формирует и заблаговременно распространяет сертификаты для независимой аутентификации, которые проверяющая сторона может впоследствии использовать для подтверждения подлинности аутентификационного обмена. Следовательно, аутентификационный обмен осуществляется автономно (независимо), без вмешательства ДТС.

Так как ДТС не нужно принимать прямого участия в информационном обмене с претендентом или проверяющей стороной в период проведения процедуры аутентификации, такой вид аутентификации может быть более эффективным с точки зрения числа требуемых процедур информационного обмена.

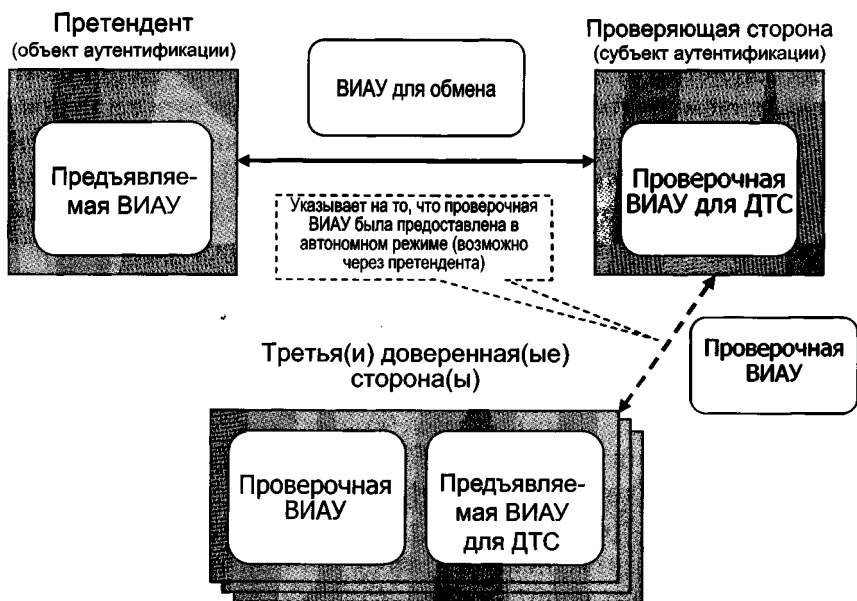


Рис. 3.5. Автономная (независимая) аутентификация

Процесс аннулирования должен зависеть от ряда дополнительных условий, таких как окончание «времени жизни» сертификатов и возобновление их действия, а также от сертифицированных списков аннулированных сертификатов.

Примерами автономных ДТС являются УЦ, которые издают сертификаты для независимой аутентификации.

3.1.5.3. Доверие претендента к проверяющей стороне

Методы и способы, которые необходимо применять для обеспечения доверия к проверяющей стороне, являются неадекватными, но до тех пор, пока все возможные проверяющие стороны не станут надежными. И объясняется это тем, что если подлинность проверяющей стороны не была подтверждена, то ее надежность (благонадежность) неизвестна. Например, простое использование паролей для аутентификации, в этом случае необходимо удостовериться в том, что проверяющая сторона не хранит и не использует повторно предоставленный претендентом пароль.

3.1.6. Типы участников информационного взаимодействия

Участники информационного взаимодействия могут быть разделены на категории различными способами, которые связаны например:

- a)* с пассивным(и) параметром(ами), например отпечатки пальцев, рисунок сетчатки глаза;
- b)* со способностью обмениваться информацией и ее обработки;
- c)* со способностью хранения информации;
- d)* с уникальным постоянным местонахождением.

Участники информационного взаимодействия могут относиться к нескольким категориям одновременно (например физические лица (граждане, пользователи) относятся к категориям *a*, *b* и *c*). В каждом случае применяется свой отличительный метод аутентификации:

- a)* измерение пассивного(ых) параметра(ов);
- b)* комплексная проверка запроса и ответа на него;
- c)* запоминание секретного слова (например пароля);
- d)* определение местоположения.

3.1.7. Аутентификация физического лица (гражданина, пользователя), или персонификация

При запросе процедуры аутентификации, последняя, скорее всего, нужна для аутентификации конечного пользователя (т.е. персонификация), а не для аутентификации процесса, действующего от имени этого конечного пользователя.

Методы персонификации должны быть приемлемыми для конечных пользователей и с точки зрения экономичности, и с точки зрения безопасности. Неприемлемые методы персонификации повышают вероятность противоправных действий со стороны нарушителей.

Методы персонификации основаны на принципах, представленных в § 3.1.3. Процедуры же персонификации включают фазы, рассмотренные в § 3.1.4. Процедуры и методы персонификации рассматриваются § 3.6.

3.1.8. Типы атак на процедуру аутентификации

В настоящее время рассматриваются три разновидности атак:

- *атаки типа «повторная передача»*, при которых ВИАУ для обмена читается и впоследствии повторяется;
- *атаки типа «подмена»*, которые инициируются нарушителем;
- *атаки типа «подмена»*, при которых нарушитель выступает в роли отвечающей стороны.

Атака типа «подмена» является атакой, в течение которой ВИАУ для обмена перехватывается и затем незамедлительно ретранслируется.

3.1.8.1. Атаки типа «повторная передача»

Основными являются два варианта проведения атаки типа «повторная передача», т.е. возможна повторная передача некоторой части ВИАУ для обмена:

- одной и той же проверяющей стороне;
- другой проверяющей стороне.

Последний случай происходит тогда, когда одна и та же проверочная информация одной из взаимодействующих сторон известна нескольким проверяющим сторонам. Успех проведения атаки типа «повторная передача» во многом зависит от атаки типа «маскарад».

Оба варианта проведения атаки типа «повторная передача» могут быть парированы за счет использования встречных запросов. Встречные запросы формируются проверяющей стороной. Один и тот же встречный запрос никогда не должен направляться одной и той же проверяющей стороной дважды. Это может быть обеспечено несколькими способами.

Повторная передача одной и той же проверяющей стороне. Повторная передача одной и той же проверяющей стороне может быть парирована за счет использования уникальных номеров или встречных запросов.

Уникальные номера формируются претендентом. Один и тот же уникальный номер никогда не должен признаваться дважды одной и той же проверяющей стороной. Это может быть обеспечено несколькими способами.

Повторная передача другой проверяющей стороне. Повторная передача другой проверяющей стороне может быть парирована за счет использования встречных запросов. С другой стороны, она может быть парирована за счет использования, в период формирования ВИАУ для обмена, любых иных признаков, которые уникальны для проверяющей стороны. Таким признаком может быть имя проверяющей стороны, ее сетевой адрес или любой иной атрибут, который уникален для проверяющих сторон, совместно использующих одну и ту же проверочную ВИАУ.

3.1.8.2. Атаки типа «подмена»

Атаки типа «подмена», инициируемые нарушителем. Этот вариант атаки связан с противоправной деятельностью нарушителя, который является инициатором процедуры аутентификации. Такая атака возможна только тогда, когда и претендент,

и проверяющая сторона могут инициировать процедуру аутентификации. При проведении этой атаки претендент и проверяющая сторона, причем, не осознавая этого, обмениваются ВИАУ через нарушителя, т.е. нарушитель «прикидывается» то некой проверяющей стороной по отношению к претенденту, то этим претендентом по отношению к реальной проверяющей стороне.

Предположим, что нарушитель C хочет выступить перед проверяющей стороной B в роли претендента A . C начинает информационное взаимодействие со сторонами A и B . C сообщает A , что он является B , запрашивает A для проведения аутентификации на стороне B , кроме того C сообщает B , что он является A и что он хочет пройти процедуру собственной аутентификации (рис. 3.6).

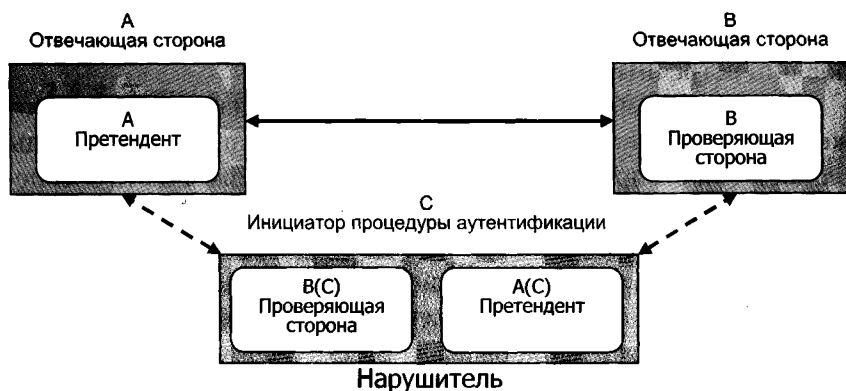


Рис. 3.6. Атака типа «подмена», инициируемая нарушителем

В течение процедуры аутентификации A действует как претендент по отношению к B (а в действительности по отношению к C , который действует как B) и, более того, он передает информацию, которую может использовать C для проведения аутентификации на стороне B . B действует как проверяющая стороны и также передает информацию, которую может использовать C для исполнения роли проверяющей стороны. По окончании

процедуры аутентификации нарушитель *C* будет представляться стороне *B* как претендент *A*, прошедший процедуру аутентификации.

Этот вариант атаки может быть парирован, если:

- a)* взаимодействующая сторона, которая инициирует информационный обмен, либо всегда является претендентом, либо всегда является проверяющей стороной (такой случай невозможен при реализации обоюдной аутентификации);
- b)* формируемая претендентом ВИАУ для обмена варьируется в соответствии с его ролью в качестве инициатора запроса процедуры аутентификации или в качестве отвечающей стороны на приглашение пройти процедуру аутентификации. Такое отличие позволяет проверяющей стороне обнаружить описанный выше перехват.

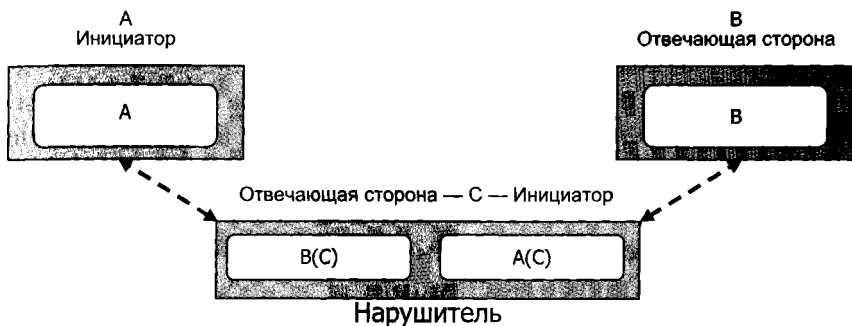


Рис. 3.7. Атака типа «подмена», в которой нарушитель выступает в роли отвечающей стороны

Атаки типа «подмена», в которых нарушитель выступает в роли отвечающей стороны. В этом варианте атаки нарушитель располагается в середине соединения (рис. 3.7), по которому осуществляется аутентификационный обмен, перехватывает ВИАУ и ретранслирует ее, беря на себя роль инициатора. Этот вариант атаки можно осуществить либо в нужное время

и в нужном месте (в этом случае нарушительвыжидает, когда отвечающая сторона сделает ошибку), либо систематически (в этом случае нарушитель объявляет, что он является отвечающей стороной, например в таблице размещения основных ресурсов).

Основной способ парирования такого варианта атак основан на использовании дополнительной службы (обеспечения целостности или конфиденциальности) в течение последующих процедур обмена данными. ВИАУ для обмена должна комбинироваться с некоторой иной информацией, предоставляющей возможность претенденту и проверяющей стороне, которые пытаются подтвердить, что они являются легитимными участниками информационного взаимодействия, сформировать ключ. Затем сформированный ключ может использоваться при реализации криптографического способа обеспечения целостности или конфиденциальности.

Другой способ нейтрализации такого варианта атак является очень важным в тех сетях передачи данных, которые не являются объектом с точки зрения внутреннего перехвата, т.е. сеть всегда доставляет данные неизменными и по корректному адресу. В такой ситуации атака может быть предотвращена путем встраивания сетевых адресов в ВИАУ для обмена (например подписание сетевого адреса).

3.2. Вспомогательная информация и средства аутентификации

3.2.1. Вспомогательная информация для аутентификации

3.2.1.1. Предъявляемая ВИАУ

Предъявляемая ВИАУ является вспомогательной информацией, которая используется при формировании ВИАУ для обмена, необходимой при аутентификации одного из участников информационного взаимодействия.

Примерами предъявляемой ВИАУ являются:

- a)* пароль;
- b)* секретный ключ (предназначен для использования в реализуемых способах аутентификации, которые основаны на симметричных алгоритмах);
- c)* закрытый ключ (предназначен для использования в реализуемых способах аутентификации, которые основаны на асимметричных алгоритмах).

3.2.1.2. Проверочная ВИАУ

Проверочная ВИАУ является информацией, которая используется проверки подлинности предъявленной путем обмена ВИАУ.

Примерами проверочной ВИАУ являются:

- a)* пароль (определяющий подлинность взаимодействующей стороны);
- b)* секретный ключ (определяющий подлинность взаимодействующей стороны или ДТС (УЦ); предназначен для использования в реализуемых способах аутентификации, которые основаны на симметричных алгоритмах);
- в)* открытый ключ (определяющий подлинность взаимодействующей стороны или ДТС (УЦ); предназначен для использования в реализуемых способах аутентификации, которые основаны на асимметричных алгоритмах).

Проверочная ВИАУ может быть представлена в форме аутентификационной таблицы и/или сертификата для независимой (offline) аутентификации.

Таблица аутентификации представляет собой совокупность записей, которые непосредственно доступны проверяющей стороне. Маршрут, который используется для доступа к таблице, является защищенным с точки зрения его целостности, и дополнительно при реализации симметричных способов он может быть защищен с точки зрения обеспечения конфиденциальности передаваемых по нему данных.

Примерами элементов, содержащихся в записях таблицы аутентификации, могут быть:

- уникальная особенность участника информационного взаимодействия;
- проверочная ВИАУ (пароль, секретный ключ или открытый ключ);
- время действия записи;
- приемлемая для записи ПЛБ;
- ответственность ДТС (УЦ) за запись.

3.2.1.3. ВИАУ для обмена

ВИАУ для обмена представляет собой информацию, которой обмениваются между собой претендент и проверяющая сторона в течение процедуры аутентификации одного из участников информационного взаимодействия. Примерами ВИАУ для обмена являются:

- предъявляемый UID;
- пароль;
- запрос;
- ответ на запрос;
- уникальный номер;
- UID проверяющей стороны;
- результат выполнения преобразующей функции, которая применяется для формирования или используется при обработке предъявляемой ВИАУ и других данных (например метка времени, случайное число, значение счетчика, уникальная особенность проверяющей стороны, цифровые отпечатки пальцев, уникальная особенность претендента); примерами преобразующих функций являются односторонние функции, функция асимметричного шифрования и функция симметричного шифрования;
- интерактивный сертификат;
- независимый сертификат.

Часть или вся ВИАУ для обмена, транспортируемая в рамках одной итерации информационного обмена, может быть представлена в форме маркера безопасности.

3.2.1.4. Сертификаты для аутентификации

Наиболее общей формой представления ВИАУ является СЕРТ|АУ. Сертификат для аутентификации представляет собой специфический тип сертификата безопасности, который заверен доверенным УЦ и может использоваться в процедурах аутентификации.

Существуют различные типы СЕРТ|АУ:

- интерактивные СЕРТ|АУ;
- независимые СЕРТ|АУ;
- СЕРТ|ОТ отзыва сертификатов;
- СЕРТ|СО перечней (списков) отозванных (аннулированных) сертификатов.

Независимые сертификаты в основном применяются для опубликования открытых ключей, которые связаны с проверочной ВИАУ. Подлинность независимых сертификатов может быть аннулирована с помощью либо СЕРТ|ОТ, либо СЕРТ|СО.

Примерами элементов, содержащихся в любом СЕРТ|АУ, могут быть:

- идентификатор метода и/или ключ, который используется при формировании криптографической проверочной суммы;
- уникальные особенности центра аутентификации (УЦ) или его уполномоченного, который издает СЕРТ|АУ (когда УЦ представлен несколькими уполномоченными, тогда уникальные особенности уполномоченного позволяют точно знать, какой ключ уполномоченного использовался);
- время издания СЕРТ|АУ (время издания может быть использовано в аудиторских целях или использовано, когда период действия сертификата не представлен; после определенного периода времени, который зависит от ПЛБ, очень старые СЕРТ|АУ могут быть удалены);
- время (временной интервал) действия (не раньше, не позже) СЕРТ|АУ (этот временной интервал может иметь значение, если ПЛБ получателя предусматривает его

применение, в противном случае время истечения срока действия СЕРТ|АУ будет определяться с момента выпуска сертификата в соответствии с ПЛБ получателя);

- ПЛБ, которая приемлема для СЕРТ|АУ;
- контрольный номер сертификата, который является уникальным для этого СЕРТ|АУ, а это касается всех СЕРТ|АУ, выпущенных одним и тем же уполномоченным УЦ;
- тип сертификата;
- характерная особенность или атрибуты проверяющей стороны, для которой предназначен СЕРТ|АУ (взаимодействующие стороны могут проверить значение этого параметра, если он представлен, а сертификаты, содержащие некорректное значение параметра, могут быть уничтожены).

Описания конкретных элементов могут содержаться в прикладных стандартах, в которых будут определены элементы, являющиеся обязательными, и элементы, являющиеся дополнительными (необязательными).

Интерактивные СЕРТ|АУ. Интерактивные сертификаты формируются ДТС на основании прямого запроса претендента. Такие СЕРТ|АУ обычно передаются проверяющей стороне как часть ВИАУ для обмена.

Примерами дополнительных элементов, которые могут входить в состав интерактивных СЕРТ|АУ, являются:

- УИД взаимодействующей стороны;
- цифровой отпечаток данных, когда применяется аутентификация источника данных;
- симметричный ключ, выданный взаимодействующей стороне для аутентификации, совместно с идентификатором алгоритма, используемого с данным ключом. Ключ необходим для обеспечения конфиденциальности этой информации;
- метод аутентификации, используемый для получения СЕРТ|АУ;
- метод(ы) аутентификации с которым(и) может использоваться СЕРТ|АУ;

- идентификатор метода, который должен использоваться для защиты СЕРТ|АУ при его доставке, и любые соответствующие параметры, необходимые для обеспечения такой защиты (примерами таких параметров защиты являются запрос, уникальный номер или ключ для защиты).

Независимые СЕРТ|АУ. Независимый сертификат «привязывает» персону (личность) к криптографическому ключу (связывают владельца СЕРТ|АУ с ключом, содержащимся в СЕРТ|АУ). Сертификат издается УЦ в отсутствие либо претендента, либо проверяющей стороны, которым необходимо напрямую взаимодействовать с УЦ. Независимые сертификаты, как правило, применяются в процедурах аутентификации, основанных на асимметричных алгоритмах. Такой сертификат может доставляться проверяющей стороне как часть ВИАУ для обмена.

Примерами дополнительных элементов, которые могут входить в состав независимых СЕРТ|АУ, являются:

- УИД взаимодействующей стороны;
- открытый ключ, выданный взаимодействующей стороне центром аутентификации (УЦ), совместно с идентификатором алгоритма, используемого с данным открытым ключом.

Независимый СЕРТ|АУ может отзываться до окончания срока его действия путем использования либо сертификата отзыва, либо списков отозванных сертификатов.

Сертификаты отзыва СЕРТ|ОТ. Сертификат отзыва представляет собой сертификат безопасности, выпускаемый ЦБ для указания того, что соответствующий независимый СЕРТ|АУ был отозван (аннулирован). Такая информация сохраняется и может запрашиваться всякий раз, когда предоставляется СЕРТ|АУ для определения того, что он по-прежнему является действительным.

Примерами дополнительных элементов, которые могут входить в состав сертификатов отзыва, являются:

- специфические свойства взаимодействующей стороны, группы взаимодействующих сторон или центра аутентификации (УЦ);

- время и дата, когда СЕРТ|АУ был аннулирован;
- уникальный номер сертификата отзыва.

Списки отозванных (аннулированных) сертификатов (СОС). СОС представляет собой заверенный список (перечень) СЕРТ|АУ, отозванных конкретным УЦ, который содержит время и дату своего издания.

Такая информация сохраняется и может запрашиваться всякий раз, когда предоставляется СЕРТ|АУ для определения того, что он по-прежнему является действительным.

СОС может включать:

- сертификаты отзыва;
- специфические идентификаторы сертификатов отзыва;
- аннулированные СЕРТ|АУ;
- специфические идентификаторы аннулированных СЕРТ|АУ;
- дату издания списка;
- дату издания следующего списка.

Последовательности (цепочки) сертификатов. СЕРТ|АУ всегда защищены с целью проведения процедуры аутентификации источника данных со стороны ДТС. Если проверяющая сторона не хранит проверочную ВИАУ с целью проверки источника сертификата, то тогда может использоваться последовательная цепочка сертификатов. Сертификат, выданный другим УЦ, удостоверяет проверочную ВИАУ, используемую для подтверждения источника первого сертификата.

Цепочка сертификатов может использоваться рекурсивно, т.е. каждый сертификат заверяет проверочную ВИАУ, используемую для подтверждения подлинности источника предшествующего сертификата. Такая цепочка определяет последовательность УЦ от проверяющей стороны до претендента. Проверяющая сторона должна сама принять решение доверять или не доверять каждому сертификату из цепочки сертификатов, основываясь при этом на информацию, которую она имеет (хранит) или может получить от ДТС.

3.2.2. Средства аутентификации

Рассмотрим общую модель процедуры аутентификации на основе ее реализации с помощью типовых средств. Используемые средства аутентификации представлены на рис. 3.8.

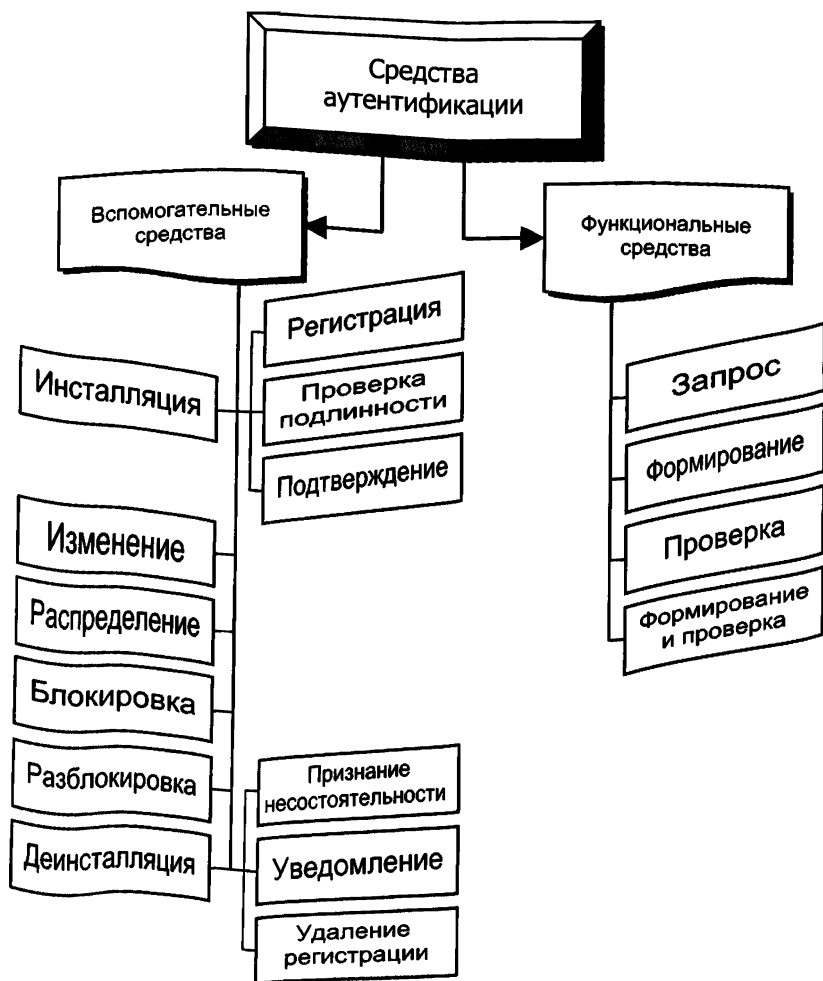


Рис. 3.8. Средства, используемые в процедурах аутентификации

3.2.2.1. Информация о состоянии процедуры аутентификации

Информация о состоянии процедуры аутентификации (ИСА) описывает состояние аутентификации, сохраняющееся между обращениями к службам аутентификации. ИСА может включать:

- сеансовые криптоключи;
- последовательные номера сообщений.

ИСА необходимо хранить в защищенном режиме. Эта информация храниться у провайдеров СЛАУ.

3.2.2.2. Вспомогательные (обеспечивающие) средства

Вспомогательные средства аутентификации могут потребоваться для распределения описательной информации, паролей или ключей (используя СЛКЛ) между объектами, которым требуется проведение процедуры аутентификации. Кроме этого, в данной ситуации может потребоваться использование протокола между взаимодействующими сторонами и другими объектами, выполняющими функции провайдеров СЛАУ. Обеспечение процедуры аутентификации также может потребовать отзыв ВИАУ.

Инсталляция. Средство инсталляции размещает предъявляемую ВИАУ и проверочную ВИАУ. Это средство в последующем может быть детализировано и представлено в терминах: средство регистрации, средство проверки подлинности и средство подтверждения.

Средство регистрации. Средство регистрации побуждает центр безопасности фиксировать некоторую проверочную ВИАУ, связанную с взаимодействующей стороной. Эта информация включает УИД, который присваивается либо взаимодействующей стороной, либо центром безопасности. (Регистрационный ЦБ может потребовать от взаимодействующей стороны подтверждение гарантий с точки зрения проведения проверки подлинности регистрации.) В этот момент времени взаимодействующая сторона является кандидатом на вхождение в ССБ,

но она пока еще официально не признана членом ССБ и обмен ВИАУ невозможен.

Средство проверки подлинности. Средство проверки подлинности, функционирующее от имени УЦ ССБ, включает взаимодействующую сторону в ССБ.

Проверка подлинности проверочной ВИАУ, связанной с взаимодействующей стороной, может потребовать организации соединения между центром безопасности и другим объектом, которое может быть установлено без использования ЭМВОС или Интернет-архитектуры. Функционирование средства проверки подлинности влечет за собой применение УИД, входящего в состав проверочной ВИАУ.

Средство подтверждения. Средство подтверждения используется после применения средства проверки подлинности. Это средство направляет взаимодействующей стороне или другим объектам ответную специфическую информацию. Простейшей формой ответной информации является квитанция, или удаление после инсталляции. Другие формы могут быть следующими:

- независимый СЕРТ|АУ;
- общепринятый УИД;
- предъявляемая ВИАУ.

В последующей процедуре подтверждения взаимодействующая сторона может быть аутентифицирована.

Изменение. Средство изменения ВИАУ применяется от имени взаимодействующей стороны или администратора с целью осуществления изменений в ВИАУ.

Распределение. Средство распределения ВИАУ позволяет любой взаимодействующей стороне получить необходимую проверочную ВИАУ, а после получения — проверить ее.

Блокировка. Средство блокировки, применяемое от имени центра безопасности, переводит процедуру аутентификации в состояние, при котором взаимодействующая сторона временно приостанавливает собственную аутентификацию.

Разблокировка. Средство разблокировки, применяемое от имени центра безопасности, переводит процедуру аутентифика-

ции в состояние, при котором служба блокировки приостанавливает свое функционирование.

Деинсталляция. Средство деинсталляции удаляет запись о взаимодействующей стороне из набора записей о взаимодействующих объектах, подлежащих аутентификации. Это средство в последующем может быть детализировано и представлено в терминах: средство признания несостоятельности, средство уведомления и средство удаления регистрации.

Средство признания несостоятельности (*invalidate*). Это средство выполняет действие, инициализированное центром безопасности, которое включает аннулирование проверочной ВИАУ и/или изменение ИСА, относящейся к взаимодействующей стороне. Средство признания несостоятельности препятствует прохождению процедуры аутентификации взаимодействующей стороной.

Средство уведомления (*notify*). Это средство может быть использовано центром безопасности после использования средства признания несостоятельности. Средство уведомления направляет взаимодействующей стороне ответное извещение о признании ее несостоятельности, которое также может содержать информацию о том, как пройти процедуру повторной регистрации.

Средство удаления регистрации. Это средство исключает взаимодействующую сторону из ССБ. Это означает удаление уникальных свойств взаимодействующей стороны и соответствующей проверочной ВИАУ. Это средство применяется центром безопасности.

3.2.2.3. Функциональные средства

Запрос (*acquire*). Средство запроса обеспечивает претенденту или проверяющей стороне получение информации, необходимой при формировании определенной ВИАУ для обмена, которая, в свою очередь, необходима для запроса процедуры аутентификации. В этом случае может понадобиться взаимодействие с ДТС (например сервером аутентификации).

Входные данные кандидата следующие:

- тип аутентификационного обмена;

- УИД взаимодействующей стороны;
- уникальный параметр проверяющей стороны;
- тип предъявляемой ВИАУ (например пароль, ключ);
- предъявляемая ВИАУ (например значение пароля);
- тип ВИАУ для обмена;
- срок действия (время начала и окончания действия).

Выходные данные для кандидата следующие:

- статус (положительное или отрицательное решение);
- информация, необходимая при формировании ВИАУ для запроса;
- срок действия (время начала и окончания действия).

Формирование (generate). Средство формирования применяется претендентом при генерировании ВИАУ для обмена и/или при обработке полученной ВИАУ для обмена.

Входные данные кандидата следующие:

- тип аутентификационного обмена;
- УИД взаимодействующей стороны;
- информация, необходимая при формировании ВИАУ для запроса, полученная после использования средства запроса;
- ссылка на сохраненную ИСА;
- ВИАУ для обмена, полученная от проверяющей стороны;
- тип ВИАУ для обмена;
- уникальный параметр проверяющей стороны;
- предъявляемая ВИАУ.

Выходные данные для кандидата следующие:

- статус (положительное решение, необходимо дальнейшее информационное взаимодействие или отрицательное решение);
- ссылка на сохраненную ИСА;
- ВИАУ для обмена, которая будет передаваться проверяющей стороне.

Тип аутентификационного обмена может быть определен на основе входных данных при первом инициировании работы средства формирования в процессе аутентификационного обмена, при условии, что претендент является инициатором процедуры аутентификации. При этом же инициировании работы средства формирования в ответном сообщении доставляется ссылка на сохраненную ИСА в качестве выходных данных. В последующих обращениях к средству формирования в рамках одного и того же процесса аутентификационного обмена эти входные и выходные данные не нужны, однако ссылка на сохраненную ИСА может использоваться в качестве входных данных.

ИСА будет сохраняться средством формирования для последующего использования в процедуре аутентификации, но до тех пор, пока не будет получен положительный или отрицательный ответ.

Если получен ответ «необходимо дальнейшее информационное взаимодействие», то претендент будет использовать средство формирования для последующего получения ВИАУ для обмена от другого субъекта. Претенденту, возможно, придется провести несколько таких операций (т.е. использование средства формирования, хранящего информацию о предыдущем состоянии процедуры аутентификации, полученную ВИАУ для обмена), причем до тех пор, пока не будет получен положительный или отрицательный ответ. Таким же образом средство формирования реализует и другие схемы формирования ВИАУ, включая многократные процедуры запрос/ответ, а также востребованные некоторыми схемами процедуры информационного обмена в условиях отсутствия соответствующих сведений.

Проверка (verify). Проверяющая сторона использует средство проверки для верификации полученной от претендента ВИАУ для обмена и/или формирования ВИАУ для обмена, которая будет передаваться претенденту.

Входные данные кандидата следующие:

- тип аутентификационного обмена;
- информация, необходимая при формировании ВИАУ для запроса, полученная после использования средства запроса;

- ссылка на сохраненную ИСА;
- полученная от претендента ВИАУ для обмена;
- проверочная ВИАУ.

Выходные данные для кандидата следующие:

- статус (положительное решение — необходимо дальнейшее информационное взаимодействие или отрицательное решение);
- ссылка на сохраненную ИСА;
- ВИАУ для обмена, которая будет передаваться претенденту (если состояние процедуры аутентификации — «необходимо дальнейшее информационное взаимодействие»);
- УИД взаимодействующей стороны (если получен положительный ответ);
- срок действия (время начала и окончания действия);
- указатель обоюдной аутентификации.

Тип аутентификационного обмена может быть определен на основе входных данных при первом инициировании работы средства проверки в процессе аутентификационного обмена, при условии, что проверяющая сторона является инициатором процедуры аутентификации. При этом же инициировании работы средства проверки в ответном сообщении доставляется ссылка на сохраненную ИСА в качестве выходных данных. В последующих обращениях к средству проверки в рамках одного и того же процесса аутентификационного обмена эти входные и выходные данные не нужны, однако ссылка на сохраненную ИСА может использоваться в качестве входных данных.

ИСА будет сохраняться средством проверки для последующего использования в процедуре аутентификации, но до тех пор, пока не будет получен положительный или отрицательный ответ.

Если был получен положительный ответ, то в нем также сохранились данные, указывающие на подтверждение подлинности взаимодействующей стороны.

Формирование и проверка. В случае обоюдной аутентификации средства формирования и проверки могут быть объединены в одно средство. Входные и выходные данные кандидата представляют собой объединение входных и выходных данных двух средств.

ПРИМЕЧАНИЕ. Средство формирования и средство проверки не доставляют какие бы то ни было данные. Доставка данных зависит от системы в которой используется аутентификация.

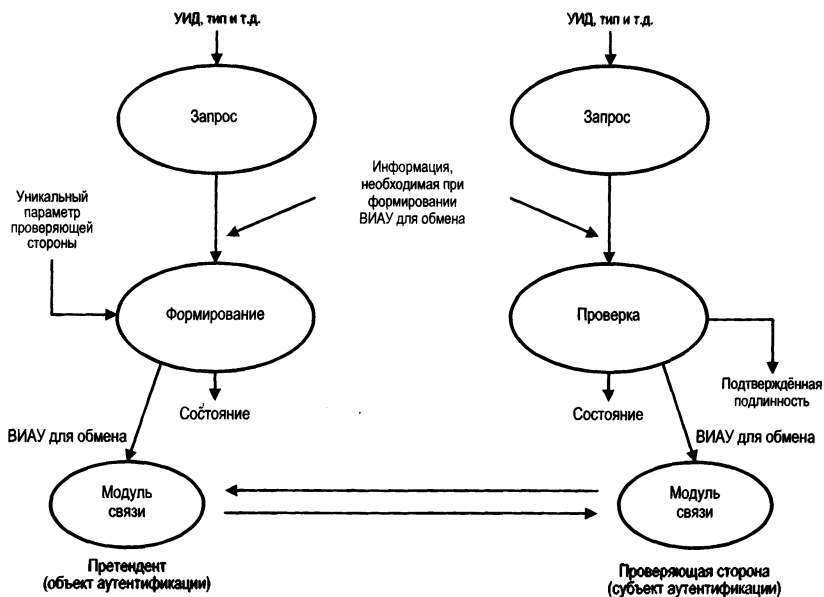


Рис. 3.9. Пример¹ информационных потоков между функционально связанными службами (средствами)

¹ В этом примере представленная служба запросов используется и претендентом, и проверяющей стороной. Но на практике, как правило, эта служба используется только одной из этих взаимодействующих сторон, либо не используется ни одной. Несмотря на то что имеют место информационные потоки между службами (средствами) формирования и проверки, ни одна из этих служб не предназначена для использования модулей связи.

Пример информационных потоков. На рис. 3.9 представлен пример информационных потоков, связанных с функционированием средств запроса, формирования и проверки, которые используются в модели проведения процедуры аутентификации (например прикладных процессов).

3.3. Свойства способов аутентификации

Способы аутентификации (СПАУ) могут основываться на принципах *a)*, *d)* и *e)*, представленных в § 3.1.3. Принцип *d)* предусматривает использование ДТС (§ 3.1.5.2), но такие способы, в конечном счете, будут зависеть от принципов *a)* или *e)*. С другой стороны, в открытых системах процедура аутентификации удаленных объектов очень часто основана на принципе *a)*, т.е. на использовании секретных последовательностей символов (СПС, secrets) в форме ключа или пароля.

3.3.1. Симметричные/асимметричные методы аутентификации

Аутентификация удаленных объектов очень часто основана на использовании СПС, которые имеют форму ключа или пароля. Процедура аутентификации влечет за собой обязательную демонстрацию знания СПС. Методы такой демонстрации (показа) делятся на две обширные категории:

- *симметричные методы*, при которых обе взаимодействующие стороны совместно используют общую ВИАУ;
- *асимметричные методы*, при которых не вся ВИАУ используется обеими взаимодействующими сторонами совместно.

Примеры симметричных методов аутентификации:

- пароль;
- обмен зашифрованными данными на основе симметричной криптографии с использованием общего криптоключа.

Примеры асимметричных методов аутентификации:

- асимметричная криптография с использованием пары криптоключей;
- методы, с помощью которых владение информацией может быть проверено без показа какой-либо части этой информации.

3.3.2. Использование криптографических/некриптографических методов

Способы аутентификации, основанные на знании чего-нибудь (§ 3.1.3), в дальнейшем могут характеризоваться использованием ими криптоалгоритмов для защиты ВИАУ. Симметричные, асимметричные и гибридные криптографические методы могут использоваться для обеспечения целостности, а в некоторых случаях для защиты конфиденциальности ВИАУ.

Некриптографические методы предусматривают использование паролей или запросно-ответные таблицы. Примером криптографических методов является использование шифрования для защиты передаваемых паролей.

3.3.3. Типы аутентификации

Подтверждение подлинности затрагивает две взаимодействующие стороны. При односторонней аутентификации одна сторона выступает в роли претендента, а другая — проверяющей стороны. При обоюдной аутентификации каждая взаимодействующая сторона выступает одновременно в роли претендента и в роли проверяющей стороны. Обоюдная аутентификация может осуществляться с использованием одних и тех же или различных способов аутентификации, причем в обоих направлениях.

3.3.3.1. Односторонняя аутентификация

Односторонняя аутентификация может быть проведена с использованием:

- либо одной процедуры доставки ВИАУ (например когда используются уникальные номера);
- либо трех процедур доставки ВИАУ, когда используется запросно-ответный метод информационного обмена;
- либо более трех процедур доставки ВИАУ. Такой вариант приемлем для некоторых специфических способов аутентификации в условиях отсутствия каких-либо начальных сведений.

В рассмотренных выше случаях предполагалось, что претендент является инициатором процедуры аутентификации. Если инициатором процедуры аутентификации является проверяющая сторона, то число процедур доставки будет другим.

3.3.3.2. Обоюдная аутентификация

При обоюдной аутентификации нет необходимости применять удвоенное число процедур доставки или один и тот же способ аутентификации в обоих направлениях.

В случае использования способов аутентификации с тремя процедурами доставки ВИАУ при односторонней аутентификации обоюдная аутентификация не требует какого-либо последующего информационного обмена. Запрос в течение запросно-ответной процедуры может быть совмещен с передачей другого запроса, используемого проверяющей стороной (затем выступающей в роли претендента) для аутентификации претендента (затем выступающего в роли проверяющей стороны).

3.3.3.3. Квитирование результатов аутентификации

В некоторых случаях весьма полезно использовать квитирование (acknowledgement) результатов процедуры аутентификации, когда объекту аутентификации был дан положительный или отрицательный ответ. Такая квитанция может быть гарантированной или может быть простым ответом «да» или «нет» без предоставления каких-либо гарантий. Отправка квитанции потребует дополнительной процедуры доставки.

3.4. Способы аутентификации

3.4.1. Классификация по критерию уязвимости

Способы (процедуры) аутентификации сами по себе могут быть уязвимы к атакам, реализация которых снижает их эффективность (§ 3.1.8).

Рассмотрим способы аутентификации, которые могут быть использованы для проведения процедуры аутентификации в фазе доставки данных. Эти способы классифицируются в соответствии с угрозой(ами), к реализации которой(ых) они устойчивы. Все описываемые далее способы основаны на принципе аутентификации «знание чего-нибудь» (§ 3.1.3, а)).

Все рассматриваемые далее способы приемлемы для подтверждения подлинности объекта, а некоторые также приемлемы для аутентификации источника данных, например цифровой отпечаток данных при аутентификационном обмене.

Существуют следующие классы способов аутентификации:

- *класс 0*: незащищенный;
- *класс 1*: защищенный от вскрытия;
- *класс 2*: защищенный от вскрытия и повторной передачи со стороны различных проверяющих субъектов;
- *класс 3*: защищенный от вскрытия и повторной передачи со стороны одного и того же проверяющего субъекта;
- *класс 4*: защищенный от вскрытия и повторной передачи со стороны одного и того же проверяющего субъекта или различных проверяющих субъектов.

ПРИМЕЧАНИЕ. В классах с 1 по 4 термин «защита от вскрытия» означает защиту от вскрытия предъявляемой ВИАУ.

При необходимости могут быть определены дополнительные классы. Для некоторых классов способов аутентификации определены подклассы. Подклассы не обязательно являются полными.

Для каждого класса способов определена соответствующая ВИАУ для обмена.

При использовании функции шифрования, как одной из функций, реализуемых средством формирования, предъявляемая ВИАУ (возможно совместно с другой информацией) используется для формирования криптоключа. При использовании функции шифрования как одной из функций, реализуемых средством проверки, проверочная ВИАУ (возможно совместно с другой информацией, полученной в период аутентификационного обмена) используется для формирования криптоключа.

Рассматриваемые далее варианты аутентификационного обмена определены с точки зрения претендента и всегда иницируются им. Варианты аутентификационного обмена, инициируемого проверяющей стороной, представлены в § 3.4.2. Такие процедуры аутентификационного обмена приемлемы для односторонней аутентификации. В § 3.4.4 представлены процедуры аутентификационного обмена, приемлемые для обоюдной аутентификации. В отдельных случаях необходимо квитирование положительного или отрицательного результата процедуры аутентификации. Для этого может понадобиться дополнительная процедура доставки. Используемые средства аутентификации представлены в § 3.2.2.

В представленных ниже диаграммах пара квадратных скобок «[]» указывает на применение дополнительного компонента в рамках доставляемых данных, включаемого в эти данные только при определенных условиях.

Дополнительный компонент [цифровой отпечаток] используется в случае аутентификации источника данных, а в других случаях отсутствует. Цифровой отпечаток может быть получен, например, с использованием алгоритма асимметричного шифрования данных, либо просто с помощью зашифрования данных, либо путем вычисления криптографической проверочной суммы по последовательности данных с использованием закрытого ключа подписанта. При аутентификации источника данных доставка данных, в которых содержится их цифровой отпечаток, может осуществляться либо полностью независимо от способа и средств установления соединения, либо в условиях совместного использования средств установления соединения, используемого для последующего проведения процедур.

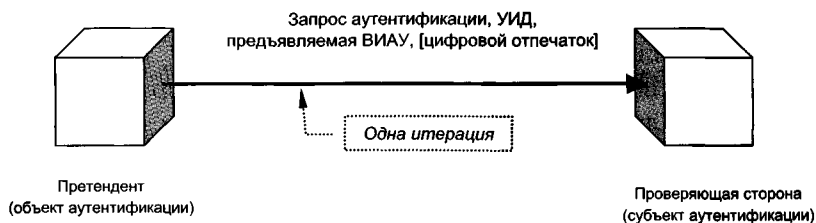


Рис. 3.10. Способ класса «0» (незащищенный)

3.4.1.1. Класс «0» (незащищенный)

В этом классе способов аутентификации предъявляемая ВИАУ вместе с УИД просто передаются претендентом проверяющей стороне в форме ВИАУ для обмена. Простым примером является передача пароля. Класс «0» является случаем симметричной аутентификации. Данный класс способов уязвим к раскрытию ВИАУ и атакам типа «повторная передача».

Средство формирования генерирует ВИАУ для обмена (рис. 3.10) непосредственно из собственных входных данных.

Средство проверки сравнивает полученную предъявляемую ВИАУ (например пароль) с проверочной ВИАУ, связанной с полученным УИД.

Способы аутентификации этого класса приемлемы для процедур аутентификации источника данных и взаимодействующей стороны (объекта).

3.4.1.2. Класс «1» (защищен от вскрытия)

Этот класс способов аутентификации обеспечивает защиту от раскрытия (вскрытия) предъявляемой ВИАУ. Способы класса «1» приемлемы для процедур аутентификации источника данных и взаимодействующей стороны (объекта).

Эти способы применяют функцию преобразования, с помощью которой предъявляемая ВИАУ (возможно вместе с УИД) трансформируется. Затем преобразованная предъявляемая ВИАУ вместе с УИД доставляется проверяющей стороне. Реальная предъявляемая ВИАУ по каналу связи не передается. Примеры:

- передача пароля, преобразованного с помощью односторонней функции — ОНФ (например криптографическая проверочная сумма или хэш-функция);
- передача цифрового отпечатка, зашифрованного с помощью секретного ключа;
- передача пароля, зашифрованного с помощью конфиденциального ключа;
- передача цифрового отпечатка, подписанного с помощью закрытого ключа.

Способы этого класса уязвимы к атакам типа «повторная передача», но обеспечивают защиту от вскрытия предъявляемой ВИАУ. Например, преобразованный пароль может быть повторно передан на уровень протокола информационного обмена, но открытый пароль, который используется на уровне системного интерфейса, вскрыт не будет.

Средство формирования использует предъявляемую ВИАУ и, если необходимо, УИД и/или цифровой отпечаток как входные данные процедуры криптографического преобразования с целью формирования ВИАУ для обмена (рис. 3.11).

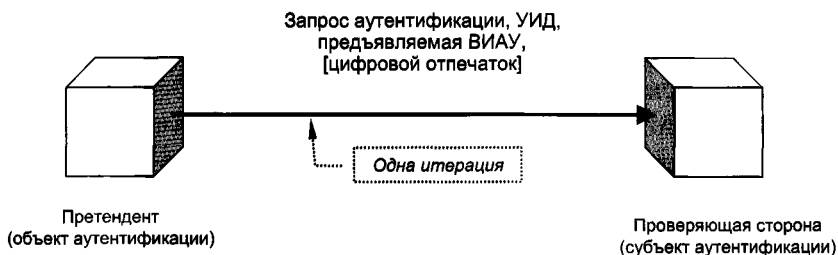


Рис. 3.11. Класс «1» (защищенный от вскрытия)

Примеры использования функции преобразования (F):

- а) в случае использования ОНФ средство проверки также с помощью ОНФ выполняет обработку проверочной

ВИАУ вместо предъявляемой информации, а затем сравнивает полученный результат обработки с полученной ВИАУ для обмена;

- b)* в случае использования симметричной криптографии средство проверки использует проверочную информацию для расшифрования полученной ВИАУ для обмена, а затем проверяет корректность расшифрованной последовательности данных путем проверки содержащихся в ней уникальных параметров, таких как УИД претендента, корректный цифровой отпечаток, пароль или значение константы;
- c)* в случае использования ЭЦП средство проверки повторно вычисляет цифровой отпечаток по полученным данным и использует проверочную ВИАУ для проверки того, что полученная ЭЦП совпадает с сформированной на основании повторно вычисленного отпечатка ЭЦП.

Кроме этого, для аутентификации источника данных цифровой отпечаток в ВИАУ для обмена сравнивается с регенерированным цифровым отпечатком данных, подлежащих аутентификации.

ПРИМЕЧАНИЕ. Там, где УИД взаимодействующей стороны включен в предъявляемую ВИАУ, проведение эффективной атаки становится еще более трудным. В этом случае возможно проведение одновременной атаки только по отношению к одному объекту, не по отношению ко всем взаимодействующим сторонам.

С целью обеспечения конфиденциальности функция преобразования не должна иметь обратной функции (т.е. быть ОНФ), а если все-таки имеется обратная функция, то она должна быть чрезвычайно сложной с точки зрения ее вычисления, для тех взаимодействующих сторон, для которых предъявляемая ВИАУ (и цифровой отпечаток) должна быть недоступна (обеспечиваться ее конфиденциальность).

3.4.1.3. Класс «2» (защищен от вскрытия и атак типа «повторная передача» со стороны различных проверяющих субъектов)

Этот класс способов обеспечивает защиту от вскрытия и повторной передачи со стороны различных проверяющих субъектов, но не от повторной передачи со стороны одного и того же проверяющего субъекта. Он идентичен классу «1» за исключением того, что элемент данных, содержащий уникальный параметр для конкретной проверяющей стороны, рассматривается как входные данные при реализации функции преобразования. Это свойство повышает защищенность процедуры аутентификации.

3.4.1.4. Класс «3» (защищен от вскрытия и атак типа «повторная передача» со стороны одного и того же проверяющего субъекта)

Этот класс способов обеспечивает защиту от вскрытия и повторной передачи со стороны одного и того же проверяющего субъекта.

В этом классе способы аутентификации, основанные на использовании уникальных чисел, образуют подкласс способов аутентификации, которые применяют функцию преобразования в сочетании с уникальной информацией с целью обеспечения защиты от «повторной передачи» одной проверяющей стороны. Предъявляемая ВИАУ и уникальное число преобразуются и доставляются вместе с УИД.

Методы получения уникального числа могут быть следующими:

- a) случайное или псевдослучайное число.* Такое число умышленно не повторяется в течение всего периода «жизни» предъявляемой ВИАУ. Случайное или псевдослучайное число, выбранное из достаточно широкого диапазона чисел, может снижать риск (вероятность) того, что такое же число уже использовалось ранее;
- b) метки времени.* Метка времени, принимаемая от доверенного источника, является уникальным числом. При этом

она является уникальным параметром в течение всего периода «жизни» предъявляемой ВИАУ. Устаревшие метки времени или метки времени, которые использовались ранее, должны уничтожаться;

- с) *счетчик*. Значение счетчика является уникальным числом, при этом значение счетчика увеличивается на единицу в течение всего периода использования предъявляемой ВИАУ;
- д) *криптографическая связка*¹. Величина, вычисленная по содержанию предыдущих данных, которыми обменивались претендент и проверяющая сторона, с использованием сцепления (связки) блоков, является уникальным числом.

Однозначность уникального числа, не формируемого претендентом, может быть гарантирована путем объединения этого числа с данными, которые уникальны для претендента (например его собственный УИД).

Для генерирования уникального числа возможно использование различных комбинаций методов его генерирования.

К функциям преобразования (F) относятся следующие:

- а) *ОНФ*. Уникальное число, предъявляемая ВИАУ и, дополнительно, УИД преобразуются с помощью ОНФ. Уникальное число также передается проверяющей стороне, которая может провести аналогичное преобразование;
- б) *асимметричный алгоритм*. Если предъявляемая ВИАУ представляет собой закрытый ключ, то уникальное число подписывается с помощью закрытого ключа;
- с) *симметричный алгоритм*. Если предъявляемая ВИАУ представляет собой секретный ключ, то уникальное число зашифровывается с помощью секретного ключа.

¹ В данном случае использование термина *криптографическая связка* соответствует определению *связка блоков* в стандарте ISO/IEC 10116.

Этот подкласс способов применим для процедур аутентификации источника данных и взаимодействующей стороны (объекта).

Средство формирования генерирует уникальное число. Затем оно осуществляет процедуру зашифрования, используя следующие параметры в качестве входных данных:

- уникальное число;
- предъявляемая ВИАУ;
- УИД (дополнительно);
- цифровой отпечаток (при аутентификации источника данных).

После зашифрования оно формирует ВИАУ для обмена (рис. 3.12).

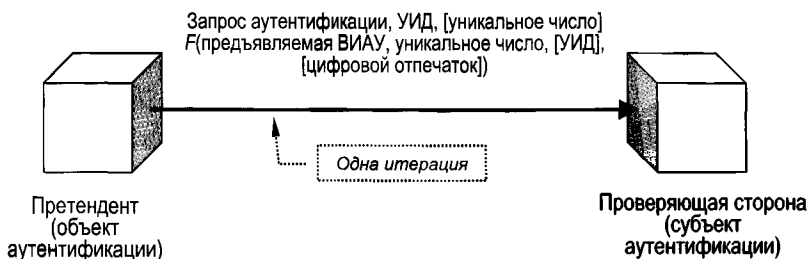


Рис. 3.12. Подкласс класса «3» (способ, основанный на применении уникальных чисел)

Средство проверки расшифровывает и проверяет ВИАУ для обмена на предмет ее подлинности, используя для этого проверочную ВИАУ, как это определено для класса «1». Также оно проверяет полученное уникальное число на предмет его возможного более раннего приема. Если такое число было принято ранее, то имеет место повторная передача. Кроме этого, при аутентификации источника данных цифровой отпечаток, переданный в составе ВИАУ для обмена, сравнивается с вновь сгенерированным отпечатком по последовательности принятых данных.

3.4.1.5. Класс «4» (защищен от вскрытия и атак типа «повторная передача» со стороны одного и того же или различных проверяющих субъектов)

Подкласс «4a» — способы, основанные на использовании уникальных чисел. Этот подкласс способов идентичен классу «3» за исключением того, что элемент данных, содержащий уникальный для конкретной проверяющей стороны параметр, включается в данные для обмена в качестве входных данных при реализации функции преобразования. Это повышает уровень защищенности.

Подкласс «4b» — способы, основанные на использовании встречного запроса. Цель этого способа — вести счет атак типа «повторная передача», т.е. гарантировать, что любая попытка аутентификации на основе повторного использования ВИАУ для обмена будет безуспешной. В ответе на запрос процедуры аутентификации проверяющая сторона направляет встречное требование (запрос) претенденту в форме элемента данных с уникальным параметром. Претендент преобразует данные из встречного требования и предъявляемую ВИАУ с использованием некоторой функции, а затем возвращает результат этого преобразования проверяющей стороне.

Вследствие этого способы, основанные на использовании процедуры встречного запроса, включают в себя следующие три итерации доставки информации:

- передача запроса на проведение процедуры аутентификации;
- отправка встречного запроса (требования);
- передача ответа, который содержит параметр, полученный на основе предъявляемой ВИАУ, возможно в сочетании с УИД, и востребованную информацию (элемент данных с уникальным параметром), преобразованные с использованием некоторой определенной функции (F).

В общем случае УИД может быть передан либо в составе запроса на проведение процедуры аутентификации, либо в составе финального ответа.

К функциям преобразования (F), используемым в способах аутентификации на основе встречного запроса, относятся следующие:

- а) ОНФ.* Востребованный элемент данных с уникальным параметром и предъявляемая ВИАУ преобразуются с помощью ОНФ;
- б) асимметричный алгоритм.* Если предъявляемая ВИАУ представляет собой закрытый ключ, то востребованный элемент данных с уникальным параметром подписывается с помощью закрытого ключа;
- с) симметричный алгоритм.* Если предъявляемая ВИАУ представляет собой секретный ключ, то востребованный элемент данных с уникальным параметром зашифровывается с помощью секретного ключа.

В качестве особого случая рассматривается аутентификация на основе встречного запроса, при которой сформированный элемент данных с уникальным параметром может зависеть от уникального свойства объекта, которое было принято в составе запроса на проведение процедуры аутентификации. Такой способ известен как специализированный способ аутентификации на основе встречного запроса. В таком случае УИД должен передаваться в составе запроса на проведение процедуры аутентификации. Поэтому возможна следующая четвертая функция преобразования:

- д) некриптографическая функция.* Одним из примеров такой функции является использование таблицы пар запрос/ответ, т.е. запрашивающий субъект требует соответствующего ответа. Другим примером является биометрическая схема, такая как система повторения речевого сообщения.

Этот подкласс способов применим для процедур аутентификации источника данных и взаимодействующей стороны (объекта).

Средство формирования вырабатывает запрос на аутентификацию (который в случае специализированного способа аутентификации на основе встречного запроса должен содержать УИД). После получения этого запроса средство проверки формирует уникальный встречный запрос в форме ВИАУ для обмена.

Затем средство формирования генерирует ВИАУ для обмена на основе преобразования входных данных (рис. 3.13).

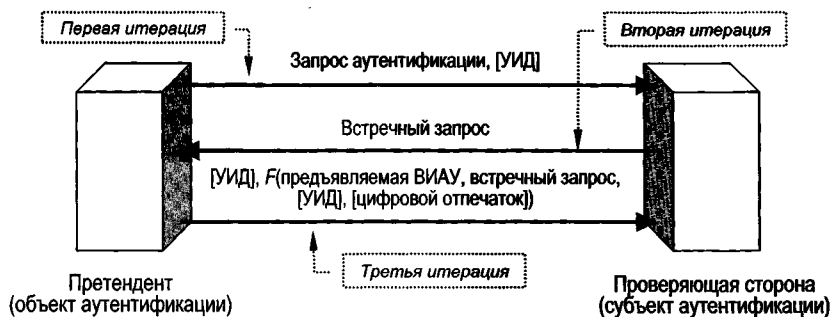


Рис. 3.13. Подкласс «4b» (способ, основанный на встречном запросе)

В случае применения ОНФ средство проверки повторяет преобразование с использованием проверочной ВИАУ вместо предъявляемой ВИАУ и проверяет результат этого преобразования с полученной ВИАУ для обмена. Для повторения этой функции проверяющая сторона должна иметь приемлемый УИД и данные, по отношению к которым применяется служба аутентификации. В случае иных функций преобразования средство проверки, либо повторяет преобразование, либо реализует обратную функцию и проверяет содержание результата с использованием проверочной ВИАУ.

Подкласс «4с» — специализированные способы, основанные на использовании зашифрованного встречного запроса. Эти способы также включают в себя следующие три итерации доставки информации:

- передача запроса на проведение процедуры аутентификации и УИД;
- отправка встречного запроса (требования) и проверочной ВИАУ, возможно вместе с УИД, преобразованных с помощью некоторой приемлемой функции (F);
- передача ответа, который содержит востребованную информацию.

Специализированные способы, основанные на использовании зашифрованного встречного запроса, могут быть следующими:

- асимметричный алгоритм.* Если предъявляемая ВИАУ представляет собой закрытый ключ, то встречный запрос зашифровывается с помощью соответствующего открытого ключа;
- симметричный алгоритм.* Если предъявляемая ВИАУ представляет собой секретный ключ, то встречный запрос зашифровывается с помощью секретного ключа. Встречный запрос зашифровывается проверяющей стороной, передающей этот запрос.

Этот тип способов применим для процедуры аутентификации взаимодействующей стороны (объекта), но не для аутентификации источника данных.

Средство формирования генерирует запрос на проведение процедуры аутентификации. После получения этого запроса и УИД средство проверки формирует непредсказуемый (уникальный) встречный запрос. Затем средство проверки реализует функцию преобразования с целью формирования ВИАУ для обмена (рис. 3.14).

Затем средство формирования осуществляет обратное преобразование с использованием предъявляемой ВИАУ вместо проверочной ВИАУ с целью получения встречного запроса, который потом направляется проверяющей стороне.

В заключение средство проверки сравнивает полученный встречный запрос с ранее сформированным.

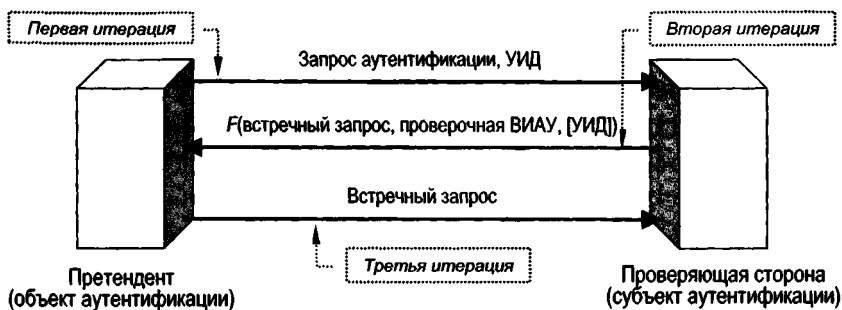


Рис. 3.14. Подкласс «4с» (специализированный способ, основанный на зашифрованном встречном запросе)

Подкласс «4d» — способы, основанные на вычислении ответа. Способы этого подкласса также включают в себя следующие три итерации доставки информации:

- передача запроса на проведение процедуры аутентификации с набором параметров, из которых может быть выбран один из них, и уникальная информация объекта;
- отправка встречного запроса (требования), содержащего те параметры, которые были выбраны проверяющей стороной;
- передача ответа, содержащего уникальное число, встречный запрос или выбранные параметры для вычисления ответа и предъявляемую ВИАУ, преобразованные в соответствии с некоторой соответствующей функцией.

Одним из примеров этого подкласса является метод аутентификации в условиях отсутствия исходных данных, при котором проверяющая сторона выбирает одну из группы проблем, которую должен решить сам претендент, причем без «подсказки как именно».

С целью обеспечения более высокого уровня гарантированности подтверждения подлинности, процедуры информационного обмена могут повторяться. Такой прием обеспечивает защиту от атак типа «маскарад», реализуемых нарушителем, способным вычислить корректный ответ для некоторых (но не

для всех) параметров, которые могла выбрать проверяющая сторона. Если имеет место только одна процедура информационного обмена, то проверяющая сторона может случайным образом выбрать параметр, для которого нарушитель знает корректный ответ. Увеличение числа процедур снижает вероятность успешного проведения таких атак.

Средство формирования в первую очередь генерирует уникальное число и выбирает параметр, а затем включает их в ВИАУ для обмена (рис. 3.15.)

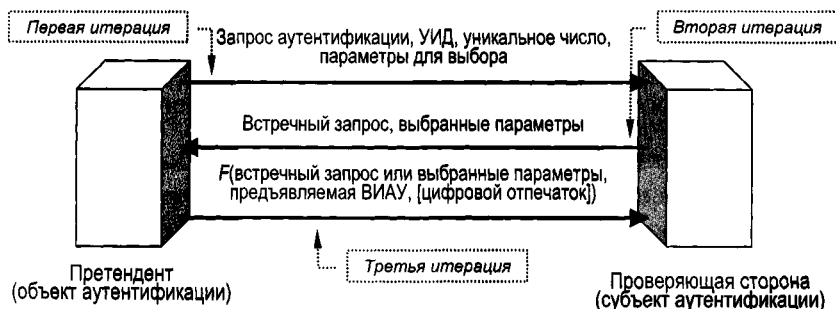


Рис. 3.15. Подкласс «4d» (способ, основанный на вычислении ответа)

Затем средство проверки выбирает параметры из предложенного списка и формирует встречный запрос в форме второго блока ВИАУ для обмена.

Средство формирования осуществляет преобразование встречного запроса или выбранных параметров с использованием предъявляемой ВИАУ.

После этого средство проверки осуществляет заключительное обратное преобразование с использованием проверочной ВИАУ и сравнивает полученные параметры.

3.4.2. Инициирование доставки

Примеры процедур информационного обмена, представленные в § 3.4.1, инициировались претендентом с использованием запроса на проведение процедуры аутентификации. Тем

не менее для подтверждения подлинности объекта могут применяться описанные ранее подклассы способов, в которых инициатором выступает проверяющая сторона, использующая для этого *приглашение для участия в процедуре аутентификации*. В таком случае число итераций доставки информации будет отличаться. Число итераций доставки информации для каждого такого случая представлено в табл. 3.1 в § 3.4.5.

3.4.3. Использование СЕРТ|АУ

Способы аутентификации могут классифицироваться по типу средств, которые используются для получения (приобретения) проверочной ВИАУ. Такими средствами могут быть:

- интерактивные СЕРТ|АУ;
- независимые СЕРТ|АУ;
- проверочная ВИАУ, полученная заблаговременно, например по защищенным каналам.

СЕРТ|АУ может использоваться для защиты процедуры аутентификации на основе принципа *d)* в § 3.1.3. СЕРТ|АУ обеспечивают защиту той ДТС, которая «привязана» к специфической проверочной ВИАУ с помощью конкретного УИД.

3.4.4. Обоюдная аутентификация

Для подклассов способов, основанных на одной итерации информационного обмена, может использоваться информационный обмен в той же самой форме (т.е. классы/подклассы «1», «2», «3» и «4а»), но в каждом направлении обоюдной аутентификации.

Способы аутентификации подкласса «4b» могут использоваться в обоих направлениях. Первый встречный запрос может быть передан вместе с запросом на проведение процедуры аутентификации, а преобразованные данные первого встречного запроса — вместе со вторым встречным запросом (рис. 3.16). В данном случае необходимо использовать такое же число ите-

раций информационного обмена, как и при однонаправленной процедуре аутентификации.

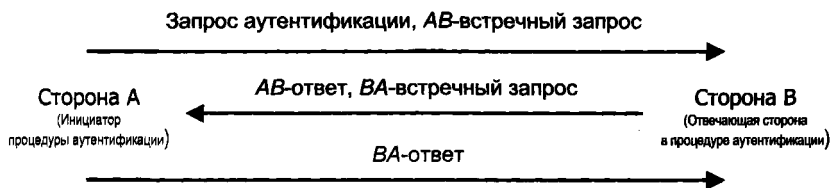


Рис. 3.16. Обоюдная аутентификация, использующая способы аутентификации, которые основаны на встречных запросах

Аналогично и при реализации способов аутентификации подкласса «4с», преобразованные данные первого встречного запроса могут передаваться вместе с запросом на проведение процедуры аутентификации, а преобразованные данные второго встречного запроса — с первым встречным запросом.

Способы аутентификации подкласса «4b» могут использоваться в сочетании со способами подкласса «4с». Две итерации информационного обмена реализуются в пределах обмена преобразованными данными. В случае использования симметричной криптографии предъявляемая и проверочная ВИАУ на каждой стороне соединения совпадают, а их преобразование осуществляется только один раз. В случае асимметричного шифрования на каждой стороне соединения осуществляются две процедуры преобразования.

При реализации способов подкласса «4d» для однонаправленной аутентификации необходимы три или более итераций информационного обмена. Обоюдная аутентификация требует четыре или более итераций информационного обмена.

3.4.5. Характеристики классов способов аутентификации

В табл. 3.1 обобщены все уязвимости и характеристики различных классов и подклассов способов аутентификации.

Таблица 3.1

Класс/подкласс	0	1	2	3	4a	4b	4c	4d
Уязвимости								
Вскрытие (раскрытие)	да	нет	нет	нет	нет	нет	нет	нет
«Повторная передача» от различных проверяющих сторон	да	да	нет	да	нет	нет	нет	нет
«Повторная передача» от одной и той же проверяющей стороны	да	да	да	нет	нет	нет	нет	нет
«Подмена», иницируемая нарушителем	нет	нет	нет	нет	нет	нет	нет	нет
«Подмена», когда нарушитель — отвечающая сторона	да	нет	нет	нет	нет	нет	нет	нет
Характеристики								
Симметричный/асимметричный алгоритм	симм.	любой	любой	любой	любой	любой	любой	асимм.
Криптографический (да)/некриптографический (нет) метод	нет	любой	любой	любой	любой	любой	да	да
Число итераций информационного обмена:								
— инициатор претендент;	1	1	1	1	1	3	3	3
— инициатор проверяющая сторона	2	2	2	2	2	2	4	4

Класс/подкласс	0	1	2	3	4a	4b	4c	4d
Поддержка аутентификации источника данных	да	да	да	да	да	да	нет	да

3.4.6. Классификация на основе конфигурации

Когда взаимодействующие стороны желают провести процедуру аутентификации, может понадобиться привлечение одной или нескольких ДТС. Должна быть определена основа (сущность) доверия между каждой взаимодействующей стороной и любой ДТС. Простейшая модель привлечения ДТС включает в себя только одну ДТС. Другие модели могут включать группу ДТС, которые доверяют друг другу, несмотря на то что более общая модель включает группу ДТС, которые не доверяют друг другу.

3.4.6.1. Принципы моделирования в условиях привлечения ДТС

В некоторых случаях проверяющая сторона может гарантированно подтвердить подлинность объекта, если только она получит гарантии надежности уникального свойства такого объекта от нескольких ДТС.

Когда к процедуре аутентификации привлекаются три или более ДТС, это позволяет обеспечить защиту от коррупции одной или более ДТС. В некоторых политиках обеспечения безопасности может использоваться мажоритарный принцип.

В дальнейшем рассматривается только простейший случай, когда в процедуре аутентификации участвует одна ДТС.

Взаимосвязи между претендентом, проверяющей стороной и одной ДТС могут быть смоделированы на основе:

- фаз, представленных в § 3.1.4 (соответственно, фаз распределения, получения, доставки и проверки);
- знания исходной информации.

Фазовая модель (на основе фаз). Следующие фазы определяют взаимодействие между различными сторонами:

- фаза распределения приемлема между претендентом, проверяющей стороной и ДТС;
- фаза получения (приобретения) приемлема между претендентом и ДТС или проверяющей стороной и ДТС;
- фаза доставки приемлема между любой парой участвующих сторон: претендентом, проверяющей стороной и ДТС;
- фаза проверки приемлема между проверяющей стороной и ДТС.

Фазы получения, доставки и проверки могут использовать способ аутентификации одного из классов, представленных в § 3.4.1.

Фаза распределения может быть интерактивной или независимой. Когда эта фаза является независимой, то она, как правило, будет проводиться перед аутентификационным обменом. В этом случае нет гарантий того, что предъявляемая ВИАУ по-прежнему является действительной (т.е. не была аннулирована).

На рис. 3.17 представлены некоторые различные схемы аутентификации. На этом рисунке сторона *А* соответствует претенденту, а сторона *В* — проверяющей стороне. Этот рисунок преследует только иллюстративные цели, поэтому не является полным.

В **схеме А** сторона *А* получает свою предъявляемую ВИАУ у ДТС после аутентификационного обмена с ДТС, а сторона *В* получает свою проверочную ВИАУ у ДТС. После этого сторона *В* проводит локальную проверку.

В **схеме В** сторона *А* получает свою предъявляемую ВИАУ у ДТС после аутентификационного обмена с ДТС, а сторона *В* предоставляет ДТС для проверки полученную от стороны *А* ВИАУ для обмена.

В **схеме С** сторона *А* получает свою предъявляемую ВИАУ у ДТС после аутентификационного обмена с ДТС, а также про-

верочную ВИАУ, которая необходима для стороны *В* при проведении ею локальной проверки.

В **схеме D** сторона *А* получает проверочную ВИАУ, которая необходима для стороны *В* при проведении ею локальной проверки, и локально формирует ВИАУ для обмена. ВИАУ для обмена и проверочная ВИАУ предоставляется стороне *В* совместно.

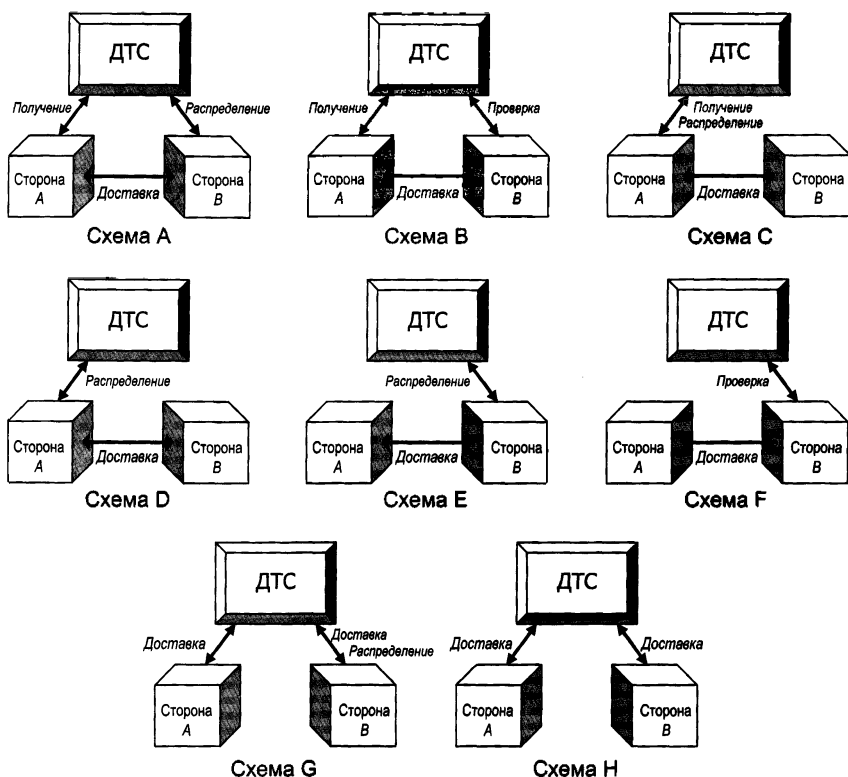


Рис. 3.17. Схемы аутентификации

В **схеме Е** сторона *А* локально формирует свою ВИАУ для обмена и предоставляет ее стороне *В*, а затем сторона *В* получает у ДТС проверочную ВИАУ, которая необходима для проведения ею локальной проверки.

В **схеме F** сторона *A* локально формирует свою ВИАУ для обмена и предоставляет ее стороне *B*, а затем сторона *B* предоставляет ДТС для проверки полученную от стороны *A* ВИАУ для обмена.

В **схеме G**, которая представляет собой поточную аутентификацию, сторона *A* локально формирует свою ВИАУ для обмена и предоставляет ее ДТС, затем ДТС передает стороне *B* СЕРТ|АУ вместе с проверочной ВИАУ, которая необходима для проведения ею локальной проверки.

В **схеме H**, которая представляет собой интерактивную аутентификацию, сторона *A* локально формирует свою ВИАУ для обмена и предоставляет ее ДТС, затем ДТС передает стороне *B* извещение о том, что подлинность стороны *A* была проверена.

Моделирование на основе знания исходной информации. Претендент (сторона *A*) и проверяющая сторона (сторона *B*) должны использовать некоторую исходную информацию до начала возможного проведения процедуры аутентификационного обмена. Если используется ДТС, то из этого следует, что претендент непосредственно не знает открытого ключа или секретного ключа, используемого проверяющей стороной. Далее рассматриваются возможные типы исходных данных.

Исходная информация, используемая совместно претендентом и ДТС. Существуют следующие возможные случаи:

- a) секретный ключ, совместно используемый претендентом и ДТС, известен претенденту и ДТС (методы на основе использования секретного ключа);
- b) закрытый ключ претендента известен только претенденту (сторона *A*), открытый ключ претендента известен ДТС (асимметричные методы);
- c) закрытый ключ претендента известен претенденту и ДТС (некоторые методы, применяемые при отсутствии исходных данных).

Исходная информация, используемая совместно проверяющей стороной и ДТС. Существуют следующие возможные случаи:

- а) секретный ключ, совместно используемый проверяющей стороной (сторона В) и ДТС, известен проверяющей стороне и ДТС (методы на основе использования секретного ключа);
- б) открытый ключ ДТС известен проверяющей стороне (сторона В) (асимметричные методы и методы, применяемые при отсутствии исходных данных).

3.4.6.2. Взаимосвязи между привлекаемыми к процедуре аутентификации ДТС

Интерактивные ДТС. При проведении процедуры аутентификации могут быть востребованы интерактивные ДТС. Последние, входящие в один и тот же ССБ, могут хранить предъявляемую ВИАУ и/или проверочную ВИАУ взаимодействующих сторон, которые были ранее зарегистрированы в этом сегменте.

Для обеспечения гарантий того, что в рамках конкретного ССБ различные участники информационного взаимодействия не могут быть зарегистрированы под одним и тем же именем, необходимо наличие специализированных протоколов и/или процедур.

Доступность интерактивных ДТС является очень важной требующей своего решения проблемой, в противном случае, процедуры аутентификационного обмена с использованием интерактивных ДТС могли бы стать объектами атак типа «отказ в обслуживании». Дублирование ВИАУ в нескольких ДТС может минимизировать уязвимость аутентификации с использованием интерактивных ДТС. Для дублирования ВИАУ также необходимо наличие специализированных протоколов. Когда проверочная ВИАУ должна доставляться в рамках процедуры аутентификации, то при взаимодействии между собой нескольких ДТС, участвующих в этой процедуре аутентификации, необходимо привлекать службы обеспечения целостности, а в некоторых случаях и службу обеспечения конфиденциальности. Когда предъявляемая ВИАУ должна доставляться в рамках процедуры аутентификации, то при взаимодействии между собой нескольких ДТС необходимо привлекать службы обеспечения целостности и конфиденциальности.

Кроме этого, может возникнуть необходимость проведения обмена результатами аудиторских проверок, которые проводились различными интерактивными ДТС, входящими в один ССБ и участвующими в процедурах аутентификации. В этом случае для передачи и приема результатов аудиторских проверок необходимо наличие специализированных протоколов.

Независимые ДТС. Очень часто независимые ДТС именуется УЦ, так как они могут выпускать независимые СЕРТ|АУ. Нет необходимости в специфической защите независимого СЕРТ|АУ, поскольку он имеет собственную защиту. Доступность независимых СЕРТ|АУ является очень важной, требующей своего решения проблемой, в противном случае процедуры аутентификационного обмена с использованием независимых СЕРТ|АУ могли бы стать объектами атак типа «отказ в обслуживании». Дублирование такой информации в нескольких различных репозиториях может минимизировать эту проблему.

3.5. Взаимодействие с другими службами и способами обеспечения безопасности

3.5.1. Управление доступом

Многим пользователям может понадобиться прохождение процедуры аутентификации перед тем, как им будет дозволено получение информации для контроля доступа. Эта информация обеспечит доступ к ресурсам, которые являются субъектом политики управления доступом. Соответственно служба аутентификации может предоставить результаты процедуры аутентификации службе управления доступом для использования последней.

Аннулирование ВИАУ может привести к прекращению существующего доступа.

3.5.2. Целостность данных

Аутентификация может использоваться совместно с обеспечением целостности данных с целью обеспечения гарантии не-

прерывности аутентификации и дополнительного подтверждения подлинности источника данных.

Некоторые способы аутентификации могут применяться для распределения в явной либо неявной форме ключевой информации, которая может использоваться службой обеспечения целостности. Когда такая ключевая информация определена неявно, должен быть известен способ получения ключевой информации из доставляемых данных либо такой способ должен быть определен в течение аутентификационного обмена. Когда такая ключевая информация определена явно, должны быть доставлены дополнительные данные, причем в обоих направлениях в течение аутентификационного обмена.

3.5.3. Конфиденциальность данных

Некоторые способы аутентификации могут применяться для распределения в явной либо неявной форме ключевой информации, которая может использоваться службой обеспечения конфиденциальности. Когда такая ключевая информация определена неявно, должен быть известен способ получения ключевой информации из доставляемых данных либо такой способ должен быть определен в течение аутентификационного обмена. Когда такая ключевая информация определена явно, должны быть доставлены дополнительные данные, причем в обоих направлениях в течение аутентификационного обмена.

3.5.4. Неотказуемость

Некоторые способы аутентификации могут применяться для распределения в явной либо неявной форме ключевой информации, которая может использоваться службой обеспечения неотказуемости. Когда такая ключевая информация определена неявно, должен быть известен способ получения такой информации из доставляемых данных либо такой способ должен быть определен в течение аутентификационного обмена. Когда такая

ключевая информация определена явно, должны быть доставлены дополнительные данные, причем в обоих направлениях в течение аутентификационного обмена.

3.5.5. Аудит

Информация, которая связана с аутентификацией и может быть использована при проведении аудиторских проверок, как правило, включает:

- a)* результаты аутентификации (т.е. достоверной идентификации);
- b)* информация, связанная с аннулированием ВИАУ;
- c)* информация о гарантии непрерывности аутентификации;
- d)* иная информация, касающаяся процедуры аутентификации.

3.6. Персонификация (аутентификация пользователей)

3.6.1. Общие положения

Корректная аутентификация пользователей (физических лиц), т.е. персонификация, может быть неотъемлемой частью обеспечения безопасности открытых систем, которые обслуживают запросы людей. Диалог между пользователем и компьютерной системой может увеличивать вероятность вторжений с использованием атак типа «маскарад». Методы персонификации должны быть приемлемы для пользователей, а также экономичны и безопасны. Неудобные методы иногда провоцируют пользователей к поиску путей для уклонения от процедур, а это, в свою очередь, — к потенциальному росту вторжений.

Персонификация зависит от принципов аутентификации в одной или нескольких следующих категорий:

- a)* знание чего-нибудь;
- b)* обладание чем-нибудь;

- с)* индивидуальные характеристики пользователя;
- д)* признание того, что определенная ДТС установила подлинность пользователя;
- е)* контекст (например адрес источника в запросе).

В общем процесс персонификации применяет сравнение представленных пользователем верительных документов (данных) с ВИАУ, полученной в фазе инсталляции.

3.6.1.1. Персонификация на основе знания чего-нибудь

В этой категории пароль является наиболее общей используемой ВИАУ. Когда происходит обращение к системе, пользователь предъявляет пароль, а система аутентификации сравнивает его с соответствующим значением из списка паролей, чтобы подтвердить подлинность пользователя. Пароли должны быть трудными для отгадывания, а также должны находиться под тщательным и непрерывным контролем. В противном случае они становятся объектами неумышленного вскрытия.

3.6.1.2. Персонификация на основе обладания чем-нибудь

В этой категории используется физический идентификатор, например:

- а)* карта с магнитной полосой (magnetic stripe card);
- б)* смарт-карта (IC card).

В случае использования карт с магнитной полосой пользователь при обращении к системе предъявляет такую карту, а система аутентификации считывает ВИАУ из карты с целью ее сравнения с хранящейся ВИАУ, чтобы подтвердить подлинность пользователя.

Карты с магнитной полосой обладают серьезной уязвимостью, т.е. они могут быть легко скопированы. Другой существенной их уязвимостью является то, что если такой картой завладел нарушитель, то данный способ аутентификации потерпит неудачу.

В случае использования смарт-карт пользователь при обращении к системе предъявляет такую карту, а система аутентификации использует хранящуюся на данной карте информацию при формировании ВИАУ для обмена, чтобы подтвердить подлинность пользователя. Преимуществом смарт-карты является то, что ее нельзя легко скопировать.

Возможны два варианта аутентификации владельца смарт-карты:

- когда смарт-карта способна аутентифицировать своего владельца, то имеет место двойная схема аутентификации, в которой пользователь аутентифицируется проверяющей стороной. Такой способ эквивалентен за счет транзитивности, аутентификации пользователя напрямую;
- когда смарт-карта не способна аутентифицировать своего владельца, а картой завладел нарушитель, то данный способ аутентификации потерпит неудачу.

3.6.1.3. Нестационарный генератор паролей

Один из способов персонификации основан на использовании портативного прибора (устройства), который функционирует как нестационарный (зависящий от времени) генератор паролей. ВИАУ для обмена формируется с использованием:

- секретной информации, хранящейся внутри прибора;
- значения времени;
- PIN-кода¹, который напрямую вводится пользователем в прибор.

Таким образом, сформированная ВИАУ для обмена выводится на дисплее прибора. Затем она передается пользователем (в открытом виде) проверяющей системе. Этой системе может понадобиться обеспечение синхронизации с картой. Такой тип персонификации требует, чтобы сам пользователь, т.е. владелец прибора, попытался себя аутентифицировать за счет:

¹ Personal Identification Number — личный опознавательный номер.

- обладания таким прибором;
- знания PIN-кода.

3.6.1.4. Персонализация на основе индивидуальной характеристики пользователя

Пароли очень уязвимы к вскрытию (раскрытию), если пользоваться ими халатно, а физические идентификаторы очень уязвимы к краже или, в случае использования карт с магнитной полосой, несанкционированному копированию. Существует метод персонализации, не имеющий таких недостатков, который основан на использовании индивидуальных характеристик пользователей, а именно:

- собственноручная подпись;
- отпечатки пальцев;
- тембр (спектр) голоса;
- рисунок сетчатки глаза;
- динамические характеристики печати на клавиатуре.

К двум наиболее важным классам, основанным на методе собственноручной подписи, относятся статические и динамические системы. В таких системах в качестве признаков могут использоваться наклон символов, нажим на бумагу, время и непосредственная информация из текста подписи.

Анализ динамических характеристик печати на клавиатуре обеспечивает непрерывность аутентификации.

В фазе регистрации пользователь фиксирует свой уникальный параметр в системе регистрации. Пользователь выполняет необходимую специфическую процедуру, например собственноручно расписывается, ставит отпечатки пальцев на электронном планшете или произносит вслух специфические слова. Такая процедура при необходимости может повторяться до тех пор, пока не будет получена достоверная эталонная информация. Система анализирует параметрическое значение действия пользователя и фиксирует это значение в качестве краткой характеристики пользователя.

В фазах доставки и проверки пользователь предъявляет свой уникальный параметр и снова выполняет необходимую

специфическую процедуру. Проверяющая система сравнивает полученную от пользователя информацию с записанной ранее краткой характеристикой пользователя.

3.6.2. Процессы, действующие от имени пользователя

В некоторых случаях пользователю может потребоваться действовать без собственного участия. В таких случаях он будет иметь свое виртуальное «представительство» (representation) внутри системы, которое может иметь независимое от фактического присутствия пользователя «время жизни».

В связи с тем, что виртуальное представительство действует так, как будто это был пользователь, то действия от имени пользователя могут продолжаться непрерывно, причем без необходимости непосредственного присутствия самого пользователя.

Например, пользователь может зарегистрироваться, а затем может использовать различные компьютеры без последующей регистрации на них.

Более предпочтительными являются виртуальные представительства пользователя, которые могут использовать дополнительные способы, обеспечивающие зависимость времени жизни представительства от присутствия самого пользователя, по сравнению с поддержкой виртуального представительства с независимым временем жизни.

3.7. Аутентификация в ЭМВОС и Интернет-архитектуре

Определены два типа услуг:

- аутентификация взаимодействующей стороны (объекта);
- аутентификация источника данных.

3.7.1. Аутентификация объекта

Аутентификация объекта может использоваться либо перед фазой передачи данных, либо в течение фазы передачи данных с

целью подтверждения подлинности одной или нескольких взаимодействующих сторон, которые имеют соединения с одной или несколькими другими взаимодействующими сторонами. Эта услуга доступна при использовании протоколов, с установлением и без установления соединения. Аутентификация объекта может использоваться и при односторонней, и при обоюдной аутентификации.

3.7.2. Аутентификация источника данных

Аутентификация источника данных обеспечивает подтверждение источника элемента данных. Эта услуга не обеспечивает защиту от дублирования элементов данных.

3.7.3. Использование аутентификации уровнями ЭМВОС и Интернет-архитектуры

Аутентификация объекта и аутентификация источника данных имеют место только на следующих уровнях ЭМВОС и Интернет-архитектуры:

- сетевом (3);
- транспортном (4);
- прикладном (7, ЭМВОС) или 5-м уровне Интернет-архитектуры.

3.7.3.1. Использование аутентификации на сетевом уровне

Аутентификация объекта на сетевом уровне позволяет подтвердить подлинность сетевого объекта. Эта услуга позволяет аутентифицировать сетевые узлы, узлы подсетей или ретрансляционные узлы.

Аутентификация источника данных на сетевом уровне позволяет подтвердить подлинность источника элемента данных. Источниками данных могут быть сетевой узел, узел подсети или ретрансляционный узел.

Способы, используемые сетевым уровнем, встроены в модуль, реализующий функции этого уровня.

3.7.3.2. Использование аутентификации на транспортном уровне

Аутентификация объекта на транспортном уровне позволяет подтвердить подлинность транспортного объекта. Эта услуга позволяет аутентифицировать оконечные системы. Различные прикладные процессы, реализуемые одной и той же оконечной системой, могут быть не аутентифицированы.

Аутентификация источника данных на транспортном уровне позволяет подтвердить подлинность источника элемента данных. Источником данных может быть оконечная система.

Способы, используемые транспортным уровнем, встроены в модуль, реализующий функции этого уровня.

3.7.3.3. Использование аутентификации на прикладном уровне

Аутентификация объекта на прикладном уровне позволяет подтвердить подлинность прикладного объекта/процесса, поддерживаемого оконечной системой. Эта услуга позволяет аутентифицировать прикладные объекты или прикладные процессы. Различные прикладные объекты или прикладные процессы, поддерживаемые одной и той же оконечной системой, могут быть аутентифицированы.

Аутентификация источника данных на прикладном уровне позволяет подтвердить подлинность источника элемента данных. Источником данных может быть прикладной объект или прикладной процесс.

Способы, используемые прикладным уровнем, встроены либо в модуль, реализующий функции прикладного уровня, либо в модуль, реализующий функции уровня представления (6). Аутентификация на прикладном уровне также может использовать услуги аутентификации, предоставляемые сетевым или транспортным уровнем.

3.8. Практические аспекты парирования атак типа «повторная передача» на основе применения уникальных чисел или встречных запросов

3.8.1. Уникальные числа

Уникальные числа формируются претендентом. Одно и то же уникальное число никогда не должно признаваться одной и той же проверяющей стороной дважды. Это может быть достигнуто несколькими способами. Некоторые методы, которые могли быть доказаны в теории, могут быть неприемлемыми на практике. Непосредственным примером такого метода может быть хранение в памяти всех принятых уникальных чисел, которые были успешно использованы в течение процедуры аутентификационного обмена. При таком решении мог бы потребоваться такой объем памяти, который бы увеличивался пропорционально числу успешно проведенных процедур аутентификации. Очевидно, что это неприемлемо с точки зрения затрат и/или с точки зрения производительности.

Одним из способов снижения объема памяти, необходимой на проверяющей стороне, является хранение всех принятых и успешно использованных уникальных чисел, но только в течение ограниченного периода времени. Такой подход предполагает применение метки времени как части уникального числа, чтобы проверяющая сторона запоминала только самые «последние» уникальные числа. На практике временной интервал в несколько минут может быть адекватным для ограничения необходимого объема памяти и для минимизации проблемы синхронизации между различными источниками эталонного времени, используемыми объектом и проверяющей стороной.

Для парирования атаки «отказ в обслуживании» самым лучшим является предотвращение неумышленных коллизий между уникальными числами, сформированными двумя взаимодействующими объектами. Для этого уникальное число должно выбираться из достаточно большого диапазона. Диапазон уникальных чисел связан с максимальным числом процедур ау-

тентификации за определенный период времени (например за секунду), который необходим для проведения аутентификации (фаза проверки) выбранной проверяющей стороной. Если источник эталонного времени, используемый объектом, не способен самостоятельно вырабатывать такое большое число, то в метку времени может быть добавлено случайное число, что позволит увеличить диапазон уникальных чисел.

3.8.2. Встречные запросы

Встречные запросы формируются проверяющей стороной. Один и тот же запрос никогда не должен передаваться одной и той же проверяющей стороной дважды. Это может быть достигнуто несколькими способами.

Некоторые методы, которые могли быть доказаны в теории, на практике могут быть неприемлемыми. Непосредственным примером такого метода может быть хранение в памяти всех переданных встречных запросов. При этом решении мог бы потребоваться такой объем памяти, который бы увеличивался пропорционально числу успешно проведенных процедур аутентификации, использующих встречные запросы. Очевидно, что это неприемлемо с точки зрения затрат и/или с точки зрения производительности.

Существует несколько способов снижения необходимого объема памяти на проверяющей стороне:

- снабжение встречных запросов последовательными номерами и хранение только последнего последовательного номера;
- снабжение встречных запросов случайными числами. Хотя это противоречит правилу о том, что «один и тот же запрос никогда не должен передаваться дважды», вероятность такого события может быть существенно снижена за счет использования случайных чисел из достаточно большого диапазона;
- использование метки времени в каждом встречном запросе;

- использование комбинации из метки времени и случайного числа.

3.9. Защита процедуры аутентификации

Рассмотрим примеры некоторых наиболее часто встречающихся типов атак на процедуры аутентификации.

3.9.1. Атаки типа «прослушивание / повторная передача»

Существуют два заслуживающих внимание варианта атаки типа «повторная передача», при проведении которых определенная ВИАУ для обмена передается повторно:

- одной и той же проверяющей стороне;
- другой проверяющей стороне.

Последний случай возможен тогда, когда проверочная ВИАУ объекта становится известна нескольким проверяющим сторонам. Если такая атака была проведена успешно, она является специфическим случаем атаки «маскарад».

Оба варианта атаки типа «повторная передача» могут быть парированы на основе применения встречных запросов. Такие встречные запросы формируются проверяющей стороной. Один и тот же запрос никогда не должен передаваться одной и той же проверяющей стороной дважды. Способы решения этой задачи представлены в § 3.8.

3.9.2. Атаки типа «повторная передача одной и той же проверяющей стороне»

Такой тип атак может быть парирован на основе применения уникальных чисел или встречных запросов.

Уникальные числа формируются претендентом. Одно и то же уникальное число никогда не должно признаваться одной и той же проверяющей стороной дважды. Способы решения такой задачи представлены в § 3.8.

3.9.3. Атаки типа «повторная передача разным проверяющим сторонам»

Такие атаки могут быть парированы на основе применения встречных запросов. С другой стороны, данная атака может быть парирована на основе использования, в течение вычисления ВИАУ для обмена, любого специфического параметра, который для проверяющей стороны является уникальным. Таким параметром может быть имя проверяющей стороны, ее сетевой адрес или какой-либо общий уникальный атрибут, связанный с проверяющими сторонами, совместно использующими одну и ту же проверочную ВИАУ.

3.9.4. Атаки типа «перехват / повторная передача»

3.9.4.1. Прямые атаки

Одним из типов атак (прямых атак) является атака, при которой нарушитель выступает в роли инициатора процедуры аутентификации. Такая атака возможна только тогда, когда оба (и претендент и проверяющая сторона) могут инициировать процедуру аутентификации. При реализации указанной атаки претендент и проверяющая сторона обмениваются ВИАУ через нарушителя, не осознавая этого, т.е. нарушитель «прикидывается» проверяющей стороной для претендента и претендентом для проверяющей стороны.

Например, предположим, что нарушитель *C* желает представиться проверяющей стороне *B* в качестве претендента *A*. *C* начинает информационное взаимодействие с обеими сторонами *A* и *B*. *C* сообщает *A*, что он *B*, и запрашивает *A* для аутентификации на стороне *B*. Кроме этого, *C* сообщает *B*, что он *A*, и что он желает аутентифицироваться.

В течение процедуры аутентификации *A* действует как претендент по отношению *B* (реально *C* действует как *B*) и, более того, обеспечивает *C* информацией, которую последний может использовать для аутентификации на стороне *B*. *B* действует как проверяющая сторона и также обеспечивает *C* информацией, ко-

торая необходима последнему для исполнения роли проверяющей стороны. После процедуры аутентификации нарушитель *C* будет представляться стороне *B* как аутентифицированная сторона *A*.

Возможные способы парирования атак такого типа требуют защиты от повторной передачи другой проверяющей стороне:

- a)* сторона, которая начинает ПИНО, всегда должна быть претендентом;
- b)* ВИАУ для обмена, сформированная претендентом, когда он выступает в роли инициатора процедуры аутентификации, должна отличаться от той, которую он предоставляет, выступая в роли отвечающей стороны на инициативный запрос процедуры аутентификации от проверяющей стороны. Такое отличие позволяет проверяющей стороне выявить описанный перехват.

3.9.4.2. Адаптивные («изохренные») атаки

К одному из типов атак относится атака, при реализации которой нарушитель располагается в середине соединения, обеспечивающего аутентификационный обмен, перехватывает ВИАУ и ретранслирует ее, выступая в роли претендента.

Основной способ парирования атаки такого типа требует использования дополнительной службы (обеспечения целостности или конфиденциальности). ВИАУ для обмена объединяется с некоторой другой информацией, которая позволяет претенденту и проверяющей стороне сформировать ключ, делая их, таким образом, легитимными участниками аутентификационного обмена. Затем сформированный ключ может использоваться как ключ для обеспечения целостности на основе криптоалгоритма или для обеспечения конфиденциальности.

Другим заслуживающим внимание способом парирования атак такого типа является способ, при котором сеть передачи данных не является объектом для внутреннего перехвата, т.е. такая сеть всегда доставляет циркулирующие в ней данные корректно в соответствии с указанными адресами. В такой ситуации

атака может быть парирована на основе использования сетевых адресов, которые будут использоваться службой (средством) формирования как входные данные. При таком подходе ВИАУ для обмена будет зависеть от сетевого адреса.

3.9.5. Использование индикатора «приглашение/запрос» для защиты от атак нарушителя

Второй тип атак, представленный в § 3.9.4, возможен при использовании либо встречных запросов, либо уникальных чисел. Защита основана на использовании претендентом индикатора, который устанавливает, после чего последовал ответ, либо за приглашением к процедуре аутентификации, либо за запросом прохождения процедуры аутентификации. Индикатор может иметь два состояния, например, «1», если ответ последовал за приглашением к процедуре аутентификации, и «0», если ответ последовал за запросом прохождения процедуры аутентификации. Так как значение индикатора участвует в определении ответа, то очевидно, что содержание ответа, формируемого претендентом, зависит от значения индикатора. В дальнейшем такой индикатор будет именоваться индикатором «приглашение/запрос».

3.9.6. Протокол на основе встречных вызовов

При использовании встречных запросов нарушитель *С* (рис. 3.18) разыгрывает роль стороны *А* и передает стороне *В* запрос на проведение процедуры аутентификации (первая итерация информационного обмена). Сторона *В* направляет встречный запрос нарушителю *С* (вторая итерация информационного обмена). Нарушитель *С* передает приглашение на аутентификацию стороне *А* и направляет полученный от *В* встречный запрос *А* (третья итерация информационного обмена). Сторона *А* вычисляет его запрос, используя для этого встречный запрос, полученный от *С*, и индикатор «приглашение/запрос», установленный в положение «приглашение». Нарушитель *С* направляет стороне *В* полученный от *А* ответ.

Сторона *B* проверяет ответ. Так как *B* получила оригинальный запрос на аутентификацию от *C*, она ожидает, что индикатор «приглашение/запрос» будет установлен в положение «запрос». А ввиду того, что *B* получила ответ, который был сформирован с использованием индикатора «приглашение/запрос», установленного в положение «приглашение», она отказывает в аутентификации.

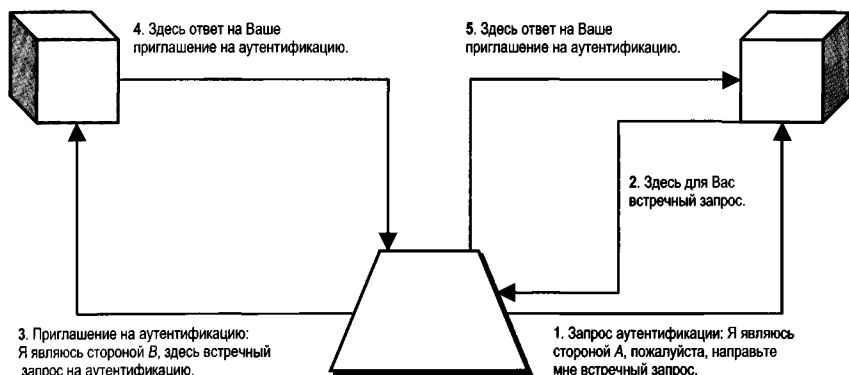


Рис. 3.18. Защита от атак нарушителя с использованием встречных запросов¹

Если сторона *B* поддерживает и запросы и приглашения на аутентификацию, то она должна обеспечить следующую дополнительную проверку. При каждой отправке стороной *B* приглашения на аутентификацию, *B* обязана запомнить какому претенденту был направлен конкретный встречный запрос, причем последний должен быть таким, чтобы нарушитель *C* не мог его использовать для другого претендента, когда ему передается приглашение на аутентификацию (третья итерация информационного обмена).

¹ Прямые атаки, представленные в 3.9.4.1. Даже если для парирования атак используются методы а) или б) из 3.9.4.1, они остаются бессильны перед адаптивными («изошренными») атаками.

3.9.7. Протокол на основе уникальных чисел

При использовании уникальных чисел нарушитель *C* разыгрывает роль стороны *B* и передает стороне *A* приглашение на проведение процедуры аутентификации (первая итерация информационного обмена). Сторона *A* формирует свой ответ, используя для этого уникальное число и индикатор «приглашение/запрос», установленный в положение «приглашение» (вторая итерация информационного обмена). Нарушитель *C* ретранслирует стороне *B* полученный от *A* ответ (третья итерация информационного обмена). Сторона *B* проверяет ответ. Последний содержит индикатор «приглашение/запрос», установленный в положение «приглашение», но сторона *B* не направляла какого-либо приглашения на аутентификацию, и поэтому сторона *B* отказывает в аутентификации (рис. 3.19).

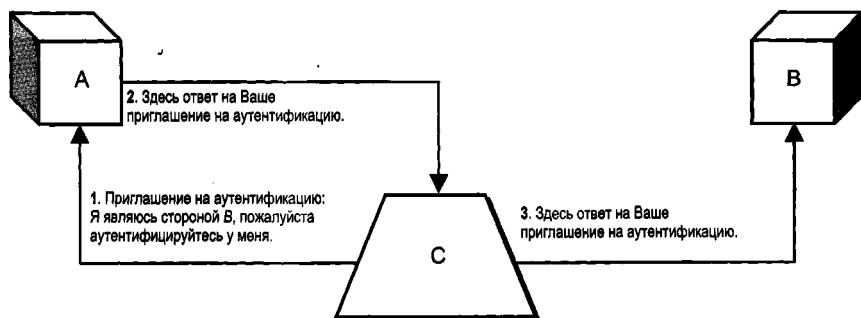


Рис. 3.19. Защита от атак нарушителя с использованием уникальных чисел

3.10. Примеры способов аутентификации

Рассмотрим некоторые специфические примеры способов аутентификации.

3.10.1. Способ аутентификации с использованием уникального числа и интерактивного СЕРТ|АУ

Этот пример иллюстрирует использование способа аутентификации на основе уникальных чисел, представленного в классе «3» (§ 3.4.1). В этом примере используется интерактивный СЕРТ|АУ, а УИД, способ защиты, параметр защиты и период действия СЕРТ|АУ включены в состав СЕРТ|АУ. В этом примере необходима только одна итерация информационного обмена, представленный СЕРТ|АУ может быть использован не один раз.

Метод защиты указывает на связь между параметром защиты, содержащимся в СЕРТ|АУ, и внешним контрольным параметром (ВКП), используемым для защиты СЕРТ|АУ от несанкционированного применения. ВКП может быть связан с параметром защиты посредством однонаправленной зависимости, такой как:

- ВКП представляет собой значение параметра подтверждения подлинности (или просто — параметра подлинности), а параметр защиты является результатом вычисления однонаправленной функции по значению параметра подлинности;
- ВКП представляет собой закрытый ключ, а параметр защиты является соответствующим открытым ключом.

Когда значение параметра подлинности используется как ВКП, тогда это значение передается проверяющей стороне, в качестве защиты права собственности на СЕРТ|АУ. В течение передачи должна быть обеспечена конфиденциальность значения параметра подлинности, т.е. оно должно передаваться в зашифрованном виде претендентом проверяющей стороне с использованием внешнего секретного ключа, связанного с конкретным каналом связи или с приемной стороной канала связи.

Защита права собственности от атак типа «повторная передача» достигается за счет использования уникального

числа и функции преобразования. В зависимости от сущности ВКП могут использоваться три функции преобразования (F):

а) ОНФ. Если ВКП представляет собой значение параметра подлинности, то уникальное число и значение параметра подлинности преобразуются с помощью ОНФ. Результат и уникальное число передаются проверяющей стороне, причем таким образом, чтобы последняя могла осуществить точно такое же преобразование;

б) Асимметричный алгоритм. Если ВКП представляет собой закрытый ключ, то уникальное число подписывается с помощью этого закрытого ключа;

с) Симметричный алгоритм. Если ВКП представляет собой секретный ключ, то уникальное число шифруется с помощью секретного ключа или защищается с помощью криптографической проверочной суммы, при вычислении которой используемый секретный ключ выступает в роли параметра подлинности.

Этот пример приемлем и для аутентификации объекта, и для аутентификации источника данных. При аутентификации источника данных данные или цифровой отпечаток данных могут также преобразовываться с помощью функции F .

Служба запроса используется для получения интерактивного СЕРТ|АУ и ВКП. Затем служба формирования генерирует уникальное число и осуществляет преобразование, используя следующие входные параметры:

- а)* уникальное число;
- б)* ВКП;
- с)* УИД (дополнительно);
- д)* цифровой отпечаток (если требуется аутентификация источника данных).

Кроме этого, если ВКП является значением параметра подлинности или секретным контрольным ключом, то служба формирования передает этот параметр в зашифрованном виде, причем таком, чтобы только конкретная проверяющая сторо-

на могла его расшифровать, и вырабатывает ВИАУ для обмена (рис. 3.20).

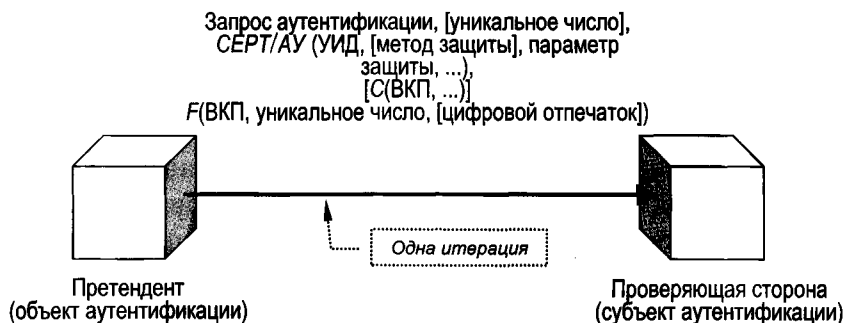


Рис. 3.20. Способ аутентификации на основе уникального числа и интерактивного CERT|AU¹

Служба проверки проверяет ВИАУ для обмена на предмет ее подлинности, используя параметр защиты из CERT|AU. Кроме этого, если используется значение параметра подлинности или секретный контрольный ключ, то служба проверки расшифровывает зашифрованное значение параметра подлинности или зашифрованный секретный контрольный ключ, которые она сравнивает с параметром защиты. Также служба проверки проверяет, что уникальное число ранее успешно не использовалось (не было получено).

3.10.2. Способ аутентификации с использованием встречного запроса и интерактивного CERT|AU

Для реализации этого способа применяется CERT|AU с целью обеспечения защиты аутентификации в соответствии

¹ 1. CERT/AU(...) используется для обозначения CERT|AU, включающего соответствующие параметры. 2. C(...) используется для обозначения прикладного процесса службы обеспечения конфиденциальности. Эта служба используется только тогда, когда ВКП является значением параметра подлинности.

с принципом «*d*» (§ 3.1.3) и способ аутентификации на основе встречных запросов, представленный в § 3.4.1.5. СЕРТ|АУ обеспечивает защиту той ДТС, которая аутентифицировала владельца этого СЕРТ|АУ, имеющего специфический УИД. Этот способ обеспечивает доказательство того, что СЕРТ|АУ, имеющий соответствующий УИД, был получен претендентом.

В данном примере используются интерактивные СЕРТ|АУ, а УИД, метод защиты, параметр защиты и период действия СЕРТ|АУ включены в состав СЕРТ|АУ. Этот пример позволяет использовать соответствующий СЕРТ|АУ не один раз.

Метод защиты указывает на связь между параметром защиты, содержащимся в СЕРТ|АУ, и ВКП, используемым для защиты СЕРТ|АУ от несанкционированного применения. ВКП может быть связан с параметром защиты посредством однонаправленной зависимости, такой как:

- ВКП представляет собой значение параметра подлинности, а параметр защиты является результатом вычисления однонаправленной функции по значению параметра подлинности;
- ВКП представляет собой закрытый ключ, а параметр защиты является соответствующим открытым ключом.

Когда значение параметра подлинности используется как ВКП, тогда это значение передается проверяющей стороне в качестве защиты права собственности на СЕРТ|АУ. В течение передачи должна быть обеспечена конфиденциальность ключа, т.е. он должен передаваться в зашифрованном виде претендентом проверяющей стороне с использованием внешнего секретного ключа, связанного с конкретным каналом связи или с приемной стороной канала связи.

Защита права собственности от атак типа «повторная передача» достигается за счет использования встречного запроса и функции преобразования. В зависимости от сущности ВКП могут использоваться три функции преобразования (*F*):

- a) ОНФ.* Если ВКП представляет собой значение параметра подлинности, то встречный запрос и значение параметра подлинности преобразуются с помощью ОНФ. Результат и встречный запрос передаются проверяющей стороне, причем таким образом, чтобы последняя могла осуществить точно такое же преобразование;
- b) Асимметричный алгоритм.* Если ВКП представляет собой закрытый ключ, то встречный запрос подписывается с помощью этого закрытого ключа;
- c) Симметричный алгоритм.* Если ВКП представляет собой секретный ключ, то встречный запрос шифруется с помощью секретного ключа или защищается с помощью криптографической проверочной суммы, при вычислении которой используемый секретный ключ выступает в роли параметра подлинности.

Этот пример приемлем и для аутентификации объекта, и для аутентификации источника данных. При аутентификации источника данных данные или цифровой отпечаток данных могут также преобразовываться с помощью функции *F*.

Служба запроса используется для получения интерактивного СЕРТ|АУ и ВКП. Затем служба формирования генерирует запрос аутентификации. После получения запроса на аутентификацию служба проверки формирует встречный запрос в качестве ВИАУ для обмена. В дальнейшем служба формирования осуществляет преобразование, используя следующие входные параметры:

- встречный запрос;
- ВКП;
- УИД (дополнительно);
- цифровой отпечаток (если требуется аутентификация источника данных).

Кроме этого, если ВКП является значением параметра подлинности или секретным контрольным ключом, то служба

формирования передает этот параметр в зашифрованном виде, причем в таком, что только бы конкретная проверяющая сторона могла его расшифровать, и вырабатывает ВИАУ для обмена (рис. 3.21).

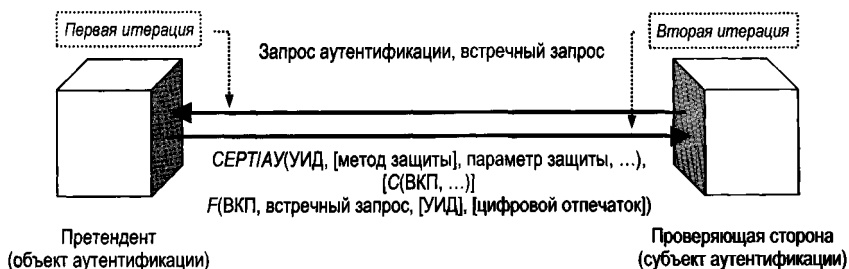


Рис. 3.21. Способ аутентификации на основе встречного запроса и интерактивного CERT/AU¹

Служба проверки проверяет ВИАУ для обмена на предмет ее подлинности, используя параметр защиты из CERT/AU. Кроме этого, если используется значение параметра подлинности или секретный контрольный ключ, то служба проверки расшифровывает зашифрованное значение параметра подлинности или зашифрованный секретный контрольный ключ, которые она сравнивает с параметром защиты. Также служба проверки проверяет, что встречный запрос совпадает с тем, который был передан.

Общая структура службы аутентификации представлена в табл. 3.2.

¹ 1. CERT/AU(...) используется для обозначения CERT/AU, включающего соответствующие параметры. 2. C(...) используется для обозначения прикладного процесса службы обеспечения конфиденциальности. Эта служба используется только тогда, когда ВКП является значением параметра подлинности.

Структура службы обеспечения безопасности (аутентификации)		Элемент	<u>Объект/субъект:</u> Претендент, проверяющая сторона, ДТС, взаимодействующая сторона, администратор	
			<u>Информационный объект:</u> ВИАУ	
		<u>Цель объекта:</u> обеспечить гарантии предъявляемого параметра подлинности объекта		
М Е Р О П Р И Я Т И Я	Объект/субъект	Центр безопасности, взаимодействующая сторона, администратор		
	Функция			
	Мероприятия, связанные с обеспечением процедуры аутентификации	— Инсталляция — Разблокировка — ВИАУ для обмена — Деинсталляция — Распределение		
	Объект/субъект	— Претендент — Проверяющая сторона — ДТС		
	Функция			
	Мероприятия, функционально связанные с процедурой аутентификации	— Запрос — Формирование — Проверка — Формирование и проверка		
И Н Ф О Р М А Ц И Я	Элемент входных/выходных данных, определяемый Центром безопасности сетевого сегмента	Предъявляемая информация, например пароль, ключи, использование протокола, таблица встречных запросов и ответов, квитирование или удаление, независимые СЕРТ АУ, информация о состоянии процедуры аутентификации, ВИАУ		
	Тип информации, используемый в процедуре аутентификации	— Предъявляемая ВИАУ — ВИАУ для обмена — Проверочная ВИАУ		
	Контрольная информация	Параметр подлинности (достоверность) Информация о состоянии процедуры аутентификации		

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ УПРАВЛЕНИЯ ДОСТУПОМ

Совместные процедуры определения разрешенных к использованию ресурсов в открытых системах ЭМВОС или Интернет-архитектуры и предотвращения несанкционированного доступа (НСД) там, где это необходимо, называются *управление доступом*. В данной главе рассмотрен общий подход к реализации СЛУД. Кроме того:

- определены общие концепции УД;
- представлен метод, в соответствие с которым базовые концепции УД могут быть использованы при обеспечении отдельных наиболее известных служб и способов УД;
- описаны такие службы и соответствующие способы УД;
- определены функциональные требования к протоколам, которые реализуют такие службы и способы УД;
- определены требования по обеспечению таких служб и способов УД;
- рассмотрено взаимодействие служб и способов УД с другими службами и способами обеспечения безопасности.

Как и в других службах обеспечения безопасности, УД может осуществляться только в рамках контекста (содержания) принятой ПЛБ для соответствующей прикладной системы.

4.1. Общие положения

4.1.1. Цель управления доступом

Основная цель УД заключается в парировании угроз, связанных с несанкционированными операциями (действиями), которые затрагивают функционирование компьютеров или систем связи. Такие угрозы, как правило, группируются в следующие классы:

- неавторизованное (несанкционированное) использование;
- раскрытие (вскрытие);
- модификация;
- разрушение;
- отказ в обслуживании.

Частными целями УД являются:

- УД процессов (которые могут функционировать от имени пользователей или других процессов) к данным, другим процессам или вычислительным ресурсам;
- УД в рамках сетевого сегмента безопасности (ССБ) или через один или несколько ССБ;
- УД в соответствии с его условиями (например зависимость от таких факторов, как время неудачной попытки доступа, размещение (местоположение) средства доступа или маршрут доступа);
- УД, которое реагирует на изменения авторизации в течение периода доступа.

4.1.2. Основные аспекты УД

В дальнейшем рассматриваются абстрактные функции УД, как правило, независящие от политик УД (ПЛУД) и системных проектов. УД в реальных системах затрагивает многие типы объектов, среди которых:

- физические объекты (например реальные системы);
- логические объекты (например объекты уровней ЭМ-ВОС или Интернет-архитектуры, файлы, организации и предприятия);
- пользователи (физические лица).

УД в реальных системах может потребовать проведения целого комплекса процедур (мероприятий). Такими процедурами являются:

- формирование структуры ПЛУД;

- определение формата данных (информации) для УД (access control information — ВИ для обеспечения УД, ВИУД-формат);
- размещение ВИУД в элементах (инициаторы, целевые объекты или запросы доступа);
- привязка ВИУД к элементам;
- преобразование вспомогательной информации, необходимой для принятия решения при УД (access control decision information — ВИПР), в форму, приемлемую для реализации (выполнения) функции принятия решения о предоставлении (отказе) доступа (access control decision function — ФПРР);
- реализация функций УД;
- изменение ВИУД (в любой момент времени после размещения соответствующей ВИУД, включая аннулирование);
- аннулирование ВИПР.

Эти процедуры могут быть разделены на две группы:

- функциональные (преобразование ВИПР в форму, приемлемую для реализации ФПРР, и выполнение ФПРР);
- обеспечивающие (все оставшиеся мероприятия).

Некоторые из процедур могут быть сгруппированы в рамках реальной системы как одна процедура по опознанию. Несмотря на то, что некоторые процедуры УД необходимо проводить прежде, чем другие, очень часто многие из них перекрывают друг друга, а некоторые процедуры могут проводиться повторно.

4.1.2.1. Реализация функций УД

На рис. 4.1 и 4.2 представлены функции, являющиеся основополагающими при УД. Другие функции могут быть необходимы в течение всей процедуры УД.

Основными объектами и функциями, привлекаемыми в процессе УД, являются инициатор (initiator), функция принуждения при УД (access control enforcement function — ФПРИ), ФПРР и целевой объект (target).

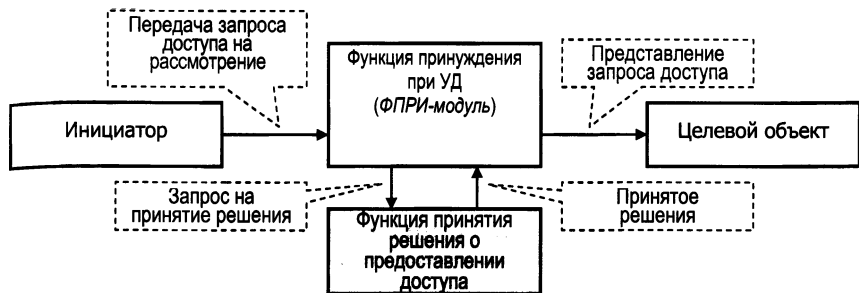


Рис. 4.1. Основополагающие функции при РД

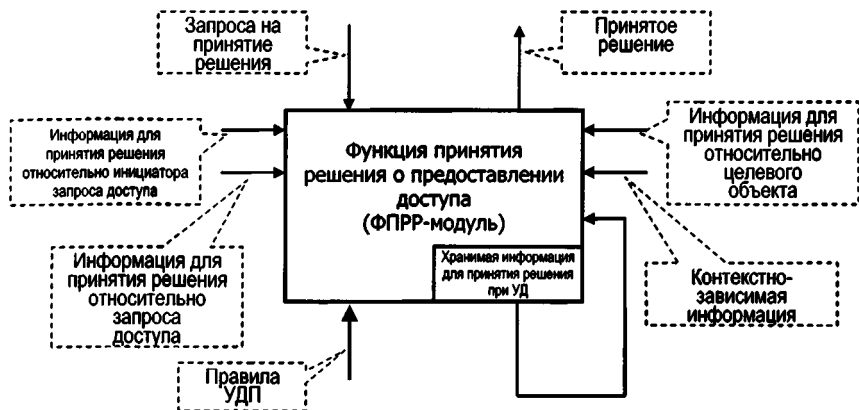


Рис. 4.2. Функция принятия решения при РД

Инициаторами могут быть пользователи (физические лица) и машинные (основанные на применении вычислительной машины) объекты (процессы), которые имеют доступ или пытаются получить доступ к целевым объектам. В реальных системах инициатором является машинный объект, несмотря на то что запросы машинного объекта на доступ от имени инициатора могут быть впоследствии ограничены ВИУД, принадлежащей машинному объекту.

Целевыми объектами являются машинные объекты (процессы) или объекты связи, по отношению к которым осуществляется попытка получения доступа или к которым инициаторы

имеют доступ. Целевым объектом может быть, например, объект уровня ЭМВОС или Интернет-архитектуры, файл или реальная система.

Запрос доступа представляет собой операции/действия и операнды (компоненты операции/действия), которые образуют субпроцедуру в процедуре (попытке) получения доступа.

ФПРИ гарантирует, что инициатору предоставляется только законный доступ к целевому объекту, на основе принятого решения, выработанного ФПРР. Когда инициатор направляет запрос на предоставление соответствующего доступа к целевому объекту ФПРИ-модуль (модуль, реализующий ФПРИ) информирует ФПРР-модуль (модуль, реализующий ФПРР) о том, что необходимо принять решение о возможности предоставления такого доступа.

С целью принятия такого решения ФПРР-модуль получает запрос доступа от инициатора (как часть запроса на принятие решения) и следующие типы ВИПР:

- информация для принятия решения относительно инициатора запроса доступа (ВИПР, извлекаемая из ВИУД, «привязанной» к инициатору);
- информация для принятия решения относительно целевого объекта (ВИПР, извлекаемая из ВИУД, «привязанной» к целевому объекту);
- информация для принятия решения относительно запроса доступа (ВИПР, извлекаемая из ВИУД, «привязанной» к запросу доступа).

Другая информация, поступающая на вход ФПРР-модуля, представляет собой правила ПЛУД (из ФПРР-модуля ЦБ ССБ; Security Domain Authority) и любую контекстно-зависимую информацию, необходимую для интерпретации ВИПР или политики. Примеры контекстно-зависимой информации включают местоположение инициатора, время доступа или соответствующий используемый маршрут соединения.

Основываясь на эту входную информацию и, возможно, на ВИПР, оставшуюся от предыдущей процедуры принятия решения, ФПРР-модуль принимает решение разрешить или отказать

инициатору в установлении доступа к целевому объекту. Затем решение направляется в ФПРИ-модуль, который либо разрешает передать запрос доступа целевому объекту, либо выполняет другие необходимые действия.

Во многих случаях успешные запросы доступа, направляемые инициатором целевому объекту, связаны между собой. Типичный пример: прикладной процесс, который устанавливает соединение с другим прикладным процессом, являющимся целевым объектом, а затем еще несколько раз пытается получить доступ, используя для этого одну и ту же (сохраняемую) ВИПР. Для некоторых успешно переданных по установленному соединению запросов доступа может понадобиться дополнительная ВИПР, которая, в свою очередь, необходима для ФПРР-модуля, который должен дать разрешение на дальнейшую доставку запроса доступа. В иных случаях ПЛБ может потребовать, чтобы некоторые связанные между собой запросы доступа между одним или несколькими инициаторами и одним или несколькими целевыми объектами могли ограничиваться. В подобных случаях с целью выработки решения относительно конкретного запроса доступа ФПРР-модуль может использовать ранее сохраненную ВИПР, которая осталась от предшествующих процедур принятия решения и касалась нескольких инициаторов и целевых объектов.

В дальнейшем полагаем, что для одного запроса доступа необходима одна итерация процедуры информационного обмена между инициатором и целевым объектом, если будет получено соответствующее разрешение от ФПРИ-модуля. Несмотря на то, что некоторые запросы доступа между инициатором и целевым объектом напрямую зависят от других запросов, очень часто возникает ситуация, при которой два объекта обмениваются несколькими связанными между собой запросами доступа, т.е. используют «запросно-ответный принцип» информационного обмена. В таких случаях инициатор и целевой объект при необходимости меняются ролями, либо одновременно, либо попеременно, и при поступлении каждого запроса доступа выполняются все функции УД, и, возможно, отдельными ФПРИ- и ФПРР-модулями и на основе разных ПЛУД.

4.1.2.2. Другие процедуры УД

Формирование структуры (формата) ПЛУД. ПЛУД, как правило, разрабатывается и официально утверждается в читабельной форме как совокупность наиболее общих принципов; например *только администраторам и менеджерам определенного ранга разрешено проверять информацию о заработной плате работников*. Переход от общих принципов к конкретным правилам относится к мероприятиям технического проектирования, которые должны предшествовать процедурам УД.

Формирование структуры (формата) ВИУД. В рамках этой процедуры делается выбор относительно формата ВИУД (структур данных) и формы информационного обмена между реальными системами (синтаксические структуры). Форматы ВИУД должны быть способны удовлетворять требованиям специфических ПЛУД. Отдельные форматы ВИУД могут быть приемлемыми и для внутреннего применения, и для использования между реальными системами. Для решения различных задач и для взаимодействия между отдельными элементами могут использоваться различные форматы ВИУД.

Выбранные форматы ВИУД могут рассматриваться как шаблоны (образцы) для назначения соответствующих значений параметров, входящих в информацию (ВИУД-параметры), для сетевых элементов в ССБ. Важным аспектом формирования структур ВИУД является определение типов и диапазонов ВИУД-параметров, которые могут назначаться сетевым элементам в ССБ (но не те, которые могут быть назначены специфическим элементам).

Для прикладных систем, соответствующих ЭМВОС или Интернет-архитектуры (и, возможно, для других), наиболее подходящей структурой ВИУД является атрибутная модель, которая включает пару значений: сам атрибут и тип атрибута.

Размещение ВИУД у инициаторов и в целевых объектах. В рамках этой процедуры (мероприятия) ЦБ ССБ, его уполномоченные (посредники) или другие объекты (например владельцы ресурсов) назначают элементам ССБ установленные для

них специфические типы атрибутов и значения этих атрибутов, входящие в состав ВИУД. Эти объекты могут определять или изменять местоположение ВИУД в соответствии с политикой обеспечения безопасности ССБ. Размещенная объектом ВИУД может быть ограничена другой ВИУД, которая была «привязана» к ней другим объектом. Размещение ВИУД в элементах ССБ является непрерывной процедурой, так как в ССБ могут появляться новые элементы.

ПРИМЕЧАНИЕ. Иногда административная процедура по разграничению «прав доступа» рассматривается как авторизация. Именно с этой точки зрения рассматривается понятие «размещение ВИУД у инициаторов и в целевых объектах».

ВИУД может представлять собой данные об одном объекте или о взаимосвязях между объектами. Размещенная у инициатора ВИУД может либо касаться только этого инициатора, либо характеризовать взаимосвязи между этим инициатором и соответствующими целевыми объектами, либо описывать связи между этим инициатором и возможным окружением. Таким образом, размещенная у инициатора ВИУД может включать ВИУД, относящуюся к инициатору, ВИУД, относящуюся к целевому объекту, или контекстно-зависимую информацию. Аналогично, размещенная в целевом объекте ВИУД может включать ВИУД, относящуюся к целевому объекту, ВИУД, относящуюся к инициатору (об одном или нескольких инициаторах), или контекстно-зависимую информацию.

В реальной процедуре ВИУД должна быть жестко «привязана» к элементу, причем так, чтобы ФПРР-модуль, который использует ВИПР, извлекаемую из «привязанной» ВИУД, был уверен в этой информации. Таким образом, несмотря на то что размещение ВИУД в элементах является необходимым предварительным условием для формирования связанной с элементом ВИУД, только ВИУД, которая «привязана» к элементу, является действительно необходимой в реальных системах.

Привязка ВИУД к инициаторам, целевым объектам и запросам доступа. Привязка ВИУД к элементу (т.е. к инициатору, целевому объекту или запросу доступа) порождает надежную

взаимозависимость между элементом и ВИУД, размещенной в этом элементе. Для функции УД и других элементов привязка обеспечивает гарантии того, что ВИУД действительно предназначена для соответствующего элемента и что невозможна какая-либо модификация, так как привязка уже выполнена. Привязка обеспечивается за счет применения службы обеспечения целостности. Возможно несколько способов привязки, включая те, которые зависят от местонахождения элемента и ВИУД, в то время как другие способы зависят от некоторых криптографических процедур формирования ЭЦП или вычисления КПС (seal). Целостность привязки ВИУД к элементам нуждается в собственной защите при ее размещении в системах инициатора и целевого объекта (например на основе доверия к функциям, реализуемым операционной системой, таким как защита файлов и разделение процессов), а также при обмене ВИУД. Так как может быть несколько структур размещаемой в элементах ВИУД (и в рамках самих систем, и между системами), то для одной и той же ВИУД могут использовать различные способы ее привязки. Кроме того, в соответствии с некоторыми ПЛБ, может обеспечиваться конфиденциальность ВИУД.

Так как в ССБ появляются новые элементы, привязка ВИУД к элементам является непрерывным процессом. ЦБ ССБ, его посредники или другие полномочные объекты могут удалять или добавлять привязки ВИУД по своему усмотрению, но в соответствии с действующей политикой обеспечения безопасности. ЦБ ССБ может изменять привязку ВИУД к элементу, как необходимое следствие изменения политики обеспечения безопасности или атрибутов. Привязанная ВИУД может включать указатели времени ее действия, что позволяет в целом минимизировать объем ВИУД, которая впоследствии может быть аннулирована.

Время, в которое осуществляется привязка ВИУД к элементу, и объект, от которого зависит применение того или иного способа привязки, определяется типом элемента. Инициаторы будут получать привязанную к ним ВИУД от ЦБ ССБ или его посредников только в тот момент времени, когда сами инициаторы будут способны организовать доступ.

Все целевые объекты будут получать привязанную к ним ВИУД от ЦБ ССБ или его посредников только тогда, когда они сами будут доступны. Целевые объекты, которые были сформированы прикладным процессом от имени пользователя или другого прикладного процесса, будут получать свою, привязанную к ним ВИУД в процессе своего формирования или после него. ВИУД, привязанная к таким целевым объектам, может быть ограничена вследствие определенных условий, содержащихся в ВИУД, привязанной к пользователю или прикладному процессу.

Пользователь или прикладной процесс осуществляют привязку ВИУД к запросу доступа. Кроме того, ВИУД, привязанная к запросу доступа, может быть ограничена вследствие определенных условий, содержащихся в ВИУД, привязанной к пользователю или прикладному процессу. Очень часто возникает ситуация, при которой запрос доступа влечет за собой необходимость формирования нового целевого объекта (например когда системы обмениваются файлами). Такая ВИУД для целевого объекта может быть определена в (или извлечена из) ВИУД, привязанной к запросу доступа.

Преобразование ВИПР в форму, приемлемую для ФПРР-модуля. Если допускает ПЛУД и если разрешено использование способа привязки, то подмножество ВИУД, привязанной к инициатору или целевому объекту, может быть отобрано инициатором или целевым объектом, для использования в ФПРР-модуле с целью принятия соответствующих решений, касающихся УД. ВИУД, привязанная к одному элементу, может быть временно привязана к другому элементу, например когда один объект действует от имени другого объекта.

Различная ВИПР (см. рис. 4.2) должна быть адаптирована для своего использования ФПРР-модулем с целью выполнения последним своих функций.

Существуют три варианта получения ВИПР, необходимой для принятия решения относительно инициатора, целевого объекта или запроса доступа:

- a) ВИПР может быть предварительно размещена в одном или нескольких компонентах ФПРР-модуля после раз-

мещения ВИУД (содержащихся в ней значений параметров);

- b)* ВИПР может быть извлечена из привязанной ВИУД, которая была доставлена для компонентов ФПРР-модуля в течение процедуры УД (возможно при попытке установления доступа);
- c)* ВИПР может быть извлечена из привязанной ВИУД, которая получена из других источников (например уполномоченный Службы единого каталога¹). Инициатор или целевой объект получают необходимую с соответствующей привязкой ВИУД (которая для ФПРР-модуля неотличима от *b*)), и ФПРР-модуль получает необходимую с соответствующей привязкой ВИУД (которая для инициатора или целевого объекта неотличима от *a*)).

Средства, с помощью которых ФПРР-модуль получает ВИУД с соответствующей привязкой, а также доставляет соответствующую ВИПР, не определены. ВИУД с соответствующей привязкой к инициатору или целевому объекту не обязательно доставляется инициатором или целевым объектом, соответственно. ВИУД с соответствующей привязкой к запросу доступа не обязательно доставляется в составе запроса доступа.

¹ Служба единого каталога (The Directory) представляет собой совокупность открытых систем, которые кооперируются с целью формирования и последующей эксплуатации логической (виртуальной) базы данных, содержащей информацию о группах объектов реального мира. Пользователи Каталога, включая физические лица и компьютерные программы, имеют возможность читать или модифицировать информацию, или ее отдельные части, если, конечно, они имеют на это разрешение. Каждый пользователь, представленный в доступном сегменте Каталога, имеет прикладной программный модуль пользователя Каталога (Directory User Agent — DUA-клиент) или прикладной программный модуль, реализующий протокол упрощенного доступа к Каталогу (Lightweight Directory Access Protocol Client — LDAP-клиент). Каталог является основой глобальной инфраструктуры открытых ключей (Public Key Infrastructure — PKI-инфраструктура), база данных которого, в частности, содержит информацию о СЕРТ открытых ключей пользователей.

ФПРР-модуль должен быть способен недвусмысленно определить, что ВИПР была извлечена соответствующим ЦБ ССБ из ВИУД, привязанной к элементам.

Изменение ВИУД. ЦБ ССБ может изменять (модифицировать) ВИУД, размещенную в элементах и привязанную к ним, если это необходимо при изменении атрибутов безопасности. ВИУД может быть изменена в любой момент времени, после ее размещения в элементах. Если такая модификация уменьшает число возможных вариантов доступа к целевому объекту, которые дозволены инициатору, то такое изменение может потребовать аннулирования ВИУД и ВИПР, извлеченной из ВИУД, которая могла быть сохранена ФПРР в ФПРР-модуле.

Аннулирование ВИПР. После аннулирования ВИУД любые попытки использования ВИПР, извлеченной из этой ВИУД, должны заканчиваться запретом на установление доступа. Дальнейшее использование ВИПР, извлеченной из аннулированной ВИУД, до ее аннулирования должно предотвращаться, а любые попытки ее использования должны заканчиваться отказом в доступе. Если доступ, основанный на такой ранее извлеченной ВИПР, продолжается, а в это время ВИУД была аннулирована, то в действительности ПЛУД может потребовать, чтобы доступ был прекращен.

4.1.2.3. Ретрансляция ВИУД

Существует общее требование в распределенных системах для объектов, которые обращаются к другим объектам с целью обеспечения доступа для них и от их имени. Объекты выступают в роли инициаторов и целевых объектов, хотя не все объекты могут исполнять обе эти роли. Один объект может быть инициатором по отношению к другому объекту и одновременно сам быть целевым объектом по отношению к третьему объекту, выступающему в роли инициатора.

На рис. 4.3 проиллюстрирована ситуация, при которой объект *А* запрашивает объект *В*, чтобы последний обеспечил доступ к объекту *С*. На этом рисунке не отображены некоторые компоненты УД, которые могли бы участвовать в процедуре установления доступа.

Существует несколько разновидностей процедуры ретрансляции ВИУД. Очевидно, что разновидности зависят от комбинации ВИУД, определяемой ПЛУД, которая обязательно должна быть представлена с целью установления порядка обработки таких последовательных (ретранслируемых) запросов доступа. Кроме того, политика обязана определять порядок обработки поступившей ВИУД, чтобы последняя была доступна для соответствующих компонентов УД. В соответствии с некоторыми политиками объекту *B* в дальнейшем может не понадобится ВИУД, которая уже привязана к нему с целью обеспечения доступа для объекта *A*. А в соответствии с некоторыми другими политиками объект *B* будет использовать только ВИУД, полученную от объекта *A*, которая очень важна для предоставления доступа, несмотря на то что в общем случае должна использоваться ВИУД, которая привязана к *A* и *B*.

Следующие примеры дают представление о диапазоне возможных разновидностей ретрансляции ВИУД:

- a)* среди наиболее простых разновидностей объект *A* может запрашивать объект *B* с целью обеспечения доступа, и при этом ВИУД, привязанная к объекту *B*, будет вполне приемлемой и достаточной для доставки запроса доступа в интересах объекта *A*;
- b)* объекту *A* может понадобиться предоставить часть или всю ВИУД, необходимую для запроса доступа, который был бы санкционирован всеми компонентами УД:
 - объект *A* может предоставить необходимую ВИУД путем ее передачи объекту *B* при запросе доступа;
 - объект *A* может запросить предварительную авторизацию у объекта *C* до того, как он запросит объект *B* обеспечить доступ. В таком случае объект *A* мог бы предоставить ВИУД объекту *C*, который, в свою очередь, мог бы в ответе передать объекту *A* соответствующий маркер доступа. Этот маркер доступа может быть передан объектом *A* объекту *B* вместе с запросом доступа. Затем объект *C* может распознать маркер доступа, как запись о предварительной авторизации.

На рис. 4.3 может быть показано произвольное число промежуточных объектов, и говоря о ФПРИ-модуле последнего целевого объекта, можно указать, что получение решения о доступе, как правило, основано на ВИУД, полученной от одного или нескольких участвующих в ретрансляции объектов.

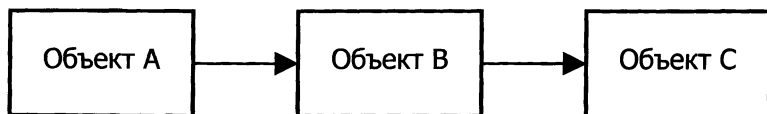


Рис. 4.3. Ретрансляция ВИУД

ПРИМЕЧАНИЕ. Разработчик ПЛУД должен осознавать, что без обеспечения промежуточных процедур УД можно предоставить доступ, который мог быть напрямую запрещен.

4.1.3. Распределение компонентов УД

ФПРИ- или ФПРР-модуль может состоять из одного или нескольких компонентов УД. Функции УД могут быть распределены между этими компонентами на основе требований ПЛУД. Рассмотренные ранее базовые функции УД не зависят от условий расположения компонентов, связей между ними или их возможного распределения.

В каждом случае ФПРИ-модуль размещается между инициатором и целевым объектом, при этом инициатор может взаимодействовать с целевым объектом только через ФПРИ-модуль. Существует несколько возможных практических реализаций ФПРИ- или ФПРР-модулей. ФПРР-модуль может быть совмещен (сильно связан) с ФПРИ-модулем или нет. ФПРР-модуль может обслуживать один или несколько ФПРИ-модулей. Аналогично, ФПРИ-модуль может использовать один или несколько ФПРР-модулей.

Совмещение (сильная связность) ФПРИ- и ФПРР-модулей может дать преимущества, касающиеся эффективности и своевременности (снижение задержки), а также может отменить

необходимую защиту соединений между ФПРИ- и ФПРР-модулями. ФПРР-модули, которые обслуживают ФПРИ-модули, могут быть полезными с точки зрения уменьшения необходимости в распределении ВИУД и реализации некоторых связанных функций по обеспечению безопасности, таких как аудит, с точки зрения снижения сложности их реализации.

Размещение компонентов может осуществляться по следующим соображениям.

4.1.3.1. УД на основе входящих запросов

ЦБ ССБ может полагать, что УД на входе целевого объекта является вполне достаточным. В этом случае ФПРИ-модуль целевого объекта «навязывает» ПЛУД на основе входящих запросов, а целевой объект не может принять запрос, который не согласуется с ПЛУД для этого целевого объекта. Это означает, что передаваемые инициатором запросы доступа будут достигать ФПРИ-модуля и становиться объектами проверки со стороны ФПРИ-модуля, который будет проверять, что они удовлетворяют ПЛУД, установленной ФПРР-модулем.

4.1.3.2. УД на основе исходящих запросов

ЦБ ССБ может полагать, что наиболее важным является парирование попыток неавторизованного доступа к целевым объектам за счет использования компонентов УД, размещенных у инициатора (например когда практическая реализация системы УД, размещенная в целевом объекте, не обладает высоким качеством или когда доступные сетевые ресурсы нецелесообразно предоставлять без первичной проверки, чтобы запрашиваемый доступ был санкционированным). В таком случае необходимо УД на основе исходящих запросов, реализуемое ФПРИ-модулем, размещенным у инициатора. В данной ситуации инициатор не может получить доступ, который не согласуется с ПЛУД, применяемой в ССБ инициатора.

4.1.3.3. Промежуточное УД

ЦБ ССБ может принять решение, что наиболее важным является фильтрация запросов доступа между инициаторами и

целевыми объектами, и в таком случае ФПРИ-модуль размещается между инициатором и целевым объектом. Впоследствии промежуточный ФПРИ-модуль может требовать исполнения обеих ПЛУД, основанных на входящих и исходящих запросах доступа. Такие ПЛУД могут быть независимы от ПЛУД, принятых в ССБ, в которых расположены инициатор и целевой объект, соответственно.

4.1.4. Распределение компонентов УД в нескольких ССБ

Возможна ситуация, при которой ССБ могут вступать в информационное взаимодействие, так как ресурсы одного ССБ могут быть доступны для другого ССБ. К процедуре УД могут привлекаться несколько ССБ, но во многих случаях не все из них будут четко выражены. Некоторые из таких ССБ предоставляют ВИУД, некоторые осуществляют контроль доступа, а некоторые делают и то и другое. Такие ССБ могут включать:

- ССБ, в котором ВИУД привязана к инициатору;
- ССБ, в котором расположен инициатор;
- ССБ, в котором ВИУД привязана к запросу доступа;
- ССБ, в котором ВИУД привязана к целевому объекту;
- ССБ, в котором расположен целевой объект;
- ССБ, в котором принимаются решения по УД;
- ССБ, в котором обеспечивают исполнение принятых решений по УД.

Процесс УД по-прежнему напоминает случай, когда все АЕФ-и ФПРР-модули находятся под управлением одного и того же ЦБ ССБ, как это было определено в § 4.1.3, но с дополнительными трудностями, вызванными взаимоотношениями между ЦБ ССБ и ССБ и связями между ССБ.

Связи (соединения) между ССБ включают:

- обмен извещениями между ЦБ ССБ и их посредниками о новых привязках ВИУД или изменениях ВИУД;

- обмен запросами в моменты попыток получения доступа с целью проверки и трансляции структур ВИУД ПЛУД и ответами на такие запросы;
- обмен запросами доступа и ответами на них.

4.1.5. Угрозы УД

ВИУД и функции УД могут быть распределены между несколькими реальными системами и ССБ. ВИУД может передаваться с использованием незащищенных средств связи, и она может управляться компонентами, функционирующими в составе различных ЦБ ССБ. Если в процедуре УД участвуют различные ЦБ ССБ, то между ними необходимы надежные взаимосвязи. Среди угроз УД можно выделить следующие:

- маскарад, устраиваемый нарушителем, пытающимся исполнить роли ФПРИ- и ФПРР-модулей;
- обход ФПРИ-модуля;
- перехват, повторная передача и модификация ВИУД или другой информации, участвующей в УД и передаваемой по другим соединениям;
- использование ВИУД другим, не имеющим на это право инициатором;
- использование ВИУД для другого целевого объекта, не предназначенной для него;
- использование ВИУД в других, не предназначенных для нее запросах доступа;
- использование ВИУД «враждебным» ФПРР-модулем;
- использование ВИУД за пределами разрешенных к ее использованию систем.

4.2. Политики УД

Политики УД отражают определенные требования к обеспечению безопасности в рамках ССБ. ПЛУД представляет собой совокупность правил, реализуемых ФПРР-модулями. Существует несколько соображений, которые могут быть учтены в

ПЛУД и в их отображении в форме правил. Одно или несколько таких соображений могут быть приемлемыми и для соответствующей ПЛБ.

ПРИМЕЧАНИЕ. Политики обеспечения безопасности, которые бы могли быть приемлемы для способов УД, но которые относятся к другим службам безопасности (например обеспечение конфиденциальности, целостности) в этом параграфе не рассматриваются.

Двумя важными и отличительными аспектами ПЛУД являются способы ее отображения и обеспечения. В большинстве случаев административно «навязываемые» ПЛУД отображаются и реализуются с использованием маркеров безопасности, в то время как ПЛУД, выбираемые пользователем, отображаются и реализуются альтернативными способами. Однако отображение ПЛУД, ее обеспечение и используемые для ее поддержки способы логически не зависят друг от друга.

4.2.1. Отображение политики УД

4.2.1.1. Категории политики УД

В главе 1 представлены две категории ПЛБ: основанные на правилах и основанные на подтверждении подлинности. ПЛУД, основанные на правилах (УДПР), предназначены для применения во всех запросах доступа, направляемых любым инициатором любому целевому объекту в рамках ССБ. ПЛУД, основанные на подтверждении (проверке) подлинности (УДПП), определяются к конкретному инициатору, группе инициаторов, объектам, действующих от имени инициаторов, или инициаторам, выполняющим специфическую роль. Окружающие обстоятельства могут изменять УДПР или УДПП. На самом деле правила окружающей среды могут определять всю политику в целом. Реальные системы обычно используют эти типы политик в различных сочетаниях. Если используется УДПР, то обычно УДПП тоже действует.

4.2.1.2. Группы и роли

ПЛУД, определенные в терминах групп инициаторов или в терминах инициаторов, выполняющих специфическую роль, являются соответствующими типами УДПП.

Под группой понимается совокупность инициаторов, члены которой в случае принудительного применения соответствующей ПЛУД рассматриваются как равноправные. Группам предоставляется доступ к соответствующим целевым объектам на основе запросов групп инициаторов, но без необходимости включения параметров подлинности конкретных инициаторов в ВИУД, привязанной к целевому объекту, и без явного размещения одной и той же ВИУД у каждого инициатора. Структура и состав группы определяется административным актом. Возможность формирования и изменения групп должны быть объектом в УД. Аудит запросов доступа, направляемых группами без распознавания членов этих групп, может быть обязательным или нет. Роль характеризуется набором функций, которые в рамках организации разрешено осуществлять пользователю. Конкретная роль может исполняться одним лицом (например директором департамента) или несколькими лицами (например банковским служащим, сотрудником отдела кредитования, членом правления).

Группы и ролевые объекты могут использоваться иерархически в различных сочетаниях объектов-инициаторов, групп и ролевых объектов.

4.2.1.3. Метки безопасности

ПЛУД, определенные в терминах меток безопасности, являются соответствующими типами УДПР. Инициаторы и целевые объекты по отдельности связаны с именными метками безопасности (например гриф секретности). Решения о предоставлении доступа основываются на сравнении меток безопасности инициатора и целевого объекта. Такие ПЛУД отображаются в правила, определяющие, какие виды доступа могут иметь место между инициаторами и целевыми объектами с конкретными метками безопасности.

Представление ПЛУД в терминах меток безопасности является весьма полезным, когда оно используется для определения формы обеспечения целостности или конфиденциальности.

4.2.1.4. ПЛУД для нескольких инициаторов

Существует много ПЛУД, которые представляются в терминах нескольких инициаторов. Такие ПЛУД могут идентифицировать либо конкретных инициаторов, либо инициаторов, которые входят в состав одних и тех же или разных групп, либо инициаторов, которые исполняют различные роли или некоторые их сочетания. Примерами таких ПЛУД для нескольких участников могут быть следующие:

- специально выделенные пользователи должны согласиться на проведение процедуры получения доступа. Очень часто инициаторы, исполняющие определенные роли, обязаны согласиться с предоставляемым доступом, например президент компании и казначей;
- два участника различных групп обязаны согласиться с предоставляемым доступом, например сотрудник компании и любой член совета директоров. В данном примере ПЛУД могла бы, скорее всего, потребовать, чтобы одни и те же пользователи не могли принадлежать к обеим группам, и поэтому параметры подлинности пользователей и взаимосвязи в группе могли быть включены в ВИПР, которая используется ФПРР-модулем;
- определенное число членов групп (может быть подавляющее большинство) обязано согласиться с предоставляемым доступом.

4.2.2. Управление политиками

Рассмотрим три аспекта из всего спектра направлений обеспечения политики.

4.2.2.1. Фиксированные политики

Фиксированными политиками являются те, которые применяются всегда и без каких-либо изменений, например по тому, что они встроены в систему.

4.2.2.2. Административно устанавливаемые политики

Административно устанавливаемыми политиками являются те, которые применяются всегда и могут быть изменены только должным образом авторизованным персоналом.

4.2.2.3. Политики, выбираемые пользователями

Политиками, выбираемыми пользователями, являются те, которые приемлемы для передачи в запросе инициатора или целевого объекта и которые применяются только при передаче запросов доступа, касающихся либо этого инициатора, либо целевого объекта, либо ресурсов этого инициатора или целевого объекта.

4.2.3. Детализация и локализация

ПЛУД могут описывать целевые объекты с различной степенью детализации. Каждый уровень детализации может иметь свою собственную логически выделенную политику и основываться на различных ФПРИ- и ФПРР-модулях (даже несмотря на то, что они могут использовать одну и ту же ВИПР). Например, доступ к серверу БД может предоставляться как единому комплексу, т.е. либо инициатору будет отказано в доступе полностью, либо ему будет разрешен доступ к компоненту сервера. В противном случае доступ может предоставляться к конкретным файлам, записям внутри файлов или даже к элементам данных внутри записей. Соответствующая БД может представлять информационную структуру каталога, УД к которой может осуществляться, либо к компонентам всего каталога, либо к отдельным элементам каталога, либо записям каталога и даже к параметрам атрибутов в записях каталога. Другим примером детализации является вычислительная си-

стема и прикладные системы в рамках этой вычислительной системы.

Локализация может использоваться для УД к группе целевых объектов на основе определения политики, которая будет разрешать доступ к этим целевым объектам, но только тогда, когда доступ разрешен к целевому объекту, который охватывает остальные объекты. Локализация может использоваться по отношению к подгруппам инициаторов, входящих в большую группу. Весьма часто понятие локализация относится к целевым объектам, которые связаны друг с другом, например файлы в БД или элементы данных в записях. В случае когда элемент входит в состав другого элемента, для инициатора необходимо прежде получить право доступа для «прохождения» «окружающего» (внешнего) элемента, а уж потом получить доступ к «окруженному» (внутреннему) элементу. Если разработчики соответствующих политик обеспечения безопасности не учитывают возможность такой ситуации, то доступ, который был запрещен одной политикой, фактически может быть разрешен другой, что означает отсутствие необходимости в таких политиках.

4.2.4. Унаследованные правила

Новый элемент может быть сформирован либо путем копирования существующего элемента, либо путем изменения существующего элемента, либо путем комбинирования существующих элементов, либо путем конструирования. ВИУД для нового элемента может зависеть от некоторых факторов, таких как ВИУД его создателя или ВИУД скопированных, модифицированных или объединенных элементов. Унаследованные правила определяют (отражают) такие факторы зависимости ВИУД даже несмотря на то, что создатель элемента в дальнейшем может сократить его ВИУД.

Унаследованные правила являются частью ПЛУД, которая определяет порядок формирования и модификации ВИУД или косвенное применение ВИУД в элементе либо основываясь на его членстве в ССБ, либо при его перемещении из одного целевого объекта в другой.

Унаследованные правила могут или не могут сами по себе наследоваться путем копирования, модификации или объединения элементов. Инициатору может быть разрешено копирование целевого объекта для своего собственного использования, но запрещено создавать его новые копии или разрешать другим инициаторам копировать или использовать его. В противном случае, когда однажды будет сделана копия, то возможно, что в дальнейшем она будет использоваться бесконтрольно.

Когда элемент содержится в другом, то часть его ВИУД (или вся) может извлекаться из ВИУД «окружающего» (внешнего) элемента в соответствии с унаследованными правилами. Такие унаследованные правила могут упрощать управление унифицированными политиками, применяемыми к большому числу элементов.

4.2.5. Приоритет среди правил ПЛУД

Существует вероятность конфликта между правилами ПЛУД. Правила приоритетности определяют порядок применения правил ПЛУД, и какие правила имеют преимущественное положение над другими. Например, если правило *A* и правило *B* из ПЛУД могут привести, каждое по отдельности, к различным результатам на основе решений, принимаемых ФПРР-модулем относительно поступающих запросов доступа, то правило приоритетности могло бы дать более высокий приоритет правилу *A*, и в таком случае правило *B* могло бы не рассматриваться. Кроме этого, правило приоритетности могло бы требовать, чтобы оба правила *A* и *B* разрешали доступ при разрешенном запросе.

Правила приоритетности могут потребоваться при использовании ограниченной инициатором ВИУД, когда инициатор выступает как член группы или в соответствующей роли. Правило приоритетности может разрешить, чтобы собственная ВИУД инициатора была объединена с ВИУД группы или исполняемой им роли. В таком случае должно быть определено, как конфликтующие АСИ-данные должны быть объединены. В противном случае правило приоритетности может требовать, чтобы при по-

ступлении соответствующего запроса доступа использовалась только ВИУД группы или ролевых объектов.

В ситуациях, когда запрос доступа «затрагивает» несколько ССБ, должны соблюдаться принципы, на основе которых формируются ПБВ.

4.2.6. Правила ПЛУД в режиме «по умолчанию»

ПЛУД может включать правила ПЛУД в режиме «по умолчанию». Такие правила могут использоваться, когда один или несколько инициаторов получают или не получают доступ к специфическому целевому объекту в неявном виде. Например, правило ПЛУД в режиме «по умолчанию» могло бы разрешить доступ к целевому объекту, если бы доступ не был запрещен в явном виде другими правилами ПЛУД, включенными в значимую ВИПР.

4.2.7. Отображение политики среди взаимодействующих ССБ

При реализации процедур УД в период обмена запросами доступа между взаимодействующими ССБ иногда возникает необходимость отображения и трансляции ВИУД, которая привязана к запросу доступа. Это может быть следствием того, что взаимодействующие ССБ имеют различные структуры ВИУД, или потому, что одна и та же ВИУД имеет различную интерпретацию, зависящую от политики обеспечения безопасности. Примерами данных, которые могут отображаться между взаимодействующими ССБ, являются:

- идентификаторы пользователей, групп или ролевого объекта (например пользователь А в ССБ Х может быть идентифицирован как пользователь ХА в ССБ Y);
- ролевые объекты и их атрибуты (например *администратор безопасности* в частной (корпоративной) сети, присоединенной к сети общего пользования, может быть

идентифицирован в сети общего пользования как *администратор безопасности присоединенной сети*);

- идентификаторы пользователей для исполнения ими конкретных ролей или для участия в группе (например все пользователи частной (корпоративной) сети могут быть исполнять в сети общего пользования роли присоединенных пользователей).

4.3. Вспомогательная информация и средства УД

4.3.1. ВИ для УД

Различные типы ВИУД включают данные об инициаторе, целевом объекте, запросе доступа, процессе, объекте обработки и контекстно-зависимые данные. ВИУД может понадобиться при взаимодействии реальных систем, которое может быть частью реализации функции УД. Когда такое информационное взаимодействие имеет место, то очень важно, чтобы взаимодействующие объекты договорились о понимании абстрактного синтаксиса.

ПРИМЕЧАНИЕ. С целью обеспечения максимальной функциональной совместимости реальных систем необходима стандартизация структуры ВИУД. Иная ВИУД, которая не нуждается в стандартизации (например хранимая ВИПР), в данном учебнике не рассматривается.

Выбор необходимой ВИУД зависит от выбранной политики обеспечения безопасности.

4.3.1.1. ВИУД об инициаторе

ВИУД об инициаторе содержит данные об инициаторе. Примеры содержания ВИУД об инициаторе:

- a) параметр подлинности пользователя для УД;
- b) идентификатор иерархической группы, членство в которой продекларировано;

- c) идентификатор функциональной группы, членство в которой продекларировано;
- d) идентификаторы ролевых объектов, которые могут быть выбраны;
- e) метки критичности;
- f) метки обеспечения целостности.

ПРИМЕЧАНИЕ. Параметр подлинности пользователя для УД не обязательно будет таким же, как и при аутентификации, аудите или загрузке. Параметр подлинности пользователя для УД является уникальным в пространстве имен, определяемом ЦБ ССБ.

4.3.1.2. ВИУД о целевом объекте

ВИУД о целевом объекте содержит данные о целевом объекте. Примеры ВИУД о целевом объекте:

- a) параметры подлинности целевого объекта для УД;
- b) метки критичности;
- c) метки обеспечения целостности;
- d) идентификатор контейнера, который транслирует данные в целевом объекте.

4.3.1.3. ВИУД о запросе доступа

ВИУД о запросе доступа содержит данные о запросе доступа. Примеры ВИУД о запросе доступа:

- a) разрешенный класс процедуры (например чтение, запись);
- b) уровень целостности, требуемый для использования процедуры;
- c) тип данных процедуры.

4.3.1.4. ВИУД об объекте обработки

ВИУД об объекте обработки содержит данные об объекте обработки в запросе доступа. Примеры ВИУД об объекте обработки:

- a) метки критичности;
- b) метки обеспечения целостности.

4.3.1.5. Контекстно-зависимая информация

Примеры контекстно-зависимой информации:

- a) периоды времени: доступ может быть предоставлен только в точно определенные периоды времени (день, неделя, месяц, год и т.д.);
- b) маршрут: доступ может быть предоставлен только в том случае, когда маршрут отвечает требуемым параметрам и характеристикам;
- c) местонахождение: доступ может быть предоставлен только инициаторам, размещенным в определенных системах, использующим определенные рабочие станции или терминалы, или только тем инициаторам, которые имеют определенное физическое местонахождение;
- d) состояние системы: доступ может быть предоставлен только при определенной ВИПР и когда система находится в соответствующем состоянии (например период восстановления после катастрофы);
- e) уровень аутентификации: доступ может быть предоставлен только тогда, когда используемые способы аутентификации имеют, по крайней мере, достаточный уровень;
- f) другие варианты доступа, которые в текущий момент времени могут быть предоставлены тем или иным инициаторам.

4.3.1.6. ВИУД, привязанная к инициатору

ВИУД, привязанная к инициатору, может включать ВИУД об инициаторе, часть ВИУД о целевом объекте и некоторые контекстно-зависимые данные. ВИУД, привязанная к инициатору, может быть представлена в форме меток безопасности, мандатов доступа и сертификатов УД (СЕРТ|УД).
Примеры:

- a) ВИУД об инициаторе;
- b) параметр подлинности для УД к целевому объекту и разрешенные варианты доступа к целевому объекту (т.е. мандат доступа);
- c) местонахождение инициатора.

4.3.1.7. ВИУД, привязанная к целевому объекту

ВИУД, привязанная к целевому объекту, может включать часть ВИУД об инициаторе, ВИУД о целевом объекте и некоторые контекстно-зависимые данные. ВИУД, привязанная к целевому объекту, может быть представлена в форме меток или списков УД. Примеры:

- a) индивидуальные параметры подлинности инициаторов для УД и разрешенные или запрещенные варианты доступа инициаторов к целевому объекту;
- b) параметры подлинности членов иерархической группы для УД и разрешенные или запрещенные варианты доступа членов группы к целевому объекту;
- c) параметры подлинности членов функциональной группы для УД и разрешенные или запрещенные варианты доступа членов группы к целевому объекту;
- d) ролевые параметры подлинности для УД и разрешенные или запрещенные варианты доступа ролевых объектов к целевому объекту;
- e) полномочные органы и варианты авторизованного доступа к ним.

4.3.1.8. ВИУД, привязанная к запросу доступа

ВИУД, привязанная к запросу доступа, может включать ВИУД об инициаторе, ВИУД о целевом объекте и контекстно-зависимые данные. Примеры:

- a) пары инициатор/целевой объект, которым разрешено участвовать в процедуре предоставления доступа;
- b) целевые объекты, которым разрешено участвовать в процедуре предоставления доступа;

- с) инициаторы, которым разрешено участвовать в процедуре предоставления доступа.

4.3.2. Защита ВИУД

4.3.2.1. Сертификаты для УД

ВИУД, которой обмениваются между собой реальные системы, требует защиты от угроз УД (§ 4.1.5). Полномочный орган (удостоверяющий центр — УЦ), который предоставил ВИУД, должен быть проверяемым на достоверность со стороны ФПРР-модуля, использующего ВИПР, извлеченную из этой ВИУД. Одним из способов обеспечения такой проверки на достоверность является размещение ВИУД в СЕРТ|ИБ, который подписывается или защищается с помощью КПС УЦ, выдавшим СЕРТ|ИБ. Такой СЕРТ|ИБ называется СЕРТ|УД.

СЕРТ|УД может содержать информацию в различных форматах. Большинство из защищаемых СЕРТ|ИБ рассматриваются в главе 2.

Следующие элементы данных, характеризующие инициатора, могут быть включены в СЕРТ|УД:

- ВИУД об инициаторе;
- способ проверки подлинности привязки СЕРТ|УД к определенному инициатору, и при этом такой, что им не мог бы воспользоваться другой инициатор;
- идентификатор клиента, которому может быть предоставлен (разрешен) доступ;
- идентификаторы объектов, которые являются ответственными за предоставление доступа при проведении процедур отчетности или аудиторских проверок;
- число процедур запроса доступа, при которых инициатор может воспользоваться СЕРТ|УД.

Следующие элементы данных, характеризующие целевой объект, могут быть включены в СЕРТ|УД:

- ВИУД о целевом объекте;

- способ проверки подлинности привязки СЕРТ|УД к определенному целевому объекту, и при этом такой, что им невозможно было воспользоваться в процедуре запроса доступа к другому целевому объекту;
- число процедур запроса доступа, при которых соответствующий инициатор может воспользоваться СЕРТ|УД.

Следующие элементы данных, характеризующие запрос доступа, могут быть включены в СЕРТ|УД:

- способ проверки подлинности привязки СЕРТ|УД к определенному запросу доступа, и при этом такой, что им невозможно было воспользоваться в другом запросе доступа;
- способ проверки подлинности привязки СЕРТ|УД к одному или нескольким запросам доступа, и при этом такой, что им можно было воспользоваться в других запросах доступа (например при ретрансляции запроса доступа);
- число процедур запроса доступа к соответствующему целевому объекту, при которых может использоваться СЕРТ|УД;
- ВИУД о запросе доступа.

4.3.2.2. Маркеры УД

Другим наиболее общим средством защиты ВИУД является размещаемый внутри этой информации маркер безопасности (security token). Маркер безопасности, в отличие от СЕРТ|УД, который может быть подписан или защищен с помощью КПС УЦ, может формироваться инициатором. В случае УД маркер безопасности непосредственно касается ВИУД, привязанной к запросу доступа.

СЕРТ|УД может быть получен из УЦ и использоваться в нескольких процедурах запросах доступа. Однако инициатор может сформировать маркер безопасности для привязки СЕРТ|УД к конкретному запросу доступа.

Маркер безопасности может включать информацию в различных форматах. Большинство из защищаемых маркеров безопасности рассматриваются в главе 2.

Одни и те же элементы данных о конкретном инициаторе, целевом объекте и запросе доступа, которые могут входить в состав СЕРТ|УД, могут быть включены в состав маркера безопасности.

4.3.3. Средства УД

Далее рассматриваются средства УД, которые могут быть использованы при выполнении процедур УД в реальных системах. Типовое описание средств УД указывает на то, что они не зависят от конкретных способов. Примитивы конкретных интерфейсов, используемых в реальных системах, не определены.

ПРИМЕЧАНИЕ. Несмотря на то что средства УД определены с наиболее общих позиций, их смысл заключается в том, чтобы продемонстрировать один общий подход к обеспечению службы УД среди других возможных подходов, которые в дальнейшем не рассматриваются.

Средства УД (рис. 4.4) разделяются на два основных класса, то есть те, которые:

- могут привлекаться к вспомогательным (обеспечивающим) процедурам, например администратором по безопасности. Такие средства обеспечивают «привязку» ВИУД к элементам, модификацию ВИУД и ее аннулирование;
- непосредственно связаны с функциональной процедурой УД. Такие средства обеспечивают доступность ВИПР для ФПРР-модуля, реализацию (выполнение) функций УД.

Если различные существующие системы или ССБ используют различные форматы ВИУД, то необходимы дополнительные средства для отображения АСИ-форматов между собой.

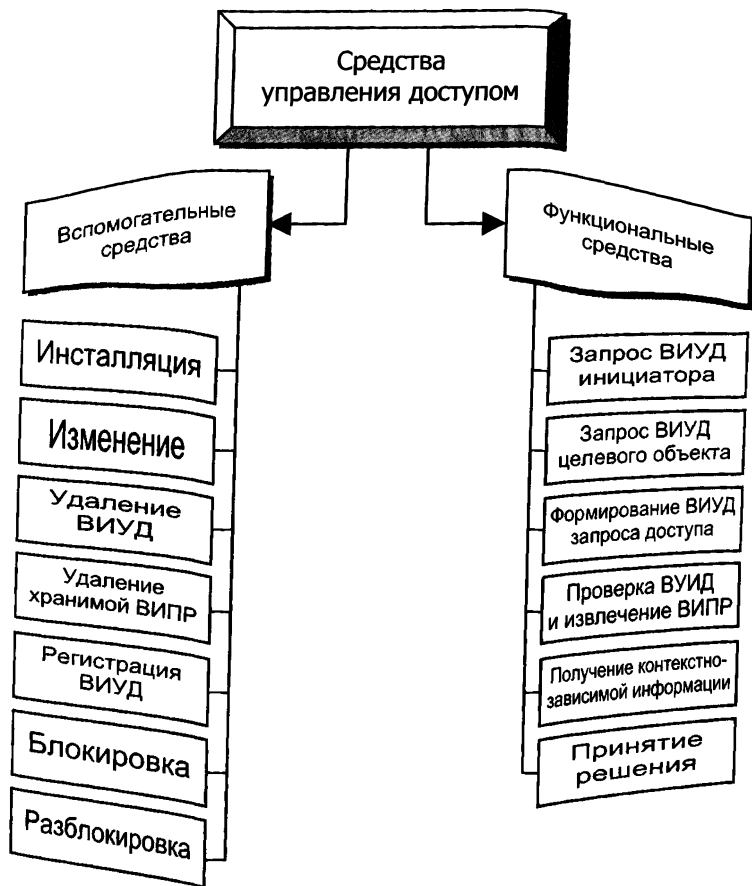


Рис. 4.4. Средства, используемые в процедурах УД

4.3.3.1. Вспомогательные (обеспечивающие) средства УД

Процедуры УД, связанные с формированием ПЛУД и структур ВИУД и размещением последних в элементах, в данном пособии не рассматриваются. Средство инсталляции ВИУД касается привязки ВИУД к элементам. Средства изменения и удаления ВИУД затрагивают процедуры модификации и аннулирования ВИУД. Средства блокировки и разблокировки

компонентов УД и регистрации ВИУД элементов являются дополнительными.

Средство инсталляции (install ACI). Это средство привязывает начальный набор ВИУД (например, мандаты доступа, используемые инициаторами, маркеры безопасности, используемые инициаторами и целевыми объектами, и перечни (списки) УД для целевых объектов) к элементу.

Средство изменения (change ACI). Это средство модифицирует (например добавляет или удаляет элементы данных) ВИУД, привязанную к элементу.

Средство удаления ВИУД (revoke ACI). Это средство удаляет (аннулирует) используемую ВИУД, привязанную к элементу, причем так, что в дальнейшем эта ВИУД больше не имеет никакого отношения к этому элементу. Это основное отличие от средства изменения ВИУД, так как в данном случае любая ВИПР, связанная с ВИУД, тоже уничтожается.

Средство удаления хранимой ВИПР (revoke retained ADI). Это средство аннулирует юридическую силу (значимость) хранимой ВИПР.

Средство регистрации ВИУД (list ACI). Это средство регистрирует специфическую ВИУД, привязанную к данному элементу.

Средство блокировки компонента (disable component). Это средство блокирует использование компонента, реализующего ту или иную функцию УД. В случае ФПРИ-модуля, средство запрещает предоставление всех видов доступа через этот ФПРИ-модуль (это предотвращает любые попытки доступа к целевым объектам, обслуживаемым только этим ФПРИ-модулем).

Средство разблокировки компонента (re-enable component). Это средство снимает запрет на использование компонента, реализующего ту или иную функцию УД.

4.3.3.2. Функциональные средства УД

Предполагается, что функциональные средства используются в качестве следующих (но не каждая процедура УД будет использовать все указанные далее итерации):

- а) инициатор первого в своей деятельности запроса доступа определяет ЦБ ССБ, но только для тех элементов, в деятельности которых используются средства идентификации доверенных ЦБ;
- б) формирование политики безопасного информационного взаимодействия для ее использования в своей основной деятельности;
- в) ВИУД привязывается к элементам, используя средства запроса и формирования ВИУД;
- г) формирование ВИПР, доступной для ФПРР-модуля, на основе использования средств проверки привязанной ВИУД и извлечения ВИПР;
- д) контекстно-зависимая информация, если она востребована политикой безопасного информационного взаимодействия, приобретаетс с помощью средства получения контекстно-зависимой информации;
- е) решение по УД принимается с помощью средства принятия решения о предоставлении доступа.

Многие из рассматриваемых средств УД допускают применение защищенной ВИУД (с целью обеспечения гарантий целостности и конфиденциальности в соответствии с требованиями политики обеспечения безопасности).

Запрос ВИУД, привязанной к инициатору. Это средство (acquire initiator-bound ACI), активизируемое инициатором или ФПРР-модулем, получает либо ВИУД, привязанную к инициатору, либо СЕРТИУД, либо маркер УД, содержащий ВИУД, привязанную к инициатору, до момента отправки запроса доступа.

Входные данные могут быть следующие:

- аутентифицированный параметр подлинности инициатора (получен средством проверки, как определено в главе 2);
- критерий отбора ВИУД, привязанной к инициатору; время действия;
- параметр подлинности целевого объекта или группы целевых объектов;
- ПБВ.

Выходные данные могут быть следующие:

- состояние (положительный или отрицательный результат выполнения запроса средством запроса ВИУД, привязанной к инициатору);
- либо ВИУД, привязанная к инициатору, либо СЕРТ|УД, либо маркер УД, содержащий ВИУД, привязанную к инициатору.

Запрос ВИУД, привязанной к целевому объекту. Это средство (acquire target-bound ACI), активизируемое ФПРР-модулем, получает ВИУД, привязанную к целевому объекту.

Входные данные могут быть следующие:

- параметр подлинности целевого объекта;
- критерий отбора ВИУД, привязанной к целевому объекту;
- время действия;
- ПБВ.

Выходные данные могут быть следующие:

- состояние;
- ВИУД, привязанная к инициатору.

Формирование ВИУД, привязанной к запросу доступа. Это средство (generate access request-bound ACI), активизируемое инициатором, формирует привязку ВИУД, привязанной к инициатору, ВИУД о запросе доступа и ВИУД, привязанной к объекту обработки, к запросу доступа, который необходим для принятия решения при УД.

Входные данные могут быть следующие:

- ВИУД, привязанная к инициатору (СЕРТ|УД, содержащий ВИУД, привязанную к инициатору, или хранимая ВИПР);
- ВИУД, привязанной к объекту обработки;
- параметр подлинности целевого объекта;
- время действия;
- ПБВ.

Выходные данные могут быть следующие:

- состояние;
- ВИУД, привязанная к запросу доступа;
- маркер УД;
- СЕРТ|УД (сформированный ЦБ ССБ от имени инициатора);
- хранимая ВИПР.

ПРИМЕЧАНИЕ. Первый запрос из последовательности запросов доступа может содержать хранимую ВИПР, которая может использоваться вместо ВИУД, привязанной к инициатору.

Проверка привязанной ВИУД и извлечение ВИПР. Это средство (verify bound ACI and derive ADI), активизируемое ФПРР-модулем, осуществляет проверку подлинности привязанной ВИУД и извлечение из нее ВИПР. В тех случаях, когда часть или вся ВИПР предварительно записывается в память в ФПРР-модуле, эта услуга могла быть дополнена или замещена извлечением предварительно сохраненной ВИПР.

Входные данные могут быть следующие:

- привязанная ВИУД (к инициатору, целевому объекту, запросу доступа или объекту обработки);
- маркер УД;
- СЕРТ|УД;
- процедуры и объекты обработки;
- время действия;
- ПБВ.

Выходные данные могут быть следующие:

- состояние;
- процедуры и объекты обработки;
- ВИПР (об инициаторе, целевом объекте, запросе доступа или объекте обработки).

Получение контекстно-зависимой информации. Это средство (get contextual information), активизируемое инициатором или ФПРР-модулем, обеспечивает получение контекстно-

зависимой информации, необходимой для принятия решение при УД.

Входные данные могут быть следующие:

- процедуры и объекты обработки;
- требуемая контекстно-зависимая информация;
- ПБВ.

Выходные данные могут быть следующие:

- состояние;
- контекстно-зависимая информация.

Принятие решения о предоставлении доступа. Это средство (decide access), активизируемое ФПРР-модулем, определяет, разрешен ли доступ или нет.

Входные данные могут быть следующие:

- процедуры и объекты обработки;
- ВИПР об инициаторе;
- ВИПР об объекте обработки;
- ВИПР о целевом объекте;
- контекстно-зависимая информация;
- сохраняемая ВИПР;
- ПБВ.

Выходные данные могут быть следующие:

- решение о предоставлении доступа;
- период действия принятого решения;
- последовательность разрешенных запросов доступа;
- сохраняемая ВИПР.

4.4. Классификация способов УД

4.4.1. Введение

Способ УД включает схему УД (например основанную на перечнях УД, мандатах доступа, метках и контексте) и обеспечивающие процедуры, формирующие ВИПР для ФПРР-

модуля в рамках этой схемы. Существует несколько схем УД, описываемых в терминах ВИУД, которую необходимо хранить в различных объектах (преимущественно у инициатора или в целевом объекте), и общих обеспечивающих способов, используемых средством принятия решения о предоставлении доступа.

Далее рассматривается большинство категорий, относящихся к схемам и способам УД. Различные схемы имеют свои преимущества и недостатки. Типовые схемы УД, которые могут быть представлены в терминах ВИУД, привязанной к инициатору и целевому объекту, следующие:

- a) если предположить, что ВИУД, привязанной к инициатору, является набор пар (параметр подлинности целевого объекта и тип процедуры), а ВИУД, привязанной к целевому объекту, являются параметры целевого объекта, то в соответствии с ПЛУД получаем мандатную схему УД (capability scheme);
- b) если предположить, что ВИУД, привязанной к инициатору, является «разрешение» («clearance»), а ВИУД, привязанной к целевому объекту, является «классификация» («classification»), то в соответствии с ПЛУД получаем схему УД на основе меток безопасности (label-based scheme);
- c) если предположить, что ВИУД, привязанной к инициатору, является параметр подлинности инициатора, а ВИУД, привязанной к целевому объекту, является набор пар (параметр подлинности инициатора и тип процедуры), то в соответствии с ПЛУД получаем схему УД, основанную на перечне (списке) доступа (access control list scheme);
- d) правила, описывающие контекстно-зависимую информацию, очень часто используются вместе с другими схемами УД, но они могут использоваться самостоятельно при формировании схемы УД, основанной на контекстно-зависимой информации (контекстная схема). Такая информация может быть частью ВИУД, привязанной к

инициатору, ВИУД, привязанной к запросу доступа, или ВИУД, привязанной к целевому объекту, либо она может быть сформирована для использования ФПРР-модулем независимо от другой ВИУД.

Весьма легко разработать более сложные варианты типовой схемы *a*), в которых параметр подлинности целевого объекта становится типом целевого объекта, включающим уже несколько целевых объектов, обладающих соответствующим атрибутом «тип», что обеспечивает более широкое применение мандата доступа. Всего лишь небольшое дополнение к рассмотренному атрибуту «тип», т.е. «разрешение» («clearance»), которое сравнивается с маркером безопасности, приводит к типовой схеме *b*). Аналогично, каждая из первых трех схем может рассматриваться как вариант соседствующей с ней схемы. Каждая схема может рассматриваться как элемент среди различных элементов непрерывного множества, в котором схемы частично перекрывают друг друга и не являются полностью различными.

Когда имена инициаторов расположены в целевых объектах и используются как ВИУД, привязанная к целевым объектам (например записи в списке УД), то каждодневная актуализация ВИУД, привязанной к целевым объектам, будет весьма обременительна в тех системах, в которых состав инициаторов постоянно изменяется. И наоборот, когда имена целевых объектов хранятся у инициаторов и используются как ВИУД, привязанная к инициаторам (например в мандатах доступа), то каждодневная актуализация ВИУД, привязанной к инициаторам, тоже будет весьма обременительна в тех системах, в которых состав целевых объектов постоянно изменяется.

Более того, очевидно, что обеспечение УД является фактором, который будет оказывать влияние на выбор структуры политики, и поэтому определить стандарт для всех систем, основываясь на том или ином способе, невозможно. Реальная система, исходя из различных целей ее функционирования, скорее всего потребует несколько схем УД.

4.4.2. Схема УД на основе списков доступа

4.4.2.1. Основные свойства

Основные свойства схемы УД на основе списков доступа (УДСД) следующие:

- a)* УД обеспечивается с помощью перечня (списка) пар (определитель инициатора, определитель процедуры), являющегося ВИУД, привязанной к целевому объекту, и с помощью идентификаторов пользователя, группы или ролевого объекта, являющихся ВИУД, привязанной к инициатору;
- b)* этот класс схем УД является наиболее приемлемым там, где требуется очень точная детализация УД;
- c)* этот класс схем УД является наиболее приемлемым там, где имеет место несколько инициаторов или групп инициаторов;
- d)* этот класс схем УД является наиболее приемлемым для аннулируемого доступа к целевому объекту или группе целевых объектов;
- e)* этот класс схем УД является наиболее приемлемым там, где обеспечение УД осуществляется скорее на основе модели обеспечения доступа к каждому целевому объекту, чем на основе модели предоставления доступа каждому инициатору;
- f)* этот класс схем УД является неприемлемым там, где совокупность пользователей или группы инициаторов изменяются очень часто, но наиболее приемлем там, где группы целевых объектов являются динамическими.

4.4.2.2. ВИУД

ВИУД, привязанная к инициатору. Основой ВИУД, привязанной к инициатору, в УДСД является идентификатор пользователя, группы или ролевого объекта.

ВИУД, привязанная к целевому объекту. Основой ВИУД, привязанной к целевому объекту, в УДСД является список (пе-

речень) УД, который представляет собой набор или последовательность записей. Каждая запись содержит два поля:

- а) определитель инициатора.* В простом списке УД определитель представляет собой УИД инициатора, для которого представлен определитель операции (процедуры). Однако определитель инициатора может быть менее специфическим и представлять собой более общую ВИУД об инициаторе, например его роль или членство в группе;
- б) определитель операции (процедуры).* Он определяет процедуры или классы процедур (в запросе доступа), которые разрешены или запрещены для конкретного определителя инициатора.

ПРИМЕЧАНИЕ. Кроме процедур или классов процедур могут налагаться ограничения на параметры объекта процедуры (операнда) с целью уточнения условий предоставления доступа.

4.4.2.3. Способы обеспечения

Для получения ВИУД, привязанной к инициатору, из которой в дальнейшем извлекается необходимая для средства принятия решения о предоставлении доступа ВИПР, могут использоваться два способа:

- а) использование аутентификации.* Если УД основано на параметре подлинности инициатора (пользователя), то подлинность такого параметра может быть подтверждена с помощью процедуры аутентификации либо непосредственно, либо косвенно. Если УД основано на групповом параметре подлинности или параметре подлинности ролевого объекта, то аутентифицированным параметром подлинности является параметр, содержащийся в средстве запроса ВИУД, привязанной к инициатору, которое используется для получения достоверных данных о группе или ролевом объекте;
- а) использование СЕРТ\УД или маркеров УД.* Инициатор получает СЕРТ\УД или маркер УД (или оба) с использова-

нием средства запроса ВИУД. Такой СЕРТ|УД или маркер УД в дальнейшем является «привязкой» к запросу доступа, сгенерированному инициатором с использованием средства формирования ВИУД, привязанной к запросу доступа. И в заключение СЕРТ|УД или маркер УД проверяется ФПРР-модулем с использованием средства проверки привязанной ВИУД и извлечения ВИПР.

Доступность УЦ, указанного в СЕРТ|УД, или инициатора в случае маркера УД определяется в рамках процедуры проверки привязанной ВИУД и извлечения ВИПР.

ВИПР об инициаторе (например идентификаторы пользователей, групп пользователей или ролевых объектов), ВИПР о запросе доступа и ВИПР о целевом объекте (например определитель запроса доступа) являются параметрами, используемыми средством принятия решения о предоставлении доступа. Используя приемлемый алгоритм сравнения, извлеченные из запроса доступа ВИПР об инициаторе и тип процедуры (операции) сравниваются с каждой записью (определитель инициатора, определитель запроса доступа) в списке (перечне) УД. Решение о предоставлении доступа принимается на основе результатов сравнения. Если обнаружено, что доступ запрещен, или сравнение выявило несовпадение, то принятое решение указывает на то, что в доступе отказано. В противном случае принятое решение указывает на то, что доступ может быть предоставлен.

4.4.2.4. Варианты УДСД

Упорядоченные списки УД. В некоторых списках УД, использующих последовательности записей, существует правило поиска, при котором в случае нахождения первой соответствующей записи поиск прекращается. Поэтому упорядочивание таких списков УД является очень важным процессом, так как допускает прямое установление политик, в соответствие с которыми конкретным инициаторам может быть отказано в доступе, даже в случае применения других более общих процедур сравнения, например инициаторам в группе и имеющим право доступа инициаторам.

Списки УД с инициаторами, объединенными в группы. Информация в списках УД может быть структурирована для отражения совокупности схожих прав доступа для некоторой группы инициаторов. Кроме этого, когда сами целевые объекты объединены в группы, список УД может быть связан с такими группами. Иерархия списков УД может использоваться для списков УД верхнего уровня, «разбивающих» информацию для УД на крупные массивы и предназначенных для большой группы целевых объектов, которые могут быть заменены списками УД для подгрупп целевых объектов.

Списки УД с определителем целевого объекта. Такое дополнение имеет значение там, где список УД не связан с определенным целевым объектом. Целевой объект должен быть определен в каждой записи списка УД. Записи в списке УД имеет форму тройного определителя, состоящего:

- из определителя инициатора;
- из определителя запроса доступа;
- из определителя целевого объекта.

Алгоритм проверки сравнивает ВИУД об объекте, запрашиваемом доступе и целевом объекте с каждой строкой списка УД, содержащей определители инициатора, процедуры и целевого объекта.

Списки УД с целевыми объектами, объединенными в группы. Данное дополнение применяется при совместном использовании одного списка УД среди нескольких целевых объектов, и при этом решения, принимаемые на основании одного списка УД, касаются нескольких целевых объектов. Когда относительно одного целевого объекта принимается решение на основе критерия, включающего данные из нескольких списков УД, то ПЛУД, устанавливающая способ УДСД, должна определять правило, необходимое для комбинированного принятия решений.

Списки УД с определителем контекстно-зависимых данных. Это дополнение применяется при использовании контекстно-зависимой информации. Записи в списке УД имеет форму тройного определителя, состоящего:

- из определителя инициатора;
- из определителя запроса доступа;
- из определителя контекстно-зависимой информации.

Определитель контекстно-зависимой информации является дополнительным определителем, который устанавливает ограничения на контекстно-зависимую информацию в конкретной записи. Средство проверки по определенному алгоритму сравнивает ВИУД об объекте, запрашиваемом доступе и контекстно-зависимой информации с каждой строкой списка УД, содержащей определители инициатора, запроса доступа и контекстно-зависимой информации.

Списки УД с частичным сравнением. В некоторых прикладных системах используется частичное сравнение определителей, т.е. в них сравниваются части параметров подлинности или другая ВИУД об инициаторе с определителем инициатора. Например, если инициатор имеет имя, сформированное из иерархической последовательности компонентов имен (таких как страна, организация, подразделение организации, персональное имя), то список УД может быть сформирован так, чтобы определять один или несколько компонентов, которые могут рассматриваться как группа параметров подлинности.

Списки УД без определителя запроса доступа. В некоторых вариантах УДСД наборы или последовательности записей в списке УД могут не включать определители запросов доступа. В таких случаях средство принятия решения о предоставлении доступа не использует определитель запроса доступа. Если доступ для инициатора разрешен, то он будет разрешен для всех запросов доступа.

4.4.3. Мандатная схема

4.4.3.1. Основные свойства

Основные свойства мандатной схемы следующие:

- а) УД обеспечивается на основе ВИУД, привязанной к инициатору (мандат доступа), которая определяет совокуп-

ность разрешенных процедур по отношению к определенной группе целевых объектов;

- b)* этот класс схем УД является наиболее приемлемым там, где имеет место несколько целевых объектов;
- c)* этот класс схем УД неприемлем для аннулирования доступа к целевому объекту на стороне этого объекта, но он обеспечивает возможность индивидуальной идентификации мандатов доступа, ранее выданных инициатору. Но он приемлем для ЦБ ССБ инициатора, который может аннулировать права доступа этого инициатора;
- d)* этот класс схем УД является наиболее приемлемым там, где обеспечение УД осуществляется инициаторами;
- e)* мандаты доступа наиболее приемлемы там, где имеет место «много» пользователей или «много» групп пользователей, запрашивающих доступ к «небольшому числу» целевых объектов, а целевые объекты и пользователи размещаются в различных ССБ.

ПРИМЕЧАНИЕ. Применение паролей для УД аналогично применению мандатов доступа, но имеет свои особенности. К основным свойствам применения паролей относятся:

- УД основано на ВИУД, используемой совместно инициатором и целевым объектом;
- УД зависит от конфиденциальности ВИУД при ее хранении у инициатора и целевого объекта, а также при ее доставке (очень часто обеспечение конфиденциальности паролей является весьма трудной задачей);
- обмен паролями может быть весьма трудным, если несколько инициаторов пользуются одним и тем же паролем.

4.4.3.2. ВИУД

ВИУД, привязанная к инициатору. ВИУД, привязанная к инициатору, представляет собой совокупность мандатов доступа. Мандат доступа имеет следующие два основных компонента:

- a)* наименование целевого объекта или группы целевых объектов;

- b)* перечень процедур, которые являются авторизованными по отношению к целевому объекту.

Мандаты доступа могут доставляться в составе СЕРТ|УД, подписанных или защищенных с помощью криптографической проверочной суммы УЦ ССБ.

ВИУД, привязанная к целевому объекту. ВИУД, привязанная к целевому объекту, представляет собой совокупность записей. Каждая запись включает следующие два компонента:

- a)* параметр подлинности ЦБ ССБ;
- b)* процедуры, которые могут быть авторизованы ЦБ ССБ.

4.4.3.3. Способы обеспечения

Инициатор получает СЕРТ|УД или маркер УД с использованием средства запроса ВИУД, привязанной к инициатору. В дальнейшем СЕРТ|УД или маркер УД «привязывается» к запросу доступа, передаваемому инициатором, с использованием средства формирования ВИУД, привязанной к запросу доступа. И в заключение СЕРТ|УД или маркер УД проверяется ФПРР-модулем с использованием средства проверки привязанной ВИУД и извлечения ВИПР.

ВИПР об инициаторе (т.е. содержание мандата доступа), наименование процедуры и ВИПР о целевом объекте являются параметрами, используемыми средством принятия решения о предоставлении доступа. ВИПР о целевом объекте сравнивается с одним из наименований целевого объекта, указанного в мандате доступа, а также сравнивается название процедуры с одним из тех, которое содержится в мандате доступа. Если все проверки совпали (дали положительный результат), то доступ считается разрешенным.

Средство принятия решения о предоставлении доступа отказывает в доступе, если:

- a)* предъявленный мандат доступа является недействительным;
- b)* доступ к целевому объекту основан на применении неразрешенных ЦБ ССБ процедур (т.е. ЦБ ССБ запретил применение таких процедур);

- с) наименование процедуры, указанной в запросе доступа, не совпало с наименованием, содержащимся в мандате доступа.

4.4.3.4. Вариант схемы мандатного доступа – мандаты доступа не содержат определенных процедур

При таком варианте схемы в мандате доступа отсутствует набор разрешенных процедур, а в средстве принятия решения о предоставлении доступа отсутствует название процедуры. В таком случае, если доступ инициатору разрешен, то разрешены все процедуры доступа.

4.4.4. Схема на основе меток безопасности

4.4.4.1. Основные свойства

Основные свойства схемы УД на основе меток безопасности (УДМБ) следующие:

- a)* эта схема основана на применении меток безопасности, которые могут быть выделены инициаторам и целевым объектам, и данных, транслируемых между системами;
- b)* эта схема УД является наиболее приемлемой там, где имеет место много инициаторов, запрашивающих доступ ко многим целевым объектам, и там, где необходимо обеспечить УД к большим ССБ;
- с)* эта схема, при условии наличия определенных ограничений в соответствии с ПЛБ, может использоваться для управления потоком данных в рамках ССБ. Кроме того, метки безопасности могут быть вполне приемлемы для предоставления доступа между ССБ;
- d)* ВИУД, привязанная к инициатору или целевому объекту, не содержит в явном виде наименования разрешенных процедур, но последние являются частью политики обеспечения безопасности.

ПРИМЕЧАНИЕ:

- метки не обязательно имеют простые форматы (структуры);
- когда инициатор является пользователем (или процесс инициатора, представляющего пользователя), метка, «привязанная» к инициатору, часто именуется «разрешение».

4.4.4.2. ВИУД

ВИУД, привязанная к инициатору. ВИУД, привязанная к инициатору, представляет собой метку безопасности.

ВИУД, привязанная к целевому объекту. ВИУД, привязанная к целевому объекту, представляет собой метку безопасности.

ПРИМЕЧАНИЕ. Структура (формат) ВИУД, привязанной к инициатору, и ВИУД, привязанной к целевому объекту, обычно определяются средством и/или способом их обработки. Однако одну и ту же структуру (формат) не обязательно использовать дважды. При передаче вспомогательной информации для обеспечения безопасности может использоваться другая структура (формат), которая рассматривается в главе 2.

ВИУД, привязанная к объекту процедуры. Объекты процедур в запросе доступа могут иметь метки, привязанные к ним. Объекты процедур с метками безопасности представляют собой частный случай помеченных данных.

Помеченные данные должны гарантированно обладать следующими двумя свойствами:

- целостность «привязки» метки к данным;
- право инициатора на формирование данных с такой меткой.

Применение меток безопасности, при условии наличия определенных ограничений в соответствии с ПЛБ, может использоваться для реализации единого УД к данным в границах ССБ или между такими сегментами.

Примеры помеченных данных следующие:

- документы;
- сообщения;
- элементы данных при использовании ПИНО без установления соединения;
- файлы в период их доставки.

4.4.4.3. Обеспечивающие способы

Для получения ВИУД, привязанной к инициатору или объекту процедуры, которая необходима для средства принятия решения о предоставлении доступа, могут использоваться следующие четыре способа:

- а) использование СЕРТ|УД и маркеров УД.* Инициатор получает СЕРТ|УД или маркер УД (или оба) с использованием средства запроса ВИУД. Такой СЕРТ|УД или маркер УД в дальнейшем является «привязкой» к запросу доступа, сгенерированному инициатором с использованием средства формирования ВИУД, привязанной к запросу доступа. И в заключение, СЕРТ|УД или маркер УД проверяется ФПРР-модулем с использованием средства проверки привязанной ВИУД и извлечения ВИПР. Доступность УЦ, указанного в СЕРТ|УД, или инициатора в случае маркера УД определяется в рамках процедуры проверки привязанной ВИУД и извлечения ВИПР;
- б) использование аутентификации и поиск.* ФПРР-модуль получает параметр подлинности аутентифицированного инициатора и использует его при поиске разрешения для этого инициатора;
- в) использование помеченного канала.* Разрешение, данное инициатору, или метка данных, может быть следствием метки канала, который использовался для доставки запроса доступа. Целостность «привязки» метки к каналу может быть гарантирована на основе привлечения службы обеспечения целостности. Гарантии того, что канал был предоставлен корректно, могут быть обеспечены доверенным провайдером службы установления соедине-

ний, и тем, что они могут быть проверены. Аналогично, гарантии могут быть обеспечены тем, что целевой объект был авторизован для признания надежности канала, который был предоставлен доверенным провайдером службы установления соединений, и тем, что авторизация целевого объекта может быть проверена перед установлением соединения;

d) использование помеченных данных. Разрешение, данное инициатору, может быть следствием меток объектов процедур (операндов), содержащихся в запросе доступа. Целостность «привязки» метки к данным может быть обеспечена либо целостностью основного канала доставки, либо использованием кода проверки целостности или цифровой подписи, сформированной ЦБ ССБ по всей последовательности данных, включая метку безопасности.

Метка безопасности может использоваться как ВИУД о целевом объекте с целью защиты этого объекта. Правила доступа описывают полномочия (процедуры), предоставляемые инициатору его меткой безопасности и меткой безопасности, назначенной целевому объекту.

Если ПЛБ устанавливает, что содержащаяся в метке безопасности ВИУД использовалась в ВИУД о целевом объекте, то оба потока данных (входящий в целевой объект и исходящий от него) могут быть полностью контролируруемыми. Отсюда следует, что оба потока данных могут анализироваться в ССБ, в которых применяется одна и та же ПЛБ.

Целевые объекты могут быть сформированы «внутри» других целевых объектов. Метка безопасности «внутреннего» целевого объекта ограничивает метки безопасности, которые могут быть назначены «внешнему» целевому объекту, в соответствии с правилами применяемой ПЛБ.

Примеры целевых объектов, в отношении которых могут использоваться метки, следующие:

- объекты *N*-уровня ЭМВОС или Интернет-архитектуры;
- объекты Службы единого каталога (Directory Service);

- файлы, находящиеся в хранилище файлов;
- записи в БД.

4.4.4.4. Помеченные каналы/соединения как целевые объекты

Организатор канала/соединения (например ЦБ ССБ) присваивает метку безопасности каналу/соединению. Для того чтобы канал использовался по назначению, ВИУД об инициаторе и метка безопасности, присвоенная каналу/соединению, должны быть входными данными средства принятия решения о предоставлении доступа, т.е. канал/соединение рассматривается (трактруется) как целевой объект. Метки данных, транслируемых по каналу/соединению, должны быть согласованы с меткой канала/соединения.

Метка, присваиваемая каналу/соединению, также может использоваться для контроля маршрута доставки. С точки зрения ЭМВОС или Интернет-архитектуры, объекты N -уровня и ретрансляционные системы получают доступ к соединениям $(N-1)$ -уровня или информационному каналу $(N-1)$ -уровня без установления соединения. Таким образом, объекты N -уровня должны выполнять правила доступа к соединениям $(N-1)$ -уровня или информационному каналу $(N-1)$ -уровня без установления соединения.

Примеры помеченных каналов следующие:

- виртуальные соединения для прикладных процессов;
- соединения $(N-1)$ -уровня ЭМВОС или Интернет-архитектуры;
- каналы связи между процессами.

4.4.5. Контекстная схема

4.4.5.1. Основные свойства

В некоторых случаях ФПРР-модуль может затребовать контекстно-зависимую информацию для корректной интерпретации ВИПР или правил ПЛБ. Основные свойства контекстной схемы следующие:

- a) УД обеспечивается на основе ВИУД, привязанной к инициатору, или ВИУД, привязанной к целевому объекту, или независимо, т.е. на основе информации, полученной ФПРР-модулем;
- b) эта схема является наиболее приемлемой для реализации ФПРИ при выполнении правил всеми инициаторами.

4.4.5.2. ВИУД

Списки управления контекстно-зависимой информацией.

Списки управления контекстно-зависимой информацией представляют собой наборы или последовательности записей. Каждая такая запись включает следующие два поля:

- a) *определитель контекстно-зависимой информации.* Этот определитель (идентификатор) представляет собой последовательность контекстно-зависимых условий (например время, маршрут, местонахождение), при которых используется определитель процедуры. Каждое контекстно-зависимое условие по отдельности связано корректным или некорректным описанием;
- b) *определитель процедуры (операции).* Этот определитель (идентификатор) указывает на разрешенные процедуры (операции) для соответствующего определителя контекстно-зависимой информации.

Контекстно-зависимая информация. Эта информация извлекается из содержания полученного запроса доступа. Содержание запроса доступа зависит от области его применения, т.е. от того, где был получен запрос доступа (каким ФПРР-модулем). Существует несколько вариантов получения контекстно-зависимой информации: либо через основной интерфейс многоуровневой службы управления, либо через интерфейс локального управления.

4.4.5.3. Обеспечивающие способы

ФПРР-модуль для получения контекстно-зависимой информации использует средство ее получения. Контекстно-зависимая информация и запрос доступа являются входными

данными средства принятия решения о предоставлении доступа. Запрашиваемая процедура (операция), извлекаемая из запроса доступа, и полученная контекстно-зависимая информация сравниваются с определителем процедуры (операции) и определителем контекстно-зависимой информации, соответственно. По результатам сравнения принимается решение о предоставлении доступа или об отказе в доступе.

4.4.5.4. Варианты контекстной схемы

В некоторых списках управления контекстно-зависимой информацией применяются последовательности записей. Правило поиска записи в таких списках заключается в том, что после нахождения первой квалифицированной записи дальнейший поиск прекращается. Правило для каждой записи состоит в том, что отказ в доступе является следствием несоответствия контекстно-зависимой информации всем контекстно-зависимым условиям. Например, доступ мог быть разрешен политиками, которые допускают соответствующую процедуру (операцию) только в случае некоторого местоположения субъекта и в течение определенного периода времени, но не учитывают соответствующего маршрута доставки.

4.5. Взаимодействие с другими СЛБ и СПБ

4.5.1. Аутентификация

Иногда сущность служб УД и аутентификации не совсем понятна. Несмотря на то что между ними существуют взаимосвязи и некоторая общность, эти службы не одно и то же. Некоторые схемы УД (например УДСД) полагаются на параметры подлинности и, таким образом, требуют проведения процедуры аутентификации для подтверждения параметров подлинности. Для проведения в дальнейшем успешной аутентификации инициатору может понадобиться предварительное получение некоторой ВИУД. Следует заметить, что в некоторых системах средство проверки, используемое в процедуре аутентификации, и ФПРР-модуль совмещены. В таких случаях обмен ВИАУ основан на

одном очевидном протоколе. В распределенных системах такие функции совмещать не обязательно, а ВИУД об инициаторе может использоваться отдельно. Параметр подлинности, таким образом, рассматривается просто как часть ВИУД, привязанной к инициатору.

Взаимосвязь между аутентификацией и УД может устанавливаться ПЛУД. Например, если инициатор прошел процедуру аутентификации с использованием СПБ, уровень надежности которого недостаточен, то ПЛУД могла бы запретить проведение определенных процедур (например модификацию) по отношению к целевому объекту. С другой стороны, если бы инициатор прошел процедуру аутентификации с использованием СПБ, уровень надежности которого более чем достаточен, то определенные процедуры по отношению к целевому объекту могли быть разрешены.

4.5.2. Обеспечение целостности данных

СЛЦД данных может использоваться для обеспечения гарантий целостности входных и выходных данных между компонентами УД, а также внутри этих компонентов, например для предотвращения модификации хранимых или транслируемых мандатов доступа, списков УД и контекстно-зависимой информации.

4.5.3. Обеспечение конфиденциальности данных

СЛКН может быть востребована некоторыми ПЛБ с целью обеспечения конфиденциальности входных и выходных данных, циркулирующих между компонентами УД, например для защиты от перехвата критической информации.

4.5.4. Аудит

ВИУД может использоваться для аудиторской проверки запросов доступа соответствующего инициатора. Она может быть

необходима для проведения нескольких аудиторских проверок с целью точного определения, какие запросы доступа отправлялись инициатором и каким инициатором.

Политика аудита может потребовать, чтобы некоторые или все попытки получения доступа были зарегистрированы (записаны). Следовательно, могут потребоваться надежные средства записи, которые должны быть доступны для реализуемого способа УД. Политика аудита также может затребовать информацию о процедуре способа УД, которая подлежит записи (например обстоятельства, на основании которых в доступе было отказано). ПЛУД может потребовать, чтобы все процедуры доступа проходили аудиторскую проверку, и в каждом таком случае способ УД будет функционально зависеть от доверенной службы регистрации (записи).

В тех случаях, когда необходима идентифицируемость инициатора, перед началом процедуры предоставления доступа инициатор всегда должен проходить процедуру аутентификации. Важно понимать, что аутентификация и УД, даже несмотря на то что они очень часто взаимосвязаны между собой, не всегда реализуются и контролируются одними и теми же ЦБ, т.е. нет необходимости совмещения этих функций. Информация, которая используется при аутентификации, может понадобиться для получения ВИУД, привязанной к инициатору.

Идентифицируемость процедуры доступа в условиях анонимности может быть обеспечена следующим образом:

- инициатор получает из ЦБ ССБ ВИУД, которая содержит соответствующий идентификатор аудита. Приобретение ВИУД регистрируется (записывается): параметр подлинности инициатора и идентификатор аудита сохраняются в файле результатов аудиторской проверки ВИУД, выданной в рамках ССБ;
- инициатор использует ВИУД, привязанную к нему, для получения доступа к целевому объекту. ФПРР-модуль ССБ, в котором расположен целевой объект, получает

ВИУД, привязанную к инициатору, и сохраняет идентификатор аудита и запрос доступа в своем файле результатов аудиторской проверки;

- на основании аудиторской информации, полученной из ССБ, в котором расположен целевой объект, и ВИУД, привязанной к инициатору, и выданной в рамках ССБ, ЦБ ССБ может идентифицировать инициатор, также используя идентификатор аудита. С помощью этих средств инициатор может стать идентифицируемым при запросе им соответствующего доступа.

Если имеет место конфликт между желанием инициатора оставаться анонимным и требованием ССБ, в котором расположен целевой объект, знать параметр подлинности инициатора, то в доступе может быть отказано. Решение в такой конфликтной ситуации зависит от ПЛУД ССБ, в котором расположен целевой объект.

4.5.5. Другие СЛБ, связанные с УД

При проведении процедуры запроса доступа привлекается не только служба УД, но могут привлекаться и другие СЛБ:

- служба аудита регистрирует (записывает) произвольную информацию о запросе доступа;
- служба идентификации дополнительно осуществляет контрольную проверку имени или наименований объектов, которые формально отвечают за активизацию процедуры запроса доступа;
- служба взимания платы гарантирует, что на счет поступит соответствующая сумма, необходимая для использования доступного ресурса.

Информация, которая необходима для обеспечения каждой из рассмотренных служб при проведении процедуры запроса доступа, если рассуждать логически, различна. ВИПР, необходимая для УД, наименование счета для оплаты и идентификатор ответственного объекта для обеспечения идентифицируемости

являются данными, которые могут быть различны. Однако в некоторых прикладных системах требуется использовать одну и ту же информацию (например параметр подлинности для УД) в каждом из указанных случаев. Это может привести к нештатной ситуации, особенно в случае ретрансляции запросов доступа. Предпочтительнее хранить различные типы информации отдельно.

4.6. Обмен СЕРТ|УД между компонентами

4.6.1. Ретрансляция нескольких СЕРТ|УД

В некоторых случаях может понадобиться несколько СЕРТ|УД для обеспечения сложной ПИНО.

4.6.1.1. Пример

Предположим (рис. 4.5), что пользователь *U* обращается к прикладной системе *A1*, чтобы последнее запросило доступ к прикладной системе *A2*. Каждый запрос доступа формируется *A1* и направляется *A2*. Однако *A2* может использовать службы другой прикладной системы *A3* с целью удовлетворения запроса. В свою очередь, *A3* для решения этой задачи могут понадобиться службы прикладной системы *A4*.

Рассмотрим взаимосвязь между *A1* и *A2*, а также СЕРТ|УД, которые могут быть использованы при запросе доступа *A1* к *A2*. Очевидно, что могут потребоваться два СЕРТ|УД: для пользователя *U* и для прикладной системы *A1*.

Существуют три класса сертификатов, которые могут потребоваться пользователю *U* и прикладной системе *A1*:



Рис. 4.5. Ретрансляция нескольких СЕРТ|УД

- СЕРТ|УД, необходимые для доступа к *A2* и действительные для всех процедур (операций);

- СЕРТ|УД, необходимые для доступа к $A2$ и действительные для группы (совокупности) процедур (операций);
- СЕРТ|УД, необходимые для доступа к $A2$ и действительные для одной процедуры (операции).

В принципе, каждый СЕРТ|УД можно получить в разных ЦБ ССБ.

СЕРТ|УД, действительные для всех процедур (операций), доставляются в фазе установления соединения или начальной фазе процедуры информационного обмена.

Когда СЕРТ|УД определяют набор допустимых процедур (операций), то они остаются неизменными до тех пор, пока не будут доставлены другие СЕРТ|УД этого класса.

СЕРТ|УД, действительные для одной процедуры (операции), ограничиваются только этой процедурой (операцией).

4.6.1.2. Обобщение

Далее рассмотрим взаимосвязь между $A2$ и $A2$, а также СЕРТ|УД, которые могут быть использованы при запросе доступа $A2$ к $A3$. Очевидно, что могут потребоваться три СЕРТ|УД: для пользователя U , для прикладной системы $A1$ и для прикладной системы $A2$.

СЕРТ|УД для пользователя U и прикладной системы $A1$, предназначенные для использования при доступе к $A2$, могут или не могут быть применимы и при доступе к $A3$. Если они применимы, то каждый из этих сертификатов может быть любым сертификатом из трех классов, рассмотренных выше. Если же они неприменимы, то пользователь U или прикладная система $A1$ (или оба) при запросе доступа к $A2$ должны получить дополнительный СЕРТ|УД для доступа к $A3$, который также может быть любым сертификатом из трех классов, рассмотренных выше.

Схема может быть обобщена и для взаимодействия между $A3$ и $A4$, при этом могут понадобиться дополнительные сертификаты для U , $A1$ или $A2$.

4.6.1.3. Упрощения

Обычно необходим только СЕРТ|УД от пользователя U или от прикладной системы $A1$. СЕРТ|УД, действительные только

для одной процедуры (операции), используются крайне редко. СЕРТ|УД от *U*, предназначенный для доступа к *A2*, может ретранслироваться системой *A1*, даже если последняя его не использует.

4.7. Управление доступом в ЭМВОС и Интернет-архитектуре

4.7.1. Общие положения

УД может использоваться в фазе доставки данных виртуального соединения или время от времени в течение функционирования виртуального соединения. Эта служба применима к протоколам с установлением или без установления соединений.

4.7.2. Использование УД внутри уровней ЭМВОС и Интернет-архитектуры

УД касается только следующих уровней ЭМВОС и Интернет-архитектуры:

- сетевой (3-й) уровень;
- транспортный (4-й) уровень;
- прикладной (7-й) уровень (5-й уровень для Интернет-архитектуры).

4.7.2.1. Использование УД на сетевом уровне

УД, применяемое на сетевом уровне, позволяет управлять доступом к сетевым узлам и/или из них, к узлам подсетей и/или из них и к ретрансляционным узлам и/или из них. УД на сетевом уровне может иметь многоцелевое применение. Например, оно позволяет оконечным системам контролировать формирование сетевых соединений или отклонять нежелательные вызовы. Кроме того, оно позволяет одной или нескольким подсетям контролировать использование ресурсов сетевого уровня. В отдельных случаях контроль использования ресурсов сетевого уровня связан с оплатой за пользование сетью.

Способы УД, используемые на сетевом уровне, не выходят за пределы одного и того же уровня.

4.7.2.2. Использование УД на транспортном уровне

УД, применяемое на транспортном уровне, позволяет управлять доступом к объектам сеанса связи и/или из них. Различные прикладные процессы (системы), обеспечиваемые одной и той же оконечной системой, не могут контролироваться отдельно, если они используют соединение на транспортном уровне совместно.

Способы УД, используемые на транспортном уровне, не выходят за пределы одного и того же уровня.

4.7.2.3. Использование УД на прикладном уровне

Модель обеспечения безопасности верхних уровней представлена в стандарте ISO/IEC 10745:1995.

4.8. Проблема уникальности (неединственность) параметров подлинности для УД

Рассмотрим следующие два примера, демонстрирующие проблемы назначения и использования параметров подлинности для УД:

- если пользователь именуется Иван Петров, и в рамках прикладной системы ему было присвоено это весьма распространенное имя, то в соответствующем ССБ будет существовать конкретная последовательность символов «Иван Петров» в качестве его индивидуального параметра подлинности для УД. Затем одна и та же последовательность символов может быть перемещена в атрибут управления с целью предоставления ему некоторых видов доступа. В дальнейшем Иван Петров может покинуть этот ССБ, а другой пользователь, также именуемый Иван Петров, может войти в этот же ССБ, и которому также может быть присвоен индивидуальный параметр подлинности «Иван Петров». Если последовательность симво-

лов «Иван Петров» по-прежнему остается в атрибуте управления, то впоследствии новый Иван Петров будет иметь возможность получить те виды доступа, которые были разрешены предыдущему Ивану Петрову;

- если целевой объект обозначен с помощью последовательности символов, которая в ССБ является его параметром подлинности для УД, то такая же последовательность символов может использоваться в привилегированном атрибуте с целью предоставления пользователю некоторых видов доступа. Позднее целевой объект может быть удален из этого ССБ, а еще позднее может быть сформирован новый целевой объект с таким же параметром подлинности для УД. Если привилегированный атрибут, предоставленный пользователю, не был изменен, то у пользователя появится возможность получения доступа к новому целевому объекту.

Предполагается, что в рамках ССБ параметры подлинности для УД являются уникальными. Однако параметр подлинности может быть действителен только в течение определенных периодов времени или, фактически, может быть назначен навсегда. Когда параметр подлинности действителен только в течение определенных периодов времени, то в любой момент времени данный типа атрибута, в котором представлен параметр подлинности для УД в качестве значения атрибута, имеет вполне определенный смысл. Однако, если этому не уделять соответствующего внимания, то один и тот же тип и значение атрибута могут использоваться повторно. Если в ССБ по-прежнему имеет место любой из ранее используемых типов атрибута или значений атрибута, то может появиться брешь (уязвимость) в системе обеспечения безопасности.

Существуют два способа решения этой проблемы. Перед тем как определить новый тип атрибута или новое значение атрибута для УД, ЦБ ССБ должен гарантировать, что этот тип атрибута или это значение атрибута для УД:

- в настоящее время не назначены;
- раньше никогда не использовались.

В первом случае ЦБ ССБ необходимо гарантировать, что каждый раз тип атрибута или значение атрибута для УД будет удалено, а инициатор или целевой объект еще не обладают данным типом атрибута или значением атрибута для УД. Когда это невозможно, то должен быть определен период действия (выраженный явно или не явно) для каждого типа атрибута или значения атрибута для УД. В течение периода действия необходимо хранить запись обо всех удаленных типах атрибута или значениях атрибута для УД.

Во втором случае должен быть определен уникальный параметр подлинности для УД (также именуемый постоянным идентификатором), значение которого было присвоено только один раз и которое никогда не будет повторно использоваться.

4.9. Распределение компонентов УД

Основные ФПРИ, ФПРР и УД могут быть реализованы с помощью одного или нескольких ФПРИ- и ФПРР-модулей, которые могут, соответственно, комбинироваться. Реализация этих функций зависит от условий размещения ФПРИ- и ФПРР-модулей, связей между ними или их возможного распределения.

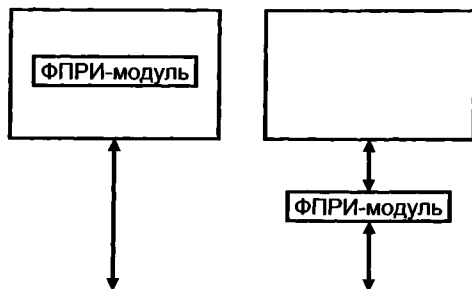


Рис. 4.6. Внутреннее и внешнее размещение ФПРИ-модуля

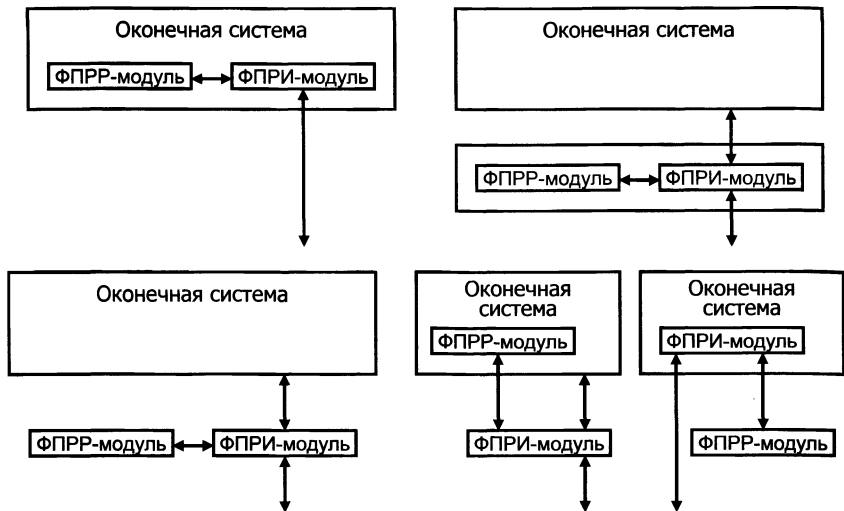


Рис. 4.7. Варианты размещения ФПРИ- и ФПРР-модулей

4.9.1. Реализационные аспекты

Наибольший практический интерес представляют следующие вопросы:

- число и размещение ФПРИ- и ФПРР-модулей;
- процедуры информационного обмена между инициаторами, ФПРИ- и ФПРР-модулями и целевыми объектами.

В любом ССБ один или несколько ФПРИ-модулей могут располагаться между каждым инициатором и целевым объектом, причем так, чтобы инициатор мог запрашивать доступ к целевому объекту только через ФПРИ-модуль. Существует несколько возможных вариантов размещения ФПРИ- и ФПРР-модулей. А именно:

- ФПРИ-модули могут быть распределены различными способами, как это показано на рис. 4.6, 4.7 и 4.8;

- ФПРР-модули могут быть совмещены (жестко связаны) с ФПРИ-модулями (а могут быть и не совмещены);
- ФПРР-модуль может обслуживать один или несколько ФПРИ-модулей;
- ФПРИ-модуль может использовать один или несколько ФПРР-модулей.

Существует несколько возможных вариантов организации соединений между представленными компонентами.

4.9.2. Размещение ФПРИ- и ФПРР-модулей

ФПРИ-модули могут быть встроены (внутри) в оконечную систему или размещаться (вне системы) между оконечной системой и сетью, используемой для связи с другими оконечными системами (рис. 4.6). Некоторые реальные системы могут иметь встроенные и внешние ФПРИ-модули одновременно, что связано с различными аспектами процедуры УД. Преимущества и недостатки встроенных и внешних ФПРИ-модулей определяются ПЛБ и связаны с их надежным внедрением в систему, а также другими условиями, которые здесь не рассматриваются.

Таким же образом и ФПРР-модули могут быть встроены (внутри) в оконечную систему или могут размещаться вне нее (рис. 4.7). При обслуживании ФПРР-модулями одного внешнего ФПРИ-модуля желательно, но не обязательно, чтобы ФПРР-модуль также размещался вне системы. При обслуживании ФПРР-модулями нескольких ФПРИ-модулей, расположенных в разных оконечных системах, ФПРР-модуль будет, как правило, размещаться вне системы. Как было отмечено ранее, оконечная система может применять несколько ФПРИ-модулей, что связано с различными аспектами процедуры УД. В таких случаях указанные ФПРИ-модули могли бы обслуживаться одиночным внутренним или внешним ФПРР-модулем, или могло бы использоваться несколько специализированных ФПРР-модулей. Совмещение (жесткая связка) ФПРИ- и ФПРР-модулей может иметь преимущества, связанные с повышением эффективности функционирования и быстродействия (снижение задержки).

4.9.3. Информационное взаимодействие между компонентами УД

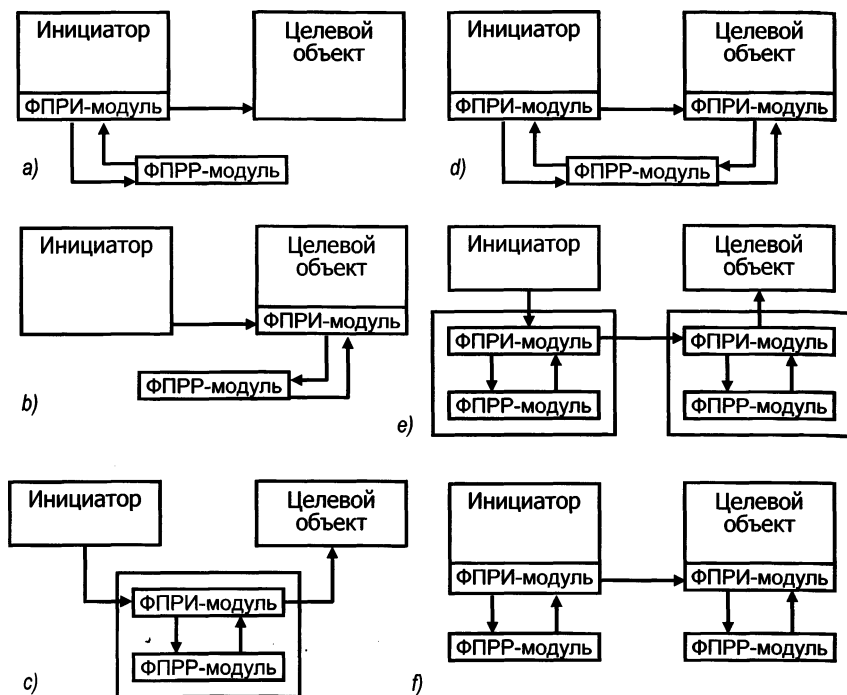


Рис. 4.8. Взаимосвязи между ФПРИ- и ФПРР-модулями

ФПРР может быть реализована с помощью одного или нескольких ФПРР-модулей. И ФПРИ может быть реализована с помощью одного или нескольких ФПРИ-модулей. Варианты взаимосвязей между компонентами УД представлены на рис. 4.8, где рассматриваются взаимосвязи только для случая с одним инициатором и с одним целевым объектом:

- a) инициатор представляет запрос доступа непосредственно в ФПРИ-модуль, расположенный у этого инициатора,

- который запрашивает разрешение у ФПРР-модуля. Если доступ разрешен, ФПРИ-модуль объявляет об этом целевому объекту, указанному в запросе;
- b)* инициатор представляет запрос доступа непосредственно в ФПРИ-модуль, расположенный у запрашиваемого целевого объекта, который, в порядке очереди, направляет его в ФПРР-модуль для принятия решения. Если доступ разрешен, ФПРИ-модуль объявляет об этом целевому объекту, указанному в запросе. Существует корреляция между функциональностью и расположением в вариантах *a)* и *b)*. ФПРИ-модуль осуществляет управление входящим или исходящим запросом доступа или обоими одновременно, следовательно, ФПРИ-модуль может запрашиваться инициатором, целевым объектом или промежуточным ФПРИ-модулем;
- c)* инициатор представляет запрос доступа в промежуточный ФПРИ-модуль, который, в порядке очереди, направляет его в ФПРР-модуль для принятия решения. Если доступ разрешен, ФПРИ-модуль объявляет об этом целевому объекту, указанному в запросе;
- d)* информационное взаимодействие представляет собой композицию вариантов *a)* и *b)* с одним и тем же ФПРР-модулем, положительно отвечающий на запрос доступа, поступивший от ФПРИ-модулей инициатора и целевого объекта. Инициатор представляет запрос доступа непосредственно в ФПРИ-модуль, расположенный у этого инициатора, который запрашивает разрешение у ФПРР-модуля. Если доступ разрешен, ФПРИ-модуль инициатора запрашивает доступ у ФПРИ-модуля, расположенного у запрашиваемого целевого объекта. ФПРИ-модуль целевого объекта, в порядке очереди, направляет запрос доступа в ФПРР-модуль для принятия решения. Если доступ разрешен, ФПРИ-модуль целевого объекта объявляет об этом целевому объекту, указанному в запросе;

е) и ф) отдельные ФПРИ-модули осуществляют функцию предоставления для входящих и исходящих запросов доступа в процедуре УД. В варианте *е)* информационный обмен подобен варианту *с)*, за исключением того, что оба ФПРИ-модуля должны выработать положительное решение для запрашиваемого доступа. В варианте *ф)* информационный обмен представляет собой композицию вариантов *а)* и *б)* с отдельными ФПРИ-модулями.

Рассмотренные варианты информационного взаимодействия существенно упрощены. Тем не менее можно рассмотреть и более сложные варианты информационного взаимодействия между инициатором, целевым объектом и ФПРИ-модулями, включив последовательные, вложенные и рекурсивные объекты.

4.10. Сравнительный анализ УДПР и УДПП

УДПР очень часто рассматриваются как политика, основанная на использовании маркеров безопасности, включая инициаторов, обладающих разрешениями, которые подобны «секретному слову» или «специальному параметру», и защищенные целевые объекты, распределенные аналогичным образом по соответствующим группам, имеющим уникальные имена.

УДПП представляет собой политику, в которой индивидуальные пользователи или их группы или ролевые объекты получают доступ (либо им доступ запрещается) на основе их параметров подлинности или ВИУД.

После детального анализа некоторые различия между УДПР и УДПП становятся неочевидными: разрешения в рамках УДПР и ВИУД об инициаторе по существу одно и то же. Разрешения, которые связаны с УДПР, могут рассматриваться, как соответствующая ВИУД об инициаторе. В самом деле, если пользователи в соответствии с УДПР обладают уникальными неиерархическими индивидуальными разрешениями, то по-

следние становятся эквивалентны параметрам подлинности пользователя, а группы целевых объектов становятся эквивалентны записям в списках УД.

Очень часто между УДПР и УДПП проявляется и другое различие, которое заключается в том, что УДПР устанавливаются административно, тогда как УДПП выбираются пользователями. С точки зрения общих основ обеспечения безопасности различие лежит в УД к ВИУД, когда сама ВИУД трактуется как целевой объект (в смысле ее модификации). Это различие не очевидно: существует различие в выборе распределения или централизации возможного управления, что зависит от ПЛУД, диапазон которых начинается от чисто административного назначения политики до ее избирания исключительно пользователем. Конкретная ситуация отображается в совокупность реальных требований, устанавливаемых администраторами безопасности или их посредниками (например менеджерами департамента или руководителями группы), в отличие от индивидуально устанавливаемых ПЛУД.

4.11. Способ обеспечения ретрансляции ВИУД через инициатора

В этом способе участвуют три объекта:

- инициатор *A*;
- объект *C*;
- объект *B*.

Основное предназначение этого способа состоит в том, чтобы позволить инициатору начать доставку информации напрямую от объекта *C* объекту *B* без участия инициатора *A* в течение фазы доставки.

Инициатор первым запрашивает доступ к объекту *C* и предоставляет ему ВИУД, привязанную к инициатору, чтобы получить доступ. Затем объект *C* предоставляет инициатору некую информацию, которая будет использоваться позднее объектом

В для получения доступа к объекту *С*. Эта информация состоит из следующих двух частей:

- уникальная ссылка на объект *С*, которая используется в течение срока действия ссылки;
- криптографический ключ, защищенный с использованием службы обеспечения конфиденциальности, для информационного взаимодействия объекта *С* и инициатора.

С целью обеспечения доступа к объекту *С*, объекту *В* необходимо получить от инициатора *А* уникальную ссылку и криптографический ключ. При доставке от инициатора до объекта *В* криптографический ключ защищается на основе использования службы обеспечения конфиденциальности.

В заключение уникальная ссылка и криптографический ключ используются объектом *В* для формирования ВИУД, привязанной к запросу доступа. Последняя состоит из уникальной ссылки и криптографической проверочной суммы, вычисленной с использованием криптографического ключа.

В дальнейшем объект *С* может предоставить доступ, если криптографический ключ, используемый для вычисления криптографической проверочной суммы, совпадет с одним из ключей, указанных в ссылке.

Общая структура службы управления доступом представлена в табл. 4.1.

Таблица 4.1

Структура службы обеспечения безопасности (управления доступом)	Элемент	<u>Объект/субъект</u> : Инициатор, Целевой объект
		<u>Функции</u> : Функция принуждения при УД, Функция принятия решения о предоставлении доступа
		<u>Информация</u> : Информация для УД, Информации для принятия решения при УД, Контекстно-зависимая информация, Правила политики УД
	<u>Цель объектов</u> : интерпретировать информацию для предоставления инициаторам доступа к целевым объектам, только как авторизованного	

Таблица 4.1 (продолжение)

М Е Р О П Р И Я Т И Я	Объект/субъект	Центр безопасности сетевого сегмента		
	Функция			
	Мероприятия, связанные с обеспечением процедуры УД	— Установка информации для УД — Изменение информации для УД — Аннулирование информации для УД — Аннулирование информации для принятия решения при УД — Регистрация информации для УД		
		— Блокировка компонента — Разблокировка компонента		
	Объект/субъект	Инициатор	Целевой объект	
	Функция			Функция принятия решения о предоставлении доступа
	Мероприятия, функционально связанные с процедурой УД	— Идентификация удаленного Центра безопасности сетевого сегмента — Формирование политики защищенного информационного взаимодействия — Запрос информации для УД — Формирование информации для УД — Аннулирование информации для принятия решения при УД	— Запрос информации для УД — Аннулирование информации для принятия решения при УД	— Запрос информации для УД — Проверка подлинности привязанной информации для УД и извлечение из нее информации для принятия решения при УД — Получение контекстно-зависимой информации — Принятие решения о предоставлении доступа

Таблица 4.1 (окончание)

И Н Ф О Р М А Ц И Я	Элементы данных, определяемые Центром безопасности сетевого сегмента	— Идентификаторы (Центра безопасности сетевого сегмента, инициатора, целевого объекта, политики защищенного информационного взаимодействия, групп, ролевых объектов) — Критерий отбора информации для УД — Время (период времени) действия — Маркер критичности — Маркер целостности		
	Информация, используемая в процедуре УД	— Информация для УД / Информация для принятия решения при УД (об инициаторе, привязанная к инициатору, о целевом объекте, привязанная к целевому объекту, о запросе доступа, привязанная к запросу доступа, об объекте процедуры, привязанная к объекту процедуры, об информационном обмене, контекстно-зависимая, сохраняемая) — Перечень УД — Мандат доступа — Метка — Сертификат для УД — Маркер УД		
	Контрольная информация	— Период времени — Состояние системы	— Структура и формат политики УД — Уровень аутентификации	— Маршрут соединения

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ НЕОТКАЗУЕМОСТИ

Цель функционирования службы обеспечения неотказуемости (СЛНТ) заключается в сборе, обработке, обеспечении доступности и признании неопровержимости доказательства¹ (свидетельства) относительно заявленного события или действия с целью урегулирования споров о произошедшем или не произошедшем событии или действии. СЛНТ может применяться во многих ситуациях и при различных обстоятельствах. Служба может использоваться для формирования данных, хранения данных или передачи данных. Она предусматривает формирование доказательства, которое может использоваться для доказательства того, что имел место некоторый вид события или действия, причем в дальнейшем невозможно отказаться от участия в этом событии или этого действия. В открытых системах ЭМВОС или Интернет-архитектуры СЛНТ может быть реализована в двух формах:

- *неотказуемость с доказательством источника*, которое используется для защиты от ложного отказа отправителя от факта передачи им данных или составных элементов этих данных;
- *неотказуемость с доказательством доставки*, которое используется для защиты от ложного отказа получателя от факта приема им данных или составных элементов этих данных (т.е. информации, которую содержат данные).

Представленные ниже концепции не ограничиваются только ЭМВОС и Интернет-архитектурой, так как они могут иметь

¹ Доказательство (свидетельство) представляет собой информацию, которая либо самостоятельно, либо в сочетании с другой информацией может использоваться для урегулирования (разрешения) спора.

весьма широкую интерпретацию, включая системы формирования и хранения данных, которые могут использоваться в дальнейшем.

В данной главе:

- расширены основные концепции СЛНТ, представленные в главе 1, и дано описание, как они могут применяться в системах ЭМВОС и Интернет-архитектуры;
- представлены альтернативные способы обеспечения таких служб;
- раскрыты взаимосвязи таких служб с другими СЛБ.

Для СЛНТ могут быть востребованы:

- судьи, которые будут урегулировать споры, возникающие в результате отказа от участия в событиях или действий;
- ДТС, которые будут гарантировать аутентичность (подлинность) и целостность данных, используемых при проверке доказательства.

5.1. Общие положения

5.1.1. Основные концепции обеспечения неотказуемости

СЛНТ применяет генерирование, проверку и регистрацию (запись) доказательства (свидетельства), а также последующее извлечение и повторную проверку этого доказательства (свидетельства) с целью урегулирования споров. Споры не могут быть разрешены, если доказательство (свидетельство) не было предварительно (заранее) зарегистрировано.

Целевое назначение СЛНТ — обеспечение доказательства (свидетельства) о соответствующем событии или действии. СЛНТ могут запрашиваться объектами, которые не принимали участие в том или ином событии или действии. Примеры действий, которые могут быть защищены с привлечением СЛНТ, могут быть следующие:

- передача электронного почтового сообщения;
- внесение записи в БД;
- вызов удаленной процедуры.

При передаче сообщений с целью подтверждения их источника должны использоваться параметр подлинности этого источника и служба обеспечения целостности данных, для обеспечения подтверждения доставки — параметр подлинности получателя и служба обеспечения целостности данных. В некоторых случаях также может потребоваться доказательство, затрагивающее контекстно-зависимую информацию (например дата, время, местоположение источника/получателя).

СЛНТ предоставляет следующие средства, которые могут быть использованы в случае попытки отказа от чего-либо:

- формирования доказательства;
- регистрации доказательства;
- проверки сформированного доказательства;
- извлечения (восстановления) и повторной проверки доказательства.

Споры между сторонами могут быть урегулированы непосредственно через проверку доказательства. Однако спор может быть урегулирован судьей, который устанавливает доказательство и определяет, произошло или нет спорное действие или событие. Судебное решение обеспечивается эффективно только тогда, когда стороны спора признали удостоверяющий центр судьи. Для обеспечения гарантированного доказательства, принятого судьей, как правило, требуется заверение одной или несколькими ДТС. Судья может быть одновременно и ДТС, которая заверяет доказательство. Применяемые способы обеспечения неотказуемости используют несколько типов ДТС и форм доказательств.

5.1.2. Роль и участие ДТС

СЛНТ может привлекать одну или несколько ДТС.

ДТС, которые обеспечивают СЛНТ без каких-либо активных действий при каждом обращении к этой службе, называются *ав-*

тономными ДТС. ДТС, которые активно участвуют в процедурах формирования или проверки доказательства, называются *интерактивными* ДТС. ДТС, которая является промежуточной системой (intermediary) во всех процедурах информационного обмена, называется *промежуточной* ДТС.

ДТС может быть востребована для записи (регистрации) и/или накопления доказательств, также она необходима в качестве поручителя за юридическую обоснованность доказательства. Привлекаемые к СЛНТ ДТС могут выступать в различном качестве (например нотариуса, службы меток времени, службы мониторинга, УЦ, службы формирования ЭЦП, службы подтверждения подлинности ЭЦП и центра доставки). Одна ДТС может выступать в одной или в нескольких из следующих ролей:

- *формирование доказательства.* ДТС взаимодействует с СЛНТ, которая запрашивает процедуру формирования доказательства;
- *регистрация доказательства.* ДТС регистрирует (записывает) доказательство, которое в дальнейшем может быть возвращено пользователю доказательством или судьей;
- *служба меток времени.* ДТС является доверенной службой, которая обеспечивает доказательство, включающее время, меткой времени при получении на нее запроса;
- *служба мониторинга.* ДТС контролирует действие или событие в качестве доверенной службы с целью обеспечения доказательства всего того, что она контролировала;
- *УЦ.* ДТС обеспечивает СЛНТ сертификатами ключей ЭЦП (СЕРТ), связанными с формированием доказательства, с целью обеспечения гарантий подлинности открытого ключа, который используется в интересах СЛНТ;
- *служба распределения ключей.* ДТС снабжает ключами объекты (устройства) формирования и/или проверки доказательства. Также она может налагать ограничения на применение ключей, если, естественно, используются методы симметричной криптографии;

- *служба формирования ЭЦП.* ДТС является доверенной службой обеспечения доказательства в форме ЭЦП от имени субъекта доказательства;
- *службы подтверждения подлинности (проверки) доказательства.* ДТС проверяет (подтверждает подлинность) доказательства по запросу объекта;
- *службы подтверждения подлинности (проверки) ЭЦП.* ДТС является доверенной службой для объекта, использующего доказательство, при проверке (подтверждении подлинности) этого доказательства в форме ЭЦП;

ПРИМЕЧАНИЕ. Формирование ЭЦП является частным случаем формирования доказательства. Подтверждение подлинности (проверки) ЭЦП является частным случаем подтверждения подлинности (проверки) доказательства.

- *нотариус.* ДТС обеспечивает гарантии свойств данных (таких как их целостность, авторство, время или получателя), которыми обмениваются между собой две или несколько взаимодействующих сторон и которые предварительно были зарегистрированы ДТС;
- *центр доставки.* ДТС взаимодействует с указанным получателем данных и пытается передать данные получателю. После этого ДТС обеспечивает доказательство того, что либо данные были доставлены, либо данные не были доставлены, либо была предпринята попытка доставки, но подтверждение приема не было получено. В последнем случае объект, использующий доказательство, не мог определить, были ли получены данные указанным получателем или нет.

5.1.3. Фазы процедуры обеспечения неотказуемости

Процедура обеспечения неотказуемости (или просто процедура неотказуемости — ПРНТ) состоит из четырех фаз:

- формирование доказательства;
- доставка, хранение и извлечение доказательства;
- проверка (подтверждение подлинности) доказательства;
- разрешение (урегулирование) спора.

На рис. 5.1 представлены первые три фазы ПРНТ, а на рис. 5.2 – четвертая фаза ПРНТ.



Рис. 5.1. Первые три фазы ПРНТ

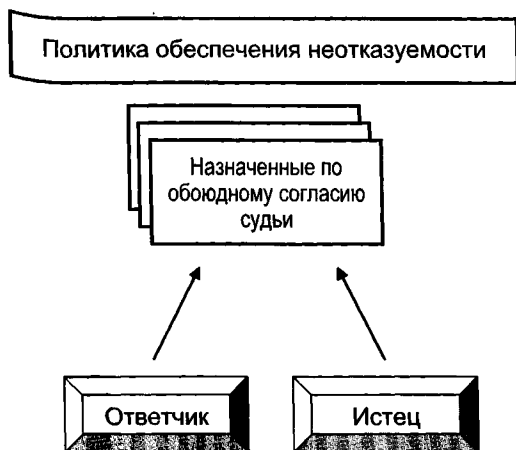


Рис. 5.2. Урегулирование спора

5.1.3.1. Формирование доказательства

В этой фазе сторона, запрашивающая формирование доказательства (Evidence Generation Requestor), направляет запрос объекту (средству) формирования доказательства (Evidence Generator) с целью сформировать доказательство события или действия. Объект, участие которого в событии или действии подтверждается доказательством, именуется субъектом доказательства (Evidence Subject). Указанные объекты могут группироваться по-разному: субъект доказательства и средство формирования доказательства могут быть одним и тем же объектом, а именно субъектом доказательства, стороной, запрашивающей формирование доказательства, и средством формирования доказательства; сторона, запрашивающая формирование доказательства, и ДТС; средство формирования доказательства и ДТС; сторона, запрашивающая формирование доказательства, средство формирования доказательства и ДТС. В зависимости от типа СЛНТ доказательство может быть сформировано субъектом доказательства, возможно, совместно со службами ДТС, или одной ДТС.

ПРИМЕЧАНИЕ. В зависимости от контекста СЛНТ важное доказательство будет, как правило, включать параметры подлинности участвующих объектов, данные, время и дату. Может быть включена и другая дополнительная информация, такая как режим доставки (например соединение ЭМВОС или Интернет-архитектуры, хранение в БД и извлечение из БД); расположение участвующих объектов, УИД; «владелец»/автор данных.

5.1.3.2. Доставка, хранение и извлечение доказательства

В течение этой фазы (Evidence Transfer, Storage and Retrieval) доказательство транслируется либо между объектами, либо доставляется в хранилище, либо извлекается из него (см. рис. 5.1).

5.1.3.3. Проверка (подтверждение подлинности) доказательства

В этой фазе доказательство проверяется объектом (средством) проверки (подтверждение подлинности) доказательства

(Evidence Verifier) по запросу пользователя доказательством (Evidence User). Сущность этой фазы: пользователь доказательством убеждается в том, что полученное доказательство будет действительно адекватным тому событию, из-за которого возник спор. Для проверки предоставленной информации могут дополнительно привлекаться службы ДТС. Пользователь доказательством и объект (средство) проверки (подтверждение подлинности) доказательства могут быть одним и тем же объектом.

5.1.3.4. Урегулирование (разрешение) спора

В фазе урегулирования спора судья несет ответственность за разрешение спора между сторонами. Конфликтующие стороны иногда называют истцом и ответчиком (см. рис. 5.2).

Когда судья разрешает спор, он собирает доказательства от конфликтующих сторон и/или ДТС. Сама процедура, применяемая судьей при урегулировании спора, не рассматривается.

Необходимость этой фазы не всегда обязательна. Если заинтересованные стороны согласились, что событие или действие имело место (или согласились, что его не было), то нет предмета спора, а значит нечего урегулировать. Более того, даже если спор возник, то он может быть разрешен непосредственно между сторонами спора без привлечения судьи. Например, если одна из сторон спора является честной, но неправильно понятой, то стороны спора могут осознать, что они ошиблись, когда представляли доказательства другой стороны.

Несмотря на то что эта фаза не всегда необходима при каждом обращении к СЛНТ, все способы обеспечения неотказуемости обязаны поддерживать фазу урегулирования (разрешения) споров, т.е. они обязаны предоставлять возможность для урегулирования споров, если таковые возникли.

5.1.4. Некоторые формы служб обеспечения неотказуемости

Существует несколько форм СЛНТ. Среди этих форм наиболее часто обсуждаемой является СЛНТ, которая связана с доставкой данных.

В процедуре доставки сообщения участвуют как минимум два объекта, именуемые «отправитель» и «получатель». Потенциальные споры, касающиеся события, могут быть следующие:

- споры, в которых участие отправителя в событии является спорным, например, сомнительный отправитель заявляет, что сообщение было подделано либо получателем, либо нарушителем, осуществившим атаку типа «маскарад»;
- споры, в которых участие получателя в событии является спорным, например, сомнительный получатель заявляет, что сообщение либо не было передано, либо было потеряно во время передачи, либо было принято только нарушителем, осуществившим атаку типа «маскарад».

В случаях обмена сообщениями СЛНТ классифицируются в соответствии с вариантом спора, который они могут урегулировать.

Доставка сообщений от отправителя (источника) к получателю может рассматриваться как последовательность следующих отдельных событий:

- передача сообщения от отправителя до посредника доставки;
- передача сообщения между посредниками доставки (если участвуют несколько посредников);
- передача сообщения от посредника доставки до получателя.

Для каждого из этих событий существует своя форма СЛНТ, которая обеспечивает доказательство для своего события. Далее приведены возможные варианты СЛНТ:

- СЛНТ с подтверждением (доказательством) получения сообщения для ретрансляции (Non-repudiation with proof of submission service) обеспечивает защиту от ложного отказа посредника доставки (ретранслятора) от факта получения им сообщения для дальнейшей передачи (либо от отправителя, либо от другого посредника доставки);

- СЛНТ с подтверждением (доказательством) передачи сообщения, подлежащего ретрансляции (Non-repudiation with proof of transport service), обеспечивает защиту от ложного отказа посредника доставки (ретранслятора) от факта передачи им сообщения (либо получателю, либо другому ретранслятору).

ПРИМЕЧАНИЕ. Оба варианта СЛНТ не обеспечивают доказательство того, что объект несет ответственность за сообщение или не понял информацию, которая содержится в сообщении.

5.1.5. Примеры доказательств неотказуемости в рамках ЭМВОС и Интернет-архитектуры

В зависимости от привлекаемых в рамках ЭМВОС или Интернет-архитектуры СЛНТ для каждого типа события или действия необходимы соответствующие формы доказательств.

5.1.5.1. Неотказуемость источника (non-repudiation of origin)

Доказательство должно включать следующие данные (которые могут быть подписаны или нотариально заверены):

- UID источника (отправителя);
- переданные данные или цифровой отпечаток данных.

Кроме того, доказательство может включать следующие данные:

- UID получателя;
- дата и время передачи данных.

5.1.5.2. Неотказуемость доставки (non-repudiation of delivery)

Доказательство должно включать следующие данные (которые могут быть подписаны или нотариально заверены):

- UID получателя;
- полученные данные или цифровой отпечаток данных.

Кроме того, доказательство может включать следующие данные:

- УИД источника (отправителя);
- дата и время получения данных.

Когда используется центр доставки, доказательство может включать следующие данные (которые могут быть подписаны или нотариально заверены):

- УИД центра доставки;
- дата и время, когда было получено сообщение от получателя о его готовности к приему;
- дата и время, когда была завершена доставка центром доставки;
- дата и время, когда центр доставки был не способен осуществить доставку;
- возможные причины того, почему не произошла доставка (например разрыв соединения);
- описание требований к управлению, которые были выполнены при доставке сообщения.

5.2. Политики обеспечения неотказуемости

Политика обеспечения неотказуемости (ПЛНТ) может включать:

- правила формирования доказательства, например, описание классов направлений деятельности, для которых целесообразно сформировать доказательство неотказуемости, описания ДТС, которые будут использоваться при формировании доказательства, роли ДТС, которые они могут исполнять, процедуры, которые должны выполнять объекты при формировании доказательства;
- правила проверки (подтверждения подлинности) доказательства, например, описание ДТС, чьи доказательства приемлемы, для каждой ДТС, формы доказательства, которые будут приниматься от конкретной ДТС;

- правила хранения доказательства, например, используемые средства, которые обеспечат гарантии (надежность) целостности хранимого доказательства;
- правила использования доказательства, например, описание целей, для достижения которых может использоваться доказательство;

ПРИМЕЧАНИЕ. При использовании некоторых способов обеспечения неотказуемости весьма трудно предотвратить несанкционированное использование доказательства;

- правила разрешения спора, например, описание привлекаемых судей, которые могут урегулировать спор.

Каждый из этих наборов правил может быть определен разными ЦБ. Например, правила формирования доказательства могли быть определены владельцем системы, в то время как правила урегулирования споров могут быть определены законом страны, в которой расположена система.

Если разные части политики противоречивы, то СЛНТ может не выполнить процедуру корректно, например за счет признания события, которое фактически прошло успешно, но завершилось отказом в течение фазы разрешения спора.

Сама ПЛНТ может использоваться судьей, когда последний разрешает спор. Например, судья может обратиться к ПЛНТ с целью определения, были ли соблюдены правила формирования доказательства.

ПЛБ могут устанавливаться однозначно или определяться внедряемыми прикладными системами в неявной форме. Точное изложение ПЛНТ (например документ на читабельном языке) может помочь при выявлении конфликтующих между собой различных частей политики, а также может помочь судье.

ПЛНТ также затрагивают случаи, при которых доказательство было скомпрометировано или при которых для формирования доказательства использовались скомпрометированные или уничтоженные ключи.

ПЛНТ, предназначенные для ПИНО между ССБ, могут быть результатом соглашений между независимыми ССБ или могут быть установлены сетевым суперсегментом.

5.3. Вспомогательная информация и средства обеспечения неотказуемости

5.3.1. Вспомогательная информация

ВИ, которая может использоваться для урегулирования конфликта (спора), называется доказательством (свидетельством). Доказательство может храниться локально пользователем доказательства или у ДТС. Конкретными формами доказательства являются ЭЦП, защитные конверты и маркеры безопасности. ЭЦП основаны на методах открытых ключей, в то время как защитные конверты и маркеры безопасности основаны на методах секретных ключей. Примеры информации, которая может являться доказательством, следующие:

- идентификатор ПЛБ для СЛНТ;
- UID отправителя (источника);
- UID получателя;
- ЭЦП или защитный конверт;
- сообщение или цифровой отпечаток сообщения;

ПРИМЕЧАНИЕ. Если цифровой отпечаток размещается в сообщении, то необходимо использовать соответствующий индикатор для определения метода извлечения отпечатка.

- идентификатор сообщения;
- признак секретного ключа, необходимого для подтверждения подлинности маркера безопасности;
- признак соответствующего открытого ключа для подтверждения подлинности ЭЦП (например UID УЦ или серийный номер СЕРТИБ);
- UID нотариата, службы меток времени ДТС, промежуточной ДТС и т.д.;
- UID доказательства;

- дата и время, когда доказательство было отправлено на хранение или зарегистрировано;
- дата и время, когда были сформированы ЭЦП или маркер безопасности.

5.3.2. Средства обеспечения неотказуемости

Средства обеспечения неотказуемости (СРНТ) могут использоваться для формирования, передачи и подтверждения подлинности доказательства или для отправки доказательства в ДТС (рис. 5.3).

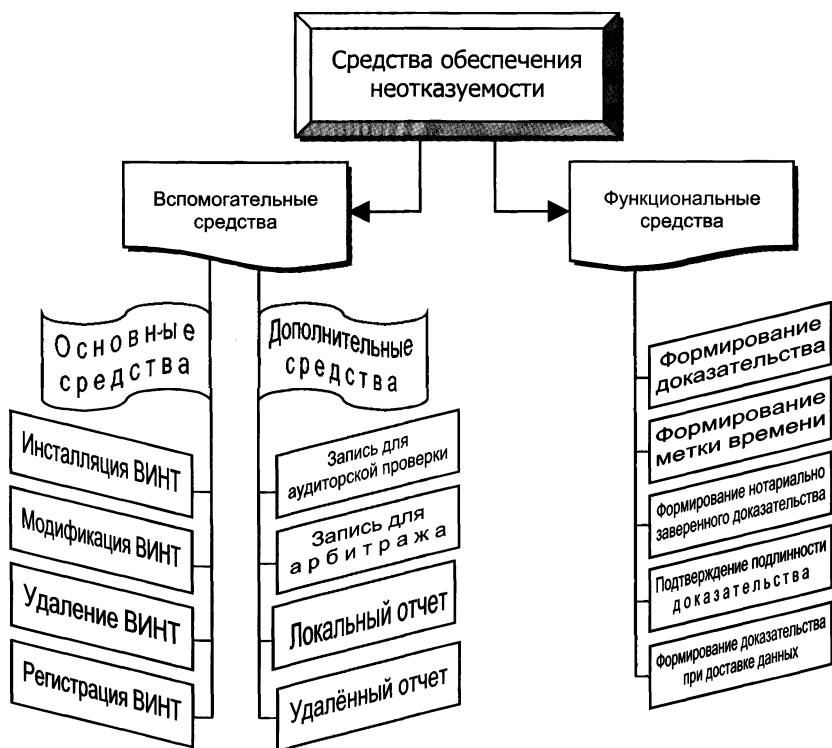


Рис. 5.3. Средства, используемые в процедурах обеспечения неотказуемости

5.3.2.1. Вспомогательные СРНТ

Деятельность, связанная с обеспечением ПРНТ, может затрагивать распределение информации, паролей или ключей (использование системы управления ключами) между объектами, которым необходимо выполнение ПРНТ. Это может повлечь использование специализированного протокола между взаимодействующими сторонами и другими объектами, обеспечивающими СЛНТ. Обеспечение ПРНТ также может включать аннулирование ключей, которые использовались при формировании доказательства.

СРНТ позволяют пользователю получить, модифицировать и удалить ВИ, которая необходима для обеспечения ПРНТ (ВИНТ). В широком смысле такими средствами являются:

- средство инсталляции ВИНТ;
- средство модификации ВИНТ;
- средство удаления ВИНТ;
- средство регистрации ВИНТ.

Для обеспечения СЛНТ могут потребоваться следующие дополнительные вспомогательные действия (процедуры):

- запись (регистрация) события для проведения последующей аудиторской проверки;
- запись (регистрация) результатов арбитражного разбирательства спора;
- локальный отчет о событии;
- удаленный отчет о событии.

В зависимости от ПЛБ при осуществлении процедуры для каждого события выбирается специфическая процедура.

5.3.2.2. Функциональные средства СЛНТ

Формирование доказательства. Это средство используется для формирования доказательства. Доказательство может формироваться непосредственно субъектом доказательства (без привлечения ДТС), одной или несколькими ДТС, действующими от имени субъекта доказательства или действующими

вместе с субъектом доказательства и одной или несколькими ДТС.

Возможные входные данные следующие:

- ПЛНТ;
- УИД субъекта доказательства;
- УИД объекта, запрашивающего СЛНТ;
- данные или цифровой отпечаток данных;
- УИД ДТС, которая будет использоваться для формирования ЭЦП, маркера безопасности или иного доказательства.

Возможные выходные данные следующие:

- доказательство (например ЭЦП или маркер безопасности);
- УИД ДТС, которая сформировала ЭЦП, маркер безопасности или иное доказательства.

Формирование метки времени. Это средство используется для формирования меток времени.

Возможные входные данные следующие:

- УИД объекта, запросившего метку времени;
- УИД ДТС, исполняющей роль службы меток времени;
- данные (например подписанное сообщение, квитанция), или ЭЦП, или цифровой отпечаток данных.

Возможные выходные данные следующие:

- «скрепляющая ЭЦП» (counter-signature), сформированная ДТС;
- опознавательный знак метода и/или криптоалгоритма, используемого для формирования «скрепляющей ЭЦП» (который указывается повторно, если используются данные или цифровой отпечаток данных);
- УИД службы меток времени;
- дата и время, когда был получен запрос на проставление метки времени;

- дата и время, когда была сформирована «скрепляющая ЭЦП»;
- подписанное сообщение, которое содержит метку времени и цифровой отпечаток входных данных.

Формирование нотариально заверенного доказательства. Это средство используется для передачи доказательства в ДТС на хранение.

Возможные входные данные следующие:

- UID объекта, запросившего формирование доказательства;
- доказательство (например маркер безопасности или ЭЦП);
- UID средства формирования доказательства;
- UID ПЛНТ.

Возможные выходные данные следующие:

- регистрационный номер доказательства;
- дата и время регистрации доказательства.

Подтверждение подлинности доказательства. Это средство используется для подтверждения (проверки) подлинности доказательства.

Возможные входные данные следующие:

- доказательство;
- UID субъекта доказательства;
- UID пользователя доказательством;
- идентификатор ключа, используемого для проверки доказательства;
- указатель использования доказательства по назначению (который может быть проанализирован с целью определения того, что доказательство является приемлемым для использования в соответствии с ПЛНТ).

Возможные выходные данные следующие:

- результат проверки подлинности (т.е. доказательство подлинное или нет);

- УИД субъекта доказательства;
- УИД средства формирования доказательства;
- УИД объекта, запрашивающего проверку подлинности доказательства;
- УИД ДТС, которая проверяла маркер безопасности (security token) или ЭЦП;
- данные или цифровой отпечаток данных.

Формирование доказательства при доставке данных через промежуточную ДТС. Вместо непосредственной передачи данных и/или ответных квитанций между отправителем и получателем, данные могут транслироваться через ДТС, и при этом доказательство СЛНТ может быть гарантированно ДТС с помощью специализированного средства. Такое средство также может использоваться тогда, когда допускается, что получатель мог бы заявить о разрыве канала связи (соединения), повлекшем отказ в доставке данных.

Для использования указанного средства, промежуточной ДТС должны быть предоставлены:

- данные;
- УИД получателя.

Кроме того, могут быть предоставлены дополнительно:

- цифровой отпечаток данных;
- УИД отправителя;
- ЭЦП;
- УИД промежуточной ДТС;
- ПЛНТ.

Возможные выходные данные от промежуточной ДТС:

- УИД промежуточной ДТС;
- УИД получателя;
- регистрационный номер доказательства;
- дата и время регистрации;
- данные или цифровой отпечаток данных.

5.4. Способы обеспечения неотказуемости

СЛНТ может быть реализована на основе применения тех или иных способов обеспечения неотказуемости (СПНТ), среди которых ЭЦП, шифрование, нотариальное заверение и обеспечение целостности данных, и на основе дополнительной поддержки со стороны, например, службы меток времени. В интересах СЛНТ могут использоваться асимметричные и симметричные криптографические алгоритмы. СЛНТ может использовать несколько из этих способов и служб одновременно, причем в различных сочетаниях, с целью удовлетворения соответствующих требований по безопасности прикладной системы, о которой идет речь.

5.4.1. СЛНТ, использующая маркеры безопасности (защитные конверты) ДТС

В этой схеме доказательство СЛНТ состоит из маркера безопасности, защищенного КПС (seal) с использованием секретного ключа, который известен только ДТС. ДТС формирует маркер безопасности по запросу стороны, которая запрашивает формирование доказательства и, соответственно, может проверить его в интересах пользователя доказательством или судьи. В таком случае ДТС является (предоставляет) объектом (средство) формирования доказательства и объектом (средство) проверки подлинности доказательства.

Сторона, запрашивающая формирование доказательства, передает ДТС данные или цифровой отпечаток данных, сопровождая их запросом на формирование маркера безопасности. Этот запрос должен быть защищен с точки зрения его целостности (например с использованием криптографической проверочной суммы), также он может быть защищен с точки зрения его конфиденциальности (например с использованием шифрования). Маркеры безопасности, защищенные с точки зрения их целостности, иногда называют *защитными конвертами* (secure envelopes).

Возможные входные данные, используемые при формировании маркера безопасности, следующие:

- указатель метода и/или криптографического алгоритма, используемого для обеспечения гарантий целостности маркера безопасности;
- указатель метода и/или криптографического алгоритма, используемого для обеспечения гарантий конфиденциальности маркера безопасности;
- UID субъекта доказательства;
- UID объекта, запрашивающего формирование доказательства;
- применяемая ПЛНТ;
- дата и время события или действия;
- данные, описывающие событие или действие.

Возможные выходные данные следующие:

- маркер безопасности;
- дата и время, когда был сформирован маркер безопасности.

5.4.2. СЛНТ, использующая маркеры безопасности и модули, защищающие от несанкционированного вмешательства

В этой схеме доказательство СЛНТ состоит из маркера безопасности, защищенного с помощью криптографической проверочной суммы (seal) с использованием секретного ключа, хранящегося внутри криптографических модулей защиты от несанкционированного вмешательства (доступа, НСД), которыми обладают объект (средство) формирования доказательства, объект (средство) проверки подлинности доказательства и судья. Модули защиты от НСД запрещают операции, которые предусматривают использование секретного ключа, и предотвращают любые попытки внешних модулей рассекретить значение этого ключа.

Модуль защиты от НСД в средстве формирования доказательства разрешает использовать секретный ключ при формировании маркера безопасности, защищенного криптографической проверочной суммой, в то время как модули, размещенные у объекта (в средстве) проверки подлинности доказательства и у судьи, позволяют только проверить маркер безопасности. Все взаимодействующие стороны должны гарантировать, что секретные ключи были инсталлированы в модули защиты от НСД корректно, причем так, что один и тот же секретный ключ может использоваться при формировании доказательства только одним объектом, а другими объектами — только для проверки подлинности доказательства.

Если имеет место спор, то пользователь доказательством предоставляет маркер безопасности, защищенный криптографической проверочной суммой на основе секретного ключа, судье и доказывает, что маркер должен быть сформирован с использованием модуля защиты от НСД, размещенным в средстве формирования доказательства, так как другие модули защиты от НСД, содержащие такой же секретный ключ, не способны сформировать маркер безопасности.

5.4.3. СЛНТ, использующая ЭЦП

В этой схеме доказательство СЛНТ состоит из формата данных, подписанных ЭЦП. При формировании ЭЦП используется ключ подписи, а при проверке ЭЦП — проверочный ключ.

В зависимости от ПЛБ могут быть востребованы данные о времени. Значение времени, которое предоставляется объектом и/или ДТС, выступающей в роли центра меток времени, может быть включено в ЭЦП. Если время не предоставляется ДТС, то нет необходимости в обеспечении гарантий надежности значения времени со стороны других объектов. Если судье необходимо значение времени и/или контекстно-зависимая информация для урегулирования спора, то такая информация должна быть получена из надежных (внушающих доверие) источников (например ДТС).

Объект (средство) проверки доказательства и судья должны быть способны получить ключ для проверки с целью подтверждения подлинности доказательства. Если нет возможности обеспечить гарантии того, что судья будет знать открытый ключ средства формирования доказательства любыми иными средствами, то доказательство также должно включать СЕРТ|ИБ для данного ключа.

ЭЦП может быть сформирована субъектом доказательства или ДТС, выступающей в роли центра формирования подписей.

Сформированная субъектом доказательства ЭЦП называется *непосредственной ЭЦП* (direct digital signature). ЭЦП, сформированная ДТС от имени субъекта доказательства, именуется *промежуточной ЭЦП* (mediated digital signature).

Сами по себе ЭЦП не эффективны при разрешении споров, в частности, когда СЕРТ|ИБ, используемый для проверки ЭЦП, был аннулирован. С целью урегулирования таких конфликтов, необходимо представить судье дополнительное доказательство об аннулировании СЕРТ|ИБ (например списки аннулированных СЕРТ|ИБ), которое подтвердит, что СЕРТ|ИБ был действителен в тот момент времени, когда была сформирована ЭЦП. Однако эта схема не позволяет урегулировать споры, когда владелец закрытого ключа своевольно использовал некорректное значение времени, или когда нарушитель скомпрометировал закрытый ключ, используемый при формировании ЭЦП. С целью урегулирования таких конфликтов необходимо дополнительно использовать доверенный источник эталонного времени или скрепляющую ЭЦП ДТС, которая выступает в роли центра меток времени.

Объект (средство) проверки подлинности доказательства может использовать Службу единого каталога (Directory) для получения информации (такой как СЕРТ|ИБ), необходимой для осуществления процедуры проверки подлинности. Объект (средство) проверки подлинности доказательства обязано получить открытый ключ, принадлежащий средству формирования доказательства. Этот ключ может содержаться в СЕРТ|ИБ, хранящемся в репозитории Единого каталога.

Иногда может понадобиться несколько СЕРТ|ИБ. Также для обеспечения гарантий того, что СЕРТ|ИБ является юридически действующим, следует запросить используемый перечень аннулированных сертификатов. Такой перечень является обязательным для каждого УЦ, который указан в маршруте сертификации (ITU-T Rec. X.509).

Пользователь доказательством может обратиться за поддержкой к ДТС, которая выступает в роли центра проверки ЭЦП, с целью проверки подлинности ЭЦП. При исполнении этой роли ДТС проверяет взаимосвязь между исходным сообщением (или, если используется, цифровым отпечатком сообщения) и ЭЦП.

В этом случае роль ДТС заключается в оказании помощи пользователю доказательством по преодолению сложности процедуры проверки доказательства и сохранении в силе результатов ранее запрошенных проверок с целью оптимизации ответов на будущие запросы проверок. Чтобы это осуществить, ДТС может запросить определенное взаимодействие со Службой единого каталога. Это предусматривает, что ДТС, исполняющая роль центра проверки ЭЦП, имеет открытый ключ по крайней мере одного УЦ. ДТС также учитывает надежные взаимосвязи, которые существуют между различными УЦ.

5.4.4. СЛНТ, использующая метки времени

Когда необходим надежный источник времени, а время, используемое объектом, формирующим ЭЦП или маркер безопасности, не может быть надежным, необходимо полагаться на ДТС, формирующую метки времени. Метки времени могут использоваться с целью установления факта того, что сообщение было подписано до компрометации ключа ЭЦП, и следовательно, что сообщение не было подделкой. ДТС, выступающая в роли центра формирования меток времени, будет снабжать меткой времени ЭЦП или маркер безопасности с целью установления факта того, когда был получен запрос метки времени. Метки времени могут запрашиваться средством формирования доказательства, стороной, обращающейся к СЛНТ, пользова-

телем доказательства или объектом (средством) проверки подлинности доказательства.

Центр формирования меток времени добавляет в данные время и дату, а также ЭЦП или криптографическую проверочную сумму. Он не требует аутентификации объекта, который запросил метку времени. Объект (средство) проверки подлинности доказательства обязан(о) определить, что метки времени были поставлены в течение разрешенного интервала времени, установленного политикой обеспечения безопасности.

Процедура формирования меток времени может быть совмещена с процедурой формирования ЭЦП или формирования маркера безопасности. Если объект, который формирует ЭЦП, включает в нее достоверное и надежное значение времени, то скрепляющая ЭЦП может не понадобиться.

5.4.5. СЛНТ, использующая промежуточную ДТС

Если имеет место соответствующее событие или действие, то средства промежуточной ДТС могут быть востребованы в явном виде или могут использоваться автоматически, без каких-либо условий. Затем промежуточная ДТС будет функционировать как посредническая система во всех процедурах информационного взаимодействия, в которых востребована СЛНТ, способная представить доказательство пользователю доказательством (например судье). Во всех случаях промежуточная ДТС ретранслирует данные и контролирует событие или действие.

ДТС обеспечивает доверенное и надежное хранение записей, которые будут использоваться в возможных последующих процедурах разрешения споров. Данные или цифровой отпечаток данных могут стать доказательством, если они хранятся у ДТС.

5.4.6. СЛНТ, использующая нотариальное заверение

В прикладных системах ЭМВОС и Интернет-архитектуры способы нотариального заверения обеспечивают гарантированность свойств данных, которыми обменивались между собой две или несколько сторон информационного взаимодействия,

а именно целостность, отправитель, время и получатель. Нотариус считается доверенным (надежным), если объекты привлекают его для хранения необходимой информации, которая может быть востребована в режиме предъявления доказательства (свидетельства) с целью обеспечения соответствующих гарантий, и для хранения записей для последующих процедур урегулирования споров. Для обеспечения функционирования службы нотариального заверения (нотариуса) возможно применение ЭЦП, соответствующих способов шифрования и обеспечения целостности.

Если нотариус выступает в роли объекта, формирующего доказательство (с помощью средства формирования доказательства), то он будет регистрировать (фиксировать) доказательство для обеспечения гарантий надежности соответствующих свойств данных. Кроме того, для идентификации этого доказательства может использоваться регистрационный номер.

Если нотариус выступает в роли объекта, проверяющего подлинность доказательства (с помощью средства проверки подлинности доказательства), то он будет подтверждать подлинность доказательства.

5.4.7. Угрозы СПНТ

СПНТ не являются полностью защищенными от всех возможных угроз. СПНТ, который обращается к ДТС, не может быть защищен, если ДТС не функционирует должным (штатным) образом. Это может произойти, либо в результате непредумышленного возникновения нештатной ситуации, либо в результате атаки, проведенной внутренним нарушителем (insider). Негативные последствия от реализации таких угроз могут быть весьма существенными, а главное — непредсказуемыми. СПНТ варьируются в зависимости от последствий нештатного функционирования ДТС и в зависимости от того, насколько тяжелыми будут последствия для ДТС с точки зрения нарушения процедурных характеристик соответствующих протоколов. В этом смысле должен проводиться соответствующий анализ угроз, с целью оценки вероятности их реализации

и тяжести последствий в соответствующей системе, с целью выбора совокупности способов, которые способны функционировать с учетом допустимых ограничений в условиях глобальных рисков.

5.4.7.1. Компрометация ключей

Компрометация ключа для формирования доказательства, принадлежащего объекту информационного взаимодействия. В течение периода с момента компрометации ключа до момента обнаружения такой компрометации законным владельцем ключа существует риск того, что нарушитель может воспользоваться скомпрометированным ключом для формирования доказательства, которое будет воспринято пользователем доказательством как правомерное. СПНТ не может выйти из нештатного состояния после какой-либо дискредитации, которая произошла вследствие такого неправомерного использования ключа для формирования доказательства. Однако существует возможность определения размеров ущерба путем привлечения центра формирования доказательства (например центра формирования ЭЦП). В дальнейшем этот центр может сохранить сформированное доказательство для последующего аудита безопасности и, следовательно, сделает возможным установление, кем и когда было сформировано доказательство. Кроме этого, желательно предать, насколько это возможно, публичной огласке факт неправомерного использования ключа. Однако не всегда можно оповестить об этом всех получателей, которым было передано доказательство, сформированное с использованием скомпрометированного ключа, предназначенного для формирования доказательства.

Как только законный владелец ключа обнаружит компрометацию своего ключа, ключ для формирования доказательства необходимо аннулировать. Если ключ для формирования доказательства является закрытым ключом, то соответствующий сертификат открытого ключа необходимо аннулировать. Для этого можно использовать списки аннулированных (отозванных) сертификатов (ITU-T Rec. X.509). Однако этого не достаточно, так как это не предотвращает отдельных случаев неправомерного

использования ключа. Возможные варианты противодействия такой угрозе включают применение СПНТ, в которых формирование доказательства требует взаимодействия с ДТС, а также с субъектом доказательства. Например, использование промежуточных или скрепляющих ЭЦП центра меток времени способно защитить от такой формы угроз. В последнем примере ПЛНТ устанавливает, что доказательство действительно только тогда, когда оно корректно подписано скрепляющей ЭЦП центра меток времени.

Компрометация ключа может быть и преднамеренной. Если ПЛНТ устанавливает, что субъект доказательства не будет нести ответственность за неправомерное использование его ключа в период с момента компрометации последнего и до момента времени обнаружения этой компрометации, то субъект доказательства может использовать это положение ПЛНТ в своих корыстных целях. Другими словами субъект доказательства может заявить, что его ключ был скомпрометирован, и, следовательно, отказаться от участия в каком-либо действии или событии, которое действительно имело место. Эта угроза может быть парирована путем определения максимального времени задержки с момента обнаружения компрометации ключа до момента оповещения об этой компрометации. В соответствии с такой политикой, если пользователь доказательством не успел оповестить о компрометации ключа субъекта доказательства в пределах установленного времени, то субъект доказательства несет ответственность за последующее неправомерное использование своего ключа. Объекты (средства) проверки подлинности доказательства могут в дальнейшем удостовериться, что допустимая задержка объявления компрометации ключа истекла еще до признания какого-либо доказательства.

Компрометация ключа для формирования доказательства, принадлежащего ДТС. Если выявлена компрометация ключа ДТС, то ключ в обязательном порядке должен быть аннулирован. Если ключ для формирования доказательства является закрытым, то необходимо аннулировать соответствующий сертификат открытого ключа. Для этого можно использовать списки аннулированных (отозванных) сертификатов. Для того

чтобы рассматривать ранее сформированное доказательство с использованием (возможно) скомпрометированного ключа необходимо, чтобы ДТС после каждого применения такого ключа регистрировала и хранила запись события для проведения последующей аудиторской проверки. Если ключ ДТС скомпрометирован, то в дальнейшем такая запись может быть использована для урегулирования споров.

Подмена ключа для проверки подлинности доказательства, принадлежащего объекту информационного взаимодействия. Если такая угроза реализована, то пользователь доказательством и/или объект проверки подлинности доказательства введены в заблуждение и ошибочно верят в то, что у них имеется корректное доказательство. Однако если необходимо провести урегулирование спора, то будет выявлено, что доказательство неприемлемо, т.е. пользователь доказательством освобождается от ответственности, так как и он, и объект проверки подлинности доказательства действовали добросовестно, полагаясь на корректное доказательство, но судья вынес решение против них обоих. Возможные способы парирования этой угрозы включают использование строгих процедур, которые позволяют убедиться, что подлинный субъект использует подлинный ключ для проверки доказательства. Предположим, что подмена ключа имела место, сразу после ее обнаружения ложный ключ для проверки подлинности доказательства должен быть удален.

Подмена ключа для проверки подлинности доказательства, принадлежащего ДТС. Если ключ для проверки подлинности доказательства является открытым ключом, используемым ДТС непосредственно для проверки доказательства, то ДТС может быть введена в заблуждение и ошибочно поверит фальшивому доказательству, которое было подделано на каком-либо этапе передачи судье ключа для проверки (например в бумажных документах, изменение в сертификате). Соответствующим примером является ситуация, при которой судейская копия открытого ключа была заменена нарушителем.

Когда обнаружена атака такого типа, желательно предать публичной огласке, насколько это возможно, факт подмены ключа.

ча. Однако не всегда возможно оповестить об этом всех пользователей, воспользовавшихся доказательством, которое могло быть искажено на основе подмены ключа. Существует возможность определения того, какое доказательство было изменено до предупреждения о подмене ключа на основе использования центра проверки подлинности доказательства (например центр проверки ЭЦП), который мог сохранить запись события для проведения последующей аудиторской проверки. Используя такой способ, можно определить, какое доказательство было изменено до и после предупреждения о подмене ключа.

Если ключ для проверки подлинности доказательства является открытым ключом, применяемым пользователями доказательством для непосредственной проверки СЕРТ, то сразу после обнаружения подмены целесообразно его сменить.

5.4.7.2. Компрометация доказательства

Информация, которая когда-то была использована в качестве доказательства, может перестать быть таковой. Такая информация называется скомпрометированным доказательством.

Несанкционированная модификация или уничтожение доказательства. В данном случае, после того как действие или событие произошло, сторона, заинтересованная в отказе от соучастия в событии, осуществляет модификацию или уничтожение доказательства. В дальнейшем эта сторона может успешно отказаться от участия в событии, которое фактически имело место. От этой угрозы можно защититься с помощью реализации соответствующих способов обеспечения безопасности, предотвращающих модификацию и разрушение доказательства (например резервное копирование и хранение). Использование ДТС для хранения доказательства может обеспечить эффективную защиту от такой угрозы, так как хранилище ДТС является более надежным и защищенным, чем средство хранения у пользователя доказательством.

Разрушение или признание доказательства недействительным. Эта угроза влечет за собой разрушение (уничтожение) хранящегося в ДТС доказательства. Она может иметь место тогда, когда ДТС недостаточно осмотрительна, а также когда ДТС не

провела адекватных мероприятий по обеспечению резервного копирования и хранения. От этой угрозы можно защититься с помощью реализации соответствующих СПНТ, которые предусматривают хранение у пользователя доказательством всех необходимых для урегулирования споров доказательств. В дальнейшем пользователь доказательством может гарантировать, что доказательство не будет уничтожено, даже если ДТС проявила халатность или захвачена злоумышленником.

5.4.7.3. Фальсификация доказательства

Фальсификация доказательства посторонним объектом. В данном случае спорного события не произошло, но посторонний объект проникает вовнутрь системы и формирует неправомерное доказательство того, что не произошло. Такое событие может случиться тогда, когда привлекается нотариус. Для защиты сохраненного доказательства от подделки или модификации со стороны нарушителя могут использоваться криптографические методы обеспечения безопасности.

Ошибочная проверка подлинности доказательства. В тех способах, в которых ДТС используется для проверки подлинности доказательства, существует угроза того, что ДТС будет информировать пользователя доказательством о наличии у нее подлинного действительного доказательства, являющегося на самом деле недействительным. Если возникнет спорная ситуация, то пользователь доказательством не сможет убедить судью в том, что имело место оспариваемое событие. Эту угрозу можно парировать с помощью использования СПНТ, при котором объект (средство), проверяющий(ее) подлинность доказательства, может напрямую подтвердить подлинность доказательство без привлечения ДТС.

Фальсификация доказательства ДТС. Эта угроза заключается в том, что ДТС может «выдумать» доказательство, относящееся к событию, которого никогда не было. Если ДТС является доверенной со стороны судьи, то последний мог бы признать сфальсифицированное доказательство и, следовательно, мог быть введен в заблуждение, что привело бы к принятию им неправильного решения. Такая угроза может быть парирована с по-

мощью использования СПНТ, при котором ДТС было бы весьма трудно фальсифицировать доказательство, или с помощью обеспечения гарантий того, что привлекаемые ДТС являются надежными (заслуживающими доверие), а также имеют определенные обязательства. Как правило, весьма трудно представить неопровержимое доказательство надежности объекта.

5.5. Взаимосвязи с другими СЛБ и СПБ

5.5.1. Аутентификация

При взаимодействии с ДТС объектам информационного взаимодействия может понадобиться подтвердить свою подлинность на основе использования СЛАУ. Последовательные итерации ПИНО могут сопровождаться определенными гарантиями, основанными на использовании службы аутентификации источника данных. Например, если ДТС используется для формирования ЭЦП, то она может быть востребована для аутентификации субъекта доказательства еще до формирования ЭЦП.

5.5.2. Управление доступом

СЛУД может использоваться для обеспечения гарантий того, что информация, хранимая у ДТС, или услуга, предлагаемая ДТС, доступна только для авторизованных субъектов.

5.5.3. Обеспечение конфиденциальности

СЛКН могут быть востребованы для защиты данных от несанкционированного вскрытия (включая, в некоторых случаях, несанкционированное вскрытие ДТС или для ДТС), а также для защиты от несанкционированного вскрытия доказательства.

5.5.4. Обеспечение целостности

СЛЦЛ будут востребованы для обеспечения гарантий, касающихся целостности доказательства.

Кроме этого, при использовании СЛНТ совместно со службой подтверждения источника данных или СЛНТ совместно со службой подтверждения доставки данных, целостность данных должна гарантировать, что данные, циркулирующие между источником и получателем, не могут быть модифицированы без обнаружения факта модификации.

5.5.5. Аудит

Пользователь доказательством может воспользоваться функцией записи результатов аудиторской проверки для сохранения доказательства в целях его последующего использования в случае возникновения спора (конфликтной ситуации).

Нотариус или промежуточная ДТС могут воспользоваться функцией записи результатов аудиторской проверки для регистрации содержания, источника, получателя и времени создания/отправки/получения сообщений.

5.5.6. Обеспечение ключами

СЛКЛ может быть использована для обеспечения ключами процедур формирования и проверки подлинности доказательства. Также эта служба может быть востребована для обеспечения ключами процедуры проверки подлинности доказательства даже если соответствующий ключ, который использовался для формирования доказательства, перестал быть действующим или доступным.

5.6. СЛНТ в системах ЭМВОС и Интернет-архитектуры

5.6.1. СЛНТ с подтверждением источника данных

СЛНТ вместе со службой подтверждения источника данных обеспечивает получателю данных защиту последних от любых ложных попыток отправителя отказаться от передачи совокупности данных или компонентов этой совокупности данных. Та-

кая защита может быть реализована путем передачи объектом (средством) формирования доказательства (как правило, это отправитель данных, но может быть ДТС) объекту (средству) проверки подлинности доказательства (как правило, это получатель данных, возможно, сторона, представляющая получателя данных) доказательства того, что данные были переданы отправителем.

Когда используется метод ЭЦП, то доказательством является ЭЦП данных или цифровой отпечаток данных. Применение СЛНТ зависит от предварительно согласованной схемы обеспечения подлинности доказательства, которая включает следующие фазы:

- a)* сторона, обращающаяся к СЛНТ, формирует доказательство или получает его от ДТС и присоединяет это доказательство к данным;
- b)* доказательство становится доступным пользователю доказательством;
- c)* в случае возникновения спора, пользователь доказательства предъявляет данные и доказательство, а судья проверяет данные, подтвержденные доказательством.

5.6.2. СЛНТ с подтверждением доставки данных

СЛНТ вместе со службой подтверждения доставки данных обеспечивает отправителю данных защиту последних от любых последующих ложных попыток получателя отказаться от приема совокупности данных или компонентов этой совокупности данных. Такая защита может быть реализована путем передачи объектом (средством) формирования доказательства (как правило, это получатель данных, но может быть ДТС) объекту (средству) проверки подлинности доказательства (как правило, это отправитель данных, возможно, сторона, представляющая отправителя данных, или ДТС) доказательства того, что данные были доставлены.

Применение СЛНТ зависит от отправки получателем данных соответствующей квитанции, содержащей доказательство.

Такая квитанция будет включать подтверждение получения данных в форме ЭЦП (или цифрового отпечатка), вычисленной по всей последовательности данных, входящих в полученное сообщение, в момент приема последнего.

Когда используется метод ЭЦП, то доказательством является подписанная квитанция.

Существуют два варианта применения СЛНТ: в условиях отсутствия ДТС или с привлечением ДТС, выступающей в роли центра доставки.

5.7. СЛНТ в системах хранения и ретрансляции

В системе хранения и ретрансляции сообщение доставляется от его отправителя до его получателя, проходя при этом через одну или несколько промежуточных систем (intermediary), именуемых посредниками доставки (transfer agent), или ретрансляторами. В таких системах передача сообщения включает в себя не только связь между отправителем и получателем, но и связь между отправителем и ретранслятором, связь между получателем и ретранслятором и связь между ретрансляторами. СЛНТ может применяться отдельно на каждом ретрансляционном участке, используемом для доставки сообщения до конечного получателя.

СЛНТ с подтверждением (доказательством) источника данных (Non-repudiation with proof of origin service) обеспечивает защиту от ложного отказа отправителя от факта передачи им сообщения или его компонентов. Доказательством, полученным этой службой, могут воспользоваться получатель или ретрансляторы.

СЛНТ с подтверждением (доказательством) доставки данных (Non-repudiation with proof of delivery service) обеспечивает защиту от ложного отказа получателя от факта получения им сообщения или его компонентов. Доказательством, полученным этой службой, могут воспользоваться отправитель или ретрансляторы.

СЛНТ с подтверждением (доказательством) получения сообщения для ретрансляции (Non-repudiation with proof of submission service) обеспечивает защиту от ложного отказа посредника доставки (ретранслятора) от факта получения им сообщения для

дальнейшей передачи (либо от отправителя, либо от другого посредника доставки). Доказательством, полученным этой службой, могут воспользоваться отправитель или другие ретрансляторы.

СЛНТ с подтверждением (доказательством) передачи сообщения, подлежащего ретрансляции (Non-repudiation with proof of transport service) обеспечивает защиту от ложного отказа посредника доставки (ретранслятора) от факта передачи им сообщения (либо получателю, либо другому ретранслятору). Доказательство, полученное этой службой, используется отправителем.

СЛНТ с подтверждением (доказательством) участия в процедуре доставки сообщения (Non-repudiation with proof of transfer service) обеспечивает защиту от ложного отказа посредника доставки (ретранслятора) от собственной ответственности за доставку сообщения (от собственного участия в процедуре доставки сообщения). Эта служба используется в случае участия нескольких посредников доставки (ретрансляторов) в процедуре доставки сообщения. Когда ретранслятор, первым принявший сообщение, передает его второму ретранслятору, то последний может предоставить первому доказательство того, что он взял на себя ответственность по дальнейшей доставке сообщения. Если в процедуре доставки сообщения участвуют более двух посредников доставки (ретрансляторов), то СЛНТ может также использоваться между вторым и третьим ретрансляторами, и т.д.

Все перечисленные варианты использования СЛНТ даны в табл 5.1.

Таблица 5.1

Наименование службы	Защита от ложного отказа	Используется
Подтверждение источника	Источника	Получателем, ретранслятором
Подтверждение получения сообщения для ретрансляции	Ретранслятора	Источником

Наименование службы	Защита от ложного отказа	Используется
Подтверждение передачи сообщения, подлежащего ретрансляции	Ретранслятора	Источником
Подтверждение участия в процедуре доставки сообщения	Ретранслятора	Ретранслятором
Подтверждение доставки	Получателя	Источником, ретранслятором

Дополнительные варианты СЛНТ (с подтверждением получения сообщения для ретрансляции и с подтверждением передачи сообщения, подлежащего ретрансляции) могут использоваться при высоких уровнях декомпозиции (модульности) системы, а в дальнейшем при снижении уровня декомпозиции (модульности) системы; может быть осуществлен переход к основным вариантам СЛНТ (с подтверждением источника данных и с подтверждением доставки данных). Например, подтверждение передачи сообщения, подлежащего ретрансляции, может быть реализовано с помощью усовершенствования процедуры передачи сообщения от отправителя к получателю на основе увеличения числа итераций информационного взаимодействия, одной из которых является итерация передачи от транслятора к отправителю положительной квитанции о доставке. Затем необходимо использовать службу подтверждения источника для защиты этой квитанции.

5.8. Восстановление в СЛНТ

Восстановление безопасности касается ситуаций, которые не могли бы произойти в штатных условиях. Однако реалии компьютерной безопасности таковы, что нештатные ситуации имеют место и лучше всего быть готовым к таким неожиданностям.

В основном это относится к большинству СПНТ, которые зависят от криптографических ключей и соблюдения необходимого для их защиты режима секретности. Потеря или вскрытие криптоключа должно упреждаться на основе немедленного ввода в действие плана восстановления.

Если СЛНТ использует закрытые криптографические ключи, то может возникнуть следующая ситуация (рис. 5.4).

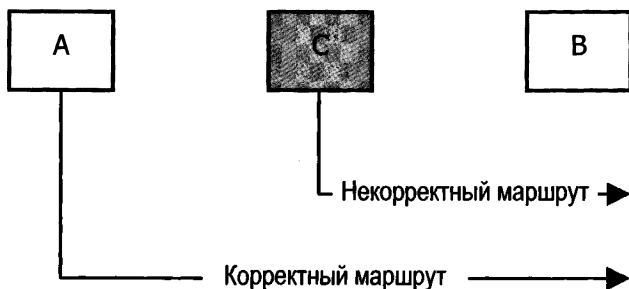


Рис. 5.4. Использование мошенником скомпрометированного ключа стороны А

Данные, подписанные мошенником (С), использующим скомпрометированный закрытый ключ стороны А, могут быть предоставлены действительному участнику информационного обмена (В). Можно предположить, что по прошествии некоторого времени В будет иметь все основания поиска А, передавая последнему подписанное сообщение в качестве доказательства его действий (или бездействия), связанных с появлением этого неавторизованного сообщения. Сторона А публично заявит о потере соответствующего закрытого ключа и сошлется на этот инцидент.

Если будет обращение к судье или в арбитраж с заявлением о рассмотрении этого инцидента, то степень ответственности А за произошедшее, вероятнее всего, будет устанавливаться на основе определения разницы во времени между моментом публичного заявления о скомпрометированном ключе и моментом появления неавторизованного подписанного сообщения. И уж точно

сторона *А* будет нести ответственность, если будет установлено, что сообщение датировано более ранним числом относительно даты публичного уведомления о скомпрометированном ключе. Более того, если мошенник *С* действительно датировал сообщение более ранним числом, то *А* понесет реальную ответственность, если, конечно, не появятся дополнительные обстоятельства, связанные с этим случаем.

Для выхода из такой ситуации необходимо попытаться узнать, когда точно было подписано сообщение (время подписи). Так как время появления сообщения, сформированного мошенником *С*, не может быть достоверным, то необходимо обратиться в ДТС для формальной регистрации сообщения, которую можно осуществить одним из следующих способов (или использовать оба):

- копирование сообщения и ЭЦП в массив данных для проведения последующей аудиторской проверки (т.е. использование нотариуса);
- применение скрепляющей ЭЦП, вычисленной по всей последовательности символов сообщения и включающей дату и время регистрации, которые были получены от независимой ДТС (т.е. Службы меток времени).

Вследствие необходимости выполнения этой процедуры мошенник мог бы неумышленно задокументировать реальное время и дату ЭЦП. В дальнейшем судья смог бы вынести мотивированное судебное решение об ответственности потерпевшей стороны *А* в зависимости:

- от временного интервала между датой/временем появлением сообщения и датой/временем формирования скрепляющей подписи, который должен укладываться в пределы достаточно небольшого временного окна (например 24 часа);
- от временного интервала между датой/временем появлением сообщения и датой/временем формального объявления о потере или компрометации ключа.

В данном случае эффективность неправомерного использования потерянного или скомпрометированного криптоключа будет снижаться с уменьшением длительности временного окна, в течение которого разрешается зарегистрировать данные в Службе меток времени.

Ответственность стороны *A* в случае компрометации ключа зависит от действующей ПЛБ. Не всегда можно выявить уязвимости системы обеспечения безопасности мгновенно. Таким образом, даже если сторона *A* заявила ДТС сразу же после того, как ей стало известно о компрометации ключа, существует вероятность того, что мошенник *C* сможет фальсифицировать сообщения после компрометации закрытого ключа стороны *A* и до момента обнаружения этой компрометации стороной *A*.

При урегулировании споров играют важную роль следующие значения времени:

- время, в которое сторона *A* сообщила о компрометации. Сторона *A* будет отвергать все сообщения, которые после этого момента времени могли бы представлены как подписанные (целесообразно, чтобы использование закрытого ключа было прекращено сразу после того, как сторона *A* узнает о его компрометации);
- время, заявленное стороной *A*, которое предшествовало компрометации ключа. Сторона *A* не будет отвергать сообщения, которые до этого момента времени могли бы представлены как подписанные. Это время вообще может не существовать, так как сторона *A* может обнаружить компрометацию, но не быть уверенной относительно реального времени произошедшего события.

5.9. Взаимодействие со Службой единого каталога

ЭЦП может быть проверена с использованием соответствующего открытого ключа. Когда открытый ключ, содержащийся в СЕРТИБ пользователя, представлен в Службе единого каталога, корректность ключа проверяется путем обращения к известному

УЦ с запросом о предоставлении его открытого ключа (проверить ЭЦП УЦ в сертификате ключа пользователя).

Так как УЦ, выпустивший СЕРТ|ИБ, может изменить свой открытый ключ уже после того, как был выдан СЕРТ|ИБ, необходимо иметь средства для проверки корректности «устаревшего» открытого ключа. В связи с тем, что обычно известен только тот ключ, который является действующим открытым ключом УЦ, необходимо наличие связи между действующим открытым ключом и «устаревшими» открытыми ключами. Вследствие того, что получатель не осведомлен об изменениях ключей УЦ, ответственность за предоставление возможности и способов проверки их «старых» СЕРТ|ИБ несут различные УЦ. Это может быть достигнуто следующими двумя способами:

- путем заверения каждого устаревшего открытого ключа УЦ с помощью действующего открытого ключа УЦ;
- путем заверения каждого устаревшего открытого ключа УЦ с помощью следующего открытого ключа УЦ (применение последовательности (цепочки) сертификатов).

В первом случае существует возможность прямой проверки подлинности устаревшего открытого ключа УЦ, который соответствует закрытому ключу, используемому УЦ для выпуска оригинального СЕРТ|ИБ.

Во втором случае необходимо иметь возможность получения всей цепочки сертификатов для поэтапной проверки подлинности устаревшего открытого ключа УЦ. Такая проверка будет выполнена путем поиска первого СЕРТ|ИБ, содержащего значение периода его действия, который соответствует дате и времени подписанного сообщения. Затем ведется последовательный поиск СЕРТ|ИБ, у которого период действия не перекрывает самый последний период, с целью определения значения предыдущего открытого ключа УЦ.

ПРИМЕЧАНИЕ. Если существует возможность компрометации старого открытого ключа УЦ, то первый метод более предпочтителен, так как при использовании второго метода цепочка сертификатов, определяющая путь к старому открытому ключу УЦ,

могла быть взломана, и таким образом старые открытые ключи УЦ могли стать полностью скомпрометированными.

В Службе единого каталога УЦ не сохраняет записи о СЕРТ|СО других УЦ или об их пользователях, когда сроки действия сертификатов истекли. Более того, пользователь доказательством или ДТС должны накапливать всю необходимую доступную информацию (включающую списки аннулированных сертификатов, даже если они пустые), чтобы доказать, что конкретный открытый ключ был юридически действующим в некоторый момент времени.

СЕРТ|СО содержит дату своего выпуска УЦ. Кроме этого, он может содержать и другую дату, которая могла бы оказать содействие при урегулировании споров в некоторых ситуациях: дата, когда пользователь был еще уверен в том, что его ключ не был скомпрометирован. Все подписи, сформированные пользователем до этой даты, будут определены им как действительные. Если такая дата не указана, так как предполагается, что это наихудший случай, то все подписи, сформированные в течение реального срока действия СЕРТ|ИБ, могли бы рассматриваться как недействительные. Это имеет огромное значение в коммерческой сфере, особенно это важно для пользователя, подписавшего документ, который по-прежнему считается действительным, даже в случае когда ключ, используемый для подписи сообщения, был потерян. Несмотря на то что наличие этой даты в СЕРТ|СО является необязательным, эта дата будет востребована, если ключ соответствующего сертификата используется СЛНТ.

Доверенные взаимосвязи могут варьироваться со временем. Например, судья может доверять УЦ сегодня, но не обязательно — завтра. Такой тип доверия должен быть приемлем и для получателя. В этом случае последний должен знать, может ли потенциальный конфликт быть решен в его пользу или нет. Тип доверенных взаимосвязей, который был выбран конкретным судьей, должен быть выражен точно и недвусмысленно. Такие доверительные условия могут быть смоделированы с использованием следующих терминов надежности:

- УЦ являются полностью надежными и для них известен действующий открытый ключ;

- УЦ являются надежными относительно выпуска сертификата УЦ и СЕРТ|ИБ пользователей;
- УЦ являются надежными относительно выпуска только СЕРТ|ИБ пользователей (но не сертификата УЦ).

Такая информация должна свободно распространяться и быть доступным для пользователя доказательством. Последний может выбрать форму СЕРТ|ИБ, в которой содержится период действия сертификата. Определены две формы сертификатов политики безопасности: сертификаты политики безопасности, в которых закреплена ответственность судьи за хранение записи о таких сертификатах, и сертификаты политики безопасности, в которых закреплена ответственность получателя за хранение записи о таких сертификатах.

Общая структура службы обеспечения неотказуемости представлена в табл. 5.2.

Таблица 5.2

Структура службы обеспечения неотказуемости	Элемент	<u>Объект/субъект</u> : Субъект доказательства, Объект (средство) формирования доказательства, Объект (средство) проверки подлинности доказательства, Пользователь доказательством, ДТС в роли службы обеспечения неотказуемости, Судья
		<u>Информационный объект</u> : Доказательство
		<u>Цель объектов</u> : сбор, обработка, обеспечение доступности и признание неопровержимости доказательства

Таблица 5.2 (продолжение)

М Е Р О П Р И Я Т И Я	Объект/субъект	ДТС, Центр безопасности			
	Функция	(не определена)			
	Мероприятия, связанные с обеспечением процедуры неотказуемости	— Инсталляция — Удаление — Модификация — Регистрация			
	Объект/субъект	Объект (средство) формирования доказательства	Объект (средство) проверки подлинности доказательства	ДТС в роли службы обеспечения неотказуемости	Судья
	Функция	(не определена)	(не определена)	(не определена)	(не определена)
	Мероприятия, функционально связанные с процедурой обеспечения неотказуемости	— формирование доказательства — формирование нотариально заверенного доказательства	— формирование доказательства — формирование нотариально заверенного доказательства	— формирование метки времени — доставка через ДТС	(не определены)

Таблица 5.2 (окончание)

И Н Ф О Р М А Ц И Я	Входные/ выходные элементы данных, определяе- мые Центром безопасности сетевого сегмента	— Обеспечивающая информация, например пароль или ключи — Тип информации — Политика обеспечения неотказуемости
	Тип ин- формации, используемой в процедуре обеспечения неотказуемо- сти	— Доказательство — ЭЦП — Маркер безопасности — Сертификат безопасности — Метка времени
	Контрольная информация	Запись (регистрация) события для проведения последующей аудиторской проверки и результатов урегулирования конфликта; отчет о взаимосвязях между объектами/субъектами

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ

Многие прикладные (открытые) системы ЭМВОС и Интернет-архитектуры предъявляют определенные требования по обеспечению безопасности, которые зависят от предотвращения раскрытия информации. Такие требования могут включать защиту информации, которая используется для информационного обеспечения других СЛБ, например СЛАУ, СЛУД или СЛЦЛ. Если же эта информация станет известна нарушителю, то эффективность таких служб обеспечения безопасности резко снизится или вообще будет сведена к нулю.

Конфиденциальность — это свойство информации, которое обеспечивает ее недоступность или нераскрываемость для неавторизованных пользователей, объектов и процессов.

В данной главе определены общие основы создания и функционирования служб обеспечения конфиденциальности (СЛКН), а именно:

- базовые концепции обеспечения конфиденциальности;
- возможные классы способов обеспечения конфиденциальности (СПКН);
- классификация и описание средств для каждого класса СПКН;
- процедуры (вспомогательные и функциональные), необходимые для реализации того или иного класса СПКН;
- взаимодействие СЛКН и СПКН с другими службами и способами обеспечения безопасности.

Как и в других службах обеспечения безопасности, обеспечение конфиденциальности может осуществляться только в рамках контекста принятой политики обеспечения безопасности для соответствующей прикладной системы.

Некоторые из рассматриваемых далее процедур обеспечивают конфиденциальность (ПРКН) с привлечением прикладных систем, реализующих криптографические методы. В целом обеспечение конфиденциальности не зависит от использования соответствующих криптографических или иных алгоритмов, однако рассматриваемые далее классы СПКН могут зависеть от свойств соответствующих алгоритмов.

Как правило, обеспечение конфиденциальности необходимо тогда, когда информация представлена в форме данных, которые являются читабельными для потенциальных нарушителей. Поэтому в дальнейшем рассматривается обеспечение конфиденциальности потока трафика.

6.1. Общие положения

6.1.1. Основные концепции обеспечения конфиденциальности

Целевое предназначение СЛКН — гарантировать, что информация доступна только тем, кто авторизован. Поскольку информация представляется в форме данных и сами данные могут повлечь за собой контекстно-зависимые изменения (например, манипуляции с файлами могут повлечь за собой непосредственные изменения или изменения числа допустимых ячеек памяти), информация может быть извлечена из данных различными способами, а именно:

- a)* на основе понимания семантики данных (например словесное значение данных);
- b)* путем использования соответствующих атрибутов данных (таких как их наличие, дата сформирования, размер, дата последнего обновления и др.);
- c)* на основе анализа контекста данных, т.е. других объектов данных, которые связаны с ними;
- d)* путем наблюдения за динамическими изменениями форм представления данных.

Информация может быть защищена либо путем обеспечения гарантий того, что данные ограничены доступом к ним только тех, кто авторизован, либо путем представления данных таким образом, чтобы их семантика оставалась доступной только тем, кто обладает некоторой критической информацией. Эффективная защита конфиденциальности требует, чтобы была обеспечена защита необходимой управляющей информации (например ключей и другой рассекречивающей информации). Такая защита может быть обеспечена с помощью способов и средств, отличающихся от тех, которые используются для защиты данных (например криптографические ключи могут быть защищены с помощью физических средств).

В данной главе используются понятия *защищенной зоны* и *перекрывающихся защищенных зон*. Данные внутри защищенной зоны защищаются прикладными процессами или системами, реализующими соответствующий способ (или несколько соответствующих способов) обеспечения безопасности. Соответственно все данные в пределах защищенной зоны являются также защищенными. Если имеют место две или более перекрывающихся защищенных зон, то данные в субзоне перекрытия являются многократно защищенными. Отсюда следует вывод, что для обеспечения непрерывной защиты данных, которые перемещаются из одной зоны в другую, необходимо использовать перекрывающиеся защищенные зоны.

6.1.1.1. Защита информации

Передача или хранение информации основаны на представлении информации в форме данных. СПКН позволяют не допустить раскрытия информации путем защиты отдельных или всех данных.

К СПКН относятся:

- a) защита знания о наличии (существовании) данных или о характеристиках данных (например размер данных или дата их сформирования);
- b) защита доступа для чтения данных;
- c) защита знания семантики самих данных.

СПКН обеспечивают защиту информации от ее вскрытия:

- либо путем защиты формы представления элемента информации от вскрытия;
- либо путем защиты правил такого представления от вскрытия.

Во втором случае защита от вскрытия наличия данных или других атрибутов данных может быть обеспечена за счет комбинирования нескольких элементов данных с целью формирования элемента смешанных данных, а также путем защиты от вскрытия правил формирования смешанного элемента данных.

6.1.1.2. Процедуры закрытия и раскрытия

Процедура закрытия может быть представлена как перемещение информации из зоны *A* в субзону перекрытия (*B*) *A* с другой зоной *C*. *Процедура раскрытия* может рассматриваться как обратная процедуре закрытия.

Когда информация перемещается из зоны, защищаемой с помощью одного СПКН, в зону, защищаемую с помощью другого СПКН, тогда:

- если процедура закрытия, реализуемая вторым способом, предшествует процедуре раскрытия, реализуемой первым способом, то информация является непрерывно защищаемой;
- если процедура раскрытия, реализуемая первым способом, предшествует процедуре закрытия, реализуемой вторым способом, то информация не является непрерывно защищаемой.

В первом случае необходимо, чтобы между раскрытием, реализуемым старым способом, и закрытием, реализуемым новым способом, существовала некая форма коммутативности (связности, commutativity). Например, процедуры закрытия и раскрытия обладают свойствами коммутативности там, где одна зона защищена с помощью процедур УД или физических средств, а другая зона защищена с помощью криптографических преобразований.

Конфиденциальность напрямую влияет на поиск, доставку и администрирование информации следующим образом:

- a)* конфиденциальность при доставке информации в открытых системах ЭМВОС, включая Интернет, обеспечивается тогда, когда процедура закрытия (при доставке используется средство $(N-1)$ -уровня ЭМВОС или Интернет-архитектуры) и процедура раскрытия объединены (совмещены) в форме службы обеспечения конфиденциальности (СЛКН) в рамках единой службы передачи N -уровня ЭМВОС или Интернет-архитектуры;
- b)* конфиденциальность при поиске хранящихся данных обеспечивается тогда, когда процедура закрытия (при хранении и поиске) и процедура раскрытия объединены в форме высокоуровневой службы хранения и поиска ЭМВОС или Интернет-архитектуры;
- c)* другие формы конфиденциальности могут быть обеспечены путем объединения процедур закрытия и раскрытия с другими процедурами (например, с теми, которые используются в целях администрирования данных).

В некоторых СПКН средство закрытия оставляет часть защищаемых данных (с точки зрения их конфиденциальности) доступной пользователю СЛКН еще до того, как это средство полностью обработает все данные. Аналогично, в некоторых СПКН средство раскрытия становится доступным для начала обработки элемента защищенных данных (с точки зрения их конфиденциальности) еще до того, как они все станут доступными. Таким образом, совокупность данных может включать компоненты, которые все еще не закрыты, компоненты, которые уже закрыты, и компоненты, которые уже раскрыты.

Рассмотрим рис. 6.1, в котором последовательности процедур закрытия/раскрытия (ПРЗК/ПРРС) защищают конфиденциальность данных, доставляемых из начальной зоны *A* в зону *E*. В данной ситуации предполагается, что зоны *A* и *E* обеспечивают конфиденциальность с помощью службы УД, в то время как зона *C* защищает конфиденциальность с помощью службы шифрования. Субзоны перекрытия *B* (зон *A* и *C*) и *D* (зон *C* и *E*)

защищают данные с помощью шифрования, а также с помощью службы УД. В этом примере представлены следующие процедуры:

- a) ПРЗК t , которая зашифровывает данные и в таком виде доставляет их в субзону перекрытия B ;
- b) ПРРС u , которая перемещает данные из B в C . Эта ПРРС доставляет данные из зоны защиты на основе УД, но не затрагивает защиту конфиденциальности, которая применялась ПРЗК t ;
- c) ПРЗК v , которая опять использует защиту на основе УД с помощью перемещения данных в субзону перекрытия D . В этой субзоне данные защищаются с помощью шифрования и службы УД зоны E ;
- d) ПРРС w , которая расшифровывает данные и в таком виде доставляет их из субзоны D в зону E .

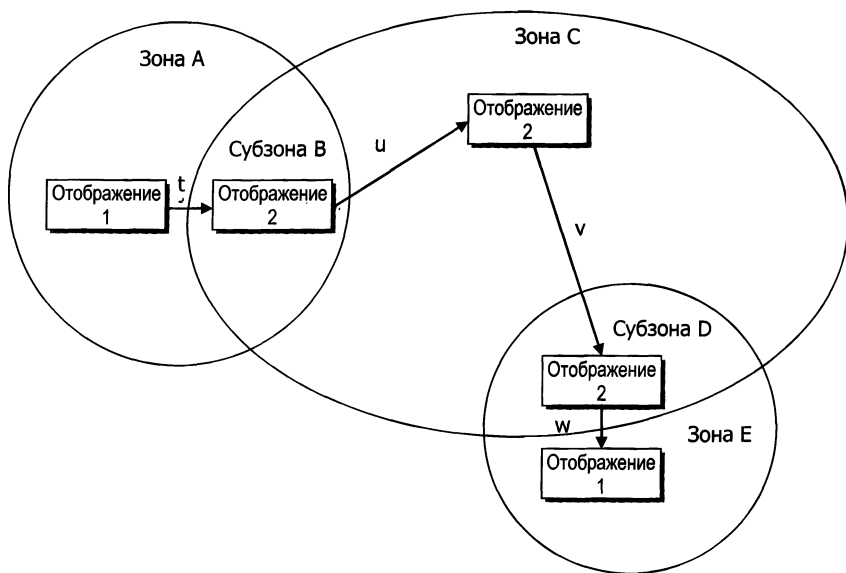


Рис. 6.1. Пример последовательности процедур закрытия/раскрытия данных, доставляемых через разные зоны защиты

6.1.2. Классы СЛКН

СЛКН могут классифицироваться по реализуемому ими типу защиты информации. К типам защиты информации относятся:

- a) защита семантики данных;
- b) защита семантики данных и связанных с ней атрибутов;
- c) защита семантики данных и связанных с ней атрибутов, а также любой другой информации, которая может быть извлечена из указанных данных.

Кроме этого, СЛКН может быть классифицирована по виду угроз, существующих в зоне функционирования этой СЛКН, от которых она защищает информацию. В соответствии с этим критерием СЛКН могут быть классифицированы следующим образом:

- 1) *защита от внешних угроз.* Функционирование таких СЛКН подразумевает, что те, кто имеет легитимный доступ к информации, не будут раскрывать ее тем, кто не авторизован. Такие СЛКН не защищают информацию, которая была раскрыта для авторизованных сторон информационного взаимодействия, а также не влияют на поведение таких сторон, несмотря на то, что они обладают ранее защищенной информацией. Например, критические файлы стороны А защищены с помощью шифрования. Но процессы, которые обладают необходимыми ключами для расшифрования, могут прочитать защищенные файлы и впоследствии записать их в незащищенной форме;
- 2) *защита от внутренних угроз.* Функционирование таких СЛКН подразумевает, что те, кто имеет право доступа (авторизован) к критической информации и данным, могут, с желанием или без него, провести ряд мероприятий, направленных на компрометацию конфиденциальности информации, которая подлежит защите. Например, метки безопасности и разрешения на доступ (clearances)

присоединяются к защищаемым ресурсам и к объектам, которые имеют право доступа к этим ресурсам. Доступ к таким ресурсам ограничивается в соответствии с вполне определенной и согласованной моделью управления потоком.

Службы, которые обеспечивают защиту конфиденциальности от внутренних угроз, должны либо не допускать использование скрытых каналов доставки, либо ограничивать скорость доставки такой информации в допустимых пределах. Кроме этого, они должны не допускать неавторизованного раскрытия информации на основе умозаключения, которое может быть следствием непредвиденного использования легитимных информационных каналов (например умозаключение на основе последовательности тщательно подобранных умышленных запросов к базам данных, каждый из которых является легитимным, или умозаключение на основе способности/неспособности программы, обслуживающей систему, выполнить команду).

6.1.3. Типы СПКН

Целевое предназначение СПКН — предотвращение неавторизованного раскрытия информации. Для решения этой основной задачи СПКН может:

- a)* предотвратить доступ к данным (например физическая защита канала). Для обеспечения доступа к данным только для авторизованных объектов могут использоваться способы УД (глава 3). Методы и способы физической защиты представлены в стандартах ISO 10202 и ANSI X9.17 / ISO 8734;
- b)* использовать методы и способы отображения, которые преобразуют информацию с целью ее защиты, т.е. чтобы она была недоступной для всех, кроме тех, кто обладает некоторой критической информацией о методах и способах отображения. К таким методам и способам относятся:

- шифрование;
- заполнение данных;
- расширение спектра.

СПКН любого из типов могут использоваться в сочетании с другими способами того же или иного типа.

СПКН могут обеспечивать различные виды защиты:

- защита семантики данных;
- защита атрибутов данных (включая наличие данных);
- защита от неавторизованного раскрытия информации на основе умозаключения.

Примерами таких классов СПКН являются:

- шифрование для закрытия данных;
- шифрование совместно с сегментацией и заполнением данных для закрытия размера (длины) протокольного элемента данных;
- методы и способы расширения спектра для маскирования самого существования канала связи.

6.1.4. Угрозы конфиденциальности

Существует единственная, наиболее общая угроза защищенной конфиденциальной информации, а именно вскрытие защищенной информации. Также существует несколько угроз защищенным конфиденциальным данным, которые соответствуют различным способам возможного извлечения защищенной конфиденциальной информации из данных. Рассмотрим некоторые угрозы.

6.1.4.1. Угрозы конфиденциальности, обеспечиваемой с помощью предотвращения доступа

К таким угрозам относятся:

- 1) преодоление защиты, основанной на предотвращении доступа. А именно:

- a) использование слабостей (уязвимостей) физической защиты каналов;
 - b) нелегальное проникновение («маскарад») или неуместное использование сертификатов;
 - c) использование слабостей (уязвимостей) в программной (программно-аппаратной) реализации способа предотвращения доступа (например, пользователь способен запросить доступ к файлу А, получить доступ к файлу А, а затем модифицировать имя этого файла так, чтобы получить доступ к другому файлу В);
 - d) встраивание программных закладок (типа «троянский конь») в доверенное программное обеспечение;
- 2) преодоление защиты, которая предотвращает доступ на основе доверенного использования других служб обеспечения безопасности (например, нелегальное проникновение («маскарад»), когда доступ основан на процедуре аутентификации (проверке параметра подлинности), некорректное использование сертификатов или взлом способа обеспечения целостности, который используется для защиты сертификатов);
- 3) использование вспомогательных программ системы с целью вскрытия (прямого или косвенного) информации о самой системе;
- 4) скрытые каналы.

6.1.4.2. Угрозы конфиденциальности, обеспечиваемой с помощью закрытия информации

К таким угрозам относятся:

- взлом криптографического способа защиты (с помощью криптоанализа, похищенных ключей, проведения атак типа «подбор открытого текста» и других способов и средств);
- анализ трафика;
- анализ заголовков протокольных элементов данных;
- скрытые каналы.

6.1.5. Типы атак на конфиденциальность

Каждая угроза, рассмотренная выше, может быть реализована в форме одной или нескольких атак.

Атаки можно разделить на активные и пассивные, т.е. атаки на конфиденциальность, в результате которых соответственно происходят или не происходят изменения в системе.

ПРИМЕЧАНИЕ. Является ли атака пассивной или активной можно определить с помощью характеристик и параметров атакуемой системы и с помощью действий, осуществляемых атакующим.

Примеры пассивных атак следующие:

- 1) прослушивание и перехват;
- 2) анализ трафика;
- 3) анализ заголовков протокольных элементов данных с целью, которая не является легитимной;
- 4) копирование данных из протокольных элементов данных в системах, которые не являются получателями этих данных;
- 5) криптоанализ.

Примеры активных атак следующие:

- 1) программные закладки типа «троянский конь» (вызывают возникновение незадокументированных свойств, что приводит к появлению уязвимостей в системе обеспечения безопасности);
- 2) скрытые каналы;
- 3) взлом способов обеспечения конфиденциальности (например взлом способа аутентификации (успешная атака «маскарад» под маской авторизованного объекта), взлом способа УД и перехват ключевой информации);
- 4) ложное применение криптографических способов защиты информации (например проведение атак типа «подбор открытого текста»).

6.2. Политики обеспечения конфиденциальности

Политика обеспечения конфиденциальности (ПЛКН) является частью общей ПЛБ и связана с обеспечением и использованием СЛКН.

Данные, представляющие информацию, конфиденциальность которой подлежит защите, являются объектом управления по отношению к тем субъектам, которые могут их читать. Более того, ПЛКН должна идентифицировать информацию, которая является объектом управления, а также определять каким субъектам предпочтительнее разрешить чтение этой информации.

Кроме этого, в зависимости от степени важности конфиденциальности различных типов информации ПЛКН может определять тип и уровень надежности каждого СПКН, которые используются СЛКН для обеспечения конфиденциальности каждого типа информации.

6.2.1. Отображение (описание) политики

При отображении (описании) ПЛКН требуются специальные средства для идентификации привлекаемых объектов и информации.

ПЛБ может быть выражена как совокупность правил. Каждое правило в ПЛКН может включать описание данных и описание объектов/субъектов. В некоторых политиках такие правила не представлены в явном виде, но могут быть извлечены из политики.

Рассмотрим некоторые возможные способы отображения ПЛКН.

ПРИМЕЧАНИЕ. Несмотря на то, что некоторые СПКН имеют очевидные аналогии со специфическими видами отображения политики, способ, по которому отображается политика, напрямую не предполагает применения специфического способа для реализации политики.

6.2.1.1. Описание информации

Политика может идентифицировать информацию различными способами:

- a) путем идентификации субъекта, который сформировал эту информацию;
- b) путем идентификации группы субъектов, каждый из которых может читать эту информацию;
- c) путем ее размещения;
- d) путем идентификации контекста, в соответствие с которым представлены данные (например их функциональное предназначение).

6.2.1.2. Описание объектов/субъектов

Существует много способов описания объектов/субъектов, включаемых в правила ПЛКН. Тем не менее существуют два наиболее общих альтернативных способа: на основе персональной и уникальной идентификации объектов/субъектов и на основе привязки атрибутов к каждому объекту/субъекту. Также существуют две формы описания объектов/субъектов, которые в итоге и определяют два типа политик обеспечения безопасности: политики, основанные на параметрах подлинности, и политики, основанные на правилах. Эти политики рассматриваются в главе 3.

6.3. Вспомогательная информация и средства обеспечения конфиденциальности

6.3.1. Вспомогательная информация

В некоторых СПКН процедуры закрытия и раскрытия основаны на использовании ВИ. Такая информация называется вспомогательной информацией для процедуры закрытия (ВИЗК, hiding confidentiality information) и вспомогательной информацией для процедуры раскрытия (ВИРС, revealing confidentiality information).

6.3.1.1. ВИ для процедуры закрытия

ВИЗК используется процедурой закрытия (ПРЗК). Примеры ВИЗК следующие:

- открытые ключи;
- симметричные ключи;
- место хранения данных;
- правила сегментирования.

6.3.1.2. ВИ для процедуры раскрытия

ВИРС используется процедурой раскрытия (ПРРС). Примеры ВИРС следующие:

- закрытые ключи;
- симметричные ключи;
- место хранения данных;
- правила сегментирования.

6.3.2. Средства обеспечения конфиденциальности

Средства обеспечения конфиденциальности (СРКН) могут быть разделены на те, которые затрагивают функциональные аспекты процедуры обеспечения конфиденциальности (ПРКН), и те, которые затрагивают вспомогательные аспекты ПРКН (рис. 6.2).

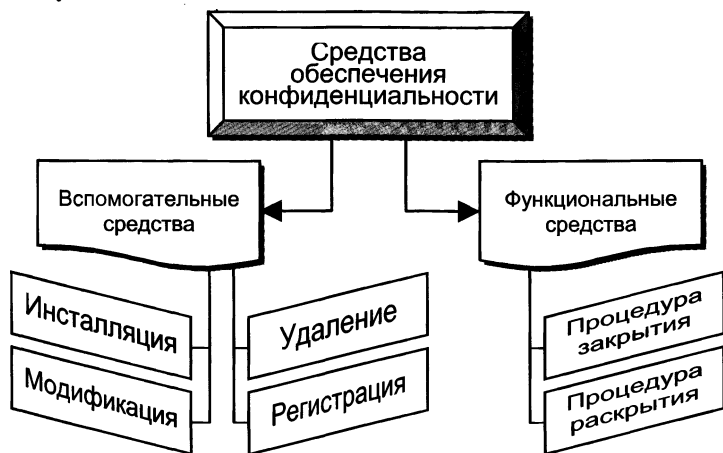


Рис. 6.2. Средства, используемые в процедурах обеспечения конфиденциальности

6.3.2.1. Функциональные СРКН

СРКН для процедур закрытия. Эти СРКН используются для защиты конфиденциальности данных. Возможные входные данные СРКН для ПРЗК следующие:

- 1) данные (конфиденциальность которых, возможно, уже защищена);
- 2) ВИПЗ;
- 3) специальные идентификаторы СПКН.

Возможные выходные данные СРКН для ПРЗК следующие:

- 1) данные, конфиденциальность которых защищена;
- 2) другие результаты проведенной ПРЗК;
- 3) УИД зоны защиты конфиденциальности, в которой были размещены данные, конфиденциальность которых защищена.

СРКН для процедур раскрытия. Это СРКН снимает защиту с данных, которые были ранее подвергнуты обработке с помощью ПРЗК.

Возможные входные данные СРКН для ПРРС следующие:

- 1) данные, конфиденциальность которых защищена;
- 2) ВИПР;
- 3) специальные идентификаторы СПКН.

Возможные выходные данные СРКН для ПРРС следующие:

- 1) данные (конфиденциальность которых, возможно, уже защищена);
- 2) другие результаты проведенной ПРРС;
- 3) УИД зоны защиты конфиденциальности, в которой были размещены выходные данные.

6.3.2.2. Вспомогательные СРКН

Вспомогательные СРКН позволяют пользователю получить, модифицировать и удалить ВИЗК и ВИРС (например ключи),

которая необходима при проведении ПРКН. В широком смысле такими СРКН являются:

- средства инсталляции ВИКН;
- средства модификации ВИКН;
- средства удаления ВИКН;
- средства регистрации ВИКН.

6.4. Способы обеспечения конфиденциальности

Конфиденциальность данных может зависеть от среды, в которой данные размещены или по которой доставляются. Более того:

- 1) конфиденциальность хранимых данных может быть гарантирована за счет использования способов, которые скрывают семантику (например шифрование) или которые фрагментируют данные;
- 2) конфиденциальность транслируемых данных может быть гарантирована за счет использования способов, которые преграждают доступ (например физическая защита каналов или управление маршрутизацией), с помощью способов, скрывающих семантику данных (например шифрование), или с помощью способов, «размазывающих» данные по спектру (например метод программно-перестраиваемой рабочей частоты, ППРЧ, frequency hopping).

Эти типы способов могут использоваться по отдельности или в сочетании.

Рассмотренная выше классификация позволяет сгруппировать СПКН следующим образом:

- 1) способы, которые предотвращают несанкционированный (неавторизованный) доступ к данным;
- 2) способы шифрования, которые скрывают данные, оставляя их доступными;
- 3) контекстно-зависимые способы, которые оставляют данные частично доступными, т.е. данные не могут быть

полностью восстановлены из ограниченного объема отобранных данных.

6.4.1. Обеспечение конфиденциальности на основе предотвращения доступа

Обеспечение конфиденциальности на основе предотвращения доступа может быть реализовано на основе процедур УД (глава 3), защиты физической среды и управления маршрутизацией.

6.4.1.1. Защита конфиденциальности на основе защиты физической среды

Средства физической защиты могут быть выбраны для обеспечения гарантий того, что данные, находящиеся в определенной физической среде, могут быть проверены только с помощью специальной и ограниченной совокупности способов. Конфиденциальность данных гарантируется за счет обеспечения того, что только авторизованные субъекты могут воспользоваться такими способами.

6.4.1.2. Защита конфиденциальности на основе управления маршрутизацией

Целевое предназначение этого способа — предотвратить несанкционированное вскрытие информации, содержащейся в доставляемых элементах данных. Этот СПКН основан на использовании только доверенных и безопасных средств маршрутизации данных.

6.4.2. Обеспечение конфиденциальности на основе шифрования

Целевое предназначение этих СПКН — предотвратить вскрытие семантики данных, которые либо доставляются, либо хранятся. Эти способы могут рассматриваться в форме функционального взаимодействия между двумя группами объектов:

- любой объект первой группы, который изначально мог обладать данными (с доступом к их семантике);
- любой объект второй группы, который является авторизованным получателем информации, представленной в формате данных.

Существуют два различных класса СПКН, которые представляют наибольший интерес:

- 1) СПКН, основанные на симметричном шифровании, в котором один и тот же ключ используется для зашифрования (ПРЗК) и для расшифрования (ПРРС) данных;
- 2) СПКН, основанные на асимметричном шифровании, в котором открытый ключ используется для зашифрования (ПРЗК) данных и соответствующий закрытый ключ используется для их расшифрования (ПРРС).

Важнейшее различие между этими двумя основными классами СПКН состоит в том, что в первом случае те СПКН, которые способны осуществлять ПРЗК, способны осуществлять ПРРС и наоборот, в то время как во втором случае, все или почти все СПКН могут осуществлять ПРЗК, а ПРРС могут осуществлять только те СПКН, которые имеют доступ к закрытому ключу.

6.4.2.1. Обеспечение конфиденциальности на основе дополнения данных

Целевым предназначением этого СПКН является предотвращение знания информации, которая представляет собой размер (длину) элемента данных. При реализации этого СПКН увеличивается длина элементов данных и причем так, что длина дополненных данных имеет незначительную корреляцию с их реальной длиной. Одним из способов выполнения этого условия является добавление случайно сформированных данных в начало или конец защищаемого элемента данных. Это должно быть сделано таким образом, чтобы дополнение могло распознаваться только авторизованными субъектами, но не могло быть выделено из реальных данных неавторизованными субъектами.

Для достижения такой цели дополнение данных может использоваться во взаимосвязи с криптографическими преобразованиями.

Этот способ может использоваться совместно с сегментированием данных на сетевом уровне ЭМВОС (стандарт ITU-T Rec. X.273|ISO/IEC 11577) или Интернет-архитектуры.

Дополнение данных может использоваться для защиты размера элементов данных, что соответствует маскированию канала доставки данных.

6.4.2.2. Обеспечение конфиденциальности на основе ложных событий (имитозащита)

Целевым предназначением этого СПКН является предотвращение атак типа «умозаключение» (глава 1), которые основываются на оценке того, что произошло события. Примеры реализации этого способа можно найти в протоколах обеспечения безопасности сетевого уровня, которые стремятся скрыть объем трафика, циркулирующего по ненадежным каналам.

Средство, реализующее этот способ, формирует имитовставки¹ (pseudo-events), например ложные протокольные элементы данных (bogus protocol data units, PDU-элемент), которые могут идентифицировать (т.е. определить, что это имитовставки) только авторизованные участники информационного взаимодействия. Данный способ может использоваться для парирования атак на закрытые каналы доставки, которые основаны на анализе передачи сигналов, зависящей от изменений интенсивности источника сообщений.

ПРИМЕЧАНИЕ. Дополнение данных и заполнение трафика являются примерами этого СПКН. В обоих примерах СПКН маскирует атрибуты объекта путем передачи нескольких имитовставок и криптографической защиты в целом.

¹ Имитозащита — защита от навязывания ложной информации. Имитозащита достигается обычно за счет включения имитовставки в передаваемый пакет данных.

6.4.2.3. Обеспечение конфиденциальности на основе защиты заголовка протокольного элемента данных

Целевым предназначением этого СПКН является предотвращение атак типа «умозаключение», основывающихся на оценке заголовков протокольных элементов данных, которыми обмениваются взаимодействующие стороны.

Одним из примеров такого способа является маскирование адреса (стандарт Rec. X.273 | ISO/IEC 11577). Промежуточная система X может принять PDU-элемент, зашифровать его и добавить в него новый заголовок, в котором адрес отправителя будет иметь значение X , а адрес получателя — Y , т.е. оконечной системы, которая расшифрует данные и таким образом восстановит оригинальный PDU-элемент. После того как оригинальный заголовок (включающий адреса) был зашифрован, атака типа «умозаключение», основанная на анализе PDU-заголовков, невозможна, так как, фактически, X и Y обмениваются зашифрованными PDU-элементами.

Другим примером, когда каждый PDU-элемент «добросовестно» передается системой A , является сформирование n дополнительных копий с различными адресами получателей и дополнительными функциями в заголовке (т.е. система формирует ложный широкополосный трафик).

Процедура маскирования адреса на сетевом уровне представлена в стандарте Rec. X.273 | ISO/IEC 11577. Процедура маскирования адреса может быть реализована и на других уровнях (например, ITU-T Rec. X.411 | ISO/IEC 10021—4 описывает использование маскирования адресов на прикладном уровне).

6.4.2.4. Обеспечение конфиденциальности на основе вставки полей, длины которых изменяются во времени

Этот способ, используемый совместно с шифрованием, предотвращает атаки типа «умозаключение», которые основываются на оценке динамических изменений элементов данных. С этой целью средство, реализующее такой способ, объединяет подлежащие защите данные с изменяемыми во времени полями

(переменные по длине имитовставки), причем таким образом, что нарушители не могут определить, какой вид изменений данных произошел: либо изменения самих защищаемых данных, либо изменения за счет изменяемых во времени длин вставленных полей. В идеальном варианте этот способ формирует свой отличительный формат данных для каждого потенциального вида наблюдения (пассивный перехват) защищаемых данных, которые позволяет парировать атаки типа «умозаключение», основывающиеся на оценке динамических изменений, так как последние отсутствуют. Примеры:

- 1) *передача PDU-элемента*. Изменяющееся во времени поле размещается перед защищаемым отрезком каждого PDU-элемента. Затем полученные таким образом составные данные зашифровываются с помощью криптографических способов с одновременным формированием непрерывной последовательности данных (chaining), например переменное поле влияет на зашифрование последовательных данных;
- 2) *хранение*. Если изменяющиеся во времени поля размещаются в начале хранящихся данных, то они скрывают возможные изменения или недостатки.

Этот способ может использоваться совместно с дополнением и сегментацией данных, что позволяет скрыть изменения длины защищаемых данных.

6.4.3. Обеспечение конфиденциальности на основе контекстно-зависимого размещения

Одной из форм защиты конфиденциальности на основе предотвращения доступа к данным может быть построение данных в любой из возможных контекстно-зависимых форм, количество которых весьма велико. Если такой способ не позволяет (вследствие вычислительных или физических проблем) проверить все возможные контекстно-зависимые формы за период времени до следующего изменения контекстно-зависимой формы, то может

быть достигнут необходимый уровень защиты конфиденциальности.

Примерами такого СПКН являются:

- 1) применение большого количества физических или виртуальных каналов передачи информации (например использование «размазанного спектра» (spread spectrum), при котором используется одна рабочая радиочастота из огромного количества возможных радиочастот);
- 2) применение большого количества элементов памяти для хранения данных (например адресов на магнитном диске);
- 3) передача информации по скрытым вторичным каналам связи, которые «спрятаны» внутри первичных каналов связи (стеганография, steganography).

Этот способ обеспечения конфиденциальности предполагает, что неавторизованные получатели не могут определить информацию, которая необходима в текущий момент времени для идентификации корректной контекстно-зависимой формы. Такая информация должна быть сама защищена с помощью СЛКН.

6.5. Взаимодействие с другими СЛБ и СПБ

6.5.1. Управление доступом

При регулировании доступа к данным может использоваться СЛУД, как это определено в главе 3.

6.6. Обеспечение конфиденциальности в ЭМВОС и Интернет-архитектуре

Взаимосвязи СЛБ в ЭМВОС и Интернет-архитектуре определены в главе 1.

Наиболее значимые услуги, предоставляемые СЛКН, следующие:

- услуга по обеспечению конфиденциальности информационного обмена с установлением соединения;
- услуга по обеспечению конфиденциальности информационного обмена без установления соединения (дейтаграммный режим);
- услуга по обеспечению конфиденциальности отдельных полей;
- услуга по обеспечению конфиденциальности потока трафика.

6.6.1. Услуга по обеспечению конфиденциальности информационного обмена с установлением соединения

Эта услуга обеспечивает конфиденциальность всех данных пользователя на N -ом уровне ЭМВОС или Интернет-архитектуры, доставляемых по соединению N -го уровня ЭМВОС или Интернет-архитектуры.

6.6.2. Услуга по обеспечению конфиденциальности информационного обмена без установления соединения (дейтаграммный режим)

Эта услуга обеспечивает конфиденциальность отдельных полей в составе данных пользователя на N -ом уровне ЭМВОС или Интернет-архитектуры, размещаемых в элементе данных службы (Service Data Unit — SDU) N -го уровня ЭМВОС или Интернет-архитектуры, который доставляется в дейтаграммном режиме.

6.6.3. Услуга по обеспечению конфиденциальности отдельных полей

Эта услуга обеспечивает конфиденциальность отдельных полей в составе данных пользователя на N -ом уровне ЭМВОС или Интернет-архитектуры, либо доставляемых по соединению N -го уровня ЭМВОС или Интернет-архитектуры, либо разме-

щаемых в одиночном SDU-элементе N -го уровня ЭМВОС или Интернет-архитектуры, который доставляется в дейтаграммном режиме.

6.6.4. Услуга по обеспечению конфиденциальности потока трафика

Эта услуга обеспечивает конфиденциальность информации, которая может быть извлечена из перехватываемых потоков трафика.

6.6.5. Использование услуг по обеспечению конфиденциальности на уровнях ЭМВОС и Интернет-архитектуры

Услуги по обеспечению конфиденциальности могут предоставляться на следующих уровнях ЭМВОС или Интернет-архитектуры:

- физическом (1-м) уровне;
- канальном (2-м) уровне;
- сетевом (3-м) уровне;
- транспортном (4-м) уровне;
- уровне представления данных (6-м) (в Интернет-архитектуре не используется);
- прикладном (7-м) уровне (5-м уровне Интернет-архитектуры).

6.6.5.1. Использование услуг по обеспечению конфиденциальности на физическом уровне

На физическом уровне СЛКН предоставляют только две услуги: (1) услуга по обеспечению конфиденциальности информационного обмена с установлением соединения и (2) услуга по обеспечению конфиденциальности потока трафика. Эти услуги могут предоставляться по отдельности или совместно. Услуга по обеспечению конфиденциальности потока трафика может иметь две формы: обеспечение конфиденциальности всего по-

тока трафика, которое может быть предоставлено только для некоторых типов передачи, и обеспечение конфиденциальности ограниченного потока трафика, которое может быть предоставлено всегда.

6.6.5.2. Использование услуг по обеспечению конфиденциальности на канальном уровне

На канальном уровне СЛКН предоставляют только две услуги: (1) услуга по обеспечению конфиденциальности информационного обмена с установлением соединения и (2) услуга по обеспечению конфиденциальности информационного обмена без установления соединения (дейтаграммный режим). Эти услуги могут использовать различные способы шифрования.

6.6.5.3. Использование услуг по обеспечению конфиденциальности на сетевом уровне

На сетевом уровне СЛКН предоставляют только три услуги: (1) услуга по обеспечению конфиденциальности информационного обмена с установлением соединения, (2) услуга по обеспечению конфиденциальности информационного обмена без установления соединения (дейтаграммный режим) и (3) услуга по обеспечению конфиденциальности потока трафика. Первые две услуги могут быть обеспечены с помощью различных способов шифрования и/или управления маршрутизацией. Третья услуга может быть обеспечена с помощью заполнения трафика совместно с услугами обеспечения конфиденциальности, предоставляемыми на сетевом уровне или более низких уровнях, и/или управления маршрутизацией. Эти услуги позволяют обеспечить конфиденциальность между узлами сетей, узлами подсетей или ретрансляционными сетевыми средствами.

6.6.5.4. Использование услуг по обеспечению конфиденциальности на транспортном уровне

На транспортном уровне СЛКН предоставляют только две услуги: (1) услуга по обеспечению конфиденциальности информационного обмена с установлением соединения и (2) услуга

по обеспечению конфиденциальности информационного обмена без установления соединения (дейтаграммный режим). Эти услуги могут быть обеспечены с помощью различных способов шифрования. Они позволяют обеспечить конфиденциальность между оконечными системами.

6.6.5.5. Использование услуг по обеспечению конфиденциальности на уровне представления данных

На уровне представления данных СЛКН предоставляют только три услуги: (1) услуга по обеспечению конфиденциальности информационного обмена с установлением соединения, (2) услуга по обеспечению конфиденциальности информационного обмена без установления соединения (дейтаграммный режим) и (3) услуга по обеспечению конфиденциальности отдельных полей. В случае предоставления третьей услуги на прикладном уровне указываются поля, конфиденциальность которых должна быть защищена.

6.6.5.6. Использование услуг по обеспечению конфиденциальности на прикладном уровне

На прикладном уровне СЛКН предоставляют все виды услуг: (1) услуга по обеспечению конфиденциальности информационного обмена с установлением соединения, (2) услуга по обеспечению конфиденциальности информационного обмена без установления соединения (дейтаграммный режим), (3) услуга по обеспечению конфиденциальности отдельных полей и (4) услуга по обеспечению конфиденциальности потока трафика. Первая и вторая услуги могут обеспечиваться с помощью различных способов шифрования, реализуемых на любом из нижних уровней. Третья услуга может быть обеспечена с помощью различных способов шифрования, реализуемых на уровне представления данных. Услуга по обеспечению конфиденциальности ограниченного трафика может быть предоставлена на основе использования различных способов заполнения трафика на прикладном уровне совместно с услугой обеспечения конфиденциальности, предоставляемой на одном из нижних уровней.

6.7. Форматы представления информации

Передача или хранение элемента данных осуществляется с использованием того или иного формата представления элемента данных (например, число семнадцать может быть закодировано как десятичное число 17, как шестнадцатеричное число 11, как девятое нечетное целое число, как седьмое простое число, как корень квадратный из 289, так как $17^2=289$). Информация может быть получена либо непосредственно из формата представления, либо из атрибутов формата представления. Таким образом, информацию можно получить одним из следующих способов:

- путем проверки объема данных, когда известны условные обозначения (установленные правила) формата представления и связанная с ними информация;
- путем установления наличия или отсутствия элемента данных;
- на основе размера (длины) элемента данных;
- на основе динамического варьирования форматов представления.

Например, информацию о том, что *«Король умер»* можно было бы получить на основе следующих умозаключений и анализа:

- путем проверки логического (булева) выражения, когда его значение справедливо, то король действительно умер, если нет, то не умер;
- путем установления наличия или отсутствия файла под названием «Сообщение о смерти короля» в каталоге файлов;
- путем проверки списка умерших монархов и обнаружения того, что размер данного списка увеличился;
- путем установления того, что счетчик, который указывает на количество дней, когда страна уже была в состоянии без монарха, может находиться под наблюдением для его ежедневной коррекции.

Процедура отображения элемента информации в некоторый формат представления определяется набором правил отображения (representation rules). Правила отображения описывают:

- как информация кодируется в данные;
- как данные могут быть отображены в информацию, которая была закодирована в них;
- какие должны быть сделаны явные и неявные контекстно-зависимые изменения, когда информация уже закодирована (например формирование файла может повлечь изменения в каталоге файлов).

СПКН защищают элемент информации следующим образом:

- либо путем защиты формата представления элемента информации от несанкционированного вскрытия на основе предоставления гарантий в рамках соответствующей зоны защиты;
- либо путем защиты знания правил отображения от несанкционированного вскрытия.

Различные зоны защиты могут иметь свои отличительные сильные стороны, зависящие от уровня защиты от несанкционированного вскрытия, обеспечиваемого для форматов представления информации в этих зонах. Также и различные наборы правил отображения могут иметь свои отличительные сильные стороны, зависящие от трудности самих правил отображения, которые становятся известны неавторизованным субъектам.

В качестве основы описания характеристик различных типов СПКН используется концепция *защиты конфиденциальности контекста*. Защита конфиденциальности контекста (для любого элемента информации) представляет собой соответствующий формат представления этого элемента информации, используемый в определенной зоне защиты.

Режим функционирования СПКН может стать понятным на основе определения того, что доставка информации, скорее всего, связана с ее многократной последовательной обработкой

в зависимости от конкретного контекста защиты конфиденциальности.

Изменение формата представления или изменение зоны защиты связано с переходом от одного способа защиты конфиденциальности контекста к другому. Изменение формата представления будет, как правило, вызывать переход к более защищенной форме представления или, наоборот, к менее защищенной. Аналогично и изменение зоны защиты будет, как правило, вызывать переход в более защищенную зону или, наоборот, в менее защищенную (рис. 6.1).

6.8. Скрытые каналы передачи

Термин *скрытый канал* (*канал утечки*) относится к способам, которые не предназначены для передачи информации, но которые могут быть использованы для доставки информации, что, в конечном счете, может привести к нарушению ПЛБ.

Атаки типа «скрытый канал» относятся к атакам, которые осуществляются внутри системы отправителем некоторых данных. Такая атака не накладывает ограничений на использование соответствующих средств доставки информации, которые обычно используются для этой цели. В достаточно сложной системе присутствует одно или несколько средств доставки информации помимо основных способов, которые обеспечивают процедуры обмена, хранения и извлечения данных. Такие средства именуются скрытыми каналами.

Многие скрытые каналы включают разрешенные процедуры управления (модуляции) состояниями или событиями, которые становятся явными для субъектов, не авторизованных для получения информации от источника такой модуляции. Информация доставляется между источником и получателем, которые одинаково понимают (распознают) ее смысл, а указанная модуляция обеспечивает перемещение такой информации.

При использовании различных процедур обмена данными, примерами каналов, которые основаны на распознавании смысла перемещаемой информации, являются:

- различные допустимые размеры PDU-элемента N -го уровня архитектуры ЭМВОС или Интернет-архитектуры;
- различные адреса получателей, которые доступны для приема или перехвата получателем по скрытому каналу при организации соединения или дейтаграммном режиме доставки на N -ом уровне архитектуры ЭМВОС или Интернет-архитектуры;
- различные допустимые промежутки времени между процедурами передачи по одному и тому же соединению или от одного и того же объекта на N -ом уровне архитектуры ЭМВОС или Интернет-архитектуры.

Последний пример представляет собой скрытый канал синхронизации.

При использовании различных способов хранения и извлечения данных, примерами каналов, которые основаны на распознавании смысла перемещаемой информации, являются:

- наименование, присвоенное области хранения;
- наличие или отсутствие определенных хранящихся данных;
- объем хранящихся данных;
- способность получения дополнительных предназначенных для хранения данных;
- продолжительность интервала времени, в течение которого хранятся или не хранятся определенные данные.

Первые из перечисленных примеров, в которых данные (их имена) могут храниться, а затем извлекаться, именуются как «скрытые каналы хранения».

Системные ресурсы и протоколы связи могут быть описаны и представлены как абстрактные характеристические объекты, используемые при проведении отдельных первичных процедур. Следовательно, в более общем представлении, примерами, которые основаны на распознавании смысла перемещаемой информации, являются:

- выбор одной из доступных процедур;

- порядок, в котором используются служебные примитивы;
- продолжительность интервала времени между используемыми процедурами, когда для получателя существует потенциальная возможность наблюдения по скрытому каналу.

Обеспечение конфиденциальности информации может быть гарантировано только тогда, когда все средства доставки (перемещения) информации выявлены и идентифицированы (включая скрытые каналы), а каждое из них контролируется на основе использования соответствующих СПКН.

Во многих примерах полная нейтрализация скрытых каналов является неразрешимой задачей (по техническим, организационным, экономическим или иным причинам). И все-таки можно добиться снижения объемов информации, которая будет перемещаться по таким каналам, до приемлемых значений.

Общая структура службы обеспечения конфиденциальности представлена в табл. 6.1.

В представленной структуре используются следующие концептуальные термины.

Объекты/субъекты обеспечения конфиденциальности в системах ЭМВОС:

- *инициатор*. Объект, который формирует предназначенные для передачи или хранения данные, конфиденциальность которых подлежит защите;
- *проверяющая сторона*. Субъект, который извлекает информацию из данных, конфиденциальность которых защищена;
- *ДТС, предоставляющая ВИ для обеспечения конфиденциальности*. Субъект, предоставляющий ВИ для процедуры закрытия или ВИ для процедуры раскрытия взаимодействующим объектам, обменивающимся данными, конфиденциальность которых защищена.

Структура службы обеспечения безопасности (обеспечения конфиденциальности)	Элемент	<u>Объект/субъект</u> : Инициатор, Проверяющая сторона, ДТС, предоставляющая ВИ для обеспечения конфиденциальности		
		<u>Функция</u> :		
		<u>Информационный объект</u> : Данные, конфиденциальность которых защищена		
	Цель Службы	Сделать информацию не доступной или не раскрываемой для неавторизованных пользователей, объектов или процессов		

М Е Р О П Р И Я Т И Я	Объект/субъект	Центр безопасности сетевого сегмента		
	Функция			
	Мероприятия, связанные с обеспечением процедуры конфиденциальности	— Инсталляция вспомогательной информации — Удаление вспомогательной информации — Блокирование вспомогательной информации — Модификация вспомогательной информации — Регистрация вспомогательной информации — Разблокирование вспомогательной информации		
	Объект/субъект	Инициатор	Проверяющая сторона	ДТС, обеспечивающая конфиденциальность
	Функция			
	Мероприятия, функционально связанные с процедурой обеспечения конфиденциальности	— Заккрытие данных — Маркер безопасности	— Раскрытие данных — Маркер безопасности	— Сертификат объекта

Таблица 6.1 (окончание)

И Н Ф О Р М А Ц И Я	Входные/выходные элементы данных, определяемые Центром безопасности сетевого сегмента	— Открытые ключи — Симметричные ключи — Маркер безопасности
	Тип информации, используемой в процедуре обеспечения конфиденциальности	— ВИ для процедуры закрытия — ВИ для процедуры раскрытия
	Контрольная информация	— Тип способа защиты конфиденциальности — Уровень защиты конфиденциальности

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ

Большинство прикладных (открытых) систем ЭМВОС и Интернет-архитектуры предъявляют определенные требования по обеспечению безопасности, которые зависят от целостности данных. Такие требования могут включать защиту информации, которая используется для информационного обеспечения других СЛБ, например службы аутентификации, управления доступом, обеспечения конфиденциальности, аудита и обеспечения неотказуемости. Если же эта информация могла быть модифицирована нарушителем, то эффективность таких СЛБ резко снизится или вообще будет сведена к нулю.

Целостность — это свойство информации, которое предотвращает ее изменение или разрушение неавторизованным способом.

В данной главе определены общие основы создания и функционирования служб обеспечения целостности данных при извлечении, доставке и управлении информацией, а именно:

- a)* определяет базовые концепции обеспечения целостности;
- b)* описывает возможные классы способов обеспечения целостности (СПЦЛ);
- c)* описывает средства для каждого класса СПЦЛ;
- d)* описывает процедуры обеспечения, необходимые для реализации того или иного класса СПЦЛ;
- e)* рассматривается взаимодействие служб и способов обеспечения целостности с другими СЛБ и СПБ.

Некоторые из рассматриваемых далее процедур обеспечивают целостность с привлечением прикладных систем, реализующих криптографические методы. В целом СПЦЛ не зависят от использования соответствующих криптографических или иных

алгоритмов, однако представленные в данном стандарте классы СПЦЛ могут зависеть от свойств соответствующих алгоритмов.

Целостность данных определяется *постоянством смыслового значения данных*. Это понятие (constancy of a data value) охватывает все случаи, в которых различные формы представления значения данных считаются эквивалентными (например различные варианты ASN.1-кодирования данных с одним и тем же смысловым значением). Другие формы инвариантности исключены.

Используемый термин *данные* (data) включает в себя все типы структур данных (например совокупности или наборы данных, последовательности данных, файловые системы и базы данных).

Обеспечение целостности данных относится, в первую очередь, к защите от потенциальных нарушителей тех данных, к которым предоставляется доступ для записи (write-accessible). Более того, в дальнейшем основное внимание сосредоточено на обеспечении целостности с использованием криптографических и некриптографических способов защиты, которые не полагаются только лишь на процедуры регулирования доступа.

7.1. Общие положения

Целевое предназначение службы обеспечения целостности (СПЦЛ) — защитить целостность данных и их соответствующие атрибуты, которые могут быть скомпрометированы с использованием одного из следующих способов:

- 1) неавторизованная (несанкционированная) модификация данных;
- 2) неавторизованное (несанкционированное) удаление данных;
- 3) неавторизованное (несанкционированное) генерирование данных;
- 4) неавторизованная (несанкционированная) вставка данных;

5) неавторизованная (несанкционированная) повторная передача данных.

СЛЦЛ обеспечивает защиту от угроз с помощью средств предотвращения или выявления, с восстановлением или без него. Эффективная защита целостности невозможна, если необходимая управляющая информация (например ключи и информация для защиты целостности) не защищена с точки зрения ее целостности и/или конфиденциальности. Такая защита очень часто зависит, в явном или не явном виде, от принципов, которые отличаются от принципов, реализуемых способом защиты соответствующих данных.

В этой главе используется понятие *защищенная зона* (protected environment), чтобы подчеркнуть идею того, что защита целостности включает защиту от несанкционированного (неавторизованного) генерирования и/или удаления. Таким образом, несанкционированное (неавторизованное) генерирование/удаление данных может рассматриваться как несанкционированная (неавторизованная) модификация некоторой защищенной зоны. Аналогично, вставка и повторная передача могут рассматриваться как модификация структурированного набора данных (например последовательности данных или структуры данных).

Следует заметить, что некоторые изменения данных могут рассматриваться как отсутствие влияния на их целостность. Например, если описание ASN.1-кода содержит тип данных **SET OF**, то нарушения целостности не последует, если символы этого типа данных были переупорядочены. Сложные СПЦЛ могут определять, что были проведены некоторые преобразования структурированных данных без компрометации их целостности. Такие способы позволяют преобразовывать данные, которые были подписаны ЭЦП или защищены с помощью криптографической проверочной суммы (КПС), без необходимости повторного вычисления ЭЦП или КПС соответственно.

Главная цель СЛЦЛ — защитить от несанкционированной (неавторизованной) модификации данных или обнаружить ее, включая несанкционированное (неавторизованное) генериро-

вание и удаление данных. Функционирование СЛЦЛ сопровождается следующими процедурами:

- 1) *защита (shield)*: формирование данных, целостность которых защищена, из исходных данных;
- 2) *подтверждение целостности (validate)*: проверка данных, целостность которых защищена, с целью выявления нарушения их целостности;
- 3) *снятие защиты (unshield)*: повторное формирование данных из данных, целостность которых защищена.

Эти процедуры делают применение криптографических методов защиты необязательным. Если эти процедуры используют криптографические методы защиты, то нет необходимости преобразования данных. Например, процедура защиты (*shield*) может быть осуществлена с использованием КПС или ЭЦП, присоединяемым к данным. В таком случае, после успешно проведенных процедур проверки целостности (*validate*) и снятия защиты (*unshield*) КПС или ЭЦП удаляются.

СЛЦЛ используется при извлечении, доставке и управлении информацией следующим образом:

- 1) для информации, доставляемой в открытых системах ЭМВОС или Интернет-архитектуры, услуга обеспечения целостности предоставляется путем объединения процедур защиты, доставки, используя средство ($N-1$)-уровня ЭМВОС или Интернет-архитектуры, и снятия защиты с целью формирования передаваемой части для последующей обработки службой N -уровня ЭМВОС или Интернет-архитектуры;
- 2) для хранимых и извлекаемых данных услуга обеспечения целостности предоставляется путем объединения процедур защиты и хранения, а также извлечения и снятия защиты.

Процедуры защиты и снятия защиты могут осуществляться параллельно, например, одни и те же данные (данные, доставляемые по соединению N -уровня ЭМВОС или Интернет-

архитектуры) могут одновременно включать части, которые еще не защищены, части, которые уже защищены, и части, у которых защита снята.

СПЦЛ обеспечивают защиту зон, а это означает, что этапы защиты и снятия защиты включают в себя доставку данных между защищаемыми зонами. Там, где данные, целостность которых защищена, доставляются из зоны, защищенной с помощью одного СПЦЛ, в другую зону, защищенную с помощью другого СПЦЛ, целесообразно, чтобы процедура защиты второго СПЦЛ предшествовала процедуре снятия защиты первого СПЦЛ с целью обеспечения непрерывности защиты данных.

7.1.1. Основные концепции обеспечения целостности

Все СЛЦЛ могут быть разделены на типы в зависимости от противоправной процедуры (генерирование, удаление, модификация, вставка и/или повторная передача), от необходимости предупреждения нарушения или только его обнаружения и от того, обеспечивается ли восстановление данных в случае нарушения целостности.

Используемые способы, которые применяются СЛЦЛ, могут быть разделены на большое число классов и групп в зависимости от уровня предполагаемой систематической обработки в случае неудавшегося нарушения целостности.

7.1.2. Типы СЛЦЛ

СЛЦЛ классифицируются по следующим критериям:

- 1) по типу нарушения, от которого они могут защитить:
 - неавторизованная модификация данных;
 - неавторизованное удаление данных;
 - неавторизованное генерирование данных;
 - неавторизованная вставка данных;
 - неавторизованная повторная передача данных;

- 2) по типу защиты, который они обеспечивают:
 - предотвращение компрометации целостности;
 - обнаружение компрометации целостности;
- 3) по наличию реализуемых способов восстановления или нет:
 - в первом случае (с восстановлением) процедура снятия защиты может обеспечивать восстановление исходных данных (и, возможно, сигнализировать о необходимости проведения процедуры восстановления или об ошибке с целью проведения, например, аудита) всякий раз, когда процедура проверки целостности выявила какое-либо изменение;
 - во втором случае (без восстановления), процедура снятия защиты не может обеспечивать восстановление исходных данных всякий раз, когда процедура проверки целостности выявила какое-либо изменение.

7.1.3. Типы СПЦЛ

Как правило, способность защищать данные зависит от используемой среды обработки данных. Почти любая среда, вследствие ее физической природы, весьма трудна для защиты (например заменяемая (съёмная) среда хранения или среда передачи данных), поэтому неавторизованные субъекты могут получить доступ и спровоцировать модификацию данных по своему желанию. В такой среде основная цель СПЦЛ — обеспечить выявление модификации и, по возможности, реконструировать поврежденные данные. Все СПЦЛ могут быть классифицированы следующим образом:

- 1) способы, которые предотвращают доступ к среде:
 - физически изолированные, «не шумящие», каналы;
 - управление маршрутизацией;
 - управление доступом;

2) способы, которые обнаруживают модификацию данных или последовательности элементов данных, включая случаи неавторизованного генерирования, удаления и повторения данных:

- КПС;
- ЭЦП;
- повторение данных (используется в качестве средства борьбы с другими типами нарушений);
- цифровой отпечаток данных в сочетании с криптографическими преобразованиями;
- нумерация последовательности сообщений.

С точки зрения надежности защиты эти СПЦЛ можно классифицировать следующим образом:

- а) не защищающие;
- б) для обнаружения модификации и генерирования;
- в) для обнаружения модификации, генерирования, удаления и повторения;
- г) для обнаружения модификации и генерирования с восстановлением;
- д) для обнаружения модификации, генерирования, удаления и повторения с восстановлением.

7.1.4. Угрозы целостности

С точки зрения предоставляемых услуг обеспечения целостности, угрозы можно классифицировать следующим образом:

- 1) неавторизованное генерирование/модификация/удаление/вставка/повторение в тех зонах, которые обеспечивают защиту целостности на основе предотвращения (например прослушивание в защищенных каналах);
- 2) неавторизованное и не обнаруживаемое генерирование/модификация/удаление/вставка/повторение в тех зонах, которые обеспечивают защиту целостности на основе обнаружения (например, целостность данных может быть гарантирована с помощью шифрования защищаемых

данных и соответствующей проверочной суммы; если взаимодействующие субъекты *A* и *B* используют один и тот же ключ шифрования и источник данных, то данные, целостность которых защищена и которые были переданы от *A* к *B*, могут быть в последствие получены *A* под видом того, что они якобы были отправлены *B* — атака типа «отражение»).

С точки зрения среды нахождения данных, угрозы можно классифицировать следующим образом:

- a*) угрозы на среду, в которой данные хранятся;
- b*) угрозы на среду, по которой данные передаются;
- c*) угрозы, не зависящие от среды нахождения данных.

7.1.5. Типы атак на целостность

Каждой из перечисленных выше угроз может соответствовать одна или несколько атак, т.е. реализации конкретной угрозы. Атаки нацелены на способ защиты, который используется для обеспечения целостности, и могут быть классифицированы следующим образом:

- 1) атаки, нацеленные на взлом криптографических способов (алгоритмов) защиты или использование уязвимостей в таких способах (алгоритмах):
 - взлом криптографического способа (алгоритма);
 - (селективное) удаление и повторение;
- 2) атаки, нацеленные на взлом используемого контекстно-зависимого способа защиты (контекстно-зависимые способы защиты обеспечивают обмен данными в определенных моменты времени и/или на определенных позициях в сообщениях):
 - массовый и скоординированный обмен копиями элементов данных;
 - получение несанкционированного доступа к средству (взлом способа) формирования контекстно-зависимой структуры данных;

- 3) атаки, нацеленные на взлом способов защиты, связанных с обнаружением нарушений и передачей ответных квитанций:
- отправка фальшивых квитанций;
 - использование некорректной последовательности передаваемых квитанций, не соответствующей смыслу принимаемых данных;
- 4) атаки, нацеленные на взлом, разрушение или компрометацию способов защиты:
- атаки на сам способ защиты;
 - получение несанкционированного доступа к службам, от которых зависит соответствующий способ защиты;
 - использование вспомогательных функций не по их прямому назначению.

7.2. Политики обеспечения целостности

Политика обеспечения целостности (ПЛЦЛ) — часть ПЛБ, которая связана с обеспечением и использованием СЛЦЛ.

Данные, целостность которых защищена, являются объектом управления со стороны субъектов, имеющих право на их формирование, изменение и удаление. ПЛЦЛ, кроме всего прочего, должна определять, какие данные являются объектом управления и каким субъектам разрешено (или может быть разрешено) формирование, изменение или удаление данных.

В зависимости от реальной значимости целостности различных типов данных ПЛЦЛ может определять типы и стойкость способов защиты, которые используются при предоставлении услуг обеспечения целостности для каждого отдельного типа данных.

7.2.1. Описание политики

При описании политики необходимы средства ПЛЦЛ, которые бы идентифицировали используемую информацию и привлекаемых объектов/субъектов.

ПЛЦЛ может быть представлена как набор правил. Каждое правило в ПЛЦЛ может включать характеристическое описание данных и объектов/субъектов, а также совокупность допустимых процедур обработки данных (как правило, генерирование, изменение и удаление). В некоторых ПЛЦЛ такие правила могут не указываться в явном виде, но могут быть установлены на основании анализа описания ПЛЦЛ.

ПРИМЕЧАНИЕ. Несмотря на то что некоторые СПЦЛ имеют определенную степень схожести с некоторыми типами описания ПЛЦЛ, способ описания ПЛЦЛ напрямую не использует описание СПЦЛ при внедрении ПЛЦЛ.

7.2.1.1. Характеристическое описание данных

Используемые в ПЛЦЛ данные могут описываться различными способами. Например:

- a) путем описания и идентификации объектов/субъектов, которые авторизованы для генерирования/изменения/удаления таких данных;
- b) путем их размещения;
- c) путем описания контекста, в котором представлены данные (т.е. их функциональное предназначение).

7.2.1.2. Характеристическое описание объекта/субъекта

Существует много способов характеристического описания объектов/субъектов, по отношению к которым применяется ПЛЦЛ. Рассмотрим два основных примера.

ПЛЦЛ, основанные на параметрах подлинности. В этой форме представления политики объекты/субъекты идентифицируются либо индивидуально, либо как часть группы одинаковых объектов/субъектов (в соответствии с целями ПЛЦЛ), либо по функциональной роли, исполняемой теми или иными объектами/субъектами. Таким образом, каждому объекту/субъекту, которому разрешено заниматься тем или иным видом обработкой данных, будет присвоено либо индивидуальное значение параметра подлинности, либо групповое значение параметра

подлинности, либо значение идентификатора функциональной роли, используемое для его характеристического описания.

В случае идентификации функциональных ролей ПЛЦЛ определяет выделенные группы функциональных ролей, которые может исполнять каждый объект/субъект, и соответственно, функциональные роли из различных групп, которые не могут исполняться одновременно.

ПЛЦЛ, основанные на правилах. В этой форме представления политики используются атрибуты, присваиваемые каждому объекту/субъекту и элементу данных, целостность которого защищена. Допускается использование глобальных всеобъемлющих правил применения атрибутов объектов/субъектов и определенных данных. ПЛЦЛ, основанные на правилах, более подробно рассмотрены в главе 1.

7.3. Вспомогательная информация и средства обеспечения целостности

7.3.1. ВИ, необходимая для обеспечения целостности

Для того чтобы данные проходили процедуры защиты, проверки целостности и снятия защиты, может использоваться ВИ. Такая ВИ называется *информацией, необходимой для обеспечения целостности* (ВИЦЛ). ВИЦЛ может быть классифицирована следующим образом:

- ВИЦЛ для процедуры защиты;
- ВИЦЛ для процедуры обнаружения модификации;
- ВИЦЛ для процедуры снятия защиты.

7.3.1.1. ВИЦЛ для защиты

ВИЦЛ для защиты является информацией, используемой для защиты данных. Такая информация может включать:

- 1) закрытые ключи;
- 2) секретные ключи;
- 3) идентификатор алгоритма и соответствующие криптографические параметры;

- 4) переменные временные параметры (например метки времени).

7.3.1.2. ВИЦЛ для обнаружения модификации

ВИЦЛ для обнаружения модификации является информацией, используемой при подтверждении целостности защищенных данных. Такая информация может включать:

- 1) открытые ключи;
- 2) секретные ключи.

7.3.1.3. ВИЦЛ для снятия защиты

ВИЦЛ для снятия защиты является информацией, используемой для снятия защиты данных, целостность которых была защищена. Такая информация может включать:

- 1) открытые ключи;
- 2) секретные ключи.

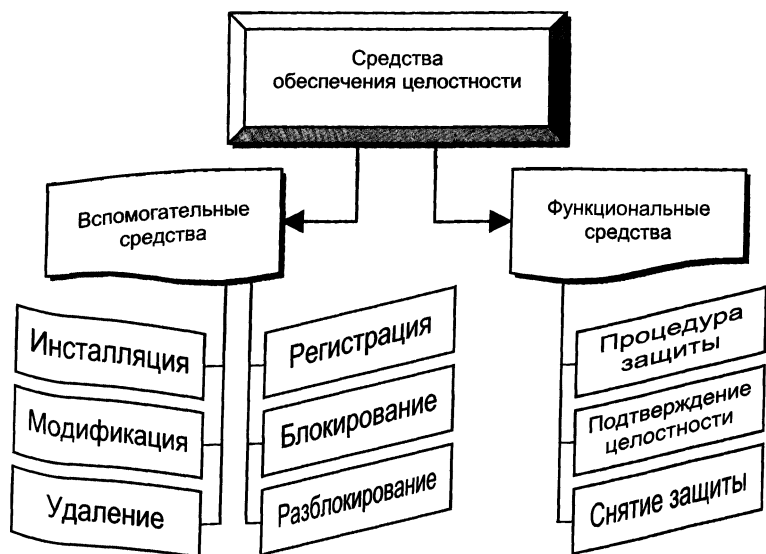


Рис. 7.1. Средства, используемые в процедурах обеспечения целостности

7.3.2. Средства обеспечения целостности

Средства обеспечения целостности (СРЦЛ) делятся на два основных класса (рис. 7.1):

- *функциональные средства*, которые непосредственно участвуют в процедурах обеспечения целостности (ПРЦЛ);
- *вспомогательные средства*, которые могут привлекаться к обеспечивающим (управляющим) процедурам.

7.3.2.1. Функциональные СРЦЛ

Такими средствами являются:

- 1) *СРЦЛ для процедуры защиты*. Это средство реализует функцию защиты целостности данных. Входными данными для этого средства являются:
 - данные, подлежащие защите;
 - ВИЦЛ для процедуры защиты;
 - идентификаторы соответствующих СПЦЛ.Выходными данными для этого средства являются:
 - данные, целостность которых защищена;
 - ответные коды завершения процедуры защиты.
- 2) *СРЦЛ для процедуры подтверждения целостности*. Это средство реализует функцию проверки целостности данных на предмет выявления каких-либо модификаций. Входными данными для этого средства являются:
 - данные, целостность которых защищена;
 - ВИЦЛ для процедуры обнаружения модификации;
 - идентификаторы соответствующих СПЦЛ.Выходными данными для этого средства являются:
 - результат процедуры обнаружения модификации (была ли обнаружена модификация или нет).
- 3) *СРЦЛ для процедуры снятия защиты*. Это средство реализует функцию снятия защиты целостности данных. Входными данными для этого средства являются:
 - данные, целостность которых защищена;
 - ВИЦЛ для процедуры снятия защиты;
 - идентификаторы соответствующих СПЦЛ.

Выходными данными для этого средства являются:

- данные, целостность которых была защищена;
- ответные коды завершения процедуры снятия защиты.

7.3.2.2. Вспомогательные СРЦЛ

Вспомогательные СРЦЛ могут применяться пользователем для получения, модификации и удаления информации (например ключей), которая необходима для ПРЦЛ. В широком смысле, этими СРЦЛ являются:

- средства инсталляции ВИЦЛ;
- средства модификации ВИЦЛ;
- средства удаления ВИЦЛ;
- средства регистрации ВИЦЛ;
- средства блокирования ВИЦЛ;
- средства разблокирования ВИЦЛ.

7.4. Классификация способов обеспечения целостности

7.4.1. Обеспечение целостности на основе криптографии

Существуют два класса криптографических СПЦЛ, к которым относятся:

1) СПЦЛ, основанные на симметричных криптографических методах, в которых проверка целостности защищенных данных возможна только в том случае, когда известен тот же самый секретный ключ, использовавшийся в процедуре защиты целостности данных;

2) СПЦЛ, основанные на асимметричных криптографических методах, в которых проверка целостности защищенных данных возможна только в том случае, когда известен открытый ключ, соответствующий закрытому ключу, использовавшемуся в процедуре защиты целостности данных.

3) СПЦЛ первого типа соответствуют процедура вычисления КПС, а СПЦЛ второго типа — ЭЦП.

Совместно с криптографическими СПЦЛ, такими как защита от атак типа «повторная передача», могут использоваться переменные временные параметры.

7.4.1.1. Обеспечение целостности на основе вычисления КПС

Процедуры вычисления КПС обеспечивают защиту целостности путем присоединения полученных КПС к защищаемым данным. При вычислении КПС один и тот же секретный ключ используется для защиты и подтверждения целостности данных. При использовании этого класса СПЦЛ все потенциальные средства подтверждения целостности данных либо должны знать заранее используемый секретный ключ, либо иметь средства для получения такого секретного ключа.

Группа объектов/субъектов, способных вычислить КПС защищаемых данных, и группа объектов/субъектов, способных подтвердить целостность защищенных данных являются, согласно определению самого СПЦЛ, полностью совместимыми.

Этот СПЦЛ позволяет обнаруживать модификации следующим образом:

- 1) *защита целостности* обеспечивается путем присоединения КПС к данным, целостность которых должна быть защищена (например, вычисление ОНФ по всей последовательности защищаемых данных, а результат вычисления ОНФ преобразуется с помощью криптографического алгоритма);
- 2) *подтверждение целостности* обеспечивается на основе использования защищенных данных, КПС и секретного ключа с целью определения, совпадает ли вновь вычисленная КПС с КПС, прикрепленной к защищенным данным (например, средство подтверждения целостности могло бы передать средству защиты целостности данные и секретный ключ, которое в ответ направило бы КПС; далее средство подтверждения целостности могло бы сравнить полученную КПС с той, которая в действительности была присоединена к защищаемым данным).

Если обе КПС совпадают, то принимается решение о том, что данные не были модифицированы;

- 3) *снятие защиты целостности* обеспечивается путем удаления КПС после того, как была подтверждена целостность защищенных данных.

7.4.1.2. Обеспечение целостности на основе ЭЦП

ЭЦП вычисляются с использованием закрытого ключа и асимметричного криптографического алгоритма. Целостность защищенных данных (данные с присоединенной к ним ЭЦП) может быть подтверждена с помощью соответствующего открытого ключа. Как правило, открытый ключ находится в открытом доступе.

ЭЦП позволяют группе объектов/субъектов, которые могут подтвердить целостность данных, проверить их размер (объем) и состав.

Этот СПЦЛ позволяет обнаруживать модификации следующим образом:

- 1) *защита целостности* обеспечивается путем присоединения КПС к данным, целостность которых должна быть защищена (например, вычисление цифрового отпечатка по всей последовательности защищаемых данных, а результат вычисления цифрового отпечатка вместе с закрытым ключом и, возможно, с другими параметрами, предназначенными для вычисления определенных необходимых значений, образуют ЭЦП);
- 2) *подтверждение целостности* обеспечивается на основе использования цифрового отпечатка принятых защищенных данных, ЭЦП, открытого ключа и соответствующего алгоритма проверки, который осуществляет проверку ЭЦП. Если проверка ЭЦП выявила изменение, то принимается решение о том, что данные были модифицированы;
- 3) *снятие защиты целостности* обеспечивается путем удаления КПС после того, как была подтверждена целостность защищенных данных.

7.4.1.3. Обеспечение целостности на основе шифрования избыточных данных

Целостность избыточных данных (например естественный язык) может быть обеспечена с помощью шифрования. Данные, которые включают коды, обнаруживающие ошибки, и цифровые отпечатки являются избыточными, а их целостность может быть защищена с помощью шифрования (в том случае, если используемый алгоритм шифрования предотвращает возможность предсказания изменений зашифрованных данных, так как изменения будут отражаться на исходных данных после расшифрования).

Протоколы безопасности нижних уровней ЭМВОС и Интернет-архитектуры используют эту группу способов в целях обеспечения целостности данных, конфиденциальность которых защищена.

Этот способ позволяет обнаруживать модификации следующим образом:

- 1) *защита целостности* обеспечивается путем зашифрования избыточных данных;
- 2) *подтверждение целостности* обеспечивается путем расшифрования защищенных данных и определения, удовлетворяют ли они условию неизменности по отношению к исходным данным. Например:
 - если исходные данные были последовательностью символов ASCII-кода, то восстановленные данные должны обладать такими же свойствами;
 - если исходные данные, предположительно, были высказыванием (выражением в словах) на определенном языке, то восстановленные данные должны быть (допускаются небольшие изменения) в целом приемлемым высказыванием (выражением в словах) на том же самом языке;
 - если исходные данные содержали проверочные суммы, то можно вычислить такие же проверочные суммы по соответствующим отрезкам последовательности защищенных данных, а затем сравнить полученные

результаты со значениями проверочных сумм, размещенных в расшифрованных данных;

3) *снятие защиты целостности* обеспечивается путем расшифрования зашифрованных данных.

ПРИМЕЧАНИЕ. Известно, что этот способ, неприемлемый для некоторых форм избыточности (например данные с кодами, обнаруживающими ошибки), используется с едиными формами шифрования (например блочные шифры в режиме сцепки или без нее). Относительно простой пример вероятной ошибки следующий:

Если текст в ASCII-коде (например электронное почтовое сообщение) был защищен с помощью шифрования, то сообщение могло быть модифицировано с помощью уменьшения его длины (truncation), при этом факт модификации не был бы обнаружен. Последнее возможно только в том случае, когда заголовок почтового сообщения не содержит указателя его длины, что бывает крайне редко.

7.4.2. Обеспечение целостности на основе контекста сообщения

Целостность может быть защищена с помощью способов, которые обеспечивают хранение или передачу данных внутри одного или нескольких предварительно согласованных элементов данных (сообщениях). Такие способы могут защитить сами данные, а также их различные структуры (например последовательности элементов данных). К таким способам относятся:

- a) повторение данных;
- b) использование предварительно согласованных элементов данных.

7.4.2.1. Повторение (дублирование) данных

Этот класс СПЦЛ основан на *повторении* (replication) *данных* в пространстве (например несколько областей хранения) или во времени (например в различные моменты време-

ни). Предполагается, что потенциальные нарушители не смогут скомпрометировать более чем ограниченное число копий защищаемых данных и что всякий раз атаки будут обнаружены, а данные можно будет реконструировать из «нетронутых» копий.

Например, такой СПЦЛ может быть реализован при защите баз данных от атак типа «проникновение».

Эти СПЦЛ позволяют обнаружить нарушения целостности типа «удаление данных» и в последующем восстановить искаженные данные. Такие способы могут использоваться совместно с другими СПБ. Они обеспечивают целостность следующим образом:

- 1) *защита целостности* обеспечивается путем формирования нескольких копий одних и тех же данных либо друг за другом по времени, либо в различных точках пространства размещения;
- 2) *подтверждение целостности* обеспечивается путем поиска копии данных в каждый момент времени или в точках пространства размещения. Затем копии сравниваются, и если не все из них идентичны, то принимается решение, что имело место нарушение целостности;
- 3) *снятие защиты целостности* (с восстановлением) может быть обеспечено тогда, когда достигнуто соответствие некоторому предварительно установленному критерию (например мажоритарный критерий, т.е. «получение 90% и более согласованного смыслового значения данных среди всех их обработанных копий») при условии выбора корректного порогового значения этого критерия. А выбранное пороговое значение позволяет минимизировать предварительно согласованный параметр ошибочного восстановления (например вероятность ошибочного восстановления).

Следует заметить, что критерий такого восстановления должен быть удовлетворен и тогда, когда все возможные варианты смыслового значения данных согласованы, и что при таких условиях смысловое значение данных, которое минимизирует

параметр ошибочного восстановления, должно быть единым смысловым значением для всех данных.

7.4.2.2. Использование предварительно согласованных элементов данных

Такие способы обеспечивают обнаружение удаления данных, целостность которых защищена, и, как правило, используются совместно с другими СПЦЛ:

- 1) *защита целостности* обеспечивается путем отправки данных в определенные моменты времени и/или их размещения в границах заданного интервала;
- 2) *подтверждение целостности* обеспечивается путем проверки данных в установленный момент времени и/или в установленном месте их размещения. Если данные в нужный момент и/или в нужном месте отсутствуют, то принимается решение, что имело место нарушение целостности.

В целях предотвращения подстановки альтернативных данных этот способ должен использоваться совместно с другими СПЦЛ.

7.4.3. Обеспечение целостности на основе обнаружения нарушений и передачи ответных квитанций

Такие способы проводят анализ целостности всякий раз, когда выполняются идемпотентные операции с положительной обратной связью (операция называется *идемпотентной*, если несколько положительных итераций операции дают один и тот же результат, как и при одиночной итерации). Примерами таких способов являются процедуры передачи с положительными ответными квитанциями и удаленные операции с обратной связью. Такие СПЦЛ предполагают, что процедуры защиты целостности и подтверждения/снятии защиты целостности осуществляются в течение одного и того же периода времени и, как правило, неприемлемы для хранения данных:

- 1) *защита целостности* обеспечивается путем многократного повторения одного и того же действия либо столько раз, сколько предписывает ПЛЦЛ, либо, во всех других случаях, пока не будет получена положительная ответная квитанция;
- 2) *подтверждение целостности* обеспечивается путем поэтапной обработки и проверки защищенных данных (если, конечно, ПЛЦЛ не предписывает ничего другого). Результаты успешных проверок отражаются в положительных ответных квитанциях, которые получает объект/субъект, осуществивший процедуру защиты целостности.

Если с целью обеспечения корректной доставки информации необходима коррекция поступивших защищенных данных, и она может быть сделана соответствующим средством, реализующим процедуру снятия защиты целостности данных от модификации, то это средство может отправить положительную ответную квитанцию (после проведенной коррекции).

Эффективность может быть достигнута лишь тогда, когда отрицательная ответная квитанция, содержащая отрицательный результат проверки целостности (имела место либо модификация, либо удаление), будет «понята» средством, реализующим процедуру защиты целостности.

Эти способы предполагают, что модификация данных может быть обнаружена и с помощью других средств и, следовательно, за счет усовершенствования самих способов защиты данных от модификации.

7.4.4. Обеспечение целостности путем препятствования (предотвращения)

Целостность может быть обеспечена путем препятствования физическому доступу к хранилищу данных или среде передачи, а также на основе регулирования физического доступа. УД рассматривается в главе 3.

7.5. Взаимосвязи с другими СЛБ и СПБ

7.5.1. Управление доступом

УД может использоваться для построения зон защиты целостности.

7.5.2. Аутентификация источника данных

Аутентификация источника данных может использоваться для обеспечения целостности, например, если протокольный элемент данных (Protocol Data Unit — PDU) не был аутентифицирован, то считается, что PDU-элемент был скомпрометирован. Аналогично, если предполагаемый источник PDU-элемента не авторизован для формирования PDU-элементов, то считается, что имело место нарушение целостности.

7.5.3. Конфиденциальность

Во многих ситуациях введение избыточности данных может совмещаться с шифрованием полученных после введения избыточности данных, которые не могут быть модифицированы без обнаружения такой модификации.

Более того, избыточные данные (например естественный язык и данные, содержащие проверочные суммы и результаты хэш-функций) обладают *свойством инвариантности* (неизменяемости, invariance). Как правило, изменения в зашифрованных данных приведут к нарушению этого свойства, что будет обнаружено в дальнейшем, т.е. сразу после того, как эти измененные данные будут «расшифрованы».

Иными словами, если k бит информации закодированы в $(k + m)$ -битовую последовательность, то все допустимые кодовые последовательности образуют распределенные подмножества всех возможных битовых последовательностей. Если изменения зашифрованных данных привели к изменениям после расшифрования, которые с точки зрения нарушителя выглядят как случайные, то вероятность того, что в результате расшифро-

вания искаженных данных будет получена допустимая кодовая последовательность, составляет примерно 2^m .

Таким образом, введение избыточности (включение проверочных сумм или результатов хэш-функций в исходные данные) совместно с обеспечением конфиденциальности на основе криптографии может обеспечить целостность данных.

7.6. Обеспечение целостности в ЭМВОС и Интернет-архитектуре

СЛЦЛ в системах ЭМВОС или Интернет-архитектуры предоставляют следующие услуги по обеспечению целостности:

- целостность соединения с восстановлением;
- целостность соединения без восстановления;
- целостность отдельных полей при виртуальном соединении;
- целостность соединения в дейтаграммном режиме (connectionless);
- целостность отдельных полей при соединении в дейтаграммном режиме.

7.6.1. Целостность соединения с восстановлением

Целостность соединения обеспечивает защиту целостности всех данных пользователя N -го уровня ЭМВОС или Интернет-архитектуры, доставляемых по соединению N -го уровня ЭМВОС или Интернет-архитектуры, а также обнаружение любой модификации, вставки, удаления и повторной передачи любых данных в пределах всей последовательности обслуживаемых элементов данных (с предполагаемым восстановлением).

7.6.2. Целостность соединения без восстановления

Целостность соединения обеспечивает защиту целостности всех данных пользователя N -го уровня ЭМВОС или Интернет-архитектуры, доставляемых по соединению N -го уровня ЭМВОС или Интернет-архитектуры, а также обнаружение любой

модификации, вставки, удаления и повторной передачи любых данных в пределах всей последовательности обслуживаемых элементов данных (восстановление не предполагается).

7.6.3. Целостность отдельных полей при виртуальном соединении

Целостность отдельных полей обеспечивает защиту целостности определенных полей внутри данных пользователя N -го уровня ЭМВОС или Интернет-архитектуры, доставляемых в обслуживаемых элементах данных N -го уровня ЭМВОС или Интернет-архитектуры по виртуальному соединению, и обнаружение модификации, вставки, удаления и повторной передачи защищаемых полей.

7.6.4. Целостность соединения в дейтаграммном режиме

Целостность соединения в дейтаграммном режиме, устанавливаемого на N -уровне ЭМВОС или Интернет-архитектуры, обеспечивает гарантии целостности, запрашиваемой объектом/ субъектом $(N + 1)$ -уровня ЭМВОС или Интернет-архитектуры.

7.6.5. Целостность отдельных полей при соединении в дейтаграммном режиме

Целостность отдельных полей обеспечивает защиту целостности определенных полей внутри одиночного обслуживаемого элемента данных, доставляемых по соединению в дейтаграммном режиме, и обнаружение модификации этих защищаемых полей.

7.6.6. Использование СЛЦЛ в рамках уровней ЭМВОС и Интернет-архитектуры

СЛЦЛ предоставляет услуги по обеспечению целостности на следующих уровнях ЭМВОС и Интернет-архитектуры:

- канальном (2-м) уровне;

- сетевом (3-м) уровне;
- транспортном (4-м) уровне;
- прикладном (7-м) уровне для ЭМВОС (5-м для Интернет-архитектуры).

7.6.6.1. Применение СЛЦЛ на канальном уровне

Услуги по обеспечению целостности могут предоставляться на канальном уровне в соответствии со стандартом IEEE 802.10.

7.6.6.2. Применение СЛЦЛ на сетевом уровне

На сетевом уровне СЛЦЛ может предоставлять только две услуги: целостность соединения без восстановления и целостность соединения в дейтаграммном режиме. Иногда эти услуги могут предоставляться с использованием СПЦЛ данных совместно со способом шифрования. Такие услуги позволяют обеспечить целостность между сетевыми узлами, узлами подсетей или ретрансляторами.

7.6.6.3. Применение СЛЦЛ на транспортном уровне

На транспортном уровне СЛЦЛ может предоставлять только три услуги: целостность соединения с восстановлением и без него и целостность соединения в дейтаграммном режиме. Иногда эти услуги могут предоставляться с использованием СПЦЛ данных совместно со способом шифрования. Такие услуги позволяют обеспечить целостность между оконечными системами.

7.6.6.4. Применение СЛЦЛ на прикладном уровне

На прикладном уровне СЛЦЛ может предоставлять все возможные услуги: целостность соединения с восстановлением и без него, целостность соединения в дейтаграммном режиме, целостность отдельных полей при виртуальном соединении и целостность отдельных полей при соединении в дейтаграммном режиме. Целостность соединения с восстановлением и без него и целостность соединения в дейтаграммном режиме могут обеспечиваться с помощью СПЦЛ данных нижних уровней ЭМВОС (иногда совместно со способом шифрования). Целостность

отдельных полей может обеспечиваться за счет использования СПЦЛ данных нижних уровней ЭМВОС на прикладном уровне.

7.7. Целостность внешних данных

В данной главе целостность рассматривается с точки зрения сохранения определенной *инвариантности данных* (постоянство их смыслового значения). Модель Кларка/Уилсона (см. CLARK, David and WILSON, David: A Comparison of Commercial and Military Computer Security Policies, *Proceedings of 1987 IEEE Symposium on Security and Privacy*) предусматривает *дополнительные типы инвариантности*. Точнее, эта модель предполагает, что компьютерная система воспроизводит и имитирует данные и процессы, которые являются внешними по отношению к компьютеру. Более того, финальной проверкой целостности является обеспечение гарантий того, что данные внутри компьютера согласуются с той сферой деятельности, которую они предназначены отображать. Из этого следует, что контроль целостности, строго говоря, не может быть «внутренним делом» компьютера.

В результате целостность данных, согласно модели Кларка/Уилсона, может рассматриваться как метод, предусматривающий два условия:

- 1) для инициирования изменений, если такие изменения необходимы, должны существовать адекватные способы, реализация которых обеспечивала бы сохранение постоянства внешних данных;
- 2) должны существовать способы, которые бы после инициирования изменений гарантировали, что такие изменения осуществляются как элементарная операция закономерной (хорошо согласованной) процедуры информационного обмена (транзакции).

Полагая, что предшествующие рассуждения точно отражают общее интуитивное понимание целостности, то очевидны следующие семантические отличия:

- *постоянство внутренних данных*: данная величина является внутренне постоянной тогда и только тогда, когда все модификации этой величины удовлетворяют соответствующим ПЛЦЛ;
- *постоянство внешних данных*: данная величина является внешне постоянной всякий раз, когда ее смысловое значение соответствует реальной ситуации в той сфере деятельности, которую она описывает.

Если описанное выше отличие принимается, то оно может быть совмещено с классификацией по уровню защиты целостности, а именно:

- высокий уровень защиты сохраняет постоянство внутренних и внешних данных;
- низкий уровень защиты выявляет нарушения постоянства внутренних и/или внешних данных.

Более того, и с точки зрения объема таких изменений в данных, которые осуществляются как элементарные операции в рамках надежных процедур, можно говорить о свойствах этих операций, например:

- 1) может ли быть нарушена элементарность самой элементарной операции?
- 2) существуют ли гарантии того, что операцию необходимо проводить?

И в заключение можно классифицировать СПЦЛ, которые касаются сохранения следующих свойств:

- внутренняя/внешняя целостность;
- низкий/высокий уровень защиты;
- элементарность/гарантированность операций над защищенными данными.

Таким образом, когда определяется СПЦЛ, целесообразно проанализировать следующие вопросы:

- 1) Какую форму целостности (внутреннюю, внешнюю, обе сразу) обеспечивают СПЦЛ?
- 2) Какой уровень защиты целостности данных обеспечивается (низкий или высокий)? Устойчив ли СПЦЛ к целенаправленным атакам, к случайным изменениям или обоим вариантам? Обеспечивает СПЦЛ восстановление?
- 3) Защищает ли СПЦЛ элементарные операции или он обеспечивает гарантии (также) того, что операция будет проведена?

Общая структура службы обеспечения целостности представлена в табл. 7.1, где используются следующие концептуальные термины.

Объекты/субъекты обеспечения целостности в системах ЭМВОС или Интернет-архитектуры:

- *инициатор*. Объект, который формирует данные, целостность которых подлежит защите, путем защиты данных и их передачи или хранения;
- *проверяющая сторона*. Субъект, который получает данные от инициатора или извлекает информацию из полученных от инициатора данных, проверяет их смысловое значение, после подтверждения целостности, проводимого с целью обнаружения нарушения целостности, и, если это необходимо, регенерирует смысловое значение данных;
- *ДТС, предоставляющая средства для обеспечения целостности*. Субъект, который предоставляет ВИ для защиты целостности данных или ВИ для обнаружения модификации данных и осуществляет соответствующие ПРЦЛ от имени инициатора или проверяющей стороны.

Структура службы обеспечения безопасности (целостности)		Элемент	<u>Объект/субъект:</u> Инициатор, Проверяющая сторона, ДТС, обеспечивающая защиту целостности		
			<u>Функции:</u>		
			<u>Информационные объекты:</u> Информация, целостность которой защищена		
		<u>Цель службы:</u> Защитить данные от неавторизованных (несанкционированных) модификации/удаления/формирования/вставки/повторения			
М Е Р О П Р И Я Т И Я	Объект/субъект	Центр безопасности сетевого сегмента			
	Функция				
	Мероприятия, связанные с обеспечением ПРЦД	— Инсталляция ВИ — Регистрация ВИ — Изменение ВИ — Блокировка ВИ — Удаление ВИ — Разблокировка ВИ			
	Объект/субъект	Инициатор	Проверяющая сторона	ДТС, обеспечивающая защиту целостности	
	Функция			Функция принятия решения о предоставлении доступа	
	Мероприятия, функционально связанные с ПРЦД	— Защита данных Маркер списка УД Проверочная сумма КПС ЭЦП	— Подтверждение целостности Маркер списка УД Проверочная сумма КПС ЭЦП — Снятие защиты (восстановленные данные) КПС ЭЦП	— Предоставление услуг Маркер списка УД КПС Проверочная сумма Сертификат	

Таблица 7.1 (окончание)

И Н Ф О Р М А Ц И Я	Входные/выходные элементы данных, определяемые Центром безопасности сетевого сегмента	– Идентификаторы (инициатора, проверяющей стороны, ДТС, обеспечивающей защиту целостности) – Криптоключи – Значение переменного временного параметра
	Информация, используемая в ПРИЛ	– Информация для защиты целостности данных – Информация для обнаружения нарушений целостности – Информация для снятия защита целостности
	Контрольная информация	– Период времени – Маршрут – Размещение – Состояние системы

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ АУДИТА БЕЗОПАСНОСТИ И ОПОВЕЩЕНИЯ ОБ ОПАСНОСТИ

В данной главе описывается базовая модель обработки сигналов службы оповещения об опасности (о нарушении безопасности) и проведения аудита безопасности открытых систем ЭМВОС и Интернет-архитектуры. *Аудит безопасности* (АДБ) представляет собой независимые ревизию и анализ системных записей и основных направлений деятельности. *Служба аудита безопасности* (СЛАД) предоставляет аудиторскому центру возможность определять, отбирать и администрировать события, которые необходимо зарегистрировать в качестве данных для последующего проведения аудиторской проверки обеспечения (состояния) ИБ.

Рассматриваемая далее концепция АДБ включает выявление событий и определяет процедуры, которые являются следствием обнаружения этих событий. В главе рассматривается не только АДБ, но и *служба оповещения об опасности* (СЛОО).

Целями АДБ являются:

- участие в процедуре идентификации и анализе неавторизованных действий (процедур) или атак;
- помощь в обеспечении гарантий того, что всем операциям в интересах объектов/субъектов, которые за них отвечают, могут быть присвоены соответствующие атрибуты;
- участие в дальнейшем совершенствовании процедур обнаружения возникающих нештатных ситуаций;
- подтверждение соответствия существующей ПЛБ;
- доведение (доклад) информации, которая может указывать на несоответствия в системных средствах управления;
- определение соответствующих изменений, которые необходимо внести в средства управления, ПЛБ и процедуры.

АДБ включает обнаружение, отбор и регистрацию различных событий, которые тем или иным образом связаны с обеспечением (состоянием) безопасности (событием безопасности), для аудиторской проверки обеспечения (состояния) безопасности и анализ таких событий.

Аудит и идентифицируемость (accountability) требуют, чтобы информация была зарегистрирована (зафиксирована). АДБ обеспечивает гарантии того, что вся необходимая информация о штатных и нештатных событиях зарегистрирована, причем так, что все последующие расследования могут установить, имели ли место нарушения безопасности, а если имели, то какая информация или другие ресурсы были скомпрометированы. Идентифицируемость обеспечивает гарантии того, что соответствующая информация о действиях пользователей или процессах, действующих от их имени, зарегистрирована, причем так, что в дальнейшем последовательности таких действий могут быть однозначно приписаны пользователю(ям), а пользователь(и), в свою очередь, может(гут) быть приписан(ы) к совершенным им(и) действиям. СЛАД может оказывать поддержку идентифицируемости.

Служба оповещения об опасности (о нарушении безопасности) вырабатывает и передает персоналу или процессу сигнал опасности (СОП), указывающий на то, что имела место нештатная ситуация, которая может повлечь за собой выполнения того или иного безотлагательного действия. Целями СЛОО являются:

- оповещение о реальных или очевидных попытках нарушения безопасности;
- оповещение о различных событиях безопасности, включая «штатные» события;
- оповещение о событиях, которые обусловлены достижением некоторых предельных ограничений.

Таким образом, *функциональным предназначением СЛАД и СЛОО является обеспечение гарантий того, что события безопасности обрабатываются, анализируются и контролируются согласно ПЛБ соответствующего ЦБ.*

Далее рассматриваются:

- базовые концепции АДБ и оповещения об опасности;
- общая модель АДБ и оповещения об опасности;
- взаимосвязи СЛАД и СЛОО с другими СЛБ.

8.1. Общие положения

АДБ позволяет целенаправленно совершенствовать ПЛБ, помогает обнаруживать нарушения безопасности, предоставляет средства идентификации пользователей (или процессов, действующих от их имени) при совершении ими определенных действий, участвует в обнаружении скомпрометированных ресурсов и выступает в роли блокиратора действий пользователей, которые могут попытаться нанести ущерб системе. При предотвращении нарушений безопасности способы АДБ (СПАД) напрямую не используются. Они предназначены для обнаружения, регистрации и анализа событий. Это позволяет вносить изменения в функциональные процедуры с последующим их внедрением в ответ на нештатные события, например нарушения безопасности.

СОП формируется вслед за обнаружением любых событий безопасности, определяемых ПЛБ как условие оповещения об опасности. Это могло бы включать предварительно согласованный предельный случай, достижение которого тоже является условием подачи СОП. Некоторые из этих случаев могут потребовать незамедлительного проведения процедуры восстановления, а другие — последующего расследования в целях определения, какое действие необходимо, если не предписано что-либо другое.

Реализация модели АДБ и СОП может потребовать использование других СЛБ в целях обеспечения самих СЛАД и СЛОО, а также для обеспечения гарантий их корректного и надежного функционирования.

Несмотря на то, что итоговые данные (результаты) АДБ и процедуры аудиторской проверки обеспечения (состояния) безопасности (ПРАД) обладают определенными характери-

ками, рассматриваемые далее средства и способы могут использоваться при формировании результатов процедур аудиторской проверки и в самих процедурах аудиторской проверки, но которые не относятся к обеспечению безопасности.

С точки зрения безопасности максимальная эффективность достигается за счет обеспечения гарантий того, что в систему будут внедрены дополнительные требования по применению АДБ. Более того, системные проектировщики должны учитывать необходимость использования средств АДБ (т.е. уже существующих средств тестирования и анализа) в разрабатываемых процессах и создаваемых ими системах.

ПРИМЕЧАНИЕ. Модель АДБ и СОП не рассматривает, как с ней связаны функциональные и вспомогательные средства обеспечения.

8.1.1. Модель и функции

8.1.1.1. Функции СЛАД и СЛОО

Для реализации СЛАД и СЛОО необходимо выполнение различных функций, среди которых:

- *определение (классификация) события* (event discriminator), которая обеспечивает предварительный анализ события и определяет, куда следует направлять данные о событии: либо средству регистрации, либо средству обработки СОП;
- *регистрация данных (результатов) АДБ* (audit recorder), которая заключается в формировании записей АДБ и хранении этих записей в базе данных для результатов АДБ (БДРА);
- *обработка СОП* (alarm processor), которая заключается в формировании сообщения аудиторской проверки и реагировании на поступивший СОП;
- *анализ результатов АДБ* (audit analyser), который заключается в проверке результатов АДБ и, если необходимо, формирует СОП и сообщения АДБ;

- *формирование отчета по результатам АДБ* (audit trail examiner), которое заключается в формировании отчетов (электронных докладов) на основе одного или нескольких результатов АДБ;
- *предоставление записей БДРА* (audit provider), которое заключается в передаче (доставке) записей БДРА по некоторому критерию;
- *архивирование записей БДРА* (audit archiver), которое заключается в передаче (доставке) некоторых записей БДРА на архивное хранение (в архив).

Для распределенных СЛАД и СЛОО необходимо выполнение следующих дополнительных функций:

- *отбор результатов АДБ* (audit trail collector), который заключается в сборе записей из распределенных БДРА в одну определенную БДРА;
- *диспетчеризация результатов АДБ* (audit dispatcher), которая заключается в доставке частей (или в целом виде) записей из распределенных БДРА средству, реализующему функцию отбор результатов АДБ.

8.1.1.2. Модель АДБ и СОП

Модель АДБ и СОП включает несколько фаз (рис. 8.1). За обнаружением события следует его обязательная классификация, т.е. связано ли это событие с обеспечением (состоянием) безопасности или нет. *Средство классификации события* анализирует событие, чтобы определить, целесообразно ли сформировать сообщение АДБ и/или сообщение для подачи СОП. Сообщения АДБ доставляются на *средство регистрации* (регистратор). СОП доставляются на средство обработки СОП для анализа и выполнения последующего действия. Затем сообщения АДБ форматируются и преобразуются в записи АДБ, которые включаются в результаты АДБ. Наиболее старые компоненты результатов АДБ могут архивироваться (направляться на архивное хранение). Результаты АДБ и архивные результаты АДБ могут использоваться при формировании отчетов по результатам АДБ путем отбора соответствующих записей резуль-

татов АДБ на основе определенного критерия. Иначе говоря, на основе анализа результатов АДБ формируются соответствующие отчеты и/или СОП.

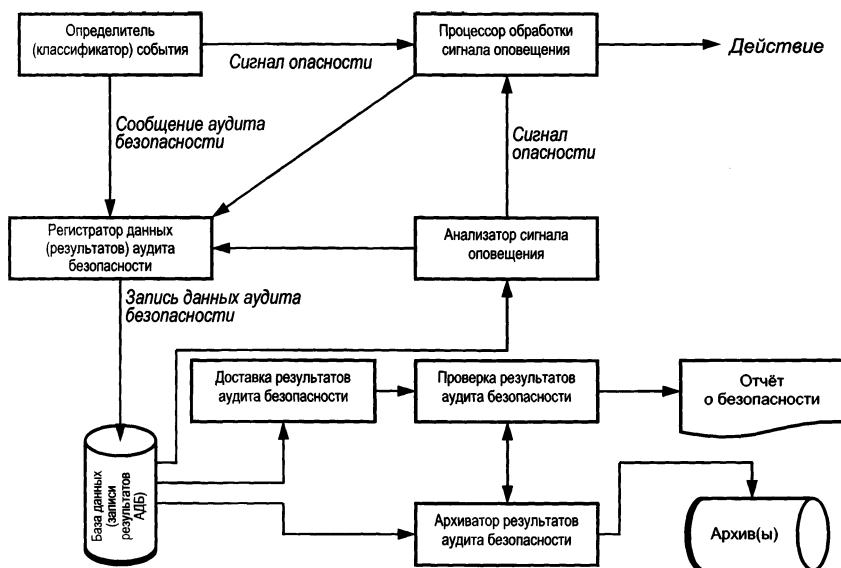


Рис. 8.1. Модель процессов аудита безопасности и оповещения об опасности

8.1.1.3. Объединение в группы функций АДБ и оповещения об опасности

Реализуемые моделью функции могут быть объединены в одном системном компоненте или распределены среди нескольких компонентов системы. Также эти функции могут сосредотачиваться в различных оконечных системах и даже могут дублироваться. В некоторых случаях, например, в зависимости от условий эксплуатации системы, объединение функций в группы было бы существенным преимуществом. Соответственно, средства регистрации, диспетчеризации и анализа результатов АДБ, функционирующие вместе на основе одних и тех же результатов

АДБ, могут быть объединены в группу, которая является частью автоматизированной оконечной системы.

Средства формирования отчетов и анализа результатов АДБ могут быть объединены в другую группу, которая может быть весьма полезной для аудиторов безопасности.

Соответственно, в распределенной БДРА последовательность функций может быть ранжирована по иерархическому принципу (рис. 8.2). Средство отбора результатов АДБ, принадлежащее одному компоненту, осуществляет сбор сообщений АДБ, поступающих от средства диспетчеризации результатов АДБ, которое принадлежит другому компоненту. Эта связка прерывается, когда компоненты не взаимодействуют со средством диспетчеризации результатов АДБ. В последнем случае компонент обязан взаимодействовать со средством архивирования записей БДРА, которое способно передавать записи БДРА в архив.

Решение о том, какие из функций следует объединять в группы, зависит от организации конкретной прикладной системы.

ПРИМЕЧАНИЕ. Рассмотренные выше примеры носят исключительно иллюстративный характер.

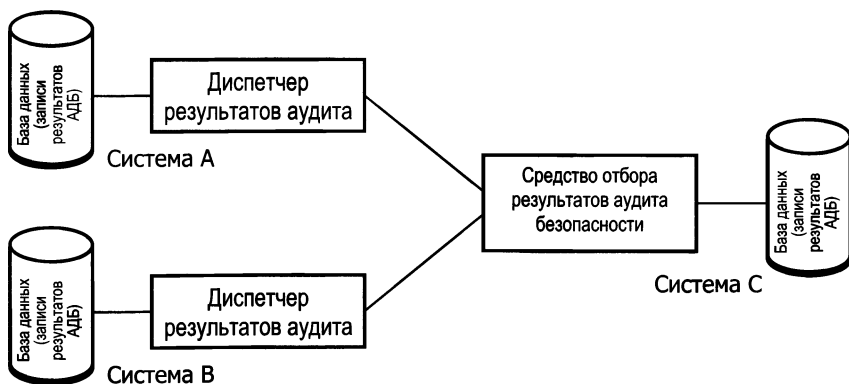


Рис. 8.2. Модель распределенной базы данных результатов АДБ

8.1.2. Фазы процедур АДБ и оповещения об опасности

СЛАД предоставляет аудиторскому центру возможность определять и выбирать события, которые подлежат обнаружению и регистрации в БДРА, и события, которые необходимы для отправки СОП и сообщений АДБ.

При реализации ПРАД можно выделить следующие фазы:

- фаза обнаружения (detection phase), в которой происходит обнаружение события безопасности;
- фаза определения (классификации; discrimination phase), в которой осуществляется предварительная классификация события, которая устанавливает необходимость регистрации события в БДРА или подачи СОП;
- фаза обработки сигнала оповещения (alarm processing phase), в которой может быть подан СОП или отправлено сообщение АДБ;
- фаза анализа (analysis phase), в которой событие, тем или иным образом затрагивающее обеспечение (состояние) безопасности, анализируется и сравнивается, исходя из контекста, с ранее обнаруженными событиями, зарегистрированными в БДРА, а также с планом ранее предпринятых действий;
- фаза объединения (aggregation phase), в которой записи из различных БДРА собираются в одну БДРА;
- фаза формирования отчета (report generation phase), в которой из записей БДРА формируются отчеты по результатам АДБ;
- фаза архивирования (archiving phase), в которой записи из БДРА доставляются на архивное хранение (в архив результатов АДБ).

Рассмотренные выше фазы не обязательно следуют одна за другой или строго разделены по времени, т.е. они могут перекрываться.

8.1.2.1. Фаза обнаружения

В этой фазе определяется, произошло ли событие безопасности. Реальное определение того, какое ответное действие долж-

но последовать после обнаружения такого события, является задачей средства определения (классификации) события, однако в отдельных случаях в соответствии с ПЛБ может незамедлительно последовать СОП.

8.1.2.2. Фаза определения (классификации)

Когда обнаружено событие безопасности, тогда средство определения (классификации) события установит соответствующее начальное ответное действие (или направление действий). Такое ответное действие может быть одним из следующих:

- a)* отсутствие какого-либо ответного действия;
- b)* формирование сообщения АДБ;
- c)* подача СОП и формирование сообщения АДБ.

Выбор конкретного ответного действия из трех перечисленных выше должен осуществляться в зависимости от каждого обнаруженного события и действующей ПЛБ.

8.1.2.3. Фаза обработки сигнала оповещения

В этой фазе процессор (средство обработки) анализирует СОП и определяет необходимое дальнейшее корректное действие. Такое дальнейшее действие может быть одним из следующих:

- a)* отсутствие какого-либо дальнейшего действия;
- b)* начало восстановительных мероприятий;
- c)* начало восстановительных мероприятий и формирование сообщения АДБ.

Выбор конкретного дальнейшего действия из трех перечисленных выше должен осуществляться в зависимости от характера каждого обнаруженного события и действующей ПЛБ.

ПРИМЕЧАНИЕ. Второе и третье действия могут вызывать прерывание события с целью привлечения внимания персонала, например администратора по безопасности или системного аудитора.

8.1.2.4. Фаза анализа

В этой фазе осуществляется обработка события безопасности с целью определения соответствующего дальнейшего действия. Указанная обработка также может использовать информацию о более ранних событиях, касавшихся обеспечения (состояния) безопасности и зарегистрированных в БДРА. Такое дальнейшее действие может быть одним из следующих:

- a) отсутствие какого-либо дальнейшего действия;
- b) подача СОП;
- c) формирование записи результатов АДБ;
- d) подача СОП и формирование записи результатов АДБ.

Выбор конкретного дальнейшего действия из четырех перечисленных выше должен осуществляться в зависимости от характера каждого обнаруженного события и действующей ПЛБ.

В качестве одной из итераций процесса анализа может быть сделана ссылка на предшествующие события путем проверки записей в БДРА и архивных записей результатов АДБ.

8.1.2.5. Фаза объединения

Отдельные записи результатов АДБ из нескольких распределенных БДРА должны периодически собираться в одну БДРА. Этот процесс, который включает использование функций отбора результатов АДБ (в точке отбора) и диспетчеризацию результатов АДБ, называется *объединением* (этот процесс может быть иерархическим).

8.1.2.6. Фаза формирования электронного отчета

Когда это необходимо или установлено ПЛБ, результаты АДБ могут проходить дополнительную обработку. Этот обработка будет применять элементы анализа и, возможно, преобразование записей результатов АДБ в соответствующий формат. Выходные данные анализа результатов АДБ представляют собой *электронный отчет*, который может указывать на то, что была попытка нарушения безопасности системы, и в таком случае может понадобиться проведение процедур восстановления

безопасности. Анализ результатов АДБ может использоваться для исследования последствий атаки и для определения соответствующих процедур контроля нарушений безопасности.

Электронный отчет по результатам АДБ может использоваться при восстановлении безопасности для определения последствий нарушения, вследствие которого возникла проблема безопасности. Соответственно, такой отчет может использоваться для определения ресурсов, которыми пользовался авторизованный клиент, и того, кто воспользовался его правами, но в нештатном режиме (некорректным образом). Также электронный отчет может использоваться при анализе любого нарушения (происшествия), после которого может возникнуть необходимость проведения восстановительных процедур.

8.1.2.7. Фаза архивирования

Результаты АДБ могут понадобиться (быть востребованными) на протяжении достаточно продолжительного периода времени. В фазе архивирования часть результатов АДБ перемещается в хранилище на длительное хранение. Хранилище, используемое для архивирования, должно обеспечивать целостность исходной(ых) записи(ей). Архивирование результатов АДБ относительно исходного источника результатов аудита может быть локальным или удаленным. Для удаленного архивирования могут понадобиться дополнительные ресурсы.

8.1.3. Корреляция аудиторской информации

Записи АДБ в рамках одной или нескольких БДРА могут быть взаимосвязаны между собой. Например, запрос соединения может передаваться через несколько промежуточных систем, вследствие чего может быть сформировано несколько записей результатов АДБ в различных БДРА. Очень важно, чтобы эти записи результатов АДБ содержали точные метки времени или идентификаторы взаимосвязей между собой. Другим примером является запись двух разных событий в двух различных БДРА, и при этом очень важно определить, какое событие произошло первым.

8.2. Политики и другие аспекты аудита безопасности и оповещения об опасности

8.2.1. Политика

Политика проведения аудита безопасности (ПЛАД) описывает события безопасности и устанавливает правила применения процедур отбора, записи (БДРА) и анализа различных событий, касающихся обеспечения (состояния) безопасности. Существует несколько условий, которые могут быть включены в ПЛАД и в правила таких ПЛАД. Некоторые (одно или более) из таких условий могут быть включены в соответствующую ПЛБ.

ПЛАД должна устанавливать требования для проведения АДБ различных уровней и типов, а также должна определять критерии формирования и подачи СОП. Проверка соответствия системных средств управления, подтверждение соответствия ПЛБ и определение имеющихся изменений в ПЛБ, средствах управления и процедурах потребуют анализа записей результатов АДБ и многих других аспектов структуры и состава системы, ее настройки (конфигурации) и функционирования.

8.2.2. Законодательные аспекты

Во многих странах существуют законы, предназначенные для защиты частной жизни граждан этих стран. В некоторых случаях это означает, что запись результатов АДБ, содержащая персональные данные, не будет удовлетворять требованиям национальных законов, в частности тех, которые связывают секретность информации и доступ к ней. Такие записи необходимо защищать от неавторизованного (несанкционированного) вскрытия.

Там, где записи результатов АДБ используются в качестве правомочного (приемлемого) доказательства, могут вводиться специальные требования к использованию, хранению и защите записи результатов АДБ.

8.2.3. Требования к защите

Существуют два основных аспекта защиты, а именно:

- защита записи результатов АДБ и аудиторской информации;
- защита совместной службы, состоящей из СЛАД СЛОО (СЛАО).

8.2.3.1. Защита аудиторской информации

Информация, отбираемая в БДРА, может поступать напрямую из сообщений АДБ или из других БДРА. Следовательно, результаты АДБ могут формироваться путем объединения записей БДРА, сформированных одним или несколькими источниками. В простейшем случае записи БДРА включают все записи результатов АДБ, сформированные одной системой.

Результаты АДБ должны быть защищены от несанкционированного вскрытия и/или несанкционированной модификации. Для их защиты могут использоваться способы УД, аутентификации, обеспечения конфиденциальности и целостности. Для хранения записей результатов АДБ используется один специальный метод, заключающийся в том, что записи хранятся среде, в которую запись данных можно сделать только один раз, при этом невозможно использовать процедуру перезаписи для удаления записи о событии.

Сообщения АДБ, СОП и электронные отчеты о результатах АДБ тоже должны быть защищены от несанкционированного вскрытия и/или несанкционированной модификации. Более того, очень важно, чтобы отправитель и получатель информации были уверены в том, что источник и получатель данных являются теми, кто был действительно определен, и что информация ни каким образом не была скомпрометирована.

По крайней мере, может быть востребована конфиденциальность некоторой части информации, возможно, на основании следующих причин:

- законодательные аспекты, связанные с персональными данными;

- необходимость хранения в тайне событий АДБ, которые были или не были зарегистрированы;
- необходимость хранения в тайне параметров подлинности получателей (или не получателей) результатов процедур (действий), последовавших после отправки СОП.

8.2.3.2. Защита СЛАО

СЛАО зависит от наличия высокого уровня доступности. Отказ в обслуживании (denial of service) является серьезной угрозой для СЛАО. Информация, предназначенная для администратора системы оповещения об опасности или аудитора системы обеспечения безопасности, могла бы задержаться в той точке, где такая информация не имеет смысла. Из этого следует очень важный вывод — информация должна достигать своего потребителя своевременно.

8.3. Вспомогательная информация и средства для аудита безопасности и оповещения об опасности

Обработка ВИ в интересах СЛАО может иметь два аспекта, а именно:

- обработка сообщений, сформированных в ответ на неожиданные («нежданные») события (т.е. не затребованной со стороны СЛАО информации);
- обработка запросов определенной информации в интересах СЛАО (т.е. затребованной информации).

Службы обеспечения необходимы для управления некоторыми аспектами процедур АДБ и оповещения об опасности, включая способы АДБ, критерии, по которым выбираются определенные действия (процедуры), осуществляемые после обнаружения события, касающегося обеспечения (состояния) ИБ, и процедуры обработки ВИ для СЛАО.

8.3.1. ВИ в интересах СЛАО

Вспомогательная информация в интересах СЛАО (ВИАО) включает СОП, сообщения АДБ, записи результатов АДБ и электронные отчеты о результатах АДБ.

8.3.1.1. Сообщения АДБ

Сообщение АДБ представляет собой сообщение, которое было сформировано в результате обнаруженного события безопасности, относящегося к вопросам АДБ.

Сообщение АДБ может быть сформировано, например, на основе первичного анализа обнаруженного события безопасности с помощью средства определения (классификации) события, или в результате последующей обработки средством обработки СОП или средством анализа результатов АДБ.

8.3.1.2. Записи результатов АДБ

Термин «*запись результата АДБ*» используется для определения одиночной записи в БДРА. Во многих случаях он будет соответствовать одиночному событию безопасности, но можно предположить, что в некоторых прикладных системах запись результата АДБ будет сформирована в результате обнаружения нескольких событий безопасности.

Типовая запись результата АДБ включает в себя информацию об источнике и причине появления сообщения, а также может включать информацию об объектах/субъектах, привлекаемых к проведению процедур обнаружения и обработки сообщения.

8.3.1.3. Сигналы оповещения об опасности

Сигнал оповещения об опасности (или *сигнал опасности*) представляет собой сообщение, следующее после обнаружения события безопасности, которое классифицировано как событие, приводящее к нарушению безопасности и возникновению условий для формирования и подачи СОП. Сигнал опасности может быть результатом обнаружения одиночного события безопасности или результатом достижения предельных значе-

ний определенных параметров. И в том и другом случае описание условий формирования и подачи СОП является предметом ПЛБ.

СОП могут быть инициированы средством определения (классификации) события (как результат первичного анализа и обработки события безопасности) или средством анализа результатов АДБ, причем в любой момент времени, если оно выявило наличие условий для формирования и подачи сигнала опасности.

8.3.1.4. Электронные отчеты о результатах АДБ

Электронные отчеты о результатах АДБ представляют собой информацию, формируемую на основе анализа результатов АДБ. Для формирования электронных отчетов на основе одного или нескольких результатов АДБ используется средство формирования отчета по результатам АДБ.

8.3.1.5. Пример объединения информации для СЛАО

Как правило, информация в интересах СЛАО включает:

- тип информации/сообщения (т.е. СОП, сообщение АДБ или электронный отчет о результатах АДБ);
- UID элементов (например инициатор/целевой объект в событиях безопасности, объект/субъект действия);
- причина появления сообщения;
- UID средств определения (классификация) события, предоставления записей БДРА и/или регистрации данных АДБ.

8.3.2. Средства для СЛАО

Для проведения эффективной ПРАД и всестороннего и тщательного анализа событий необходим метод, который бы обнаруживал события безопасности и определял способ их обработки. Анализ сообщений осуществляется с помощью способа фильтрации, который, в свою очередь, определяет, какое дей-

ствие необходимо выполнить при получении сообщения АДБ. Фильтр функционирует в соответствии с критерием (установленным аудиторским центром), который определяет вид обработки для каждого типа сообщения. Применяемый критерий может включать:

- время суток/дня;
- пороговый счетчик;
- тип события;
- объект/субъект, повлекший возникновение события.

С точки зрения процедуры обеспечения, фильтр может быть описан как объект обеспечения с определенным алгоритмом функционирования и соответствующими параметрами.

Вспомогательные (обеспечивающие) средства СЛАО (рис. 8.3) решают задачу формирования критерия отбора, который дает пользователю возможность обрабатывать информацию, необходимую для функционирования СЛАО. В широком смысле, такими средствами являются:

- a)* средства формирования, модификации и удаления критерия при обработке событий безопасности;
- b)* средства блокирования и разблокирования функции формирования определенных сообщений АДБ;
- c)* средства блокирования и разблокирования функции формирования результатов АДБ;
- d)* средства блокирования и разблокирования функций формирования и обработки СОП.

Функциональными средствами СЛАО являются (см. рис. 8.3):

- a)* средство формирования ВИ для СЛАО (например для формирования СОП, сообщения АДБ, электронного отчета по результатам АДБ);
- b)* средство записи ВИ для СЛАО;
- c)* средство отбора/объединения ВИ для СЛАО;
- d)* средство анализа ВИ для СЛАО;
- e)* средство архивирования ВИ для СЛАО.

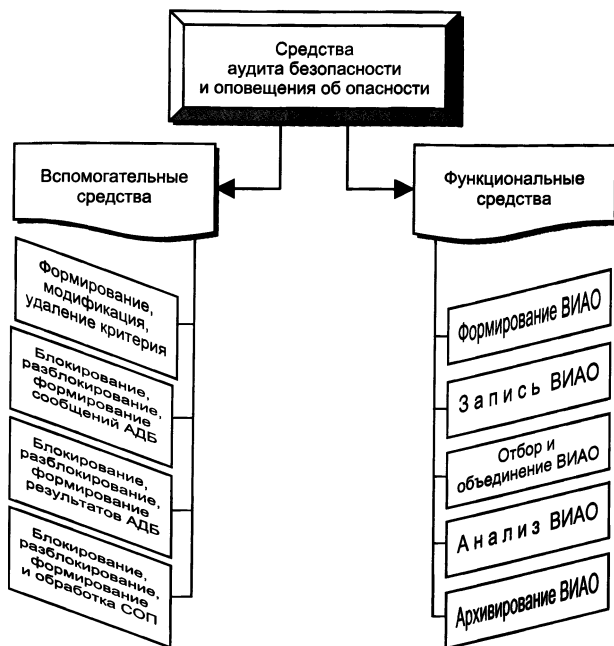


Рис. 8.3. Средства, используемые в процедурах аудита безопасности и оповещения об опасности

8.3.2.1. Определение и анализ событий безопасности — критерии для функций СЛАО

СОП и сообщение АДБ определяют тип события, причину события, время обнаружения события, параметр подлинности средства обнаружения события и параметры подлинности объектов/субъектов, тем или иным образом связанных с этим событием (т.е. объект и субъект действия, повлекшего возникновение события безопасности).

Формирование критериев необходимо для выбора того или иного действия (процедуры) при обработке различных типов информации. Для определения и анализа событий безопасности используются следующие критерии:

- 1) *критерии для классификации событий безопасности.* По этим критериям будут определяться действия (процедуры)

ры), которые следует осуществить после обнаружения события безопасности.

Входные данные могут быть следующие:

- тип события безопасности;
- время суток;
- объект/субъект, повлекший возникновение события.

Выходные данные могут быть следующие:

- выбранное действие (процедура);
- СОП, который должен быть сформирован и передан;
- сообщение АДБ, которое должно быть сформировано и передано;

2) *критерии для формирования отчета по результатам АДБ.* Эти критерии являются основой отбора информации, содержащейся в одном или нескольких результатах АДБ, в целях составления электронных отчетов по результатам АДБ.

Входные данные могут быть следующие:

- тип записи результата АДБ;
- тип события безопасности;
- время проверки события;
- объект/субъект, информация о котором затребована.

Выходные данные могут быть следующие:

- перечень отобранных записей результатов АДБ;

3) *критерии для анализа результатов АДБ.* По этим критериям определяется способ (алгоритм) обработки результатов АДБ средством анализа результатов АДБ. Перед тем как будет определено последующее действие (процедура), результаты АДБ будут анализироваться путем исследования самого происшествия и частоты возникновения таких происшествий (и им подобных).

Входные данные могут быть следующие:

- тип события;
- число происшествий (событий);
- период времени.

Выходные данные могут быть следующие:

- действие, которое должно быть выполнено.

ПРИМЕЧАНИЕ. Для регистрации и архивирования результатов АДБ критерии не нужны.

8.4. Способы проведения АДБ и применения СОП

Основное отличие СЛАО от других ранее рассмотренных СЛБ состоит в том, что в последних не используются специализированные СПБ, которые могли бы применяться в СЛАО (СПАО). СПАО могут описываться процедурной характеристикой, основу которой составляет определенное число управляющих и функциональных запросов. По этой причине СПАО детально не рассматриваются. Однако в качестве примера некоторого типа запросов, используемых в СПАО, можно привести способы анализа событий безопасности:

- сравнение деятельности объекта/субъекта с известным описанием его деятельности, например, неприемлемый доступ, основанный на недопустимом использовании ресурсов с точки зрения времени или географии и др.;
- обнаружение нескольких событий одного или нескольких типов за определенный интервал времени;
- наблюдение за отсутствием событий одного или нескольких типов за определенный интервал времени.

Перечень приведенных выше примеров является неполным.

8.5. Взаимосвязи с другими СЛБ и СПБ

8.5.1. Аутентификация объекта/субъекта

Доставка результатов АДБ между средством диспетчеризации и средством отбора результатов АДБ требует обоюдной аутентификации, чтобы средство диспетчеризации передавало бы результаты АДБ предназначенному для приема средству отбора

результатов АДБ, а средство отбора результатов АДБ получало бы результаты АДБ от предназначенного для их передачи средства диспетчеризации.

8.5.2. Аутентификация источника данных

Аутентификация источника данных используется для того, чтобы мог быть установлен источник сообщений АДБ и СОП. Кроме того, аутентификация источника данных используется средством анализа результатов АДБ для обеспечения гарантий того, что все сообщения от неизвестных средств формирования сообщений о событиях безопасности или анализа результатов АДБ будут удалены.

8.5.3. Управление доступом

Службы УД должны использоваться при хранении и доставке записей результатов АДБ. Кроме того, СЛУД могла бы использоваться для предотвращения неавторизованного (несанкционированного) доступа к результатам АДБ.

8.5.4. Обеспечение конфиденциальности

СЛКН может использоваться при доставке результатов АДБ, записей результатов АДБ, сообщений АДБ и СОП. Кроме того, СЛКН может использоваться для защиты конфиденциальности хранящихся записей результатов АДБ.

8.5.5. Обеспечение целостности

При функционировании СЛАД и СЛОО первостепенное значение имеет обнаружение любой неавторизованной (несанкционированной) модификации результатов АДБ, совокупностей записей результатов АДБ, сообщений АДБ и СОП. В этих целях может использоваться СЛЦЛ.

8.5.6. Обеспечение неотказуемости

Так как доставка результатов АДБ, как правило, будет осуществляться в пределах одного и того же ССБ, СЛНТ обычно не используется.

8.6. Общие принципы АДБ и СОП в ЭМВОС и Интернет-архитектуре

Следующие типы событий безопасности должны всегда находиться под непрерывным аудиторским контролем:

- процедуры, связанные с предоставлением ВИ;
- процедуры, которые могут изменить совокупность событий, находящихся под аудиторским контролем;
- процедуры, которые могут изменить идентификацию событий, находящихся под аудиторским контролем.

Далее рассматриваются события (процедуры, процессы) при взаимодействии открытых систем, которые могут стать реальной причиной возникновения события безопасности. При необходимости под аудиторским контролем могут находиться штатные и нештатные события, например, процедура «запрос соединения» может стать объектом записи результатов АДБ вне зависимости от того, был ли или нет запрос корректным или удовлетворен.

Следующие события, среди прочих, могут быть объектами аудиторского контроля. Этот перечень неполный и носит только демонстративный характер.

События безопасности, связанные с установлением соединения:

- запросы на установление соединения;
- согласие на установление соединения;
- запросы на разъединение;
- согласие на разъединение;
- обмен служебной информацией, включая статистические данные, в течение соединения.

События безопасности, связанные с использованием СЛБ:

- запросы на использование СЛБ;
- использование СПБ;
- СОП.

События безопасности, связанные с обеспечением службы:

- обеспечивающие процедуры;
- процедуры оповещения, связанные с обеспечением службы.

Также целесообразно включить в перечень событий, подлежащих аудиторскому контролю, по крайней мере, следующие события:

- запрет доступа;
- аутентификация;
- изменение атрибута;
- формирование, удаление и модификация объекта;
- использование привилегий.

С точки зрения предоставления персональных услуг по обеспечению безопасности, следующие события безопасности являются чрезвычайно важными:

- аутентификация: положительный результат проверки;
- аутентификация: отрицательный результат проверки;
- УД: положительное решение о предоставлении доступа;
- УД: отрицательное решение о предоставлении доступа;
- обеспечение неотказуемости: неотказуемость источника сообщения;
- обеспечение неотказуемости: неотказуемость получателя сообщения;
- обеспечение неотказуемости: отказ в отрицании спорного события;
- обеспечение неотказуемости: подтверждение отрицания спорного события;
- обеспечение целостности: формирование защиты;
- обеспечение целостности: снятие защиты;

- обеспечение целостности: положительное подтверждение целостности;
- обеспечение целостности: отрицательное подтверждение целостности;
- обеспечение конфиденциальности: использование процедуры закрытия;
- обеспечение конфиденциальности: использование процедуры раскрытия;
- АДБ: выбор события в период проведения АДБ;
- АДБ: отказ от выбранного события в период проведения АДБ;
- АДБ: изменение критериев выбора события, в отношении которого аудиторский контроль обязателен.

ПРИМЕЧАНИЕ. Если УД используется качестве основы СПЦЛ и СПКН, то записи результатов АДБ, связанные с «решением отказать в доступе», могут быть преобразованы в прямое подтверждение попыток нарушения конфиденциальности или целостности.

Все результаты АДБ, непосредственно связанные с соответствующим используемым соединением, должны быть однозначно идентифицированы в целях обеспечения гарантий того, чтобы эти записи могли быть найдены и при необходимости скопированы.

Для создания соответствующих СЛАО рекомендуется использовать международные стандарты ITU-T Rec. X.734 | ISO/IEC 10164–5, ITU-T Rec. X.735 | ISO/IEC 10164–6, ITU-T Rec. X.736 | ISO/IEC 10164–7 и ITU-T Rec. X.740 | ISO/IEC 10164–8.

8.7. Реализация модели АДБ и СОП

Функции модели АДБ и СОП представлены на рис. 8.1. Вся процедура может быть распределена между несколькими отдельными открытыми системами, каждая из которых отвечает

за один или несколько аспектов выполнения этой процедуры. Пример такого распределения представлен на рис. 8.4.

Примером события безопасности могла быть попытка регистрации доступа в систему с использованием неверного пароля, т.е. отсутствующего в системе учета. Анализ результата АДБ может позволить установить, что это была одна из последовательности попыток зарегистрироваться в системе с ложным паролем, а СОП может быть сформирован и послан, когда число таких нарушений (попыток) достигло своего предельного допустимого значения.

Система *S1 (система распознавания)* способна (см. рис. 8.4) обнаруживать события безопасности и проводить их анализ в соответствии с выбранными критериями (1-я группа критериев, § 8.3.2.1), но не способна зафиксировать результаты АДБ, поэтому ее СОП передается в систему *S2 (система оповещения об опасности)*, а ее сообщения АДБ передаются в систему *S3 (система регистрации и обеспечения результатов аудита безопасности)* для их включения в БДРА.

Система *S3* отвечает за пополнение результатов АДБ (БДРА). Кроме этого, *S3* обеспечивает систему *S6 (система экспертизы результатов аудита безопасности)*, т.е. предоставляет последней доступ к БДРА и архиву результатов АДБ. При этом *S6* может отбирать записи результатов АДБ в соответствии с установленными критериями (2-я группа критериев, § 8.3.2.1) и включать их в электронные отчеты по результатам АДБ.

Система *S4 (система архивирования результатов аудита безопасности и анализа)* отвечает за архивирование и извлечение записей результатов АДБ.

Система *S5 (система анализа)* включает прикладной (программный или программно-аппаратный) модуль. Этот модуль осуществляет анализ записей результатов АДБ (и архивных записей результатов АДБ) в соответствии с установленными критериями (3-я группа критериев, § 8.3.2.1) и передает СОП в систему *S2*, когда пороговые значения превышены или обнаружены иные причины подачи СОП.

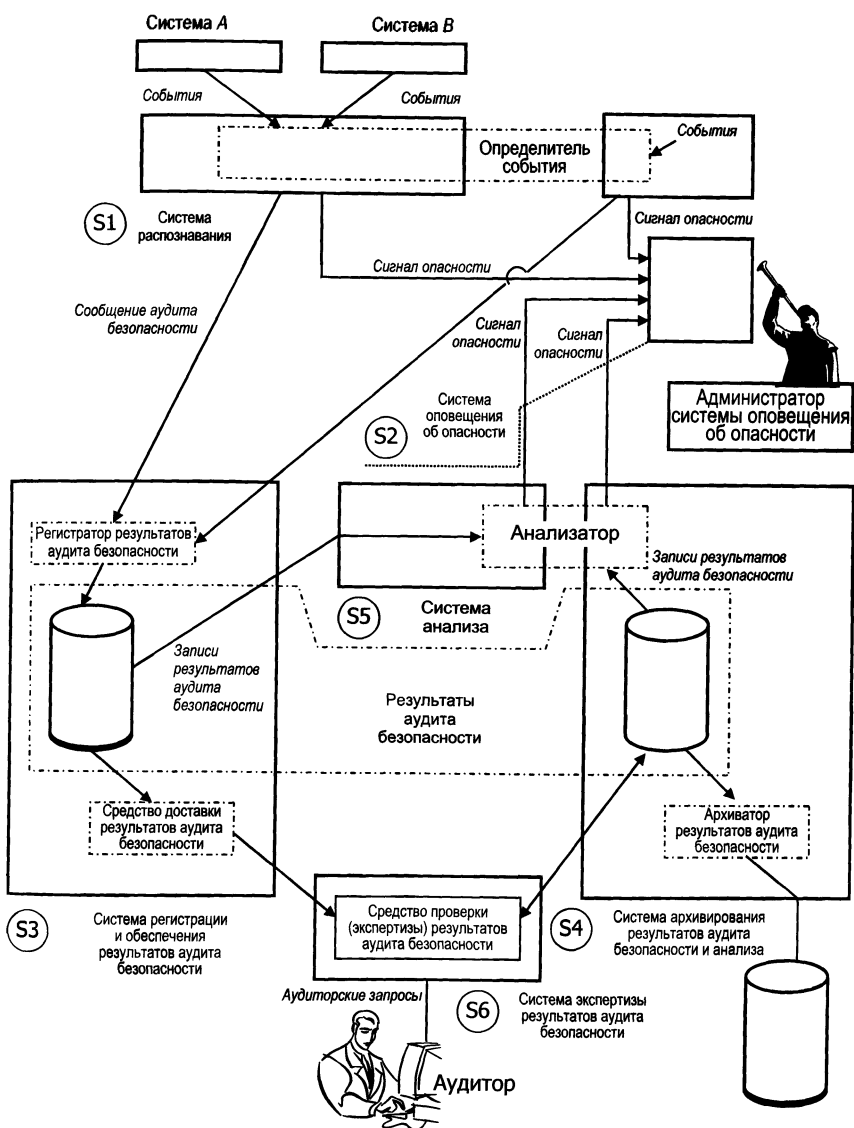


Рис. 8.4. Пример реализации модели АДБ и СОП (СЛАД и СЛОО)

8.8. Регистрация времени возникновения событий, подлежащих аудиторскому контролю

На практике надежная и точная синхронизация между различными генераторами событий или регистраторами событий просто невозможна или весьма затратна. В таком случае необходимо средство фиксации времени получения результатов АДБ. Запись результата АДБ формируется на основе полученного сообщения АДБ, которое может содержать метку времени или нет. Если сообщение АДБ содержит метку времени, то формируется *специализированная запись АДБ с указанием времени (ЗВАД)*, изъятая из этого сообщения. В последнем случае специализированная запись АДБ, сформированная после получения сообщения о событии безопасности, подлежащего аудиторскому контролю, содержит метку времени, которая была сформирована с использованием генератора эталонного времени, встроенного в средство регистрации данных (результатов) АДБ. В обоих случаях должна быть сформирована ЗВАД, отражающая разницу во времени между генератором событий и средством регистрации данных (результатов) АДБ.

В предыдущем случае должна быть проведена оценка расхождения во времени между генераторами эталонного времени генератора событий и средства регистрации данных (результатов) АДБ. ЗВАД должна включать идентификатор генератора событий, эталонное время генератора событий и средства регистрации данных (результатов) АДБ, задержку между значениями эталонного времени и допустимое значение девиации задержки. В последнем случае ЗВАД должна содержать идентификатор генератора событий, эталонное время генератора событий и средства регистрации данных (результатов) АДБ, оценку задержки между генератором событий и средством регистрации данных (результатов) АДБ и допустимый диапазон значений задержки.

Но с практической точки зрения, чрезвычайно обременительно иметь записи, формирующиеся для каждого события. Такие записи, в принципе, могут быть сформированы в зави-

симости от «физической природы» транспортного соединения или расхождения (дрейфа) времени между эталонными источниками времени. Если после определенного периода наблюдения окажется, что задержка ничтожно мала, то такими записями можно пренебречь. Если измерения задержки отсутствуют, то можно использовать метод линейной интерполяции.

Аналогичный тип проблем имеет место между источниками эталонного времени, размещенными в средствах регистрации и диспетчеризации результатов АДБ, когда средство диспетчеризации расположено в другой оконечной системе. Однако в этом случае обе системы будут иметь источники эталонного времени.

Измерения разницы во времени могут быть проведены в любой момент времени между двумя взаимодействующими сторонами или в момент доставки результатов АДБ. ЗВАД должна включать идентификатор генератора событий, идентификатор средства диспетчеризации результатов АДБ, значение эталонного времени средства регистрации результатов АДБ, оценку задержки между средствами регистрации и диспетчеризации результатов АДБ, а также допустимый диапазон значений задержки.

Определение, какое из двух событий произошло первым, может быть произведено путем добавления или вычитания значений задержек между серией значений эталонного времени и прибавлением всех диапазонов значений задержки. Если результирующая задержка будет меньше, чем допустимый диапазон значений задержки, то различием можно пренебречь.

Аналогичный аргумент применяется также тогда, когда необходимо сформировать электронный отчет по результатам АДБ. Использование информации, содержащейся в результатах АДБ, позволяет классифицировать события по различным значениям эталонного времени. Однако такой порядок событий может быть гарантирован только тогда, когда допустимый диапазон значений задержки короче, чем разница во времени плюс допу-

стимый диапазон значений задержки каждого события. С этой целью должна быть обеспечена возможность вычисления совокупного допустимого диапазона значений задержки каждого события.

Общая структура единой службы аудита безопасности и оповещения об опасности представлена в табл. 8.1.

Таблица 8.1

Структура единой службы аудита безопасности и оповещения об опасности		Элемент	<u>Объект/субъект</u>: Аудиторский центр, Администратор службы оповещения об опасности, Аудитор безопасности <u>Функции</u>: определение (классификация) события, регистрация данных (результатов) АДБ, обработка СОП, анализ результатов АДБ, формирование отчета по результатам АДБ, предоставление записей БДРА, архивирование записей БДРА, отбор результатов АДБ, диспетчеризация результатов АДБ <u>Информационные объекты</u>: Сообщения АДБ, Записи результатов АДБ, Электронные отчеты по результатам АДБ
		<u>Цель службы</u>: Гарантировать, что информация, связанная безопасностью открытых информационных систем, регистрируется и при необходимости на ее основе формируются электронные отчеты	
М Е Р О П Р И Я Т И Я	Объект/субъект	Аудиторский центр	
	Функция	Распознавание и анализ событий безопасности	
	Мероприятия, связанные с обеспечением СЛАО	Определение критерия 1: для классификации событий безопасности Определение критерия 2: для формирования отчета по результатам АДБ Определение критерия 3: для анализа результатов АДБ	

Таблица 8.1 (продолжение)

М Е Р О П Р И Я Т И Я	Объект/субъект	Администратор службы оповещения об опасности	Аудитор безопасности	Инициатор/целевой объект Субъект/объект
	Функция	— Определение (классификация) события — Обработка СОП — Анализ результатов АДБ	— Выбор события — Классификация выбранного события — Анализ результатов АДБ — Регистрация результатов АДБ — Формирование отчета по результатам АДБ — Предоставление записей БДРА — Архивирование записей БДРА	
	Мероприятия, функционально связанные с СЛАО	— Формирование информации — Отбор информации (информация, содержащаяся в СОП)	— Формирование информации — Отбор информации — Анализ информации (информация, содержащаяся в сообщении АДБ)	

Таблица 8.1 (окончание)

И Н Ф О Р М А Ц И Я	Входные/выходные элементы данных, определяемые Аудиторским центром	Критерий 1 — Тип события — Время — Объект/субъект	Критерий 2 — Тип записи — Тип события	Критерий 3 — Тип события — Число происшествий — Период времени
		— Действие (процедура), которое должно быть выполнено — ВИ, которая должна быть сформирована	— Списки записей	— Действие (процедура), которое должно быть выполнено
	Информация, используемая в процедурах СЛАО	— Тип сообщения/информации — УИД элементов — Причина формирования сообщения — УИД средств определения (классификации) события, предоставления записей БДРА и/или регистрации данных (результатов) АДБ		
	Контрольная информация	— Время — Происшествия		

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ КЛЮЧАМИ

Современные ИТС все больше и больше нуждаются в использовании криптографических методов для защиты данных от их вскрытия или модификации при проведении процедур аутентификации или обеспечении неотказуемости. Уровень защищенности и надежности, обеспечиваемый такими методами, напрямую зависит от обеспечения и защиты используемого параметра безопасности, ключа. Безопасное обеспечение такими ключами является критической процедурой, особенно в сочетании с реализуемыми в системе криптографическими функциями, так как даже самая наиболее тщательно продуманная концепция обеспечения безопасности станет неэффективной, если обеспечение ключами будет ненадежным. *Целью обеспечения ключами* является проведение специализированных процедур обработки криптографической ключевой информации при ее использовании в симметричных или асимметричных криптографических методах.

В данной главе представлена общая модель обеспечения ключами, которая не зависит от применения какого-либо криптоалгоритма. Однако определенные способы распределения ключей могут зависеть от свойств соответствующего алгоритма, например свойств асимметричных криптоалгоритмов.

Особое внимание обращено на реализационные аспекты автоматизированных и обычных («ручных») систем обеспечения ключами, включая структуры элементов данных и последовательностей процедур, которые используются при предоставлении услуг по обеспечению ключами.

Как и в других СЛБ, обеспечение ключами может осуществляться только в рамках контекста принятой ПЛБ.

Главной проблемой является формирование ключевой информации, происхождение, целостность, своевременность и

конфиденциальность (в случае секретных ключей) которой может быть гарантирована как прямым, так и косвенным пользователям. *Обеспечение ключами*, в соответствии с ПЛБ, включает функции генерации (формирования), хранения, распределения, удаления и архивирования ключевой информации.

В настоящей главе представлены:

- a) формирование общей модели, на основе которой строятся способы обеспечения ключами;
- b) описание основных концепций обеспечения ключами;
- c) описание характеристик служб по обеспечению ключами (СЛКЛ);
- d) формирование единых принципов обеспечения ключевой информацией в течение ее жизненного цикла;
- e) формирование концептуальной модели распределения ключей.

9.1. Общая модель обеспечения ключами

9.1.1. Общие положения

Целевое назначение обеспечения ключами — безопасное администрирование и предоставление услуг по обеспечению ключами. По этой причине чрезвычайно важна защита ключей.

Процедуры обеспечения ключами зависят от основных криптографических методов, предполагающих использование ключа, и от реализуемой ПЛБ. Обеспечение ключами также включает те функции, которые реализованы в криптографических устройствах.

9.1.2. Защита ключей

9.1.2.1. Общие аспекты обеспечения ключами

Ключи являются наиболее важной и критической частью системы безопасности, которая зависит от криптографических методов защиты. Необходимая защита ключей зависит от не-

скольких факторов, таких как тип прикладной системы (прикладного процесса), использующей ключи, явные угрозы, которые необходимо парировать, различные состояния, в которых могут находиться ключи, и др. В первую очередь, в зависимости от криптографического метода они должны быть защищены от вскрытия, модификации, разрушения и повторного использования. Для парирования угроз может понадобиться использование нескольких методов и способов защиты. Период действия ключа должен быть ограничен во времени и числом его применений. Такие ограничения обусловлены временем и совокупностью данных, которые необходимы для проведения атак типа «восстановление ключа», и важным семантическим содержанием защищаемой информации на протяжении длительного времени. Ключи, которые используются для формирования ключей, нуждаются в еще большей защите по сравнению с формируемыми ключами. Другим важным аспектом защиты ключей является предотвращение их неправильного использования, например, использование ключа, предназначенного для зашифрования ключа, для зашифрования данных.

9.1.2.2. Защита с помощью криптографических методов

Некоторые угрозы для ключевой информации могут быть парированы путем использования криптографических методов. Например: шифрование предотвращает вскрытие ключа и его несанкционированное использование; способы защиты целостности предотвращают модификацию; способы аутентификации объекта, ЭЦП и способы аутентификации источника данных парировуют атаки типа «маскарад».

Разделение криптографических методов и способов предотвращает неправильное использование ключей. Такое разделение функционального применения может сопровождаться привязкой информации к ключу. Например: привязка управляющей информации к ключу гарантирует, что специфические ключи используются в специфических задачах (например шифрование ключа, целостность данных); управление ключами необходимо при обеспечении неотказуемости на основе использования симметричных криптографических методов.

9.1.2.3. Защита с помощью некриптографических методов

При ограничении времени действия ключей путем обозначения начала и конца периода их правомерного применения могут использоваться *метки времени*. Кроме того, применение меток времени совместно с *последовательными номерами* может парировать атаки типа «воспроизведение зарегистрированной информации о согласованном ключе».

9.1.2.4. Защита с помощью физических средств

Криптографическое устройство, размещенное внутри защищаемой системы, как правило, будет необходимо для защиты ключевой информации от угроз модификации, удаления и вскрытия (за исключением открытых ключей). Обычно устройство формирует защищенную зону для хранения ключей, использования ключей и реализации (встраивания) криптографических алгоритмов. Такое устройство может предоставлять средства:

- для загрузки ключевой информации из отдельного защищенного устройства хранения ключей;
- для взаимодействия с криптоалгоритмами, реализуемыми отдельными защищенными средствами (например смарт-карты);
- для автономного хранения ключевой информации (например карты памяти).

Как правило, зоны безопасности защищаются с помощью физических способов обеспечения безопасности. Физические способы обеспечения безопасности могут включать пассивные способы, предотвращающие прямой доступ к зоне безопасности, а также активные способы обнаружения вмешательства, которые направлены на разрушение ключевой информации в случае возможного проникновения в зону безопасности. Используемые физические способы обеспечения безопасности зависят от стратегической значимости защищаемых ключей на протяжении длительного периода времени.

9.1.2.5. Защита с помощью организационных средств

Такие средства защиты ключей организованы в соответствии с иерархией ключей. За исключением самого нижнего уровня иерархии, ключи одного уровня используются исключительно для защиты ключей на следующем нижнем уровне иерархии. Только ключи самого нижнего уровня напрямую используются для обеспечения служб обеспечения безопасности данных. Такой иерархический подход позволяет использовать каждый ключ ограниченно, уменьшая таким образом возможность вскрытия и затрудняя проведение атак. Например, результат компрометации одного сеансового ключа ограничивается только компрометацией информации, защищенной с помощью этого ключа.

Предоставление пользователям возможности доступа к ключам может вызвать соответствующие проблемы, связанные со способностью предотвратить вскрытие и доказать (при обеспечении неотказуемости), что ключ не мог использоваться неправильно. Ключи должны быть доступны в открытом виде только тогда, когда устройства обеспечения безопасности размещены внутри системы. Если ключи должны экспортироваться, то необходимо предпринимать специальные меры, такие как деление ключа на компоненты и запрет доступа одного человека ко всем компонентам.

Кроме того, использование ключа должно находиться под контролем с целью предотвращения его использования не по назначению, что может привести к вскрытию самого ключа или данных, защищенных с помощью этого ключа.

9.1.3. Общая модель жизненного цикла ключа

9.1.3.1. Описание жизненного цикла ключа

Криптографический ключ проходит последовательность состояний, которые определяют его жизненный цикл (ЖЦ). Существуют три следующих основных состояния:

- *ожидание активного состояния (pending active)*: В период ожидания активного состояния ключ был сформирован, но не был активирован к использованию по назначению;

- *активное состояние (active)*: В активном состоянии ключ используется либо для криптографической обработки данных, либо для расшифрования, либо для проверки обработанных данных;
- *послеактивное (постактивное) состояние (post active)*: В этом состоянии ключ должен использоваться только при расшифровании или проверке.

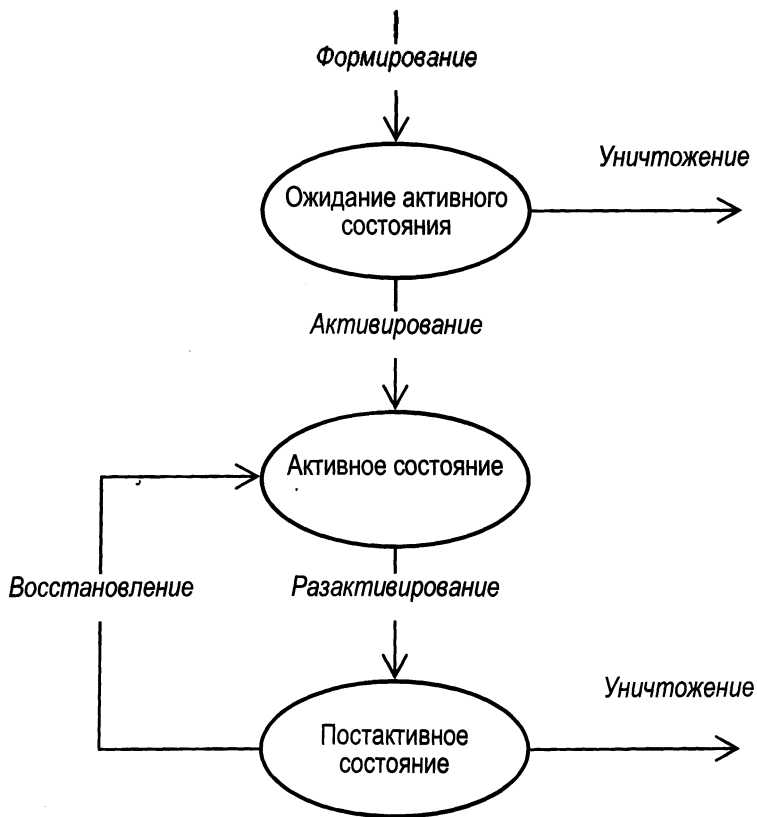


Рис. 9.1. ЖЦ ключа

Ключ, о котором стало известно, что он скомпрометирован, должен быть незамедлительно переведен в постактивное состоя-

ние и в разряд ненадежных ключей для выполнения каких-либо процедур, кроме как расшифрование и процедура проверки данных, которые были обработаны до его компрометации. Соответственно скомпрометированный ключ не должен быть повторно активирован (восстановлен).

Говорят, что ключ скомпрометирован, если он стал известен, когда был «целевым объектом» неавторизованного (несанкционированного) доступа или управления.

На рис. 9.1 представлены рассмотренные выше состояния, а также соответствующие переходы из одного состояния в другое, т.е. общая модель ЖЦ. Другие модели ЖЦ могут иметь дополнительные детали, которые являются промежуточными (частными) состояниями этих трех представленных состояний. Большинство моделей ЖЦ требуют наличия процедуры архивирования. Эта процедура может быть связана с любым из состояний, что зависит от соответствующих деталей ЖЦ.

9.1.3.2. Преобразования при переходе ключа из одного состояния в другое

Когда ключ переходит из одного состояния в другое, он подвергается одному из следующих преобразований (см. рис. 9.1):

- *формирование (generation)*: это процесс (процедура) формирования (генерирования) ключа. Формирование ключа должно производиться в соответствии с принятыми правилами формирования ключей. В течение этого процесса может привлекаться процедура тестирования с целью проверки соблюдения правил. Необходимо заметить, что в течение формирования ключа источник непредсказуемых случайных чисел является, в конечном счете, самым важным элементом, так как даже сильнейшие криптоалгоритмы не могут обеспечить адекватную защиту в случае компрометации такого источника или выбора источника с плохими характеристиками;

- *активирование (activation)*: этот процесс (процедура) делает ключ доступным для криптографических процедур;
- *разактивирование (deactivation)*: этот процесс (процедура) ограничивает использование ключа. Это может произойти вследствие истечения срока действия или аннулирования ключа;
- *повторное активирование или восстановление (reactivation)*: этот процесс (процедура) позволяет вновь использовать ключ, находящийся в постактивном состоянии, в криптографических процедурах;
- *уничтожение (destruction)*: этот процесс (процедура) завершает ЖЦ ключа. Данный процесс охватывает логическое уничтожение ключа, а также может включать его физическое разрушение.

Преобразования могут быть вызваны некоторыми событиями, например потребность в новых ключах, компрометация ключа, просроченный срок действия ключа и завершение ЖЦ ключа. Все эти преобразования включают в себя несколько служб (услуг по) обеспечения(ю) ключами.

9.1.3.3. Преобразования, службы и ключи

Ключи для соответствующих криптографических методов будут использовать различные сочетания служб (услуг) в течение своих ЖЦ. Рассмотрим два примера.

В симметричных криптографических методах за формированием ключа следует переход из ожидания активного состояния в активное состояние, который включает процедуру инсталляции ключа, а также может включать процедуры регистрации и распределения ключа. В отдельных случаях процедура инсталляции может привлекать процедуру извлечения специального ключа. Время жизни ключа должно ограничиваться зафиксированным временным интервалом (периодом). Разактивирование завершает активное состояние, обычно по окончании периода действия ключа. Кроме этого, если компрометация ключа в его активном состоянии стала допускаться или известна, то аннулирование

ключа повлечет за собой его переход в постактивное состояние. Находясь в постактивном состоянии, ключ может быть заархивирован. Если архивный ключ понадобится снова, то он будет восстановлен, может потребоваться его инсталляция или распределение, причем еще до его полного активирования. В противном случае последует разактивирование ключа, и он может быть снят с регистрации и уничтожен.

В асимметричных криптографических методах формируется пара ключей (открытый и закрытый), и оба ключа переходят в состояние ожидания активного состояния. Следует заметить, что ЖЦ двух ключей взаимосвязаны, но не идентичны. Перед тем как оба перейдут в активное состояние, закрытый ключ может быть дополнительно зарегистрирован, дополнительно представлен своему пользователю и всегда будет проинсталлирован. Преобразования закрытого ключа между его активным и постактивным состоянием, включающие разактивирование, восстановление и уничтожение, аналогичны тем, которые описаны выше и использовались для симметричных ключей. Когда открытый ключ сертифицирован, то, как правило, СЕРТ содержит открытый ключ (СЕРТ|ОК), сформированный УЦ, что гарантирует подлинность и принадлежность открытого ключа. Такой СЕРТ|ОК может быть помещен в репозиторий (БДК) Службы единого каталога (Directory) или другую аналогичную службу для распространения или может быть отправлен назад владельцу при выполнении процедуры распределения. Когда владелец СЕРТ|ОК передает данные, которые подписаны с помощью его закрытого ключа, он может дополнительно присоединять к данным свой СЕРТ|ОК. Пара ключей становится активной, когда открытый ключ сертифицирован. Если пара ключей используется для формирования ЭЦП, то после того, как закрытый ключ был разактивирован или уничтожен, открытый ключ продолжает оставаться в активном или постактивном состоянии в течение неопределенного времени. Доступ к открытому ключу может понадобиться при проверке ЭЦП, которые были сформированы до истечения срока действия соответствующего закрытого ключа. Если асимметричные методы

используются в интересах служб обеспечения конфиденциальности, а ключ, используемый для зашифрования, был разактивирован или уничтожен, соответствующий парный ключ может оставаться в активном или постактивном состоянии для последующего более позднего расшифрования.

Более того, при использовании ключей для формирования ЭЦП открытая часть ключа будет оставаться в активном или постактивном состоянии, а при использовании ключей для зашифрования закрытая часть ключа будет оставаться в активном или постактивном состоянии.

Использование или прикладное применение ключа может определить услуги для этого ключа. Например, система может решить отказать в регистрации сеансового ключа, так как процедура регистрации могла продолжаться гораздо дольше, чем ЖЦ этого ключа. В противоположность этому обязательно следует зарегистрировать секретный ключ, когда симметричные методы используются при формировании ЭЦП.

9.2. Основные концепции обеспечения ключами

9.2.1. Службы (услуги по) обеспечения(ю) ключами

9.2.1.1. Общие положения

Обеспечение ключами представляет собой администрирование и предоставление (использование) услуг по формированию, регистрации, сертификации, снятию с регистрации, распределению, инсталляции, хранению, архивированию, аннулированию, извлечению и уничтожению ключевой информации.

Обеспечение ключами зависит от базовых служб формирования, регистрации, сертификации, распределения, инсталляции, хранения, архивирования, аннулирования, извлечения, снятия с регистрации и уничтожения. Эти службы могут быть частью системы обеспечения ключами или аналогичные услуги будут предоставляться другими провайдерами служб. В зависимости от типа услуги ее провайдер будет выполнять определенный минимальный набор требований по обеспечению безопасности (например защищенный информационный обмен), чтобы вызвать к

себе доверие у всех взаимодействующих сторон. Например, провайдер услуг может быть ДТС. На рис. 9.2 показано, что услуги по обеспечению ключами расположены на одном и том же уровне и могут использоваться различными группами пользователей и процессов. Последние могут воспользоваться различными средствами обеспечения ключами в рамках различных прикладных систем, причем в соответствии со своей спецификой. В табл. 9.1 перечислены службы обеспечения ключами.

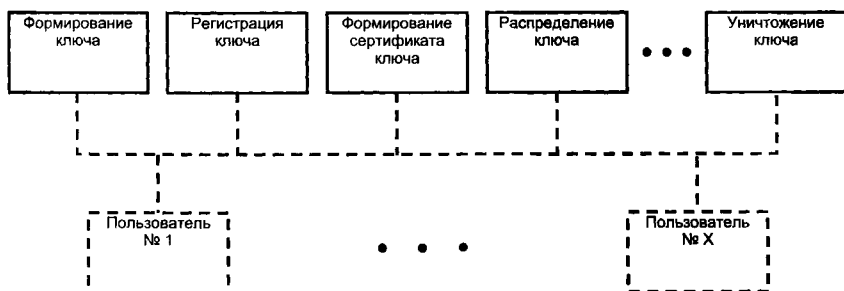


Рис. 9.2. Службы (услуги по) обеспечения(ю) ключами

Взаимосвязи между преобразованиями и услугами (службами) также представлены в табл. 9.1. Любой соответствующий криптографический способ (метод) будет использовать только подмножество услуг (служб), представленных в табл. 9.1.

Таблица 9.1

Службы (услуги по) обеспечения(ю) ключами

Преобразования	Услуги (службы)	Примечания
Формирование	Формирование ключа	Обязательная
	Извлечение ключа	Необязательная
	Регистрация ключа	Необязательная (здесь или при активировании)

Таблица 8.2 (продолжение)

Преобразования	Услуги (службы)	Примечания
	Формирование СЕРТ ключа	Необязательная
	Распределение ключа	Необязательная
	Хранение ключа	Необязательная
Активирование	Формирование СЕРТ ключа	Не бязательная
	Распределение ключа	Необязательная
	Извлечение ключа	Необязательная
	Инсталляция ключа	Обязательная
	Хранение ключа	Необязательная
	Регистрация ключа	Необязательная (здесь или при формировании)
Разактивирование	Хранение ключа	Необязательная
	Архивирование ключа	Необязательная (здесь или при уничтожении)
	Аннулирование ключа	Необязательная
Восстановление	Формирование СЕРТ ключа	Необязательная
	Распределение ключа	Необязательная
	Извлечение ключа	Необязательная
	Инсталляция ключа	Обязательная
	Хранение ключа	Необязательная

Преобразования	Услуги (службы)	Примечания
Уничтожение	Снятие с регистрации	Обязательная, если был зарегистрирован
	Уничтожение ключа	Обязательная
	Архивирование ключа	Необязательная (здесь или при реактивировании)

9.2.1.2. Формирование ключа

Эта служба (услуга) привлекается (предоставляется) при формировании ключей безопасным способом для соответствующего криптографического алгоритма. Это предполагает, что процедура формирования ключа не может подвергаться манипулированию и что ключи были сформированы непредсказуемым способом и соответствующим образом были распределены. Такое распределение определяется криптоалгоритмом, для которого оно будет использоваться, и необходимым уровнем криптографической защиты. Формирование некоторых ключей, например мастер-ключей, требует специализированной поддержки, так как знание этих ключей предполагает доступ ко всем связанным или извлекаемым ключам.

Процедура формирования ключей всегда основана на генераторах случайных чисел (ГСЧ). Очень важно, чтобы ГСЧ не генерировали случайные числа, которые являются предсказуемыми, а также, чтобы ГСЧ генерировали случайные числа, которые охватывали бы весь диапазон ключей алгоритма равномерным образом. Например, если ГСЧ формирует ключи для 128-битового симметричного криптоалгоритма, а вырабатывает эффективно только 32 бита (т. е. обеспечивая наилучшую энтропию) ключа из 128 бит, то такой процесс формирования ключей считается непригодным. Стандарт ISO/IEC 18031 вводит требования к ГСЧ.

9.2.1.3. Регистрация ключа

Служба регистрации ключей «привязывает» ключ к объекту. Эта процедура осуществляется Центром регистрации (ЦР) и, как правило, при использовании асимметричных криптографических методов. Когда объект желает зарегистрировать ключ, он должен обратиться к ЦР. Процедура регистрации ключа использует запрос на регистрацию и подтверждение такой регистрации.

ЦР ведет реестр ключей и необходимой информации, обеспечивая его безопасность.

Процедурами, осуществляемыми ЦР, являются регистрация и снятие с регистрации (учета).

9.2.1.4. Формирование СЕРТ ключа (сертификация ключа)

Служба формирования СЕРТ ключа гарантирует связь открытого ключа с субъектом, которая обеспечивается УЦ. Если УЦ получает запрос на сертификацию ключа, то он формирует СЕРТ ключа.

9.2.1.5. Распределение ключа

Процедура распределение ключа представляет собой совокупность субпроцедур по безопасному (защищенному) представлению авторизованным сторонам информационного обмена определенных данных, относящихся к обеспечению ключами. Далее в качестве отдельного случая процедуры распределения ключа рассматривается процедура трансляции ключа, при которой ключевая информация формируется между взаимодействующими сторонами информационного обмена с привлечением центра доставки ключей (ЦДК, Key Translation Centre).

9.2.1.6. Установка ключа

Услуга по установке ключа всегда предоставляется еще до начала использования ключа. Процедура установки ключа означает размещение и формирование ключа внутри средства обеспечения ключами, причем соответствующим способом, обе-

спечаивающим защиту ключа от его компрометации. В своем минимальном варианте функция (процедура) инсталляции ключа представляет собой пометку ключа как «используемого».

9.2.1.7. Хранение ключа

Служба хранения ключей обеспечивает защищенное хранение ключей, предназначенных для текущего или предстоящего использования, либо используемых в качестве резервных. В основном, это достигается за счет физически разделенного хранения ключей. Например, это гарантирует конфиденциальность и целостность ключевой информации или целостность открытых ключей. Хранение может осуществляться на всех стадиях (т.е. ожидание активного состояния, активное состояние и постактивное состояние) ЖЦ ключа. В зависимости от важности ключей они могут быть защищены следующими способами:

- физическая защита (например путем хранения ключей в устройстве, которое защищено от любого внешнего воздействия, или путем использования внешних средств, таких как карта памяти);
- зашифрование с помощью ключей, которые сами защищены физически;
- защищенный доступ к ключам с помощью пароля или PIN-кода.

Любая неудавшаяся попытка компрометации какой-либо ключевой информации должна быть обнаруживаема. Как правило, весьма затруднительно обнаружить неудавшуюся попытку компрометации ключа, если защита основывалась только на пароле/PIN-коде, хранящемся в программном обеспечении. В таком случае защищаемые ключи могут быть скопированы, а пароль/PIN-код могут быть взломаны автономно (off-line), что обнаружить практически невозможно. В таких случаях, в зависимости от прикладной системы, должны быть предложены другие процедурные средства обеспечения безопасности.

9.2.1.8. Извлечение ключа

Служба извлечения ключа формирует максимально возможное количество производных ключей, используя для этого оригинальный секретный ключ, который называется «начальный», или «генерирующий ключ» (derivation key), несекретные переменные данные и процедуру преобразования (которая также может быть пессекретной). В результате этой процедуры извлекается (формируется) производный ключ. Начальный ключ нуждается в специализированной защите. Процесс извлечения (формирования) должен быть необратимым и непредсказуемым с целью обеспечения гарантий того, что компрометация производного ключа не позволит вскрыть начальный ключ или любые другие производные ключи.

9.2.1.9. Архивирование ключа

Архивирование ключей представляет собой их предварительную обработку для их же последующего безопасного и длительного хранения по истечении срока их штатного использования. При архивировании ключей может привлекаться служба хранения ключей, исключая какую-либо иную реализационную процедуру, например автономное хранение. Заархивированные ключи могут быть востребованы и восстановлены через достаточно большой промежуток времени для доказательства или опровержения правомочности определенных исков, после того как штатное использование этих ключей было прекращено.

9.2.1.10. Аннулирование ключа

Когда компрометация ключа стала потенциально возможной или была установлена, служба аннулирования ключей гарантирует проведение безопасной процедуры деактивирования ключа. Эта услуга также востребована ключами, срок действия которых истек. Кроме того, аннулирование ключа может иметь место тогда, когда у владельца ключа произошли какие-либо изменения. После того как ключ был аннулирован, он должен использоваться только в процедурах расшифрования и проверки. Если ключ был аннулирован вследствие его компрометации, то с его помощью могут расшифровываться или проверяться толь-

ко те данные, которые были обработаны с помощью этого ключа до его компрометации.

ПРИМЕЧАНИЕ. Некоторые прикладные системы для обозначения этой службы используют термин «удаление ключа»¹.

9.2.1.11. Снятие ключа с регистрации

Услуга по снятию ключа с регистрации представляет собой проводимую ЦР ключа процедуру, которая заключается в удалении связи между ключом и объектом. Эта процедура является частью процедуры уничтожения ключа.

9.2.1.12. Уничтожение ключа

Услуга по уничтожению ключа представляет собой процедуру по безопасному уничтожению ключей, которые больше не нужны. Уничтожение ключа означает ликвидацию всех записей этого ключа, содержащихся в соответствующем информационном объекте, причем так, чтобы после уничтожения ключа не осталось никакой информации, с помощью которой было бы возможно восстановить уничтоженный ключ. Эта процедура включает уничтожение всех заархивированных копий ключа. Однако прежде чем заархивированные ключи будут уничтожены, необходимо провести проверку, которая гарантирует, что незаархивированные данные, защищенные с помощью этих ключей, в дальнейшем не понадобятся.

Некоторые ключи могут храниться во внешних устройствах или системах. Уничтожение таких ключей требует проведения дополнительных административных мероприятий.

9.2.2. Обеспечивающие службы (услуги)

9.2.2.1. Услуги по поддержке службы обеспечения ключами

Услуги по поддержке процедур обеспечения ключами могут привлекать и другие службы, которые связаны с обеспечением безопасности. К таким службам относятся:

¹ Delete-Key.

- *управление доступом.* Эта служба гарантирует, что ресурсы системы обеспечения ключами могут быть доступны только авторизованным объектам и могут использоваться только разрешенными способами;
- *аудит.* Эта служба обеспечивает слежение за действиями (процессами), связанными с обеспечением безопасности, которые происходят в системе обеспечения ключами. Данные для проведения аудита могут помочь в определении рисков безопасности и выявлении «брешей» в системе безопасности;
- *аутентификация.* Эта служба обеспечивает подтверждение подлинности объекта как авторизованного члена сетевого сегмента безопасности (ССБ);
- *криптографические службы.* Эти службы используются при предоставлении услуг по обеспечению ключами с целью обеспечения целостности, конфиденциальности, неотказуемости и проведения аутентификации;
- *служба времени.* Эта служба используется при формировании переменных временных параметров (ПВП), например допустимый срок действия.

9.2.2.2. Службы (услуги), ориентированные на пользователей

Существуют службы (услуги), которые необходимы для обеспечения требуемой функциональности, например службы регистрации пользователей. Такие службы рассматриваются ниже.

9.3. Концептуальные модели распределения ключей между двумя взаимодействующими сторонами

9.3.1. Общие положения

Распределение ключей между двумя взаимодействующими сторонами (объектами) может быть сложным. Оно зависит от природы каналов (линий) связи (виртуальных соединений),

надежности и степени доверия к устанавливаемым взаимосвязям и используемых криптографических методов. Взаимодействующие объекты могут устанавливать соединения непосредственно друг с другом или через посредников, могут входить в состав одних и тех же или разных ССБ и могут или не могут пользоваться услугами доверенных центров безопасности (ЦБ). Рассматриваемые далее концептуальные модели показывают, как эти различные ситуации влияют на распределение ключей и информации.

9.3.2. Распределение ключей между связанными объектами

Установленное между объектами соединение определяется физическим каналом (линией) связи между этими объектами, доверием к этим объектам и используемыми криптографическими методами.

Положим, что между объектами *A* и *B* установлено соединение, а сами объекты желают обмениваться информацией, используя для этого криптографические методы. Такое соединение представлено на рис. 9.3.

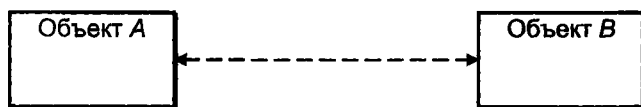


Рис. 9.3. Канал (линия) связи между взаимодействующими объектами

К случаям, в которых взаимодействующие объекты устанавливают прямое соединение, относятся согласование и подтверждение ключей, а также управление (контроль) ключами(ей).

9.3.3. Распределение ключей в рамках одного ССБ

Данная концептуальная модель основана на концепции ССБ с ЦБ, представленной в главе 2.

Такой ЦБ может предоставлять услуги по обеспечению ключами, например доставка ключей. Когда взаимодействующие стороны используют асимметричный метод для безопасного обмена данными, то можно выделить следующие случаи:

- *при обеспечении целостности данных или аутентификации источника данных* получатель требует СЕРТ соответствующего открытого ключа отправителя;
- *при обеспечении конфиденциальности* отправитель требует от получателя действующего СЕРТ открытого ключа;
- *при аутентификации, обеспечении конфиденциальности и целостности* каждая сторона информационного обмена требует от другой стороны СЕРТ открытого ключа. Это позволяет обеспечить обоюдную неотказуемость. Каждой стороне может понадобиться взаимодействие со своим УЦ с целью получения соответствующего СЕРТ открытого ключа. Если же взаимодействующие стороны доверяют друг другу и могут провести обоюдную аутентификацию своих СЕРТ открытых ключей, то обращение к УЦ не требуется.

Существуют криптографические прикладные системы, в которых ЦБ не привлекается. В такой ситуации взаимодействующие стороны вместо использования своих СЕРТ открытых ключей могут осуществить только защищенный обмен некоторой открытой информацией.

Если между такими партнерами используется симметричная криптография, то формирование ключей может быть инициировано одним из следующих способов:

- а) одна сторона формирует ключ и передает его в ЦДК;
- б) одна сторона запрашивает Центр распределения ключей (ЦРК, Key Distribution Centre) с целью формирования ключа для последующего распределения последнего.

Если формирование ключа осуществляется одной из взаимодействующих сторон, то безопасное распределение ключа может контролироваться ЦДК (рис. 9.4). Номера, указанные на этом

рисунке, обозначают итерации процедуры обмена. ЦДК получает зашифрованный ключ от стороны *A* (1), расшифровывает его и опять зашифровывает его с помощью ключа, который известен этому ЦДК и стороне *B*. После этого он может:

- либо доставить зашифрованный ключ непосредственно стороне *B* (2);
- либо передать обратно зашифрованный ключ стороне *A* (3), которая доставит его непосредственно стороне *B* (4).

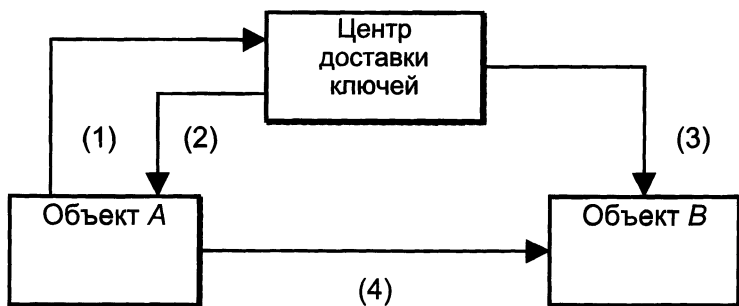


Рис. 9.4. Центр доставки ключей

Если формирование ключа осуществляется ДТС, то существуют две процедуры последовательного распределения ключа взаимодействующим сторонам. Эти процедуры отображены на рис. 9.5 (концептуальная модель ЦРК) и рис. 9.6 (распределение ключа путем его доставки от стороны *A* стороне *B*).

На рис. 9.5 показан случай, когда ЦРК способен организовать защищенные (безопасные) соединения с обеими взаимодействующими сторонами. В этом случае, как только будет сформирован ключ по запросу одной из сторон, ЦРК несет ответственность за безопасное распределение ключа обоим взаимодействующим сторонам. Запрос на предоставление ключа обозначен (1), а процедура распределения ключа взаимодействующим сторонам — (2*a*) и (2*b*).

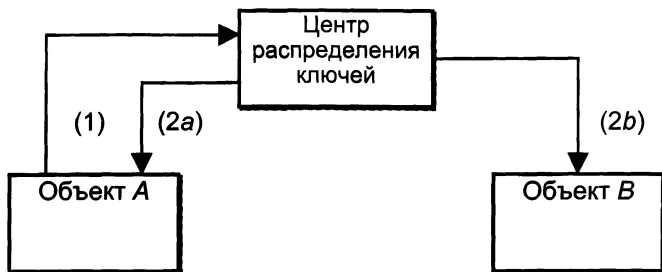


Рис. 9.5. Концептуальная модель ЦРК

Если распределение секретного ключа между сторонами *A* и *B* запрашивает только сторона *A*, то ЦРК может действовать двумя различными способами. Если он способен установить защищенное соединение с обеими сторонами информационного обмена, то он может предоставить секретный ключ каждой из них, как это описано выше. Если ЦРК может установить связь только с одной стороной *A*, то ответственность за предоставление ключа стороне *B* несет сторона *A*. На рис. 9.6 показан этот вариант распределения ключа. Запрос к ЦРК на распределения ключа обозначен (1), а доставка ключа стороне *A* — (2). Передача этого ключа от *A* к *B* обозначена (3).

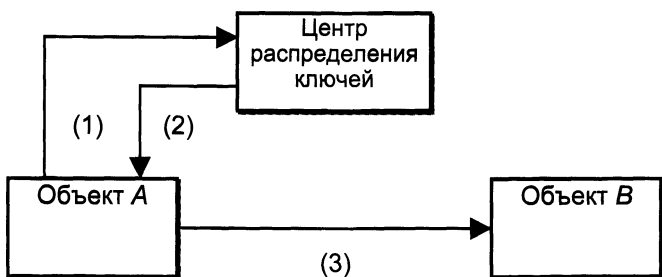


Рис. 9.6. Распределение ключа путем его доставки от стороны *A* стороне *B*

9.3.4. Распределение ключей между двумя ССБ

В следующей модели рассматриваются два взаимодействующих объекта *A* и *B*, принадлежащие двум разным ССБ, которые совместно используют, по крайней мере, один криптографический метод (т.е. симметричный или асимметричный). Каждый ССБ имеет свой собственный ЦБ: одному доверяет *A*, а другому доверяет *B*. Если *A* и *B* доверяют друг другу или каждый доверяет ЦБ другого ССБ, то ключи могут быть распределены способами, рассмотренными в § 9.3.2 и § 9.3.3.

При установлении ключа между *A* и *B* можно рассмотреть два случая:

- получение СЕРТ открытого ключа *B* (если пригоден);
- формирование общего секретного ключа между *A* и *B*.

С точки зрения обеспечения ключами между этими объектами могут возникать различные взаимосвязи. Такие взаимосвязи являются отражением природы (сущности) доверия между взаимодействующими сторонами.

Если в период информационного обмена взаимодействующие стороны используют асимметричные методы, то каждой стороне необходим доступ к СЕРТ другой стороны (рис. 9.7). Если УЦ объекта *A* выдал последнему СЕРТ (2) в соответствие с его запросом (1), то данный СЕРТ указывается в Службе единого каталога (Каталог), либо самим объектом *A* (3), либо его УЦ (3'). База данных Каталога (БДК) может быть открытой, и если это так, то *B* может получить СЕРТ объекта *A* непосредственно из сегмента БДК этого объекта (7). Если УЦ объектов *A* и *B* имеют соглашение по перекрестной рассылке (8), то *B* может найти СЕРТ объекта *A* в своем собственном сегменте БДК (10). В противном случае *A* направит свой собственный СЕРТ объекту *B* в рамках информационного взаимодействия или в период процедуры формирования ключа, определяемой соответствующим протоколом (11).

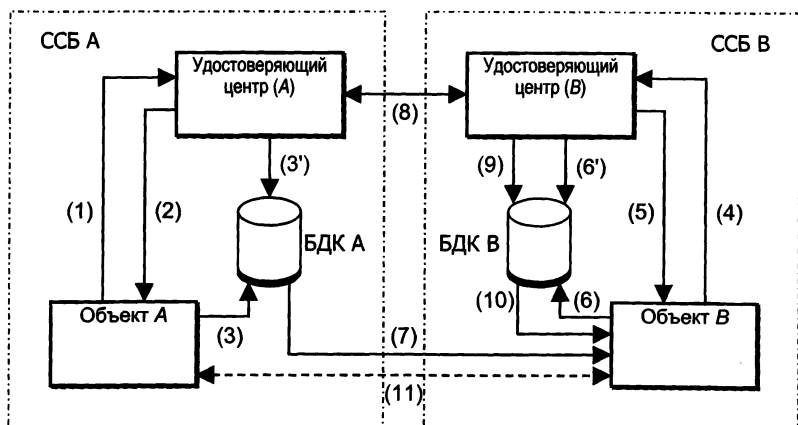


Рис. 9.7. Распределение ключей между двумя ССБ с использованием асимметричных методов

Если взаимодействующие стороны используют симметричный метод (рис. 9.8), то кроме этого каждая сторона должна взаимодействовать в защищенном режиме со своим соответствующим ЦБ (1) с целью получения секретного ключа, который позволит им установить соединение. ЦБ «договариваются» об общем секретном ключе (2), который будет использоваться сторонами. Один из ЦБ распределяет секретный ключ обеим сторонам, используя для этого другой ЦБ в качестве ЦРК. Последний может осуществить доставку ключа (2 и 3).

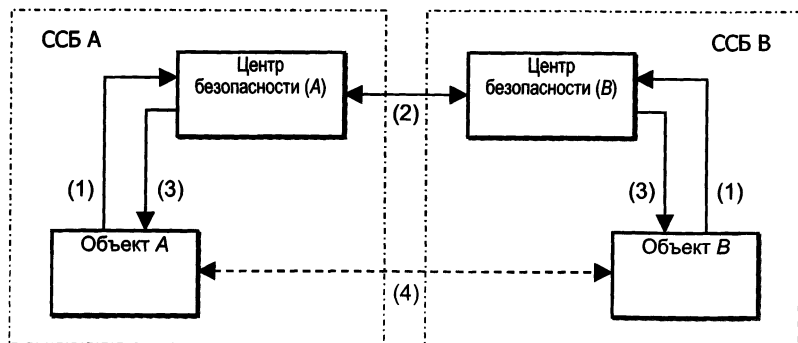


Рис. 9.8. Распределение ключей между двумя ССБ с использованием симметричных методов

Когда только один объект *A* запрашивает секретный ключ для связи с *B*, тогда ЦБ может использовать один из следующих способов. Если ЦБ может установить соединение с двумя объектами, он может распределить секретный ключ обоим, как это было показано ранее. Если ЦБ может установить соединение только с одним объектом, то объект, получивший ключ, отвечает за доставку ключа другому объекту.

Иногда ЦБ объектов *A* и *B* не имеют обоюдных доверенных отношений или прямых соединений. В таких случаях они обращаются в ЦБ *X* (рис. 9.9), которому они оба доверяют (2а и 2b). ЦБ *X* может сформировать ключ и передать его ЦБ объектов *A* и *B* (3а и 3b). В противном случае, ЦБ *X* может ретранслировать полученный от ЦБ *A* секретный ключ или СЕРТ открытого ключа (2а) в ЦБ *B* (3b). Кроме этого, ЦБ должны ретранслировать полученный ключ своим соответствующим объектам (4а и 4b), которые затем могут обмениваться информацией безопасным способом (5). Последнее может понадобиться для поиска последующих ЦБ до тех пор, пока не будет сформирована структура (цепочка) доверия.

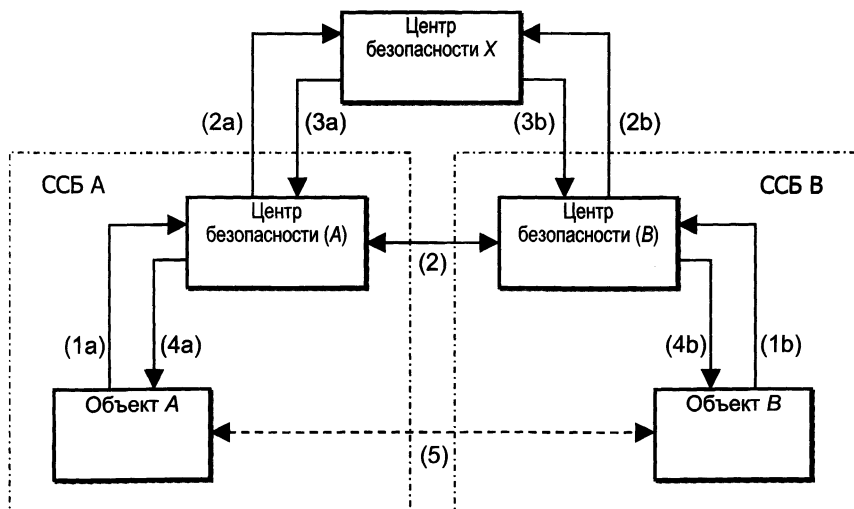


Рис. 9.9. Цепочка (структура) доверия между ЦБ

9.4. Провайдеры специализированных услуг

Некоторые из услуг (служб), которые востребованы системой обеспечения ключами, могут предоставляться внешними провайдерами. К этим услугам (службам) относятся услуги, предоставляемые:

- УЦ (центр (пункт) регистрации ключей или центр сертификации ключей);
- ЦРК;
- ЦДК.

9.5. Угрозы системе обеспечения ключами

Система обеспечения ключами уязвима к различным угрозам, среди которых:

- 1) *вскрытие ключевой информации.* Ключевая информация либо содержалась в открытом тексте, не была защищена и таким образом могла быть доступной, либо была зашифрована и могла быть дешифрована;
- 2) *модификация ключевой информации.* Изменение ключевой информации таким образом, что она становится функционально не пригодной по своему назначению;
- 3) *несанкционированное (неавторизованное) удаление ключевой информации.* Удаление ключа или данных, связанных с ключом;
- 4) *неполное уничтожение ключевой информации.* Это может привести к компрометации действующих или перспективных ключей;
- 5) *несанкционированное (неавторизованное) аннулирование.* Прямое или опосредованное изъятие действующего ключа или ключевой информации;
- 6) *«маскарад».* Выдача себя за авторизованного пользователя или объект;
- 7) *задержка при реализации функций по обеспечению ключами.* Это может привести к сбоям при формировании, распределении, аннулировании или регистрации ключа,

задержке необходимого обновления данных в ключевом репозитории, нештатной ситуации при определении уровней авторизации пользователей и др. Угроза задержки может быть следствием реализации вышеперечисленных угроз или физического сбоя в работе оборудования, затрагивающего обеспечение ключами;

8) *неправильное применение (злоупотребление) ключей(ами).*

К этому классу угроз относятся:

- использование ключа нецелевым образом, например использование ключа, предназначенного для зашифрования другого ключа, для зашифрования данных;
- использование средства обеспечения ключами нецелевым образом, например неавторизованное зашифрование или расшифрование данных;
- использование просроченного ключа;
- чрезмерное использование ключа;
- предоставление ключей неавторизованному получателю.

9.6. Информационные объекты в службе обеспечения ключами

Информационный объект (ИО) СЛКЛ содержит ключ или ключи, а также другую (необязательную) информацию, которая контролирует как могут быть использованы ключи. Управляющая информация может, скорее всего в явном виде, использоваться на основе соглашений, которые предназначены для контроля использования ИО СЛКЛ. Например, использование одного ключа из пары асимметричных ключей контролируется на основе согласованного использования другого ключа пары, т.е. первый — для зашифрования, а другой — для расшифрования.

Управляющая информация контролирует следующее:

- тип объекта, который может быть защищен с помощью ключа (например данные или ИО СЛКЛ);

- разрешенные процедуры (например зашифрование и расшифрование);
- авторизованный пользователь;
- возможная область применения ключа;
- другие аспекты в соответствии с определенным методом управления или конкретной прикладной системой, которые используют ИО СЛКЛ.

В целях оптимизации ИО СЛКЛ может частично или полностью генерироваться в рамках процедуры формирования ключа.

Частным примером ИО СЛКЛ является СЕРТ ключа. Последний содержит, по крайней мере, следующую, подписанную УЦ, информацию:

- открытую ключевую информацию;
- параметр подлинности пользователя, который может использовать соответствующий ИО СЛКЛ;
- процедуры, которые могут осуществляться с помощью соответствующего ИО СЛКЛ;
- срок (период) действия;
- параметр подлинности УЦ.

9.7. Классы прикладных криптографических систем

9.7.1. Единая классификация криптографических систем

Единая классификация криптографических систем определяется двумя основными криптографическими методами, т.е. симметричным и асимметричным. Так как система обеспечения ключами должна обслуживать оба метода, необходим еще один подход. В дальнейшем криптографические системы классифицируются в соответствии с той функциональностью, которую обеспечивает метод.

В целом криптосистема предлагает два различных типа криптографических услуг: услуги аутентификации и по обеспе-

чению целостности и услуги по обеспечения конфиденциальности. СЛКН используются для криптографической защиты информации (т.е. они обеспечивают конфиденциальность данных). СЛАУ и СЛЦЛ в первую очередь используются для аутентификации объекта/субъекта, аутентификации источника данных, обеспечения целостности данных и неотказуемости. На рис. 9.10 представлены типы криптосистем и соответствующие им процедуры.

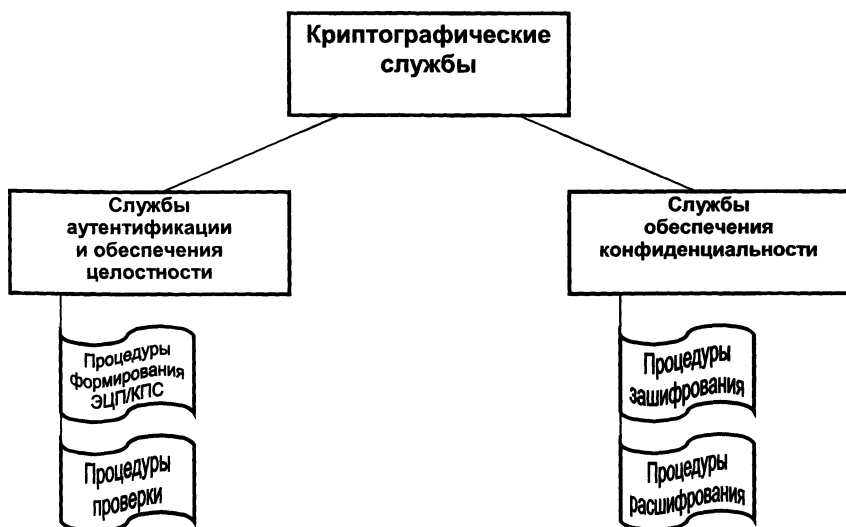


Рис. 9.10. Криптографические службы (услуги) и реализуемые ими способы (процедуры)

9.7.2. СЛАУ и СЛЦЛ и ключи

Службы аутентификации и СЛЦЛ предоставляют услуги по аутентификации взаимодействующих сторон (аутентификация объекта/субъекта), аутентификации отправителя данных (аутентификация источника данных), обеспечению неотказуемости и целостности данных. Эти службы используют следующие способы:

- *КПС элемента данных (seal a data unit)*. Этот способ формирует криптографическую проверочную сумму совокупности данных с целью обеспечения их целостности, например формирование аутентификационного кода сообщения на основе симметричного алгоритма (ISO/IEC 9797);
- *ЭЦП элемента данных (sign a data unit)*. Этот способ формирует ЭЦП с целью аутентификации источника данных, обеспечения целостности данных и/или неотказуемости;
- *проверка элемента данных, защищенного с помощью КПС (verify a sealed data unit)*. Этот способ осуществляет формирование КПС элемента данных и сравнивает ее значение со значением представленной КПС (доказательство целостности данных);
- *проверка элемента данных, защищенного с помощью ЭЦП (verify a signed data unit)*. Этот способ осуществляет проверку ЭЦП с целью определения, была ли она сформирована заявленным источником и/или с целью доказательства целостности данных.

При запросе услуг по аутентификации и обеспечению целостности процедуры формирования ЭЦП и КПС используют информацию, которая является либо закрытой (т.е. уникальной и конфиденциальной) для отправителя, либо секретной и известной только отправителю и получателю. Кроме этого, процедура проверки использует либо процедуры и информацию, открытые для доступа, но из которых невозможно сделать вывод о закрытой информации отправителя, либо ключ, находящийся в совместном использовании отправителем и получателем. Важнейшей характеристикой процедуры формирования ЭЦП является то, что ЭЦП может быть сформирована только с использованием закрытой информации отправителя, т.е. его *закрытого ключа (private key)*. Соответственно, если ЭЦП проверяется с использованием *открытого ключа (public key)* отправителя, то она может быть впоследствии подтверждена ДТС (например центром нотаризации, notarisisation authority), которая, являясь

единственно возможным обладателем закрытой информации, могла сформировать ЭЦП.

СЛАУ и СЛЦЛ используют два из трех типов ключей, а именно:

- *ключ для формирования КПС.* Секретный ключ, используемый совместно взаимодействующими сторонами;
- *ключ для формирования ЭЦП.* Уникальный закрытый ключ, который однозначно связан с отправителем;
- *ключ для проверки.* Это либо открытый ключ, либо секретный ключ.

При реализации симметричных криптографических методов службы аутентификации и СЛЦЛ используют ключ для формирования КПС и ключ для проверки, которые представляют собой один и тот же секретный ключ. При реализации асимметричных криптографических методов СЛАУ и СЛЦЛ используют ключ для формирования ЭЦП и ключ для проверки, которые представляют собой пару ключей, состоящую из открытого и закрытого ключей.

9.7.3. СЛКН и ключи

СЛКН в первую очередь обеспечивают конфиденциальность информации. Они могут использовать два основных способа:

- *зашифрование.* Этот способ формирует зашифрованный текст из представленных данных;
- *расшифрование.* Этот способ формирует открытый текст из соответствующего зашифрованного текста.

СЛКН могут характеризоваться используемым криптографическим методом, т.е. симметричным или асимметричным. Если используются симметричные методы, то процедуры зашифрования и расшифрования осуществляются с помощью одного и того же ключа (совместно используемого секретного ключа). Если используются асимметричные методы, то проце-

дуры зашифрования и расшифрования осуществляются с помощью двух различных, но взаимосвязанных ключей, т.е. открытого ключа и закрытого ключа.

9.7.4. Совмещенные службы

Некоторые схемы шифрования могут также обеспечивать конфиденциальность, целостность данных и/или аутентификацию источника. Соответственно, аутентифицированные схемы шифрования (см. ISO/IEC 19772 и ISO/IEC 18033–4), использующие симметричные криптографические методы, обеспечивают конфиденциальность, целостность данных и аутентификацию источника. Схемы совместного формирования ЭЦП и шифрования (см. ISO/IEC 29150), использующие асимметричные криптографические методы, обеспечивают конфиденциальность, целостность данных и аутентификацию источника. Кроме того, в зависимости от используемого метода могут быть реализованы дополнительные функции обеспечения безопасности, например аутентификация и обеспечение неотказуемости.

9.8. Обеспечение жизненного цикла СЕРТ|ОК

9.8.1. Общие положения

Если прикладными системами используются УЦ (Certification Authority), то они должны следовать рассматриваемым далее рекомендациям, которые касаются выполнения обязательных требований и процедур при обеспечении жизненного цикла СЕРТ|ОК.

9.8.2. Удостоверяющий центр

9.8.2.1. Ответственность УЦ

УЦ является надежным (доверенным) по отношению к своим пользователям. Такое доверие основано на использовании

соответствующих криптографических способов и оборудования, а также на профессионализме персонала УЦ и реальном управлении со стороны менеджмента УЦ. Это доверие должно подтверждаться независимыми аудиторскими проверками (внутренними, внешними или обеими), результаты которых должны быть доступны пользователям УЦ.

УЦ несет ответственность за:

- a) идентификацию объектов/субъектов, информация о которых представлена для получения СЕРТ|ОК;
- b) обеспечение безопасности процедуры сертификации и закрытого ключа, используемого для подписи информации об открытом ключе;
- c) формирование определяемых системой данных, которые будут включены в информацию об открытом ключе, например серийный номер СЕРТ|ОК, идентификация УЦ и др.;
- d) назначение и проверку периодов действия, например СЕРТ|ОК;
- e) оповещение владельца СЕРТ|ОК, указанного в данных об открытом ключе, о выпуске его СЕРТ|ОК;
- f) предоставление гарантий того, что двум различным объектам/субъектам не может быть присвоен один и тот же параметр подлинности, и таким образом каждый из них может быть однозначно аутентифицирован;
- g) обслуживание и выпуск списков аннулированных СЕРТ|ОК;
- h) регистрацию всех итераций, осуществляемых в процедуре формирования СЕРТ|ОК.

Один УЦ может сертифицировать информацию об открытом ключе другого УЦ с целью предоставления СЕРТ|ОК. Следовательно, процедура аутентификации может использовать последовательность (цепочку) СЕРТ|ОК. Первый СЕРТ|ОК в этой цепочке должен быть получен и аутентифицирован с помощью других средств, отличных от СЕРТ|ОК.

9.8.2.2. Пара асимметричных ключей УЦ

УЦ должен иметь доступ к средству обеспечения безопасности (СРБ), которое способно сформировать пару асимметричных ключей для использования этим УЦ. Процедура формирования должна гарантировать непредсказуемость ключевой информации. Ни один нарушитель не должен извлечь какой-либо пользы от знания процедуры формирования.

Закрытый ключ УЦ используется для подписи информации об открытом ключе объекта/субъекта. Так как обладание таким ключом могло бы позволить нарушителю разыграть «маскарад» под маской УЦ и сформировать фальшивые СЕРТ|ОК, закрытый ключ должен иметь высокий уровень защиты. Таким образом, закрытый ключ УЦ должен быть хорошо защищен, когда он используется внутри средства обеспечения ключами. Ключ должен иметь максимальную защиту, если он используется за пределами средства обеспечения ключами.

Целостность проверочного открытого ключа УЦ является обязательным условием безопасности системы сертификации открытых ключей. Если открытый ключ УЦ не указан в СЕРТ|ОК, то должны быть предприняты дополнительные меры предосторожности, которые гарантировали бы аутентифицированное (надежное) распределение этого ключа. На стороне пользователя также должны быть соблюдены необходимые условия, которые гарантировали бы подлинность хранящейся копии открытого ключа УЦ.

Проверочный открытый ключ УЦ используется для подтверждения подлинности СЕРТ|ОК других пользователей. Перед тем, как использовать открытый ключ УЦ, пользователь должен удостовериться, что на текущий момент проверочный ключ является действительным.

9.8.3. Процедура сертификации

9.8.3.1. Модель сертификации открытого ключа

Базовая модель. На рис. 9.11. представлена базовая модель, которая распределяет основные функции между логическими объектами:

- *УЦ (certification authority)*. Несет ответственность за сертификацию информации об открытом ключе пользователя;
- *Центр эксплуатации и сопровождения службы Единого каталога (ЦКТ, Directory maintenance authority)*. Несет ответственность за изготовление СЕРТ|ОК, доступных в интерактивном режиме (on-line) и готовых к использованию их владельцами (пользователями);
- *генератор ключей (key generator)*. Несет ответственность за формирование пары асимметричных ключей;
- *Центр регистрации (ЦРГ, registration authority)*. Несет ответственность за предоставление в УЦ достоверных параметров подлинности пользователей;
- *пользователь (объект А)*. Связи между логическими объектами модели и соответствующие требования к безопасности этих связей будут рассмотрены ниже более детально. Логические объекты могут быть совмещенными. Например, объект А и генератор ключей могут рассматриваться как один объект, если пользователь формирует пару асимметричных ключей самостоятельно, или УЦ и генератор ключей также могут рассматриваться как один объект, если УЦ формирует пары ключей от имени пользователей.

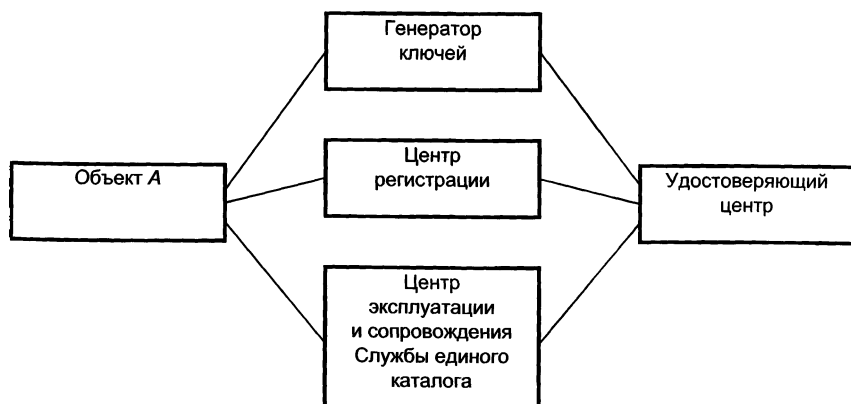


Рис. 9.11. Базовая модель сертификации открытого ключа

Следует обратить внимание на то, чтобы СЕРТ|ОК, изготовленный совмещенным УЦ и ЦРГ был бы точно таким же, как если бы он был изготовлен УЦ или ЦРГ, которые разделены и функционируют самостоятельно.

Связи в процедуре сертификации. Рассмотрим связи между логическими объектами базовой модели и соответствующие требования к безопасности этих связей. Не все из рассматриваемых ниже связей будут устанавливаться в реальных ИТС. Например, задачи, решаемые ЦРГ, УЦ и генератором ключей, могут быть объединены. В базовой модели возможны следующие связи:

- *объект $A \Leftrightarrow$ генератор ключей.* Объект A запрашивает генератор ключей о формировании пары асимметричных ключей. Генератор ключей является надежным с точки зрения формирования пар асимметричных ключей хорошего качества. Генератор ключей формирует пару ключей (S_A, V_A) , такую что S_A является ключом подписи, а V_A — проверочный ключ, который доставляется генератором ключей объекту A . Такая доставка должна быть аутентифицирована, а также обеспечена ее конфиденциальность. Генератор ключей и объект A должны быть абсолютно уверены в том, что никакая третья сторона не сможет модифицировать пару асимметричных ключей и прочесть содержание ключей в течение их доставки;
- *объект $A \Leftrightarrow$ ЦРГ.* Объект A запрашивает регистрацию у ЦРГ. Объект A должен предоставить ЦРГ свою информацию о параметре подлинности. ЦРГ проверяет достоверность информации объекта A и, возможно, добавляет к ней некоторую системную информацию. После этого итоговая информация доставляется в УЦ безопасным способом;
- *объект $A \Leftrightarrow$ УЦ.* Объект A запрашивает УЦ на предмет сертификации своей информации об открытом ключе (или часть из нее), включая свой открытый ключ и свое уникальное имя. Доставка информации об открытом ключе в УЦ должна быть организована таким образом, чтобы гарантировать подлинность и целостность этой

информации. УЦ проверяет подлинность информации об открытом ключе объекта A , при необходимости добавляет к ней некоторую системную информацию, а затем подписывает полностью сформированную информацию об открытом ключе объекта A с целью формирования СЕРТ|ОК объекта A . После этого СЕРТ|ОК может быть передан обратно объекту A .

После получения СЕРТ|ОК объект A проверяет его корректность, используя для этого открытый ключ проверки V_{CA} УЦ. Этот ключ должен быть доступен объекту A надежным и достоверным способом с использованием процедуры аутентификации. С этой точки зрения открытый ключ объекта A может распространяться в качестве СЕРТ|ОК и использоваться любым иным объектом, имеющим доступ к открытому ключу проверки УЦ.

Тем не менее если УЦ запросит генератор ключей сформировать пару асимметричных ключей от имени объекта A , то пара ключей для объекта A должна быть доставлена от генератора ключей объекту A . Процедуры такой доставки должны удовлетворять требованиям обеспечения конфиденциальности, целостности и подлинности. Кроме того, УЦ является доверенным объектом с точки зрения обеспечения конфиденциальности, целостности и подлинности для всех пар асимметричных ключей в течение их обработки и хранения.

И в заключение УЦ должен доставлять открытый ключ объекта A последнему, обеспечивая при этом абсолютную гарантию того, что никакая третья сторона не сможет ни модифицировать, ни прочитать содержание передаваемой информации;

- *объект $A \Leftrightarrow ЦКТ$.* Объект A передает свой СЕРТ|ОК в ЦКТ и регистрирует его в службе Единого каталога. Для регистрации СЕРТ|ОК в службе Единого каталога необходимы процедуры аутентификации объекта и УД. Между объектом A и ЦКТ должно быть заключено соглашение о том, кто авторизован (уполномочен) для сопро-

вождения записи об объекте в каталоге (в БДК). Существуют два варианта обслуживания записей в БДК: либо служба Единого каталога обслуживает все записи в БДК, либо каждый объект X отвечает за свою собственную запись БДК и обслуживает ее;

- $ЦРГ \Leftrightarrow УЦ$. ЦРГ запрашивает УЦ с целью сертификации информации об открытом ключе объекта A . Доставка информации об открытом ключе объекта A из ЦРГ в УЦ должна быть организована достоверным (надежным) способом с использованием процедуры аутентификации. УЦ проверяет подлинность информации об открытом ключе объекта A , при необходимости добавляет к ней некоторую системную информацию, а затем подписывает полностью сформированную информацию об открытом ключе объекта A с целью формирования СЕРТ|ОК объекта A . УЦ извещает ЦРГ о сертификации;
- $УЦ \Leftrightarrow \text{генератор ключей}$. УЦ запрашивает генератор ключей с целью формирования пары асимметричных ключей от имени объекта A . Генератор ключей является надежным с точки зрения формирования пар асимметричных ключей хорошего качества. Генератор ключей формирует пару ключей и доставляет ее назад в УЦ. Такая доставка должна отвечать требованиям по аутентификации и обеспечению конфиденциальности. Генератор ключей и УЦ должны быть абсолютно уверены в том, что никакая третья сторона не сможет модифицировать пару асимметричных ключей и прочитать содержание ключей в течение их доставки. УЦ является доверенным объектом с точки зрения обеспечения конфиденциальности и подлинности для всех пар асимметричных ключей в течение их обработки и хранения;
- $УЦ \Leftrightarrow ЦКТ$. УЦ доставляет сформированные СЕРТ|ОК в ЦКТ и регистрирует их в службе Единого каталога. Для регистрации СЕРТ|ОК в службе Единого каталога необходимы процедуры аутентификации объекта и УД.

9.8.3.2. Процедура регистрации

Требования к регистрации. Процедура регистрации ключа объекта включает направление запроса на получение СЕРТ|ОК объектом и подтверждение подлинности этого СЕРТ|ОК со стороны ЦРГ или УЦ. Далее рассматриваются требования, применяемые к подаче запроса на получение СЕРТ|ОК объектом. Запрос на получение СЕРТ|ОК может включать, а может и не включать значение открытого ключа.

Подача запроса на получение СЕРТ|ОК пользователем. Прикладные системы с низким уровнем рисков, которые принимают запросы на получение СЕРТ|ОК, должны основываться на идентификации пользователей, использующих СЕРТ|ОК. Запросы на получение СЕРТ|ОК не должны быть персонализированными, но, исходя из реальной практики ведения бизнеса, должны иметь идентификаторы пользователей.

Прикладные системы с высоким уровнем рисков, которые принимают запросы на получение СЕРТ|ОК, должны основываться на внешних персональных признаках пользователя (или его авторизованного представителя), запрашивающего СЕРТ|ОК, и на использовании приемлемых коммерческих стандартов по идентификации пользователя (и если необходимо, представителя пользователя). В этом случае может понадобиться проверка подлинности со стороны ДТС.

Подача запроса на получение СЕРТ|ОК легальным объектом. Прием запроса на получение СЕРТ|ОК должен осуществляться путем персонального вручения информации с запросом на получение СЕРТ|ОК, по крайней мере, одним из представителей объекта, а также основываться:

- a) на ЭЦП и КПС (если используется) на фирменных бланках авторизованной заявки на СЕРТ|ОК;
- b) использовании приемлемой коммерческой практики по идентификации ЭЦП или КПС (если используется) объекта;
- c) использовании приемлемой коммерческой практики по идентификации представителей, которые доставляют информацию о запросе сертификата.

9.8.3.3. Взаимосвязи между легальными объектами

К легальным объектам предъявляется требование по установлению договорных взаимосвязей с другими легальными объектами. Такие связи могут быть согласованы двумя различными способами:

- а) сотрудники компании имеют персональные пары асимметричных ключей.* Легальный объект действует как УЦ для сотрудников своей компании. Все процедуры информационного обмена санкционируются их участниками, использующими свои открытые ключи, сертифицированные УЦ компании. Получатели данных удостоверяются в том, что их источник сертифицирован компанией, у которой ключ, в свою очередь, сертифицирован некоторым более высоким в иерархии УЦ;
- б) сотрудники компании не имеют персональных пар асимметричных ключей.* Только легальный объект имеет одну или несколько пар асимметричных ключей. Получатели данных удостоверяются в том, что процедуры информационного обмена, в результате которых были приняты эти данные, подтверждены открытым ключом компании. Получателям данных нет необходимости описывать самих себя в соответствии с установленными привилегиями и политиками компании, которая является источником полученных ими данных.

9.8.3.4. Формирование СЕРТ|ОК

Перед началом использования пары асимметричных ключей должна быть проведена процедура формирования СЕРТ|ОК. Процедура включает следующие обязательные итерации:

- а) проверка информации об открытом ключе на наличие ошибок;*
- б) получение информации об открытом ключе;*
- с) подготовка и добавление данных, необходимых для формирования СЕРТ|ОК. Кроме того, УЦ может дополни-*

тельно сформировать пару(ы) асимметричных ключей объекта(ов);

- d)* вычисление ЭЦП СЕРТ|ОК. При этом может использоваться хэш-функция;
- e)* проверка регистрационной записи. Все действия УЦ при формировании СЕРТ|ОК должны быть зарегистрированы.

Для прикладных систем с высоким уровнем рисков может понадобиться несколько ЭЦП:

- 1) одного УЦ на одном СЕРТ|ОК. При этом все ЭЦП будут сформированы с помощью различных закрытых ключей, что обеспечивает их независимость с точки зрения криптографических свойств;
- 2) разных УЦ на информации об открытом ключе.

9.8.3.4. Обновление/время жизни СЕРТ|ОК

СЕРТ|ОК обладает временем жизни, которое определяется периодом действия, указанным в самом СЕРТ|ОК, или, в противном случае, определяется УЦ (системой обслуживания СЕРТ|ОК).

9.8.4. Распределение и использование СЕРТ|ОК

9.8.4.1. Распределение и хранение СЕРТ|ОК

После того как был сформирован СЕРТ|ОК, не нужно принимать какие-либо меры по обеспечению гарантий его конфиденциальности или целостности. СЕРТ|ОК могут храниться в открытой БДК с целью обеспечения упрощенного доступа пользователей к ним.

9.8.4.2. Проверка СЕРТ|ОК

Для подтверждения подлинности СЕРТ|ОК проверяющая сторона *B* должна, по крайней мере, проверить ЭЦП УЦ на СЕРТ|ОК. Если СЕРТ|ОК был выпущен в юридически обоснованный период действия, то сторона *B* должна убедиться в том,

что в текущее время СЕРТ|ОК стороны А является законным. Кроме того, для подтверждения подлинности СЕРТ|ОК проверяющая сторона должна обладать действительной копией открытого ключа проверки, принадлежащего УЦ.

9.8.5. Маршруты сертификации

Не всем УЦ следует знать или сертифицировать друг друга, нет необходимости в строгой иерархии УЦ. Если бы УЦ сертифицировали друг друга («кросс-сертификация»), это позволило бы динамичное использование и обмен СЕРТ|ОК. Такая кросс-сертификация могла быть проведена с использованием наивысших уровней гарантированности и с соблюдением всех мер предосторожности. После того как появится сеть с кросс-сертифицированными СЕРТ|ОК, можно сформировать маршруты проверки подлинности СЕРТ|ОК. Пользователю остается только доверять проверочному ключу одного из УЦ. Затем такое доверие распространяется по всему маршруту сертификации до открытого ключа партнера, выданного ему известным УЦ.

9.8.6. Аннулирование сертификатов

9.8.6.1. Требования к аннулированию

СЕРТ могут аннулировать (отзывать) еще до истечения срока их действия, установленного УЦ. Это может быть вызвано несколькими причинами, а именно:

- a) компрометация закрытого ключа объекта;*
- b) запрос со стороны объекта на аннулирование;*
- c) изменение принадлежности объекта;*
- d) завершение деятельности объекта;*
- e) ложная идентификация объекта;*
- f) компрометация закрытого ключа УЦ;*
- g) завершение деятельности УЦ.*

В целях обеспечения безопасности и аутентификации аннулирования должны использоваться специализированные процедуры и средства высокоскоростной связи. Таким образом, исходя из указанных причин, потребуется аннулирование:

- либо одного или нескольких СЕРТ|ОК одного или нескольких объектов;
- либо совокупности СЕРТ|ОК, выпущенных УЦ и подписанных им с помощью одной пары асимметричных ключей, которая используется этим УЦ для подписи информации об открытых ключах;
- либо всех СЕРТ|ОК, выданных УЦ, невзирая на функцию, для реализации которой предназначена пара асимметричных ключей.

Последние два требования определяют средства удаления СЕРТ|ОК, когда имели место компрометация или подозрение на компрометацию закрытого ключа УЦ или когда была изменена пара асимметричных ключей, используемая для подписи СЕРТ|ОК. Если СЕРТ|ОК были просрочены или аннулированы, то копии старых СЕРТ|ОК должны храниться ДТС в течение некоторого периода времени, длительность которого определяется сложившейся практикой деловых отношений, законами и нормативными правовыми актами.

Если закрытый ключ объекта или УЦ был удален по какой-либо причине, то УЦ, выпустивший соответствующий СЕРТ|ОК, должен незамедлительно принять меры по оповещению всех объектов системы о том, что все соответствующие СЕРТ|ОК будут аннулированы. Например, это может быть аутентифицированное УЦ сообщение, которое будет передано всем объектам, сообщение, аутентифицированное другим УЦ, ведение ДТС списка аннулированных СЕРТ|ОК в интерактивном режиме (on-line) или даже опубликование списка аннулированных или действующих СЕРТ|ОК.

Если СЕРТ|ОК был аннулирован вследствие компрометации или подозрения на компрометацию закрытого ключа, то закрытый ключ не должен больше никогда использоваться.

СЕРТ|ОК целесообразно использовать только с целью проверки для подтверждения того, что данные были подписаны еще до момента аннулирования. Кроме того, любая ключевая информация, зашифрованная с помощью СЕРТ|ОК (независимо от типа), должна быть немедленно запрещена к использованию.

Если СЕРТ|ОК был аннулирован по каким-либо иным причинам, отличным от реальной компрометации или подозрения на компрометацию закрытого ключа, то закрытый ключ не должен больше никогда использоваться. СЕРТ|ОК может по-прежнему использоваться для проверки подлинности или в процедурах расшифрования. Любая ключевая информация, которая была передана и защищена с помощью СЕРТ|ОК (независимо от типа), должна быть перемещена как можно быстрее и в наиболее подходящее место.

9.8.6.2. Списки отзыва

Список отзыва включает помеченный меткой времени перечень последовательных номеров или идентификаторов СЕРТ|ОК для тех СЕРТ|ОК, которые были аннулированы УЦ. В списках отзыва могут использоваться два типа меток времени, а именно:

- a)* дата и время аннулирования УЦ СЕРТ|ОК;
- b)* дата и время известной или предполагаемой компрометации.

Последняя дата позволит провести аудиторскую проверку сомнительных сообщений на более ранней стадии. СЕРТ|ОК остается в списке отзыва по крайней мере до истечения своего срока действия. Проставление меток времени является очень важной процедурой, так как необходимо знать, в какое время произошел «разрыв связки» между открытым ключом объекта и его параметром подлинности.

После того как произошло аннулирование вследствие известной или предполагаемой компрометации, вся информация, подписанная соответствующим закрытым ключом, не должна более признаваться как имеющая юридическую силу, если подпись была сформирована после предполагаемой даты ком-

прометации или если дата подписи не может быть достоверно определена. Никакая информация не должна зашифровываться с использованием аннулированного открытого ключа.

Список отзыва должен:

- быть датирован и подписан УЦ так, чтобы объекты могли проверить подлинность списка и дату распределения;
- издаваться УЦ на постоянной основе и регулярно, даже если не было никаких изменений после последнего издания;
- быть доступным для всех объектов системы, за исключением случаев, когда для этого имеются препятствия, например обусловленные законодательством, нормативными правовыми актами и постановлениями судов.

Для распределения списков отзыва могут использоваться различные способы, среди которых:

- доставка ДТС каждому пользователю списка отзыва в форме сообщения, используя процедуру информационного обмена;
- направление пользователем запроса доверенной третьей стороне о текущем состоянии выданного ему СЕРТ|ОК;
- направление запроса ДТС на получение ее текущего списка отзыва.

УЦ должен периодически публиковать и распределять новый список отзыва.

Список используемых сокращений

ASN.1	— описание абстрактного синтаксиса (алфавита), 1-я версия
БД	— база данных
ВИ	— вспомогательная информация, необходимая для обеспечения ИБ
ВКП	— внешний контрольный параметр
БДК	— база(ы) данных Службы единого каталога (Directory)
ДТС	— доверенная третья сторона
ИБ	— информационная безопасность
ИТС	— информационно-технологическая сеть (система)
КПС	— криптографическая проверочная сумма
МАС	— аутентификационный код сообщения (message authentication code)
ОНФ	— однонаправленная функция
ПБВ	— правило(а) безопасного взаимодействия
ПЛАО	— политика аудита ИБ и оповещения об опасности
ПЛАУ	— политика аутентификации
ПЛБ	— политика обеспечения ИБ
ПЛКЛ	— политика обеспечения ключами
ПЛКН	— политика обеспечения конфиденциальности
ПЛНТ	— политика обеспечения неотказуемости
ПЛЦЛ	— политика обеспечения целостности
ПЛУД	— политика управления доступом
ПРБ	— процедура обеспечения ИБ
ПРНТ	— процедура обеспечения неотказуемости
СЕРТ АО	— СЕРТ ИБ для проведения аудита
СЕРТ АУ	— СЕРТ ИБ для аутентификации
СЕРТ ИБ	— сертификат обеспечения ИБ
СЕРТ КЛ	— СЕРТ ИБ для обеспечения ключами
СЕРТ КН	— СЕРТ ИБ для обеспечения конфиденциальности
СЕРТ НТ	— СЕРТ ИБ для обеспечения неотказуемости
СЕРТ ОТ	— сертификат отзыва (аннулирования)
СЕРТ СО	— сертификат списка отозванных СЕРТ ИБ
СЕРТ УД	— СЕРТ ИБ для УД

СЕРТ ЦЛ	— СЕРТ ИБ для обеспечения целостности
СЛАО	— служба аудита ИБ и оповещения об опасности
СЛАУ	— служба аутентификации
СЛБ	— служба обеспечения ИБ
СЛКЛ	— служба обеспечения ключами
СЛКН	— служба обеспечения конфиденциальности
СЛНТ	— служба обеспечения неотказуемости
СЛУД	— служба управления доступом
СЛЦЛ	— служба обеспечения целостности
СПАУ	— способ аутентификации
СПБ	— способ обеспечения ИБ
СПКН	— способ обеспечения конфиденциальности
СПНТ	— способ обеспечения неотказуемости
СПУД	— способ управления доступом
СПЦЛ	— способ обеспечения целостности
СРБ	— средство обеспечения безопасности
ССБ	— сетевой сегмент безопасности
УД	— управление доступом
УИД	— уникальный идентификатор
УЦ	— удостоверяющий центр
ЦБ	— центр безопасности ССБ
ЭМВОС	— эталонная (7-уровневая) модель взаимодействия открытых систем
ЭЦП	— электронная цифровая подпись

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: Гелиос-АРВ, 2002.
2. Анин Б., Петрович А. Радиошпионаж. М.: Международные отношения, 1996.
3. Бабаш А.В., Шанкин Г.П. Криптография. М.: СОЛОН-Р, 2002.
4. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: учеб. пособие для вузов. М.: Горячая линия — Телеком, 2006.
5. Григорьев В.А. Передача сообщений по зарубежным информационным сетям. Л.: ВАС, 1989.
6. Дворянкин С.В. Речевая подпись. М.: РИО МТУСИ, 2003.
7. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999.
8. Мельников Д.А. Организация информационного обмена в информационно-вычислительных сетях: учеб. пособие. М.: ФАПСи, 1998.
9. Мельников Д.А. Информационные процессы в компьютерных сетях. Протоколы, стандарты, интерфейсы, модели. М.: КУДИЦ-ОБРАЗ, 1999.
10. Мельников Д.А., Савельев М.С. Скрытые под маской // PCWeek. 2005. № 6.
11. Орлов В.А., Мельников Д.А. Современная криптография и архитектура безопасности компьютерных сетей: учеб. пособие. М.: МГУПИ, 2009.
12. Петраков А.В. Защитные информационные технологии аудиовидео-электросвязи: учеб. пособие. М.: Энергоатомиздат, 2010.
13. Мельников Д.А. К вопросу обнаружения атак типа «маскарад» // Экономика, статистика и информатика. 2010. №1.
14. Мельников Д.А. Метод защиты неподвижных изображений // Информационные технологии управления в социально-экономических системах. 2010. №4.

15. Мельников Д.А. Организация и обеспечение безопасности информационно-технологических сетей и систем: учебник. М.: IDO Press: Университетская книга, 2012.
16. Мельников Д.А., Хоменок А.В. Современное состояние отечественной инфраструктуры электронной коммерции // Экономика, статистика и информатика. 2012. №1.
17. Диффи У., Хеллман М.Э. Защищенность и имитостойкость: Введение в криптографию // ТИИЭР. 1979. Т. 67. № 3.
18. Диффи У. Первые десять лет криптографии с открытым ключом // ТИИЭР. 1988. Т. 76. № 5.
19. ITU-T, Security Architecture for Open Systems Interconnection for CCITT Applications. Recommendation X.800, 1991.
20. ISO, Information Processing Systems – Open Systems Interconnection Reference Model – Part 1: Basic Reference Model, ISO/IEC 7498-1.
21. ISO, Information Processing Systems – Open Systems Interconnection Reference Model – Part 2: Security Architecture, ISO/IEC 7499-2.
22. ITU-T, Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview. Recommendation X.810, 1995.
23. ITU-T, Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework. Recommendation X.811, 1995.
24. ITU-T, Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework. Recommendation X.812, 1995.
25. ITU-T, Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework X.813, 1995.
26. ITU-T, Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framework X.814, 1995.
27. ITU-T, Information technology – Open Systems Interconnection – Security frameworks for open systems: Integrity framework X.815, 1995.

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: Гелиос-АРВ, 2002.
2. Анин Б., Петрович А. Радиошпионаж. М.: Международные отношения, 1996.
3. Бабаш А.В., Шанкин Г.П. Криптография. М.: СОЛОН-Р, 2002.
4. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: учеб. пособие для вузов. М.: Горячая линия — Телеком, 2006.
5. Григорьев В.А. Передача сообщений по зарубежным информационным сетям. Л.: ВАС, 1989.
6. Дворянкин С.В. Речевая подпись. М.: РИО МТУСИ, 2003.
7. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 1999.
8. Мельников Д.А. Организация информационного обмена в информационно-вычислительных сетях: учеб. пособие. М.: ФАПСи, 1998.
9. Мельников Д.А. Информационные процессы в компьютерных сетях. Протоколы, стандарты, интерфейсы, модели. М.: КУДИЦ-ОБРАЗ, 1999.
10. Мельников Д.А., Савельев М.С. Скрытые под маской // PCWeek. 2005. № 6.
11. Орлов В.А., Мельников Д.А. Современная криптография и архитектура безопасности компьютерных сетей: учеб. пособие. М.: МГУПИ, 2009.
12. Петраков А.В. Защитные информационные технологии аудиовидеоэлектросвязи: учеб. пособие. М.: Энергоатомиздат, 2010.
13. Мельников Д.А. К вопросу обнаружения атак типа «маскарад» // Экономика, статистика и информатика. 2010. №1.
14. Мельников Д.А. Метод защиты неподвижных изображений // Информационные технологии управления в социально-экономических системах. 2010. №4.

15. Мельников Д.А. Организация и обеспечение безопасности информационно-технологических сетей и систем: учебник. М.: IDO Press: Университетская книга, 2012.
16. Мельников Д.А., Хоменок А.В. Современное состояние отечественной инфраструктуры электронной коммерции // Экономика, статистика и информатика. 2012. №1.
17. Диффи У., Хеллман М.Э. Защищенность и имитостойкость: Введение в криптографию // ТИИЭР. 1979. Т. 67. № 3.
18. Диффи У. Первые десять лет криптографии с открытым ключом // ТИИЭР. 1988. Т. 76. № 5.
19. ITU-T, Security Architecture for Open Systems Interconnection for CCITT Applications. Recommendation X.800, 1991.
20. ISO, Information Processing Systems – Open Systems Interconnection Reference Model – Part 1: Basic Reference Model, ISO/IEC 7498-1.
21. ISO, Information Processing Systems – Open Systems Interconnection Reference Model – Part 2: Security Architecture, ISO/IEC 7499-2.
22. ITU-T, Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview. Recommendation X.810, 1995.
23. ITU-T, Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework. Recommendation X.811, 1995.
24. ITU-T, Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework. Recommendation X.812, 1995.
25. ITU-T, Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework X.813, 1995.
26. ITU-T, Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framework X.814, 1995.
27. ITU-T, Information technology – Open Systems Interconnection – Security frameworks for open systems: Integrity framework X.815, 1995.

28. ITU-T, Information technology – Open Systems Interconnection – Security frameworks for open systems: Security audit and alarms framework X.816, 1995.
29. ISO, Information technology – Security techniques – Key management – Part 1: Framework. ISO/IEC 11770-1, 2010-12-01.
30. ITU-T, Information technology – Security techniques – Guidelines for the use and management of trusted third party services. Recommendation X.842, 2000.
31. McNamara J. Secrets of Computer Espionage: Tactics and Countermeasures. N.Y.: John Wiley & Sons Inc., 2003.
32. Denning D.E. Cryptography and Data Security. Addison-Wesley, 1982.
33. American National Standards Institute, Public key Cryptography for the Financial Service Industry: Agreement of Symmetric Keys Using Diffie-Hellman and MQV Algorithms. X9.42, 29 Jan 1999.
34. American Bar Association, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce. Chicago, IL, 1 Aug 1996.
35. British Standards Institution, Information Security Management – Part 1: Code of Practice for Information Security Management. BS 7799-1:1999, effective 15 May 1999.
36. British Standards Institution, Information Security Management – Part 2: Specification for Information Security Management Systems. BS 7799-2:1999, effective 15 May 1999.
37. Bell D.E., LaPadula L.J., Secure Computer Systems: Mathematical Foundations and Model. M74-244, The MITRE Corporation, Bedford, MA, May 1973.
38. Common Criteria Implementation Board, Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and General Model. Ver. 2.1, CCIB-99-01, Aug 1999.
39. U.S. Department of Defense Computer Security Center, Computer Security Requirements: Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments. CSC-STD-003-85, 25 Jun 1985.

40. Denning D.E. A Lattice Model of Secure Information Flow // Communications of the ACM. Vol. 19. No. 5. May 1976. P. 236–243.
41. U.S. Department of Defense, Department of Defense Trusted Computer System Evaluation Criteria. DoD 5200.28-STD, 26 Dec 1985.
42. U.S. Department of Defense, Directive 5200.28, Security Requirements for Automated Information Systems (AISs). 21 March 1988.
43. U.S. Department of Defense, X.509 Certificate Policy. Ver. 2, March 1999.
44. Ford W. Computer Communications Security: Principles, Standard Protocols and Techniques. 1994.
45. Ford W., Baum M. Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption. 1997.
46. U.S. Department of Commerce, Glossary for Computer Systems Security. FIPS PUB 39, 15 Feb 1976.
47. U.S. Department of Commerce, Public Key Infrastructure (PKI) Technical Specifications – Part A: Technical Concept of Operations. National Institute of Standards, 4 Sep 1998.
48. U.S. Department of Commerce, Underlying Technical Models for Information Technology Security. National Institute of Standards Special Publication, Dec 2001.
49. Kahn D. The Codebreakers: The Story of Secret Writing. N.Y.: The Macmillan Company, 1967.
50. Kuhn M.G. , Anderson R.J. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations // Aucsmith, ed., Information Hiding, Second International Workshop, IH'98. Portland, Oregon, USA, 15–17 Apr 1998, LNCS 1525, Springer-Verlag.
51. U.S. Department of Commerce, Minimum Interoperability Specification for PKI Components (MISPC). Ver. 1. National Institute of Standards Special Publication 800-15, Sep 1997.
52. National Computer Security Center, A Guide to Understanding Audit in Trusted Systems. NCSC-TG-001, 1 Jun 1988.

53. National Computer Security Center, Glossary of Computer Security Terms. NCSC-TG-004. Ver. 1, 21 Oct 1988. (Part of the Rainbow Series.)
54. National Computer Security Center, Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria. NCSC-TG-005. Ver. 1, 31 Jul 1987. (Part of the Rainbow Series.)
55. Lloyd B., Simpson W. PPP Authentication Protocols. RFC-1334, Oct 1992.
56. Finseth C. An Access Control Protocol, Sometimes Called TACACS. RFC-1492, Jul 1993.
57. Kaufman C. DASS: Distributed Authentication Security Service. RFC-1507, Sep 1993.
58. Kohl J., Neuman C. The Kerberos Network Authentication Service (V5). RFC-4120 (RFC-4537), Jul 2005.
59. Eastlake D., Crocker S. and Schiller J. Randomness Recommendations for Security. RFC-4086, Jun 2005.
60. Eastlake D. 3rd, ed., CyberCash Credit Card Protocol Version 0.8. RFC-1898, Feb 1996.
61. Leech M., Ganis M., Lee Y., Kuris R., Koblas D. and Jones L. SOCKS Protocol Version 5. RFC-1928, March 1996.
62. Haller N., Metzner C. A One-Time Password System. RFC-1938, May 1996.
63. Linn J. Generic Security Service Application Program Interface, Version 2. RFC-2078, Jan 1997.
64. Rigney C., Rubens A., Simpson W. and Willens S. Remote Authentication Dial In User Service (RADIUS). RFC-2138, Apr 1997.
65. Gwinn A. Network Security For Trade Shows. RFC-2179, Jul 1997.
66. Fraser B. Site Security Handbook. FYI 8, RFC-2196, Sep 1997.
67. Myers J. Simple Authentication and Security Layer (SASL). RFC-2222, Oct 1997.
68. Dierks T., Allen C. The TLS Protocol, Version 1.0. RFC-2246, Jan 1999.

69. Haller N., ed., A One-Time Password System. RFC-2289, Feb 1998.
70. Ramos A. IETF Identification and Security Guidelines. RFC-2323, Apr 1998.
71. Brownlee N., Guttman E. Expectations for Computer Security Incident Response. RFC-2350, Jun 1998.
72. Kent S., Seo K. Security Architecture for the Internet Protocol. RFC-4301, Dec 2005.
73. Kent S. IP Authentication Header. RFC-4302, Dec 2005.
74. Kent S. IP Encapsulating Security Payload (ESP). RFC-4303, Dec 2005.
75. Kaufman C., ed., The Internet Key Exchange (IKEv2) Protocol. RFC 4306, Dec 2005.
76. Newman C. The One-Time-Password SASL Mechanism. RFC-2444, Oct 1998.
77. Guttman E., Leong L. and Malkin G. Users' Security Handbook. RFC-2504, Feb 1999.
78. Cooper D., Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC-5280, May 2008.
79. Housley R. Cryptographic Message Syntax. RFC-2630, Jun 1999.
80. Ramsdell B., ed., S/MIME Version 3 Message Specification. RFC-2633, Jun 1999.
81. Shirey R. Internet Security Glossary. RFC-2828, May 2000.
82. Raymond E.S., ed., The On-Line Hacker Jargon File. Ver. 4.0.0, 24 Jul 1996.
83. The New Hacker's Dictionary. 2d edition, MIT Press, Sep 1993.
84. Russell D., Gangemi Sr. G.T. Computer Security Basics. 1991.
85. Schneier B. Applied Cryptography. N.Y.: John Wiley & Sons, Inc., 1994.
86. U.S. Department of Defense, National Security Agency, Secure Data Network Systems, Security Protocol 3 (SP3). Document SDN.301, Revision 1.5, 15 May 1989.

87. U.S. Department of Defense, National Security Agency, Security Protocol 4 (SP4). Document SDN.401, Revision 1.2, 12 Jul 1988.
88. U.S. Department of Defense, National Security Agency, Secure data Network System, Message Security Protocol (MSP). Document SDN.701, Revision 4.0, 7 Jun 1996, with Corrections to Message Security Protocol, SDN.701, Rev 4.0, 96-06-07, 30 Aug 1996.
89. Melnikov D., Jones A. 'Masquerade' Attacks and a Process for Their Detection. Proceedings of the 3rd European Conference on Information Warfare and Security. Royal Holloway University of London, UK, 28–29 Jun 2004. P. 269.
90. Melnikov D., Jones A. Static Image Data Hiding and Encryption Method. Proceedings of the 3rd European Conference on Information Warfare and Security. Royal Holloway University of London, UK, 28–29 Jun 2004. P. 279.

Учебное издание

Мельников Дмитрий Анатольевич

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
ОТКРЫТЫХ СИСТЕМ**

Учебник