

Государственное образовательное учреждение
высшего профессионального образования
«Нижегородский государственный лингвистический университет
им. Н.А. Добролюбова»

Кафедра «математики и информатики»

Р. А. Васильев

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Нижний Новгород
2012

Государственное образовательное учреждение
высшего профессионального образования
«Нижегородский государственный лингвистический университет
им. Н.А. Добролюбова»

Кафедра «математики и информатики»

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Курс лекций для студентов специальности

090900 – Информационная безопасность

Нижний Новгород
2012

В данном курсе лекций рассмотрены методы и средства проектирования и использования комплекса мероприятий по управлению информационной безопасностью, проведен анализ лучших мировых практических разработок по внедрению и совершенствованию управления информационной безопасностью.

Курс лекций предназначен для освоения теоретического курса по дисциплине: «Управление информационной безопасностью» для студентов специальности «Информационная безопасность».

Составитель: Р. А. Васильев, старший преподаватель кафедры «математики и информатики»

Рецензенты: В.В. Савченко, д.т.н., профессор, зав. кафедрой «математики и информатики»

Оглавление

Введение	6
Тема 1: "Основные понятия информационной безопасности"	14
1.1 Понятие информационной безопасности	14
1.2 Объект защиты информации	15
1.3 Основные составляющие информационной безопасности.....	18
1.4 Управление информационной безопасностью	19
1.5 Важность и сложность проблемы информационной безопасности	21
Тема 2: "Угрозы информационной безопасности в информационных системах"	23
2.1 Основные определения и критерии классификации угроз	23
2.2 Основные угрозы доступности.	25
2.3 Основные угрозы целостности.....	28
2.4 Основные угрозы конфиденциальности	29
2.5 Вредительские программы	31
Тема 3: "Оценочные стандарты в информационной безопасности"	32
3.1 Роль стандартов ИБ.	32
3.2 «Оранжевая книга» как оценочный стандарт.....	34
3.3 Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.....	37
Тема 4: "Стандарты управления информационной безопасностью"	41
4.1 Стандарты управления информационной безопасностью.....	41
BS 7799 и ISO/IEC 17799. Их основные положения	41
4.2. Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования"	43
4.3 Сертификация СУИБ на соответствие ISO 27001	48
Тема 5: "Создание СУИБ на предприятии"	50
5.1. Этапы создания системы управления ИБ	50
5.2 Категорирование активов компании.....	51
5.3 Оценка защищенности информационной системы компании	53
5.4 Оценка информационных рисков	53
Тема 6: "Методика оценки рисков информационной безопасности компании"	58
6.1 Управление рисками. Основные понятия.....	58
6.2 Метод оценки рисков на основе модели угроз и уязвимостей.	60
Тема 7: "Методика оценки рисков информационной безопасности компании Digital Security"	67
7.1 Метод оценки рисков на основе модели информационных потоков.....	67
7.2.Описание архитектуры ИС.....	67
7.3 Расчет рисков по угрозе конфиденциальность	70
Тема 8: "Методики и технологии управления рисками"	77
8.1 Качественные методики управления рисками	78
8.2 Количественные методики управления рисками. Метод CRAMM	79
Тема 9: "Разработка корпоративной методики анализа рисков"	89
9.1 Постановка задачи	89

9.2 Методы оценивания информационных рисков	92
9.3 Табличные методы оценки рисков.....	93
9.4 Методика анализа рисков Microsoft.....	96
Тема 10: "Современные методы и средства анализа и управление рисками информационных систем компаний"	98
10.1 Обоснование необходимости инвестиций в информационную безопасность компании	98
10.2 Методика FRAP	99
10.3 Методика OCTAVE (октэйв).....	102
10.4 Методика RiskWatch (риск вэтч).....	105
Тема 11: "Правовые меры обеспечения информационной безопасности "	110
11.1 Основные направления обеспечения информационной безопасности ..	110
11.2 Законодательно-правовая база обеспечения информационной безопасности на предприятии	111
11.3 Нормативные акты предприятия по информационной безопасности ...	112
11.4 Формы правовой защиты информации на предприятии	115
11.5 Другие документы предприятия, в которых отражаются вопросы обеспечения информационной безопасности	116
Тема 12: "Организационные меры обеспечения безопасности компьютерных информационных систем"	119
12.1 Общие положения организационной защиты	119
12.2. Особенности организационной защиты компьютерных информационных систем и сетей.....	120
12.3 Служба безопасности предприятия	123
Тема 13: "Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом "	126
13.1 Основные программно-технические меры.	126
13.2 Идентификация и аутентификация. Основные понятия.....	128
13.3 Управление доступом. Основные понятия.....	133
Тема 14: "Протоколирование и аудит, шифрование, контроль целостности" ..	135
14.1 Протоколирование и аудит.....	135
14.2 Активный аудит	137
14.3 Шифрование.....	138
14.4 Контроль целостности	141
14.5 Цифровые сертификаты.....	143
Тема 15: «Управление информационной безопасностью на государственном уровне. Общие принципы и российская практика»	144
15.1 Организационно-правовые формы управления безопасностью.....	144
15.2 Предпосылки развития государственного управления в сфере информационной безопасности	147
15.3 Общая методология и структура организационного обеспечения информационной безопасности на уровне государств	149
15.4 Общая политика России в сфере информационной безопасности.....	154

15.5 Структура органов государственной власти, обеспечивающих информационную безопасность в РФ	156
15.6 Государственная граница и ее охрана.....	161
Библиографический список.....	166

Введение

Управление информационной безопасностью (Information Security Management или ISM) - процесс, который обеспечивает конфиденциальность, целостность и доступность активов, информации, данных и услуг организации. Управление информационной безопасностью обычно является частью Организационного подхода к Управлению безопасностью, который имеет более широкую область охвата, чем поставщик услуг, и включает обработку бумажных документов, доступ в здания, телефонные звонки и т.п., для всей организации.

Основной целью ISM является обеспечение эффективного управления информационной безопасностью всех услуг и деятельности в рамках Управления услуг. Информационная безопасность предназначена для защиты от нарушения конфиденциальности, доступности и целостности информации, информационных систем и коммуникаций.

1. **Конфиденциальность** - состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.

2. **Целостность** - состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

3. **Доступность** - состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

Цель обеспечения информационной безопасности достигнута, если:

1. Информация доступна тогда, когда это требуется, а информационные системы устойчивы к атакам, могут избегать их или быстро восстанавливаться.

2. Информация доступна только тем, кто имеет соответствующие права.

3. Информация корректна, полна и защищена от неавторизованных изменений.

4. Обмен информацией с партнерами и другими организациями надежно защищен.

Бизнес определяет, что и как должно быть защищено. При этом для эффективности и целостности обеспечения информационной безопасности необходимо рассматривать бизнес процессы от начала до конца, так как слабое место может сделать уязвимой всю систему.

Процесс ISM должен включать в себя:

- формирование, управление, распространение и соблюдение Политики информационной безопасности и других вспомогательных политик, которые имеют отношение к информационной безопасности. **Политика информационной безопасности (Security Policy)** - система политик, процессов, стандартов, руководящих документов и средств, которые обеспечивают организации достижение целей Управления информационной безопасностью.

- понимание согласованных текущих и будущих требований бизнеса к безопасности;

- использование контролей безопасности для выполнения Политики информационной безопасности и управления рисками, связанными с доступом к информации, системам и услугам. Термин "контроль безопасности" является заимствованным из английского языка и в данном контексте означает набор контрмер и мер предосторожности, применяемых для аннулирования, уменьшения рисков и противостояния им. То есть контроль безопасности состоит из проактивных и реактивных действий;

- документирование перечня контролей безопасности, действий по их эксплуатации и управлению, а также всех связанных с ними рисков;

- управление поставщиками и контрактами, требующими доступа к системам и услугам. Осуществляется при взаимодействии с процессом Управления поставщиками;

- контроль всех "брешей" безопасности и инцидентов, связанных с системами и услугами;

- проактивное улучшение контролей безопасности и уменьшение рисков нарушения информационной безопасности;

- интеграция аспектов информационной безопасности во все процессы Управления услуг.

Политика информационной безопасности должна включать в себя следующее:

- реализация аспектов Политики информационной безопасности;
- возможные злоупотребления аспектами Политики информационной безопасности;

- политика контроля доступа;
- политика использования паролей;
- политика электронной почты;
- политика интернета;

- политика антивирусной защиты;
- политика классификации информации;
- политика классификации документов;
- политика удаленного доступа;
- политика доступа поставщиков к услугам, информации и компонентам;
- политика размещение активов.

Перечисленные политики должны быть доступны пользователям и заказчикам, которые в свою очередь обязаны письменно подтвердить свое согласие с ними.

Политики утверждаются руководством бизнеса и IT и пересматриваются в зависимости от обстоятельств.

Чтобы обеспечивать информационную безопасность и управлять ею, необходимо поддерживать Систему управления информационной безопасностью. **Система управления информационной безопасностью (Information Security Management System или ISMS)** - система политик, процессов, стандартов, руководящих документов и средств, которые обеспечивают организации достижение целей управления информационной безопасностью. На рис. 1 показана структура ISMS, наиболее широко используемая организациями.



Рис. 1 ISMS

На рис. 1 представлены 5 элементов структуры ISMS:

1. Контроль. Цели контроля:

- формирование системы управления информационной безопасностью в рамках организации;
- формирование организационной структуры для подготовки, утверждения и реализации Политики информационной безопасности;
- распределение ответственностей;
- формирование документации по контролю.

2. Планирование. Цель планирования - разработать и рекомендовать подходящие метрики и способы измерения информационной безопасности. В первую очередь планирование должно учитывать требования и особенности конкретной организации. Источниками информации для формирования требований к информационной безопасности являются бизнес, риски, планы, стратегия, соглашения (в первую очередь OLA и SLA). При этом важно учитывать моральную, законодательную и этическую ответственности в контексте информационной безопасности.

3. Реализация. Цель реализации - обеспечение подходящих процедур, инструментов и контролей безопасности для поддержки Политики информационной безопасности.

В рамках реализации проводятся следующие мероприятия:

- идентификация активов - совместно с Управлением конфигурациями;
- классификация информации - информация и информационные хранилища должны быть классифицированы в соответствии с их чувствительностью и значимостью по отношению к трем аспектам информационной безопасности (конфиденциальности, целостности, доступности).

4. Оценка. Цель оценки в рамках ISMS:

- проверка соответствия политики информационной безопасности требованиям к информационной безопасности из SLA и OLA;
- проведение регулярных проверок технической составляющей информационной безопасности для IT систем;
- предоставление информации для регуляторов и внешних аудиторов при необходимости;

5. Поддержка. Цели поддержки ISMS:

- улучшение соглашений в отношении информационной безопасности, например, SLA и OLA
- совершенствование средств и контролей информационной безопасности.

Ключевые деятельности в рамках ISM:

1. формирование, пересмотр и корректирование Политики информационной безопасности и набора поддерживающих ее вспомогательных политик;
2. реализация и соблюдение политик информационной безопасности, а также обеспечение взаимодействия между ними;
3. оценка и классификация всех информационных активов и документов;
4. использование, пересмотр и корректирование набора контролей безопасности, мер по оценке рисков и ответных действий;
5. мониторинг и управление "брешами" безопасности и инцидентами;
6. анализ, ведение отчетности и уменьшение влияния "брешей" в безопасности и инцидентов;
7. составление расписания и проведение аудитов, тестирования и обзоров.

Взаимодействие указанных деятельности представлено на рис. 2.

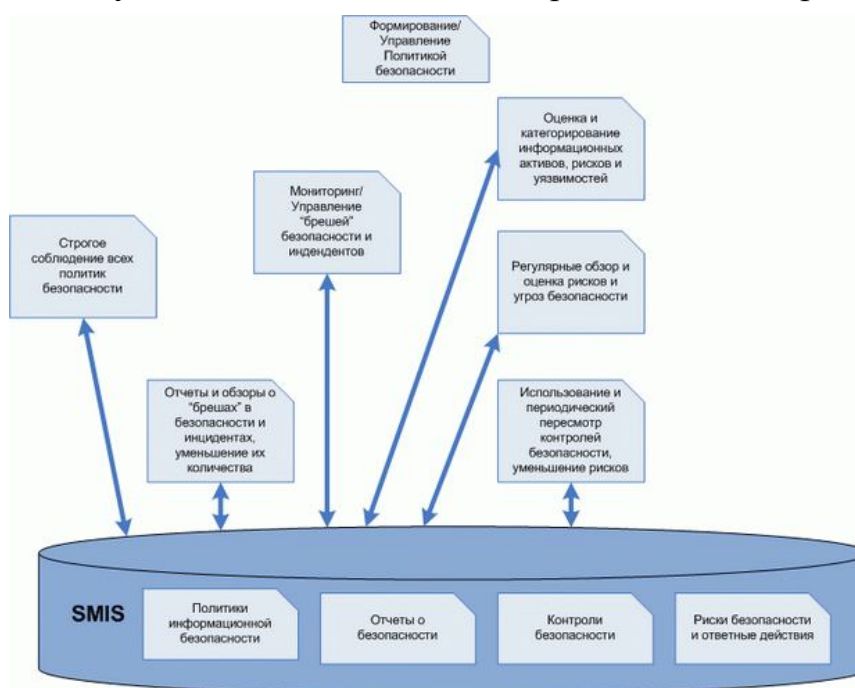


Рис. 2 Ключевые деятельности в рамках ISM

Для обеспечения и поддержки Политики информационной безопасности необходимо сформировать и использовать набор контролей безопасности. Для предотвращения инцидентов и правильного реагирования в случае их возникновения используют меры безопасности, представленные на рис. 3

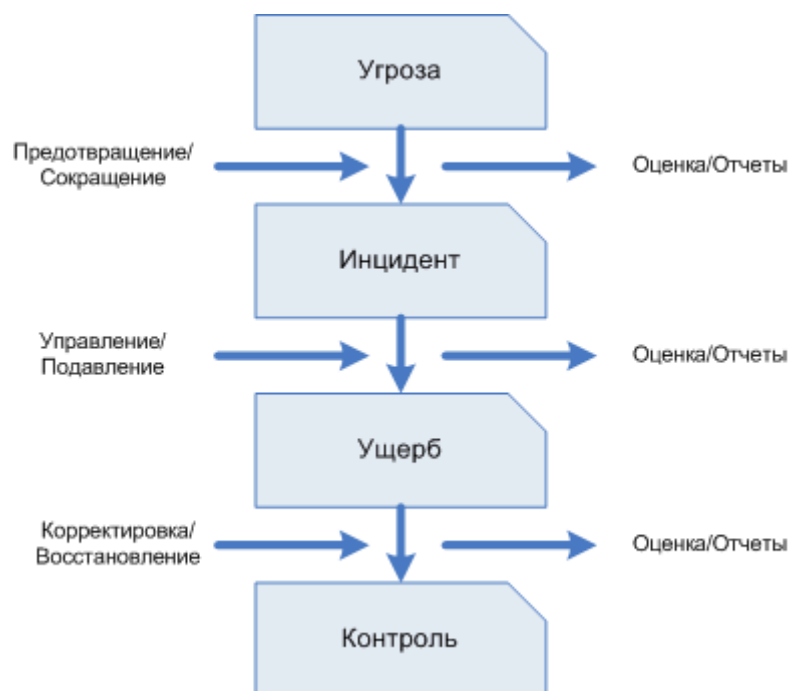


Рис. 3 Контроли безопасности

На рис. 3 выделено четыре стадии. Первая стадия - возникновение угрозы. Угрозой является все, что может негативно повлиять на бизнес-процесс или прерывать его. Инцидент - это реализованная угроза. Инцидент является отправной точкой для применения контролей безопасности. В результате инцидента появляется ущерб. Для управления или устранения рисков также применяются контроли безопасности. Для каждой стадии необходимо подобрать подходящие меры обеспечения информационной безопасности:

1. превентивные - меры безопасности, которые предотвращают появление инцидента информационной безопасности. Например, распределение прав доступа.
2. восстановительные - меры безопасности, направленные на уменьшение потенциального ущерба в случае инцидента. Например, резервное копирование.
3. обнаруживающие - меры безопасности, направленные на обнаружение инцидентов. Например, антивирусная защита или система обнаружения вторжений.
4. подавляющие - меры безопасности, которые противодействуют попыткам реализации угрозы, то есть инцидентам. Например, банкомат забирает у клиента карту после определенного количества неправильных вводов PIN-кода.

5. корректирующие - меры безопасности, направленные на восстановление после инцидента. Например, восстановление резервных копий, откат на предыдущее рабочее состояние и т.п.

Входами процесса ISM являются:

1. информация от бизнеса - стратегии, планы, бюджет бизнеса, а также его текущие и будущие требования;
2. политики безопасности бизнеса, планы безопасности, Анализ рисков;
3. информация от IT - стратегия, планы и бюджет IT;
4. информация об услугах - информация от SLM, в частности Портфеля услуг и Каталога услуг, SLA/SLR;
5. отчеты процессов и анализа рисков от ISM, Управления доступностью и Управления непрерывностью услуг;
6. детальная информация обо всех инцидентах информационной безопасности и "брешах" в ней;
7. информация об изменениях - информация от процесса Управления изменениями, в частности расписание изменений и их влияние на планы, политики и контроли информационной безопасности;
8. информация о взаимоотношениях бизнеса с услугами, вспомогательными услугами и технологиями;
9. информация о доступе партнеров и поставщиков к услугам и системам, предоставляемая процессами Управления поставщиками и Управления доступностью.

Выходами ISM являются:

1. всеобъемлющая Политика информационной безопасности и другие вспомогательные политики, которые имеют отношение к информационной безопасности;
2. Система управления информационной безопасностью (ISMIS), которая содержит всю информацию, необходимую для обеспечения ISM;
3. результаты переоценки рисков и ревизии отчетов;
4. набор контролей безопасности, описание их эксплуатации и управления, а также всех связанных с ними рисков;
5. аудиты информационной безопасности и отчеты;

6. расписание тестирования планов информационной безопасности;
7. классификация информационных активов;
8. отчеты о существующих "брешах" в информационной безопасности и инцидентах;
9. политики, процессы и процедуры для управления доступом поставщиков и партнеров к услугам и системам.

В качестве ключевых показателей производительности процесса Управления информационной безопасностью можно использовать множество метрик, например:

1. защищенность бизнеса от нарушений информационной безопасности
 - процентное уменьшение сообщений о "брешах" в Сервис-деск;
 - процентное уменьшение негативного влияния на бизнес со стороны "брешей" и инцидентов;
 - процентное увеличение пунктов, касающихся информационной безопасности, в SLA.
2. формирование четкой и согласованной политики информационной безопасности, учитывающей потребности бизнеса, то есть уменьшение количества несовпадений между процессами ISM и процессами и политиками информационной безопасности бизнеса.
3. процедуры по обеспечению безопасности, которые оправданы, согласованы и утверждены руководством организации:
 - увеличение согласованности и пригодности процедур обеспечения безопасности;
 - увеличение поддержки со стороны руководства
4. механизмы улучшения:
 - количество предложенных улучшений в отношении контролей и процедур;
 - уменьшение количества несовпадений, обнаруженных в процессе тестирования и аудита.
5. информационная безопасность является неотъемлемой частью услуг и процессов ITSM, то есть увеличение количества услуг и процессов, в которых предусмотрены меры безопасности.

ISM сталкивается со множеством трудностей и рисков на пути обеспечения информационной безопасности. К сожалению, на практике достаточно часто бизнес считает, что вопросами информационной безопасности должна заниматься только IT. Еще хуже, когда бизнес не понимает, зачем вообще нужно уделять внимание информационной безопасности. Создание эффективной системы защиты информации влечет за собой большие затраты, которые должны быть понятны руководству, так как именно оно принимает решение о финансировании. При этом важно соблюдать баланс - обеспечение информационной безопасности не должно стоять больше самой защищаемой информации.

Тема 1: "Основные понятия информационной безопасности"

1.1 Понятие информационной безопасности

Информация - самый ценный ресурс в компании, а в некоторых случаях является и производственным ресурсом, от сохранности которого зависят важные технологические процессы. С развитием информационных технологий увеличивается риск утечки информации, заражение вирусами, вмешательства в работу системы.

Информация существует в различных формах. Ее можно хранить на компьютерах, передавать по вычислительным сетям, распечатывать или записывать на бумаге, а также озвучивать в разговорах. С точки зрения безопасности все виды информации, включая бумажную документацию, базы данных, пленки, микрофильмы, модели, магнитные ленты, дискеты, разговоры и другие способы, используемые для передачи знаний и идей, требуют надлежащей защиты.

Защитные меры оказываются значительно более дешевыми и эффективными, если они встроены в информационные системы и сервисы на стадиях задания требований и проектирования. Чем скорее организация примет меры по защите своих информационных систем, тем более дешевыми и эффективными они будут для нее впоследствии.

Словосочетание «информационная безопасность» в разных контекстах может иметь различный смысл.

В широком смысле информационная безопасность (ИБ) – это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

В данном курсе наше внимание будет сосредоточено на хранении, обработке и передаче информации вне зависимости от того, каким образом она закодирована, кто или что является ее источником. Поэтому термин «информационная безопасность» будет использоваться в узком смысле.

Под информационной безопасностью в узком смысле мы будем понимать ***защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственно-***

го характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуре. (Чуть дальше мы поясним, что следует понимать под поддерживающей инфраструктурой.)

Защита информации — это комплекс мероприятий, направленных на обеспечение информационной безопасности.

1.2 Объект защиты информации

Объектом защиты информации является информационная система (предприятия, коммерческой организации) или автоматизированная система обработки данных. Что же понимается под этим термином?

В большинстве изданий по ИБ под ИС понимается ***комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации.***

Наряду с термином "информация" применительно к ИС часто используют термин "данные". Используется и другое понятие "информационные ресурсы". **Под информационными ресурсами** понимаются отдельные документы и отдельные массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных и других информационных системах).

Понятие ИС очень широкое и оно охватывает следующие системы:

- ЭВМ всех классов и назначений;
- вычислительные комплексы и системы;
- вычислительные сети (локальные, региональные и глобальные).

Такой широкий диапазон систем объединяется одним понятием по двум причинам: во-первых, для всех этих систем основные проблемы защиты информации являются общими; во-вторых, более мелкие системы являются элементами более крупных систем.

Если защита информации в каких-либо системах имеет свои особенности, то они рассматриваются отдельно.

Предметом защиты в ИС является информация. Материальной основой существования информации в ИС являются электронные и электромеханические устройства (подсистемы), а также машинные носители. С помощью устройств ввода или систем передачи данных (СПД) информация попадает в ИС. В системе информация хранится в запоминающих устройствах (ЗУ) различных уровней, преобразуется (обрабатывается) процессорами (ПЦ) и выводится из системы с помощью устройств вывода или СПД. В качестве машинных носителей используются магнитные ленты, диски различных типов, флеш-накопители. Ранее в качестве машинных носителей информации использовались бумажные перфокарты и перфоленты, магнитные барабаны и карты. Большинство типов машинных носителей информации являются съемными, т.е. могут сниматься с устройств и использоваться или храниться (ленты, диски, флеш) отдельно от устройств.

Таким образом, для защиты информации (обеспечения безопасности информации) в ИС необходимо защищать устройства (подсистемы) и машинные носители от несанкционированных (неразрешенных) воздействий на них.

Однако такое рассмотрение ИС с точки зрения защиты информации является неполным. Компьютерные системы относятся к классу человеко-машинных систем. Такие системы эксплуатируются специалистами (обслуживающим персоналом) в интересах пользователей. Причем, в последние годы пользователи имеют самый непосредственный доступ к системе. В некоторых ИС (например, ПЭВМ) пользователи выполняют функции обслуживающего персонала. Обслуживающий персонал и пользователи являются также носителями информации. Поэтому от несанкционированных воздействий необходимо защищать не только устройства и носители, но также обслуживающий персонал и пользователей.

Таким образом, более полное определение ИС будет таковым:

Информационная система — взаимосвязанная совокупность средств, методов и персонала, которые используются для хранения, обработки, передачи и получения информации в интересах достижения поставленной цели.

При решении проблемы защиты информации в ИС необходимо учитывать также противоречивость человеческого фактора системы. Обслуживающий персонал и пользователи могут быть как объектом, так и источником несанкционированного воздействия на информацию.

Понятие "**объект защиты**" или "**объект**" чаще трактуется в более широком смысле. Для сосредоточенных ИС или элементов распределенных систем понятие "объект" включает в себя не только информационные ресурсы, аппаратные, программные средства, обслуживающий персонал, пользователей, но и помещения, здания, и даже прилегающую к зданиям территорию.

Одними из основных понятий теории защиты информации являются понятия "безопасность информации" и "защищенные ИС".

Безопасность (защищенность) информации в ИС – это такое состояние всех компонент информационной системы, при котором обеспечивается защита информации от возможных угроз на требуемом уровне. ИС, в которых обеспечивается безопасность информации, называются **защищенными**.

Безопасность информации в ИС (информационная безопасность) является одним из основных направлений обеспечения безопасности государства, отрасли, ведомства, государственной организации или частной фирмы.

Информационная безопасность достигается проведением руководством соответствующего уровня **политики информационной безопасности**. Одноименный документ разрабатывается и принимается как официальный руководящий документ, ведомством, организацией. В документе приводятся цели политики информационной безопасности и основные направления решения задач защиты информации в ИС. В программах информационной безопасности содержатся также общие требования и принципы построения систем защиты информации в ИС.

Под **системой защиты информации в ИС** понимается единый комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в ИС в соответствии с принятой политикой безопасности.

Правильный подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС). Из этого положения можно вывести два важных следствия:

1. Трактовка понятия «информационная безопасность», для разных категорий субъектов может существенно различаться. Для иллюстрации достаточно сопоставить режимные государственные организации и учебные институты. В первом случае «пусть лучше все сломается, чем враг узнает хоть один секретный бит», во втором — «да нет у нас никаких секретов, лишь бы все работало».

Зачем надо защищаться? Ответов на этот вопрос может быть множество, в зависимости от структуры и целей предприятия. Для одних первой задачей является предотвращение утечки информации (маркетинговых планов, перспективных разработок и т.д.) конкурентам. Другие могут пренебречь конфиденциальностью своей информации и сосредоточить внимание на ее целостности. Например, для банка важно в первую очередь обеспечить неизменность обрабатываемых платежных поручений, чтобы злоумышленник не смог несанкционированно дописать в платежку еще один нолик или изменить реквизиты получателя. Для третьих на первое место поднимается задача обеспечения доступности и безотказной работы информационных систем. Для провайдера Internet-услуг, компании, имеющей Web-сервер, или оператора связи первой задачей является именно обеспечение безотказной работы всех (или наиболее важных) узлов своей информационной системы. Расставить такого рода приоритеты можно только по результатам анализа деятельности предприятия.

2. Информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации, это принципиально более широкое понятие. Субъект информационных отношений может пострадать (понести убытки и/или получить моральный ущерб) не только от несанкционированного доступа, но и от **поломки системы, вызвавшей перерыв в работе**. Более того, для многих открытых организаций (например, учебных) собственно защита от несанкционированного доступа к информации стоит по важности отнюдь не на первом месте. Главное для них – это обеспечение непрерывности работы информационной системы.

Согласно определению информационной безопасности, она зависит не только от компьютеров, но и от **поддерживающей инфраструктуры**, к которой можно отнести системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и, конечно, обслуживающий персонал. Эта инфраструктура имеет самостоятельную ценность, но нас будет интересовать лишь то, как она влияет на выполнение информационной системой предписанных ей функций.

Обратим внимание, что в определении ИБ перед существительным «ущерб» стоит прилагательное «неприемлемый». Очевидно, застраховаться от всех видов ущерба невозможно, тем более невозможно сделать это экономически целесообразным способом, когда стоимость защитных средств и мероприятий не превышает размер ожидаемого ущерба. Значит, с чем-то приходится мириться и защищаться следует только от того, с чем смириться никак нельзя. Иногда таким недопустимым ущербом является нанесение вреда здоровью людей или состоянию окружающей среды, но чаще порог неприемлемости имеет материальное (денежное) выражение, а *целью защиты информации становится уменьшение размеров ущерба до допустимых значений.*

1.3 Основные составляющие информационной безопасности

Информационная безопасность — многогранная область деятельности, в которой успех может принести только систематический, комплексный подход.

Цель информационной безопасности – обеспечить бесперебойную работу организации и свести к минимуму ущерб от событий, таящих угрозу безопасности, посредством их предотвращения и сведения последствий к минимуму.

Основными задачами и составляющими ИБ является: обеспечение **доступности, целостности и конфиденциальности** информационных ресурсов и поддерживающей инфраструктуры.

Поясним понятия доступности, целостности и конфиденциальности.

Доступность — это возможность за приемлемое время получить требуемую информационную услугу.

Под **целостностью** информации подразумевается, ее защищенность от разрушения и несанкционированного изменения.

Наконец, **конфиденциальность** — это защита от несанкционированного доступа к информации.

Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем субъектам информационных отношений. Поэтому, не противопоставляя **доступность** остальным аспектам, мы выделяем ее как важнейший элемент информационной безопасности.

Особенно ярко ведущая роль доступности проявляется в разного рода системах управления — производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия — и материальные, и моральные — может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.).

Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)). Средства контроля динамической целостности применяются, в частности, при анализе потока фи-

нансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

Целостность оказывается важнейшим аспектом ИБ в тех случаях, когда информация служит «руководством к действию». Рецепт лекарства, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса - все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным. Неприятно и искажение официальной информации, будь то текст закона или страница ВЭБ-сервера какой-либо правительственной организации.

Конфиденциальность — самый проработанный у нас в стране аспект информационной безопасности. Обеспечение конфиденциальности достигается использованием криптографии и выполнением соответствующих организационных и технических мероприятий направленных на выявление и блокирование возможных каналов утечки информации.

Почти для всех, кто реально использует ИС, на первом месте стоит доступность. Практически не уступает ей по важности целостность — какой смысл в информационной услуге, если она содержит искаженные сведения?

Наконец, конфиденциальные моменты есть также у многих организаций (даже в упоминавшихся выше учебных институтах стараются не разглашать сведения о зарплате сотрудников) и отдельных пользователей (например, пароли).

1.4 Управление информационной безопасностью

Обеспечение ИБ – это непрерывный процесс, основное содержание которого составляет управление. ИБ невозможно обеспечить разовым мероприятием, поскольку средства защиты нуждаются в постоянном контроле и обновлении.

Управление информационной безопасностью – это управление людьми, рисками, ресурсами, средствами защиты и т.п. УИБ является неотъемлемым элементом управления предприятием и позволяет коллективно использовать конфиденциальную информацию, обеспечивая при этом ее защиту, а так же защиту вычислительных ресурсов.

Управление информационной безопасностью - это циклический процесс, включающий:

- осознание степени необходимости защиты информации;
- сбор и анализ данных о состоянии информационной безопасности в организации;
- оценку информационных рисков;
- планирование мер по обработке рисков;
- реализацию и внедрение соответствующих механизмов контроля;
- распределение ролей и ответственности;
- обучение и мотивацию персонала;
- оперативную работу по осуществлению защитных мероприятий;
- мониторинг функционирования механизмов контроля,
- оценку их эффективности и соответствующие корректирующие воздейст-

вия.

Для обеспечения необходимого уровня информационной безопасности (предприятия, учреждения и т.д.) на предприятии создается **комплексная система управления информационной безопасностью (СУИБ)**. Конечной целью создания такой системы является предотвращение или минимизация ущерба (прямого или косвенного, материального, морального или иного), преднамеренно наносимого злоумышленниками либо непреднамеренно - нерадивыми работниками предприятия посредством нежелательного воздействия на информацию, ее носители и процессы обработки.

Согласно стандарту ISO 27001, **система управления информационной безопасностью (СУИБ)** - это «та часть общей системы управления организации, основанной на оценке бизнес рисков, которая создает, реализует, эксплуатирует, осуществляет мониторинг, пересмотр, сопровождение и совершенствование информационной безопасности». Система управления **включает в себя** организационную структуру, политики, планирование, должностные обязанности, практики, процедуры, процессы и ресурсы.

Основной задачей системы является обеспечение необходимого уровня доступности, целостности и конфиденциальности компонентов (ресурсов) ИС.

Какие преимущества компании дает внедрение СУИБ и ее сертификация на соответствие международным стандартам:

- повышение управляемости и надежности бизнеса компании;
- повышение защищенности ключевых бизнес-процессов компании;
- повышение доверия к компании как к партнеру, так и клиенту;
- соответствие компании требованиям международного стандарта подчеркивает чистоту и прозрачность бизнеса компании;
- наличие СУИБ и международного сертификата упрощает процедуру выхода компании на внешние рынки;
- международное признание и повышение авторитета компании как на внутреннем, так и внешнем рынках;
- повышение доходности бизнеса в целом.

Для структурных подразделений компании внедрение СУИБ и ее сертификация на соответствие международным стандартам дает следующие преимущества:

- Систематизация процессов обеспечения информационной безопасности;
- Расстановка приоритетов компании в сфере ИБ;
- Управление ИБ компании в рамках единой корпоративной политики;
- Своевременное выявление и управление рисками;
- Снижение рисков от внутренних и внешних угроз;
- Оптимизация управленческих процессов;
- Повышение эффективности функционирования СУИБ и защищенности информационных систем;
- Повышение общей корпоративной культуры сотрудников и вывод управления бизнесом на новый уровень.

1.5 Важность и сложность проблемы информационной безопасности

Информационная безопасность является одним из важнейших аспектов интегральной безопасности, на каком бы уровне мы ни рассматривали последнюю — национальном, отраслевом, корпоративном или персональном.

Для иллюстрации этого положения ограничимся несколькими примерами.

- В Доктрине информационной безопасности Украины отмечено, что информационная безопасность является неотъемлемой составляющей каждой из сфер национальной безопасности. В то же время информационная безопасность является важной самостоятельной сферой обеспечения национальной безопасности. Именно поэтому развитие Украины как суверенного, демократического, правового и экономически стабильного государства возможно только при условии обеспечения надлежащего уровня ее информационной безопасности.
- Американский ракетный крейсер «Йорктаун» был вынужден вернуться в порт из-за многочисленных проблем с программным обеспечением (июль 1998). Таким оказался побочный эффект программы ВМФ США по максимально широкому использованию **коммерческого** программного обеспечения с целью снижения стоимости военной техники.
- Заместитель начальника управления по экономическим преступлениям Министерства внутренних дел России сообщил, что российские хакеры с 1994 по 1996 год предприняли почти 500 попыток проникновения в компьютерную сеть Центрального банка России. В 1995 году ими было похищено 250 миллиардов рублей (ИТАР-ТАСС, АР, 17 сентября 1996 года).
- Как сообщил журнал "Интернет уек" от 23 марта 1998 года, потери крупнейших компаний, вызванные компьютерными вторжениями, продолжают увеличиваться, несмотря на рост затрат на средства обеспечения безопасности. Согласно результатам совместного исследования Института информационной безопасности и ФБР, в 1997 году ущерб от компьютерных преступлений достиг 136 миллионов долларов, что на 36% больше, чем в 1996 году. Каждое компьютерное преступление наносит ущерб примерно в 200 тысяч долларов.
- В феврале 2001 года двое бывших сотрудников одной из компаний, воспользовавшись паролем администратора, удалили с сервера файлы, составлявшие крупный (на несколько миллионов долларов) проект для иностранного заказчика. К счастью, имелась резервная копия проекта, так что реальные потери ограничились расходами на следствие и средства защиты от подобных инцидентов в будущем. В августе 2002 года преступники предстали перед судом.
- Одна студентка потеряла стипендию в 18 тысяч долларов в Мичиганском университете из-за того, что ее соседка по комнате воспользовалась их общим системным входом и отправила от имени своей жертвы электронное письмо с отказом от стипендии.

Понятно, что подобных примеров множество, можно вспомнить и другие случаи — недостатка в нарушениях ИБ нет и не предвидится.

Приведем еще несколько цифр. В марте 1999 года был опубликован очередной, четвертый по счету, годовой отчет «Компьютерная преступность и безопасность-1999: проблемы и тенденции». В отчете отмечается резкий рост числа обращений в правоохранительные органы по поводу компьютерных преступлений (32% из числа опрошенных); 30% респондентов сообщили о том, что их информационные системы были взломаны внешними злоумышленниками; атакам через Интернет подвергались 57% опрошенных; в 55% случаях отмечались нарушения со стороны собственных сотрудников. Примечательно, что 33% респондентов на вопрос «были ли взломаны ваши ВЭБ-серверы и системы электронной коммерции за последние 12 месяцев?» ответили «не знаю».

В аналогичном отчете, опубликованном в апреле 2002 года, цифры изменились, но тенденция осталась прежней: 90% респондентов (преимущественно из крупных компаний и правительственных структур) сообщили, что за последние 12 месяцев в их организациях имели место нарушения информационной безопасности; 80% констатировали финансовые потери от этих нарушений; 44% (223 респондента) смогли и/или захотели оценить потери количественно, общая сумма составила более 455 млн. долларов. Наибольший ущерб нанесли кражи и подлоги (более 170 и 115 млн. долларов соответственно).

Столь же тревожные результаты содержатся в обзоре Информейшен Уек, опубликованном 12 июля 1999 года. Лишь 22% респондентов заявили об отсутствии нарушений информационной безопасности. Наряду с распространением вирусов отмечается резкий рост числа внешних атак.

Увеличение числа атак — еще не самая большая неприятность. Хуже то, что постоянно обнаруживаются новые уязвимые места в программном обеспечении (выше мы указывали на ограниченность современной технологии программирования) и, как следствие, появляются новые виды атак.

Так, в информационном письме Национального центра защиты инфраструктуры США от 21 июля 1999 года сообщается, что за период с 3 по 16 июля 1999 года выявлено девять проблем с ПО, риск использования которых оценивается как средний или высокий (общее число обнаруженных уязвимых мест равно 17). Среди «пострадавших» операционных платформ — почти все разновидности ОС Юникс, Виндус, МакОС, так что никто не может чувствовать себя спокойно, поскольку новые ошибки тут же начинают активно использоваться злоумышленниками.

В таких условиях системы информационной безопасности должны уметь противостоять разнообразным атакам, как внешним, так и внутренним, атакам автоматизированным и скоординированным. Иногда нападение длится доли секунды; порой прощупывание уязвимых мест ведется медленно и растягивается на часы, так что подозрительная активность практически незаметна. Целью злоумышленников может быть нарушение всех составляющих ИБ — доступности, целостности или конфиденциальности.

Тема 2: "Угрозы информационной безопасности в информационных системах"

2.1 Основные определения и критерии классификации угроз

Угроза — это действие, которое потенциально может привести к нарушению информационной безопасности.

Попытка реализации угрозы называется **атакой**, а тот, кто предпринимает такую попытку — **злоумышленником**. Потенциальные злоумышленники являются источниками угрозы.

Источником угрозы могут быть: злоумышленники, обслуживающий персонал, техногенные аварии, стихийные бедствия.

Свойством угрозы является перечень уязвимостей, при помощи которых может быть реализована угроза.

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Уязвимость — это слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы. Свойствами уязвимости являются: вероятность (простота) реализации угрозы через данную уязвимость и критичность реализации угрозы через данную уязвимость.

Вероятность реализации угрозы через данную уязвимость в течение года — степень возможности реализации угрозы через данную уязвимость в тех или иных условиях. Указывается в процентах.

Критичность реализации угрозы — степень влияния реализации угрозы на ресурс, т.е. как сильно реализация угрозы повлияет на работу ресурса. Задается в процентах. Состоит из критичности реализации угрозы по конфиденциальности, целостности и доступности (ERc, ERi, ERa).

Механизм деструктивного воздействия на информационную систему показан на слайде 1.

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется **окном опасности**, ассоциированным с данным уязвимым местом. Пока существует окно опасности, возможны успешные атаки на ИС.

Если речь идет об ошибках в ПО, то окно опасности «открывается» с появлением средств использования ошибки и ликвидируется при наложении заплат, ее исправляющих.

Для большинства уязвимых мест окно опасности существует сравнительно долго (несколько дней, иногда — недель), поскольку за это время должны произойти следующие события.

- должно стать известно о средствах использовании пробела в защите;

- должны быть выпущены соответствующие заплаты;
- заплаты должны быть установлены в защищаемой ИС.

Мы уже указывали, что новые уязвимые места и средства их использования появляются постоянно; это значит, во-первых, что почти всегда существуют окна опасности и, во-вторых, что отслеживание таких окон должно производиться постоянно, а выпуск и наложение заплат — как можно более оперативно.

Отметим, что некоторые угрозы нельзя считать следствием каких-то ошибок или просчетов, они существуют в силу самой природы современных ИС. Например, угроза отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения ИС от качественного электропитания.

Рассмотрим наиболее распространенные угрозы, которым подвержены современные информационные системы.

Сведения о возможных угрозах, а также об уязвимых местах, через которые эти угрозы могут быть реализованы, необходимы для того, чтобы с одной стороны – выработать требования к создаваемой КСЗИ в ИС, с другой стороны – для того, чтобы выбрать наиболее экономичные средства обеспечения безопасности. Незнание в данном случае ведет к перерасходу средств и, что еще хуже, к концентрации ресурсов там, где они не особенно нужны, за счет ослабления действительно уязвимых направлений.

На начальном этапе создания комплексной системы защиты информации в ИС разрабатывается документ, который называется "Модель угроз".

Модель угроз - это документ, определяющий перечень и характеристики основных (актуальных) угроз безопасности и уязвимостей при их обработке в ИС, которые должны учитываться в процессе организации защиты информации, проектирования и разработки систем защиты информации, проведения проверок (контроля) защищенности ИС.

Цель разработки модели угроз – определение актуальных для конкретной ИС угроз безопасности, источников угроз и уязвимостей. Результаты моделирования должны использоваться в качестве исходных данных для выработки требований ИБ к разрабатываемой системе защиты (СУИБ).

Подчеркнем, что само понятие «угроза» в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнута открытой организации угроз конфиденциальности может просто не существовать — вся информация считается общедоступной. Однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, угрозы, как и все в ИБ, зависят от интересов субъектов информационных отношений, т. е. владельцев ИС, и от того, какой ущерб является для них неприемлемым.

Угрозы можно классифицировать по нескольким критериям.

- **по аспекту информационной безопасности** (доступность, целостность, конфиденциальность), против которых угрозы направлены в первую очередь;
- **по компонентам информационных систем**, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);

• **по происхождению и способу осуществления** (непреднамеренные/преднамеренные действия природного/техногенного характера);

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

По некоторым данным, до 65% потерь — следствие непреднамеренных ошибок. Пожары и наводнения не приносят столько бед, сколько безграмотность и небрежность в работе.

Очевидно, самый радикальный способ борьбы с непреднамеренными ошибками — максимальная автоматизация и строгий контроль.

• **по расположению источника угроз** (внутренние/внешние).

Внутренние угрозы безопасности объекта защиты:

- неквалифицированная политика по управлению безопасностью корпорации;

- отсутствие должной квалификации персонала по обеспечению деятельности и управлению объектом защиты;

- преднамеренные и непреднамеренные действия персонала по нарушению безопасности и т.д.

Внешние угрозы безопасности объекта защиты:

- негативные воздействия недобросовестных конкурентов и государственных структур;

- преднамеренные и непреднамеренные действия заинтересованных структур и физических лиц (сбор информации, шантаж, искажение имиджа, угрозы физического воздействия и др.);

- утечка конфиденциальной информации из носителей информации и обусловленных каналов связи;

- несанкционированное проникновение на объект защиты;

- несанкционированный доступ к носителям информации и каналам связи с целью хищения, искажения, уничтожения, блокирования информации.

Данный вариант классификации не единственный. Есть другие схемы классификации по другим критериям (по способу доступа, по этапу доступа, по текущему месту расположения информации и т.д.)

В качестве **основного критерия** мы будем использовать первый (по аспекту ИБ), привлекая при необходимости остальные.

Таким образом, **базовые угрозы информационной безопасности** — это нарушение доступности (отказ в обслуживании), нарушение целостности и нарушение конфиденциальности.

2.2 Основные угрозы доступности.

Доступность — это возможность за приемлемое время получить требуемую информационную услугу.

Угрозы доступности данных возникают в том случае, когда объект (пользователь или процесс) не получает доступа к законно выделенным ему службам или ресурсам. В соответствии с определением доступности, лицо, используя ресурсы информационной системы (ИС) по правилам политики безопасности, должно получить информацию в необходимом ему виде, месте и своевременно.

Нарушение доступности реализуется либо по техническим причинам (отказ ИС, отказ поддерживающей инфраструктуры), либо связаны с человеческим фактором (ошибки, саботаж, диверсии, хакерские атаки).

Причинами отказа ИС могут быть:

- нарушения правил эксплуатации;
- перегрузка ИС (например, из-за превышения расчетного числа запросов, превышения объема обрабатываемой информации);
- отказ программного обеспечения ИС;
- выход из строя (либо разрушение) аппаратуры ИС;
- разрушение данных.

Отказами поддерживающей инфраструктуры могут быть:

отказ системы электропитания, системы отопления, системы кондиционирования, системы заземления, разрушение зданий, инженерных сооружений и т.д.

Причинами отказа ИС и поддерживающей инфраструктуры могут быть стихийные бедствия (пожар, ураган, наводнение, землетрясение) и природные явления (удары молнии). По статистике, на долю огня, воды и тому подобных «злоумышленников» (среди которых самый опасный — перебой электропитания) приходится 13% потерь, нанесенных информационным системам.

Весьма опасны так называемые «обиженные» сотрудники нынешние и бывшие. Как правило, они стремятся нанести вред организации «обидчику», например:

- испортить оборудование;
- встроить логическую бомбу, которая со временем разрушит программы и/или данные;
- удалить данные.

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

Некоторые примеры угроз доступности

Угрозы доступности могут выглядеть грубо — как повреждение или даже разрушение оборудования (в том числе носителей данных). Такое повреждение может вызываться естественными причинами (чаще всего — грозами). К сожалению, находящиеся в массовом использовании источники бесперебойного пи-

тания не защищают от мощных кратковременных импульсов, и случаи выгорания оборудования — не редкость.

В принципе, мощный кратковременный импульс, способный разрушить данные на магнитных носителях, можно сгенерировать и искусственным образом — с помощью так называемых высокоэнергетических радиочастотных пушек. Но, наверное, в наших условиях подобную угрозу следует все же признать надуманной.

Действительно опасны протечки водопровода и отопительной системы. Часто организации, чтобы сэкономить на арендной плате, снимают помещения в домах старой постройки, делают косметический ремонт, но не меняют ветхие трубы. В связи с этим возникает угроза затопления.

Летом, в сильную жару, норовят сломаться кондиционеры, установленные в серверных залах, набитых дорогостоящим оборудованием. В результате значительный ущерб наносится и репутации, и кошельку организации.

Общеизвестно, что периодически необходимо производить резервное копирование данных. Однако даже если это предложение выполняется, резервные носители зачастую хранят небрежно (к этому мы еще вернемся при обсуждении угроз конфиденциальности), не обеспечивая их защиту от вредного воздействия окружающей среды. И когда требуется восстановить данные, оказывается, что эти самые носители никак не желают читаться.

Перейдем теперь к угрозам доступности, которые реализуются путем **программных хакерских атак**.

В качестве средства вывода системы из штатного режима эксплуатации может использоваться агрессивное потребление ресурсов (обычно полосы пропускания сетей, вычислительных возможностей процессоров или оперативной памяти). По расположению источника угрозы такое потребление подразделяется на *локальное* и *удаленное*. При просчетах в конфигурации системы локальная программа способна практически монополизировать процессор и/или физическую память, сведя скорость выполнения других программ к нулю.

Простейший пример удаленного потребления ресурсов атака, получившая наименование «SYN-наводнение». Она представляет собой попытку переполнить таблицу «полуоткрытых» TCP-соединений сервера (установление соединений начинается, но не заканчивается). Такая атака, по меньшей мере затрудняет установление новых соединений со стороны легальных пользователей, то есть сервер выглядит как недоступный.

По отношению к атаке «Papa Smurf» уязвимы сети, воспринимающие ping-пакеты с широкоэмитательными адресами. Ответы на такие пакеты «съедают» полосу пропускания.

Удаленное потребление ресурсов в последнее время проявляется в особенно опасной форме — как скоординированные распределенные атаки, когда на сервер с множества разных адресов с максимальной скоростью направляются вполне легальные запросы на соединение и/или обслуживание.

Для вывода систем из штатного режима эксплуатации могут использоваться уязвимые места в виде программных и аппаратных ошибок. Например, известная ошибка в процессоре Pentium 1 дает возможность локальному пользователю путем выполнения определенной команды «подвесить» компьютер, так что помогает только аппаратный REZET.

2.3 Основные угрозы целостности

Под **целостностью** информации подразумевается, ее защищенность от разрушения и несанкционированного изменения.

Угрозы целостности данных, программ, аппаратуры. Целостность данных и программ нарушается при несанкционированном уничтожении, добавлении лишних элементов и модификации записей о состоянии счетов, изменении порядка расположения данных, формировании фальсифицированных платежных документов в ответ на законные запросы, при активной ретрансляции сообщений с их задержкой. Несанкционированная модификация информации о безопасности системы может привести к несанкционированным действиям (неверной маршрутизации или утрате передаваемых данных) или искажению смысла передаваемых сообщений. Целостность аппаратуры нарушается при ее повреждении, похищении или незаконном изменении алгоритмов работы.

Юридически некоторые нарушения целостности квалифицируются как **кражи и подлоги**. Эти нарушения занимают второе место по размерам причиняемого ущерба (после непреднамеренных ошибок и упущений).

По данным газеты USA Today, еще в 1992 году в результате подобных противоправных действий с использованием персональных компьютеров американским организациям был нанесен общий ущерб в размере **882 миллионов долларов**. Можно предположить, что реальный ущерб был намного больше, поскольку многие организации по понятным причинам скрывают такие инциденты; не вызывает сомнений, что в наши дни ущерб от такого рода действий вырос многократно.

В большинстве случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и мерами защиты. Это еще раз подтверждает опасность внутренних угроз, хотя говорят и пишут о них значительно меньше, чем о внешних.

С целью нарушения **статической целостности** злоумышленник (как правило, штатный сотрудник) может:

- ввести неверные данные;
- изменить данные.

Иногда изменяются содержательные данные, иногда — служебная информация.

Показательный случай нарушения целостности имел место в 1996 году. Служащая Ogasle (личный секретарь вице-президента) предъявила судебный иск, обвиняя президента корпорации в незаконном увольнении после того, как она отвергла его ухаживания. В доказательство своей правоты женщина приве-

ла электронное письмо, якобы отправленное ее начальником президенту. Содержание письма для нас сейчас не важно; важно время отправки. Дело в том, что вице-президент предъявил, в свою очередь, файл с регистрационной информацией компании сотовой связи, из которого явствовало, что в указанное время он разговаривал по мобильному телефону, находясь вдалеке от своего рабочего места. Таким образом, в суде состоялось противостояние «файл против файла». Очевидно, один из них был фальсифицирован или изменен, то есть была нарушена его целостность. Суд решил, что подделали электронное письмо (секретарша знала пароль вице-президента, поскольку ей было поручено его менять), и иск был отвергнут...

(Теоретически возможно, что оба фигурировавших на суде файла были подлинными, корректными с точки зрения целостности, а письмо отправили пакетными средствами, однако, на наш взгляд, это было бы очень странное для вице-президента действие.)

Из приведенного случая можно сделать вывод не только об угрозах нарушения целостности, но и об опасности слепого доверия компьютерной информации. Заголовки электронного письма могут быть подделаны; письмо в целом может быть фальсифицировано лицом, знающим пароль отправителя (мы приводили соответствующие примеры). Отметим, что последнее возможно даже тогда, когда целостность контролируется криптографическими средствами.

Здесь имеет место взаимодействие разных аспектов информационной безопасности: *если нарушена конфиденциальность, может пострадать целостность.*

Еще один урок: угрозой целостности является не только фальсификация или изменение данных, но и отказ от совершенных действий. Если нет средств обеспечить "неотказуемость", компьютерные данные не могут рассматриваться в качестве доказательства.

Потенциально уязвимы с точки зрения нарушения целостности не только данные, но и программы. Внедрение вредоносного ПО — пример подобного нарушения.

Угрозами динамической целостности являются нарушение атомарности транзакций, переупорядочение, кража, дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т.п.). Соответствующие действия в сетевой среде называются активным прослушиванием.

2.4 Основные угрозы конфиденциальности

Конфиденциальность — это защита от несанкционированного доступа к информации.

Угрозы конфиденциальности данных и программ реализуются при несанкционированном доступе к данным (например, к сведениям о состоянии счетов клиентов банка), программам или каналам связи. Информация, обрабатываемая на компьютерах или передаваемая по локальным сетям передачи данных, может быть снята через технические каналы утечки. При этом используется аппаратура, осуществляющая анализ электромагнитных излучений, возникающих

при работе компьютера. Такой съём информации представляет собой сложную техническую задачу и требует привлечения квалифицированных специалистов. С помощью приемного устройства, выполненного на базе стандартного телевизора, можно перехватывать информацию, выводимую на экраны дисплеев компьютеров с расстояния в сто и более метров. Определенные сведения о работе компьютерной системы извлекаются даже в том случае, когда ведется наблюдение за процессом обмена сообщениями без доступа к их содержанию.

Конфиденциальную информацию можно разделить на **предметную** и **служебную**. Служебная информация (например, *пароли пользователей*) не относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной.

Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы ее конфиденциальности могут носить некомпьютерный и вообще нетехнический характер.

Многим людям приходится выступать в качестве пользователей не одной, а целого ряда систем (информационных сервисов). Если для доступа к таким системам используются многообразные пароли или иная конфиденциальная информация, то наверняка эти данные будут храниться не только в голове, но и в записной книжке или на листках бумаги, которые пользователь часто оставляет на рабочем столе, а то и попросту теряет. И дело здесь не в неорганизованности людей, а в изначальной непригодности парольной схемы. Невозможно помнить много разных паролей; рекомендации по их регулярной (по возможности — частой) смене только усугубляют положение, заставляя применять несложные схемы чередования или вообще стараться свести дело к двум-трем легко запоминаемым (и столь же легко угадываемым) паролям.

Описанный класс уязвимых мест можно назвать размещением конфиденциальных данных в среде, где им не обеспечена (зачастую — и не может быть обеспечена) необходимая защита. Угроза же состоит в том, что кто-то не откажется узнать секреты, которые сами просятся в руки. Помимо паролей, хранящихся в записных книжках пользователей, в этот класс попадает передача конфиденциальных данных в открытом виде (в разговоре, в письме, по сети), которая делает возможным перехват данных. Для атаки могут использоваться разные технические средства (подслушивание или прослушивание разговоров, пассивное прослушивание сети и т.п.), но идея одна — осуществить доступ к данным в тот момент, когда они наименее защищены.

Угрозу перехвата данных следует принимать во внимание не только при начальном конфигурировании ИС, но и, что очень важно, при всех изменениях. Весьма опасной угрозой являются... выставки, на которые многие организации, недолго думая, отправляют оборудование из производственной сети, со всеми хранящимися на них данными. Остаются прежними пароли, при удаленном доступе они продолжают передаваться в открытом виде. Это плохо даже в пре-

делах защищенной сети организации; в объединенной сети выставки — это слишком суровое испытание честности всех участников.

Еще один пример изменения, о котором часто забывают, — **хранение данных на резервных носителях**. Для защиты данных на основных носителях применяются развитые системы управления доступом. Копии же нередко просто лежат в шкафах, и получить доступ к ним могут многие.

Перехват данных — очень серьезная угроза, и если конфиденциальность действительно является критичной, а данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их, например на кабельную сеть, может кто угодно, так что эту угрозу нужно принимать во внимание по отношению не только к внешним, но и к внутренним коммуникациям.

Кражи оборудования являются угрозой не только для резервных носителей, но и для компьютеров, особенно портативных. Часто ноутбуки оставляют без присмотра на работе или в автомобиле, иногда просто теряют.

Опасной угрозой конфиденциальности являются методы морально-психологического воздействия, такие как **маскарад** — выполнение действий под видом лица, обладающего полномочиями для доступа к данным.

К неприятным угрозам, от которых трудно защищаться, можно отнести **злоупотребление полномочиями**. На многих типах систем привилегированный пользователь (например, системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т.д. Другой пример — нанесение ущерба при сервисном обслуживании. Обычно сервисный инженер получает неограниченный доступ к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

2.5 Вредительские программы

Одним из основных источников угроз безопасности информации в КС является использование специальных программ, получивших общее название «вредительские программы».

В зависимости от механизма действия вредительские программы делятся на четыре класса:

- 1) «логические бомбы»;
- 2) «черви»;
- 3) «троянские кони»;
- 4) «компьютерные вирусы».

«Логические бомбы» — это программы или их части, постоянно находящиеся в ЭВМ или вычислительных системах (ВС) и выполняемые только при соблюдении определенных условий. Примерами таких условий могут быть: наступление заданной даты, переход КС в определенный режим работы, наступление некоторых событий установленное число раз и т.п.

«Червями» называются программы, которые выполняются каждый раз при загрузке системы, обладают способностью перемещаться в ВС или сети и само-

воспроизводить копии. Лавинообразное размножение программ приводит к перегрузке каналов связи, памяти и, в конечном итоге, к блокировке системы.

«Троянские кони» - это программы, полученные путем явного изменения или добавления команд в пользовательские программы. При последующем выполнении пользовательских программ наряду с заданными функциями выполняются несанкционированные, измененные или какие-то новые функции.

«Компьютерные вирусы» - это небольшие программы, которые после внедрения в ЭВМ самостоятельно распространяются путем создания своих копий, а при выполнении определенных условий оказывают негативное воздействие на КС.

Поскольку вирусам присущи свойства всех классов вредительских программ, то в последнее время любые вредительские программы часто называют вирусами.

Таковы основные угрозы, которые наносят наибольший ущерб субъектам информационных отношений.

Тема 3: "Оценочные стандарты в информационной безопасности"

3.1 Роль стандартов ИБ.

Зачем нужны стандарты в области ИБ?

В общем случае стандартом принято называть документ, в котором устанавливаются требуемые характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт может задавать и другие требования — например, к символике или терминологии.

Цель: 1)обеспечение необходимого уровня *качества* продуктов, товаров и услуг;

2)обеспечения *единых характеристик* продуктов, товаров и услуг.

Причиной необходимости использования стандартов является то, что необходимость соблюдения некоторых из них закреплена законодательно. Реальные причины гораздо глубже — обычно стандарт является обобщением опыта лучших специалистов в той или иной области, и потому представляет собой надёжный источник оптимальных и проверенных решений.

Стандартизация в области ИБ необходима по трем основным причинам:

- 1) необходимость выработки **единых требований** по ИБ (единый набор требований);
- 2) необходимость выработки **единых подходов** к решению проблем ИБ;
- 3) необходимость выработки **единых качественных показателей для оценки безопасности ИС** и средств защиты.

Потребители (заказчики) продуктов информационных технологий без стандартов не смогут сформулировать свои требования по ИБ производителям информационных систем (нужны какие-то критерии, показатели, единицы измерения ИБ и т.д.).

Производители продукции ИТ и средств защиты (программных, технических) нуждаются в стандартах для того, чтобы можно было бы объективно оценить свою продукцию с точки зрения обеспечения ИБ, то есть **СЕРТИФИЦИРОВАТЬ** ее. Им также необходим стандартный набор требований для того, чтобы ограничить фантазию заказчика и заставить выбирать конкретные требования из этого набора.

Стандарты нужны экспертам по ИБ и специалистам по сертификации как инструмент для оценки **уровня безопасности**, обеспечиваемого конкретными механизмами и средствами защиты информации (техническими, программными и т.д.) либо комплексами таких средств (КСЗИ).

В настоящее время существует довольно много стандартов, а также других нормативных и руководящих документов в области информационной безопасности. Все их рассмотреть в рамках данного курса не представляется возможным. Поэтому мы будем рассматривать **только базовые** стандарты в области информационной безопасности, которыми руководствуются при создании, сертификации и эксплуатации систем управления информационной безопасностью (СУИБ).

Эти стандарты можно разбить на две группы рис. 1.

1 группа – оценочные стандарты. Они предназначены для оценки и классификации информационных систем и средств защиты информации по требованиям безопасности. Ими руководствуются для того, чтобы ответить на вопрос: ***Соответствует ли ваша ИС и ваши механизмы и средства защиты требованиям безопасности?*** К ним относятся:

1) стандарт «Критерии оценки доверенных компьютерных систем» или разговорное название «Оранжевая книга»;

2) международный стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» или разговорное название «Общие критерии».

2 группа стандартов – это так называемые спецификации. Они регламентируют различные вопросы реализации и использования методов и средств защиты информации. Ими руководствуются для того, чтобы ответить на вопрос: ***Как обеспечить информационную безопасность, какие подходы, какие методы и какие средства необходимо для этого использовать?*** К этим стандартам относятся :

1) рекомендации X.800, «Архитектура безопасности для взаимодействия открытых систем» – регламентирует методы и средства обеспечения ИБ в компьютерных сетях;

2) международный стандарт ISO/IEC 17799 «Практические правила управления информационной безопасностью», разработанный на основе одноименного британского стандарта BS 7799;

3) международный стандарт ISO/IEC 27001:2005 «Системы менеджмента информационной безопасности. Требования».

Далее мы рассмотрим более подробно названные стандарты.

3.2 «Оранжевая книга» как оценочный стандарт.

Стандарт «Критерии оценки доверенных компьютерных систем», более известный как «Оранжевая книга», был разработан Министерством обороны США в 1983 г. и стал первым в истории общедоступным оценочным стандартом в области информационной безопасности.

Требования «Оранжевой книги» имеют следующую структуру:

1. Политика безопасности (совокупность управленческих решений по защите информации и ресурсов).

1.1. Система должна поддерживать точно определённую политику безопасности. Возможность доступа субъектов к объектам должна определяться на основании их идентификации и набора правил управления доступом. По мере необходимости должна использоваться политика мандатного управления доступом.

1.2. С объектами должны быть ассоциированы метки безопасности, используемые в качестве исходной информации для процедур контроля доступа. Для реализации мандатного управления доступом система должна обеспечивать каждому объекту набор атрибутов, определяющих степень конфиденциальности объекта и режимы доступа к этому объекту.

2. Подотчётность

2.1. Все субъекты должны иметь уникальные идентификаторы. Контроль доступа должен осуществляться на основе идентификации субъекта и объекта доступа, аутентификации и правил разграничения доступа. Данные, используемые для идентификации и аутентификации, должны быть защищены от несанкционированного доступа, модификации и уничтожения и должны быть ассоциированы со всеми активными компонентами компьютерной системы, функционирование которых критично с точки зрения безопасности.

2.2. Для определения степени ответственности пользователя за действия в системе, все происходящие в ней события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищённом протоколе. Система регистрации должна осуществлять анализ общего потока событий и выделять из него только те события, которые оказывают влияние на безопасность. Протокол событий должен быть надёжно защищён от несанкционированного доступа, модификации и уничтожения.

3. Гарантии

3.1. Средства защиты должны содержать независимые аппаратные или программные компоненты, обеспечивающие работоспособность функций защиты. Это означает, что все средства защиты, обеспечивающие политику безопасности, управление атрибутами и метками безопасности, регистрацию и учёт, должны находиться под контролем средств, проверяющих корректность их функционирования. Средства контроля должны быть полностью независимы от средств защиты.

3.2. Все средства защиты должны быть защищены от несанкционированного вмешательства и отключения, причём эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и инфор-

мационной системы в целом. Данное требование распространяется на весь жизненный цикл информационной системы.

Напомним, что «Оранжевая книга» является оценочным стандартом — а значит, предназначена в первую очередь для проведения анализа защищенности информационных систем. По результатам такого анализа ИС должна быть отнесена к одному из определённых в документе классов защищённости.

«Оранжевая книга» определяет четыре группы классов защищённости:

A — содержит единственный класс A1.

B — содержит классы B1, B2 и B3.

C — содержит классы C1 и C2.

D — содержит единственный класс D1.

Требуемый уровень защищенности системы возрастает от группы D к группе A, а в пределах одной группы — с увеличением номера класса. Каждый класс характеризуется определённым фиксированным набором требований к подсистеме обеспечения информационной безопасности, реализованной в ИС.

Приведём краткие характеристики каждого из классов защищенности.

1. Группа D — минимальная защита.

К данной категории относятся те системы, которые были представлены для сертификации по требованиям одного из более высоких классов защищенности, но не прошли испытания.

2. Группа C — дискреционная защита.

данная группа характеризуется наличием дискреционного управления доступом и регистрации действий субъектов.

- Класс C1 — дискреционная защита.

Система включает в себя средства контроля и управления доступом, позволяющие задавать ограничения для отдельных пользователей. Класс C1 рассчитан на однопользовательские системы, в которых осуществляется совместная обработка данных одного уровня конфиденциальности.

- Класс C2 — управление доступом

Система обеспечивает более избирательное управление доступом путём применения средств индивидуального контроля за действиями пользователей, регистрации, учёта событий и выделения ресурсов.

3. Группа B — мандатная защита

Система обеспечивает мандатное управление доступом с использованием меток безопасности, поддержку модели и политики безопасности. Предполагается наличие спецификаций на функции ядра безопасности. Реализуется концепция монитора безопасности обращений, контролирующего все события в системе.

- Класс B1 — защита с применением меток безопасности

Помимо выполнения всех требований к классу C2, система должна поддерживать маркировку данных и мандатное управление доступом. При экспорте из системы информация должна подвергаться маркировке.

- Класс B2 — структурированная защита

Ядро безопасности должно поддерживать формально определенную и четко документированную модель безопасности, предусматривающую дискреционное и мандатное управление доступом, которое распространяется на все субъекты. Должен осуществляться контроль скрытых каналов передачи информации. В структуре ядра безопасности должны быть выделены элементы, критичные с точки зрения безопасности. Интерфейс ядра безопасности должен быть четко определен, а его архитектура и реализация должны быть выполнены с учётом возможности проведения тестовых испытаний. Управление безопасностью должно осуществляться администратором безопасности.

- Класс ВЗ — домены безопасности

Ядро безопасности должно поддерживать монитор безопасности обращений, который контролирует все типы доступа субъектов к объектам и который невозможно обойти. Ядро безопасности содержит исключительно подсистемы, отвечающие за реализацию функций защиты, и является достаточно компактным для обеспечения возможности эффективного тестирования. Средства аудита должны включать механизмы оповещения администратора о событиях, имеющих значение для безопасности системы. Необходимо наличие средств восстановления работоспособности системы.

4. Группа А — верифицированная защита

Группа характеризуется применением формальных методов верификации корректности функционирования механизмов управления доступом. Требуется дополнительная документация, демонстрирующая, что архитектура и реализация ядра безопасности отвечает требованиям безопасности. Функциональные требования совпадают с классом ВЗ, однако на всех этапах разработки ИС требуется применение формальных методов верификации систем защиты.

Разработка и публикация «Оранжевой книги» стали важнейшей вехой в становлении теории информационной безопасности. Такие базовые понятия, как «политика безопасности», «монитор безопасности обращений» или «администратор безопасности» впервые в открытой литературе появились именно в «Оранжевой книге».

В то же время с течением времени стали проявляться многочисленные недостатки «Оранжевой книги» и предложенного подхода к классификации ИС в целом. Во многом её устаревание было связано с принципиальными изменениями аппаратной базы средств вычислительной техники, произошедшими с 1983 г. — и прежде всего, с распространением распределённых вычислительных систем и сетей, особенности которых в «Оранжевой книге» никак не учитываются.

Стараясь не отстать от развивающихся информационных технологий, разработчики «Оранжевой книги» вплоть до 1995 г. выпустили целый ряд вспомогательных документов, известных как «Радужная серия». Эти документы содержали рекомендации по применению положений «Оранжевой книги» для различных категорий информационных систем, а также вводили ряд дополнительных требований. Наибольший интерес в «Радужной серии» представля-

ют три документа: «Интерпретация для защищённых сетей», «Интерпретация для защищённых СУБД» и «Руководство по управлению паролями».

В настоящее время «Оранжевая книга» не используется для оценки информационных систем и представляет интерес исключительно с исторической точки зрения.

3.3 Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.

Как для «Оранжевой книги», так и для аналогичных ей руководящих документов, характерны многочисленные недостатки. Перечислим наиболее существенные из них:

- документы ориентированы на обеспечение защиты информации от угроз нарушения конфиденциальности и, в определенной степени, целостности. Угрозы нарушения доступности практически не рассматриваются.

- Используемый «табличный» подход не позволяет учесть специфику конкретных систем или продуктов, в том числе порядок обработки информации в информационной системе.

- Документы содержат перечень механизмов, наличие которых необходимо для отнесения ИС к тому или иному классу защищенности. При этом совершенно не оговорены методы проверки корректности и адекватности реализации функциональных требований.

- Формулировки ряда требований чрезвычайно туманны и допускают неоднозначную интерпретацию.

В целом, «Оранжевая книга», как и все другие оценочные стандарты первого поколения, создавались для давно ушедшей в прошлое материально-технической базы и по целому ряду аспектов являются морально устаревшими.

Стандарт ISO/IEC 15408 был разработан совместными усилиями специалистов Канады, США, Великобритании, Германии, Нидерландов и Франции в период с 1990 по 1999 год, развитие стандарта непрерывно продолжается. Исторически за стандартом закрепилось разговорное название «Общие критерии».

В России перевод «Общих критериев» версии 2.0 принят в качестве ГОСТа в 2002 году и введен в действие с 1 января 2004 г.

«Общие критерии» предназначены служить основой при оценке характеристик безопасности продуктов и систем ИТ. Заложенные в стандарте наборы требований позволяют сравнивать результаты независимых оценок безопасности. На основании этих результатов потребитель может принимать решение о том, ***достаточно ли безопасны ИТ-продукты или системы для их применения с заданным уровнем риска.***

Стандарт ГОСТ Р ИСО/МЭК 15408 состоит из трех частей.

В первой части (ГОСТ Р ИСО/МЭК 15408-1 «Введение и общая модель») устанавливается общий подход к формированию требований безопасности и оценке безопасности, на их основе разрабатываются основные конструкции (профиль защиты и задание по безопасности) представления требований безо-

пасности в интересах потребителей, разработчиков и оценщиков продуктов и систем ИТ. Требования безопасности объекта оценки (ОО) по методологии «Общих критериев» определяются исходя из целей безопасности, которые основываются на анализе назначения ОО и условий среды его использования (угроз, предположений, политики безопасности).

Часть вторая (ГОСТ Р ИСО/МЭК 15408-2 «Функциональные требования безопасности») содержит универсальный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определенным правилам.

Третья часть (ГОСТ Р ИСО/МЭК 15408-3 «Требования доверия к безопасности») включает в себя систематизированный каталог требований доверия, определяющих меры, которые должны быть приняты **на всех этапах жизненного цикла продукта или системы ИТ** для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям. Здесь же содержатся оценочные уровни доверия (ОУД), определяющие шкалу требований, которые позволяют с возрастающей степенью полноты и строгости оценить проектную, тестовую и эксплуатационную документацию, правильность реализации функций безопасности ОО, уязвимости продукта или системы ИТ, стойкость механизмов защиты и сделать заключение об уровне доверия к безопасности объекта оценки.

Обобщая вышесказанное, можно отметить, что каркас безопасности, заложенный частью 1 стандарта ГОСТ Р ИСО/МЭК 15408, заполняется содержанием из классов, семейств и компонентов в части 2, а третья часть определяет, как оценить прочность всего «строения».

Стандарт «Общие критерии безопасности информационных технологий» отражает достижения последних лет в области информационной безопасности. Впервые документ такого уровня содержит разделы, адресованные потребителям, производителям и экспертам по оценке безопасности ИТ-продуктов.

В перспективе «Общие критерии» должны заменить руководящие документы во всех системах сертификации средств защиты информации. В настоящий момент в России «Общие критерии» используются одновременно с РД Гостехкомиссии, причём «Общие критерии» применяются исключительно при проведении сертификации продуктов, не предназначенных для обработки информации, составляющей государственную тайну.

Основные идеи «Общих критериев»

Основное свойство «Общих критериев» (ОК) - это максимально возможная универсальность: под объектом оценки (ОО) понимается произвольный продукт информационных технологий или система с руководствами администратора и пользователя.

Продукт рассматривается как совокупность программных, программно-аппаратных или аппаратных средств информационных технологий, предоставляющая определённые функциональные возможности и предназначенная для непосредственного использования или включения в состав различных систем.

В свою очередь, **система** — это специфическое воплощение информационных технологий с конкретным назначением и условиями эксплуатации.

Предполагается, что общие критерии могут быть использованы следующими категориями пользователей:

1. Потребители.

ОК позволяют определить, вполне ли оцениваемый продукт или система удовлетворяют их потребностям в безопасности.

2. Разработчики

ОК могут быть использованы для формирования утверждения о соответствии объекта оценки установленным требованиям.

3. Оценщики

Стандарт может быть использован при формировании заключения о соответствии ОО предъявляемым к ним требованиям безопасности.

Объект оценки рассматривается в контексте среды безопасности, в которую включаются:

- ***законодательная среда*** — законы и нормативные акты, затрагивающие ОО;
- ***административная среда*** — положения политик безопасности, затрагивающих ОО и учитывающих его особенности;
- ***процедурная среда*** — меры физической защиты, персонал и его специфика;
- ***программно-техническая среда*** — назначение ОО, предполагаемые области его применения.

При подготовке к оценке формализуются следующие **аспекты среды ОО**:

1. Предположения безопасности

Предположения выделяют ОО из общего контекста и задают границы его рассмотрения. Предполагается, что среда ОО удовлетворяет данным предположениям. Иными словами предполагается, что объект оценки будет использоваться в нормальных условиях (а не в условиях боевых действий) и требования относительно среды безопасности соблюдены. При проведении оценки предположения безопасности принимаются без доказательств.

2. Угрозы безопасности

Выделяются угрозы, наличие которых в рассматриваемой среде установлено или предполагается. Угроза характеризуется следующими параметрами:

- источник угрозы;
- предполагаемый способ реализации угрозы;
- уязвимости, которые являются предпосылкой для реализации угрозы;
- активы, которые являются целью нападения;
- нарушаемые свойства безопасности активов;
- возможные последствия реализации угрозы.

3. Политика безопасности

Излагаются положения политики безопасности, применяемые в организации, которые имеют непосредственное отношение к ОО.

На основании сформулированных предположений безопасности, при учёте угроз и политик формулируются **цели безопасности** для ОО, направленные на обеспечение противостояния угрозам и выполнение положений политики безопасности.

Для достижения поставленных целей к ОО и его среде предъявляются требования безопасности.

Вторая и третья части «Общих критериев» представляют собой каталоги требований безопасности двух типов: функциональных и доверия.

- **Функциональные требования безопасности** (Часть 2) — предъявляются к функциям безопасности ОО и реализующим их механизмам. Функциональные требования относятся к сервисам безопасности, таким как идентификация, аутентификация, управление доступом, аудит и т.д.

- **Требования доверия** (Часть 3) — предъявляются к технологии разработки, тестированию, анализу уязвимостей, поставке, сопровождению, эксплуатационной документации и т.д.

Описание обоих типов требований выполнено в едином стиле: они организованы в иерархию "класс - семейство - компонент - элемент". Термин "класс" используется для наиболее общей группировки требований безопасности, а элемент - самый нижний, неделимый уровень требований безопасности.

При формулировании требований к ОО могут быть разработаны два документа:

1. Профиль защиты — типовой набор требований для некоторой категории ОО. Профиль защиты определяется как "независимая от реализации совокупность требований безопасности для некоторой категории ОО, отвечающая специфическим запросам потребителя".

Профиль защиты (ПЗ) не привязан к конкретному ОО и представляет собой обобщенный стандартный набор функциональных требований и требований доверия для определенного класса продуктов или систем. Например, может быть разработан профиль защиты на межсетевой экран корпоративного уровня, на операционную систему для правительственных организаций, и т.д.

2. Задание по безопасности — документ, содержащий требования безопасности для конкретной разработки, выполнение которых обеспечивает достижение поставленных целей безопасности. В задании по безопасности (ЗБ) может быть заявлено соответствие одному или нескольким профилям защиты.

ЗБ можно рассматривать как техническое задание на подсистему обеспечения информационной безопасности для ОО.

Задание по безопасности служит основой для проведения оценки ОО с целью демонстрации соответствия его требованиям безопасности.

При проведении оценки изделия ИТ главными являются следующие вопросы:

- 1) отвечают ли функции безопасности ОО функциональным требованиям?
- 2) корректна ли реализация функций безопасности?
- Если оба ответа положительны, можно говорить о достижении целей.

Тема 4: "Стандарты управления информационной безопасностью"

4.1 Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения

Информационная безопасность представляет собой проблему высокой сложности. Обеспечение информационной безопасности нуждается в комплексном подходе к разработке средств защиты, как на техническом, так и на организационном уровне.

ИБ не может быть обеспечена разовым мероприятием, например, покупкой конкретного набора средств защиты. Арсенал средств защиты нуждается в постоянном обновлении, поскольку новые угрозы и новые уязвимости все время появляются в процессе жизненного цикла ИС. Данное обстоятельство вынуждает рассматривать обеспечение ИБ как постоянный процесс, который принято называть ***процессом управления информационной безопасностью***.

Несколько лет назад Британский Институт Стандартов (BSI) при поддержке группы коммерческих организаций приступил к разработке стандарта управления информационной безопасностью, который потом получил название BS 7799.

При разработке стандарта ставилась ***задача обеспечения государственных и коммерческих организаций инструментом для создания эффективных систем информационной безопасности на основе современных методов управления***. В 2000 году этот стандарт был признан международным под названием "Международный стандарт ISO/IEC 17799. «Информационные технологии — Управление информационной безопасностью».

Стандарт ISO/IEC 17799 — это модель системы управления, которая определяет общую организацию, классификацию данных, системы доступа, направления планирования, ответственность сотрудников, использование оценки риска и т.п. в контексте информационной безопасности. В процессе внедрения стандарта создается так называемая система управления (управления) информационной безопасности, цель которой — сокращение материальных потерь, связанных с нарушением информационной безопасности. ***Основная идея стандарта*** — помочь коммерческим и государственным хозяйственным организациям решить достаточно сложную задачу: не только обеспечить надежную защиту информации, но также организовать эффективный доступ к данным и нормальную работу с ними.

Структура стандарта позволяет выбрать те средства управления, которые имеют отношение к конкретной организации или сфере ответственности

внутри организации. Содержание стандарта включает следующие разделы (рис. 1):

- политика безопасности;
- организация защиты;
- классификация ресурсов и контроль;
- безопасность персонала;
- физическая безопасность и безопасность окружающей среды;
- администрирование компьютерных систем и вычислительных сетей;
- управление доступом к системе;
- разработка и сопровождение информационных систем;
- планирование непрерывной работы организации;
- выполнение требований (соответствие законодательству).

В связи с этим выделяется ряд ключевых элементов управления, которые представляются как фундаментальные:

- политика информационной безопасности;
- распределение ответственности за информационную безопасность;
- образование и тренинг по информационной безопасности;
- отчетность за инциденты по безопасности;
- защита от вирусов;
- обеспечение непрерывности работы;
- контроль копирования лицензионного программного обеспечения;
- защита архивной документации организации;
- защита персональных данных;
- реализация политики информационной безопасности.

Как видно, наряду с элементами управления для компьютеров и компьютерных сетей, стандарт уделяет большое внимание вопросам разработки политики безопасности, работе с персоналом (прием на работу, учебу, освобождение от работы), обеспечению непрерывности производственного процесса, юридическим требованиям.

Безусловно, что не все 109 пунктов стандарта можно применять в условиях абсолютно каждой организации. Поэтому авторами стандарта был выбран подход, при котором стандарт используется как некоторое "меню", из которого следует выбрать элементы, которые можно применить для конкретных условий. Этот выбор осуществляется на основе оценки риска и тщательным образом обосновывается.

Риск определяется как произведение показателя возможных потерь (ущерба) на вероятность того, что эта потеря произойдет. Под потерями понимают материальные потери, связанные с нарушением следующих свойств информационного ресурса:

- конфиденциальность — защищенность информации от несанкционированного доступа;
- целостность — защищенность информации от несанкционированного изменения, обеспечения ее точности и полноты;

- доступности — возможность использования информации, когда в этом возникает необходимость, работоспособность системы.

Стандарт не сосредотачивается только на обеспечении конфиденциальности.

В коммерческих организациях, с точки зрения материальных потерь, вопросы целостности и доступности чаще всего более весомые. В упрощенном виде анализ риска сводится к ответам на следующие вопросы:

- Что может угрожать информационным ресурсам?
- Какова уязвимость этим угрозам, то есть, что может произойти с тем или другим информационным ресурсом?
- Если это произойдет, то насколько тяжелыми будут последствия? Какие возможны убытки?
- Как часто следует ожидать подобные случаи?

В настоящее время, разработана следующая версия данного стандарта.

4.2. Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасностью. Требования"

Информационная безопасность тесно связана с работой бизнеса, его конкурентоспособностью, успешностью имиджа предприятия и, в конечном итоге, доходами компании. Лучшей мировой практикой в области управления информационной безопасностью признан стандарт ISO/IEC 27001:2005.

Область применения

Все виды организаций (например, коммерческие и некоммерческие организации, правительственные организации)

Определяет требования к средствам контроля безопасности, специально разработанные для нужд организации, или ее части.

Цель - выбор адекватных и соразмерных средств контроля ИБ, которые защищают информационные активы и предоставляют уверенность заинтересованным сторонам.

Назначение:

Устанавливает требования к системе управления информационной безопасности для демонстрации способности организации защищать свои информационные ресурсы.

Основа стандарта ИСО 27001 - система управление рисками, связанными с информацией.

Система управления рисками позволяет получать ответы на следующие вопросы:

- На каком направлении информационной безопасности требуется сосредоточить внимание?
- Сколько времени и средств можно потратить на данное техническое решение для защиты информации?

Менеджмент рисков происходит по классической схеме: поиск, классификация, ранжирование, оценка, план по снижению рисков, принятие остаточных рисков и регулярный пересмотр рисков.

Общие положения стандарта:

Данный Стандарт определяет информационную безопасность как: "сохранение конфиденциальности, целостности и доступности информации; кроме того, могут быть включены и другие свойства, такие как подлинность, невозможность отказа от авторства, достоверность".

Основной задачей информационной безопасности является защита информационных ресурсов компании от внутренних и внешних умышленных и неумышленных угроз (подделка, вандализм, кража, пожар, системный сбой и др.).

Целью информационной безопасности является обеспечение непрерывности бизнеса компании и минимизация бизнес-рисков путем предупреждения инцидентов безопасности и уменьшения размеров потенциального ущерба.

Стандарт определяет следующие аспекты информационной безопасности:

- Конфиденциальность - обеспечение доступности информации только для тех, кто имеет соответствующие полномочия (авторизированные пользователи);
- Целостность - обеспечение точности и полноты информации, а также методов ее обработки;
- Доступность - обеспечение доступа к информации авторизованным пользователям, когда это необходимо (по требованию).

Структура стандарта

Общие положения:

1. Область применения
2. Нормативные ссылки
3. Термины и определения
4. Система информационной безопасности
5. Обязательства руководства
6. Внутренние аудиты системы управления
7. Анализ системы управления информационной безопасностью руководством
8. Совершенствование системы управления информационной безопасностью

Процессный подход

Стандарт декларирует два основных принципа управления:

1 Процессный подход к управлению безопасностью, который рассматривает управление как процесс – набор взаимосвязанных непрерывных действий,

акцентирует внимание на достижении поставленных целей, а также ресурсах, затраченных для достижения целей.

2. Применение PDCA – модели как основы для всех процедур управления ИБ. PDCA – модель (или модель Шухарта-Деминга) определяет четыре этапа, которые должны выполняться последовательно для каждого процесса.

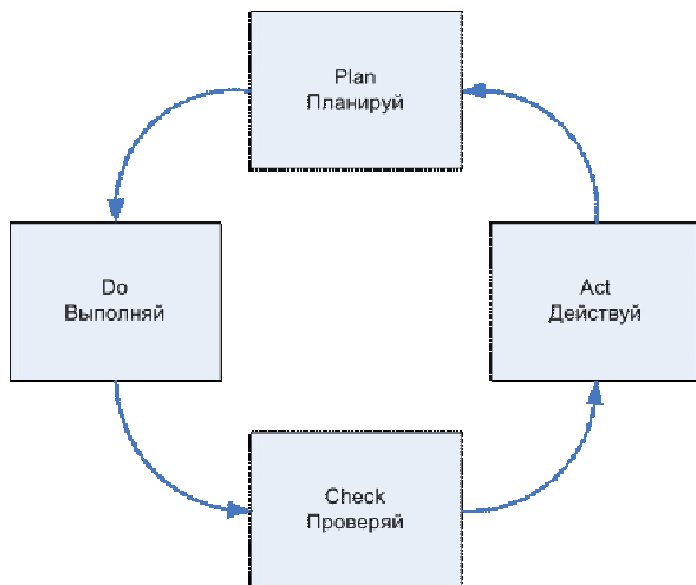


Рис. 4 Применение PDCA

Создание и эксплуатация СУИБ требует применения такого же подхода, как и любая другая система управления. Используемая в ISO 27001 для описания СУИБ процессная модель предусматривает непрерывный цикл мероприятий: планирование, реализация, проверка, действие (ПРПД).

Процессная модель включает 4 группы процессов:

1) Планирование. 2) Реализация. 3) Проверка. 4) Действие.

На стадии планирования обеспечивается правильное задание контекста и масштаба СУИБ, оцениваются риски информационной безопасности, предлагается соответствующий план обработки этих рисков. В свою очередь, на стадии реализации внедряются принятые решения, которые были определены на стадии планирования. На стадиях проверки и действия усиливают, исправляют и совершенствуют решения по безопасности, которые уже были определены и реализованы.

Этапы создания СУИБ

В соответствии с процессной моделью, стандарт определяет 4 этапа создания СУИБ.

1. На этапе "***Разработка системы управления информационной безопасностью***" организация должна осуществить следующее:

1) определить область и границы действия СУИБ;

- 2) определить политику СУИБ на основе характеристик бизнеса, организации, ее размещения, активов и технологий;
- 3) определить подход к оценке риска в организации;
- 4) идентифицировать риски;
- 5) проанализировать и оценить риски;
- 6) определить и оценить различные варианты обработки рисков;
- 7) выбрать цели и меры управления для обработки рисков;
- 8) получить утверждение руководством предполагаемых остаточных рисков;
- 9) получить разрешение руководства на внедрение и эксплуатацию СУИБ;
- 10) подготовить Положение о применимости.

2. Этап "Внедрение и функционирование системы управления информационной безопасностью" предполагает, что организация должна выполнить следующее:

- 1) разработать план обработки рисков, определяющий соответствующие действия руководства, ресурсы, обязанности и приоритеты в отношении управления рисками ИБ;
- 2) реализовать план обработки рисков для достижения намеченных целей управления, включающий в себя вопросы финансирования, а также распределение функций и обязанностей;
- 3) внедрить выбранные меры управления;
- 4) определить способ измерения результативности выбранных мер управления;
- 5) реализовать программы по обучению и повышению квалификации сотрудников;
- 6) управлять работой СУИБ;
- 7) управлять ресурсами СУИБ;
- 8) внедрить процедуры и другие меры управления, обеспечивающие быстрое обнаружение событий ИБ и реагирование на инциденты, связанные с ИБ.

3. Третий этап "Проведение мониторинга и анализа системы управления информационной безопасностью" требует:

- 1) выполнять процедуры мониторинга и анализа;
- 2) проводить регулярный анализ результативности СУИБ;
- 3) измерять результативность мер управления для проверки соответствия требованиям ИБ;
- 4) пересматривать оценки рисков через установленные периоды времени, анализировать остаточные риски и установленные приемлемые уровни рисков, учитывая изменения;
- 5) проводить внутренние аудиты СУИБ через установленные периоды времени;
- 6) регулярно проводить руководством организации анализ СУИБ в целях подтверждения адекватности ее функционирования и определения направлений совершенствования;
- 7) обновлять планы ИБ с учетом результатов анализа и мониторинга;

- 8) регистрировать действия и события, способные повлиять на результативность или функционирование СУИБ.

4. И наконец, *этап "Поддержка и улучшение системы управления информационной безопасностью"* предполагает, что организация должна регулярно проводить следующие мероприятия:

- 1) выявлять возможности улучшения СУИБ;
- 2) предпринимать необходимые корректирующие и предупреждающие действия, использовать на практике опыт по обеспечению ИБ, полученный как в собственной организации, так и в других организациях;
- 3) передавать подробную информацию о действиях по улучшению СУИБ всем заинтересованным сторонам, при этом степень ее детализации должна соответствовать обстоятельствам и, при необходимости, согласовывать дальнейшие действия;
- 4) обеспечивать внедрение улучшений СУИБ для достижения запланированных целей.

Далее в стандарте приводятся требования к документации, которая в частности должна включать положения политики СУИБ и описание области функционирования, описание методики и отчет об оценке рисков, план обработки рисков, документирование связанных процедур. Также должен быть определен процесс управления документами СУИБ, включающий актуализацию, использование, хранение и уничтожение.

Для предоставления свидетельств соответствия требованиям и результативности функционирования СУИБ необходимо вести и поддерживать в рабочем состоянии учетные записи и записи о выполнении процессов. В качестве примеров называются журналы регистрации посетителей, отчеты о результатах аудита и т.п.

Стандарт определяет, что руководство организации ответственно за обеспечение и управление ресурсами, необходимыми для создания СУИБ, а также организацию подготовки персонала.

Как уже ранее отмечалось, организация должна в соответствии с утвержденным графиком проводить внутренние аудиты СУИБ, позволяющие оценить ее функциональность и соответствие стандарту. А руководство должно проводить анализ системы управления информационной безопасностью.

Также должны проводиться работы по улучшению системы управления информационной безопасностью: повышению ее результативности и уровня соответствия текущего состояния системы и предъявляемым к ней требованиям.

В приложении к стандарту перечисляются рекомендуемые меры управления, взятые из ранее рассмотренного стандарта ISO/IEC 17799:2005.

Наряду с элементами управления для компьютеров и компьютерных сетей, стандарт уделяет большое внимание вопросам разработки политики безопасности, работе с персоналом (прием на работу, обучение, увольнение с рабо-

ты), обеспечению непрерывности производственного процесса, юридическим требованиям.

4.3 Сертификация СУИБ на соответствие ISO 27001

Для подтверждения соответствия существующей в организации СУИБ требованиям стандарта, а также ее адекватности существующим бизнес рискам используется процедура добровольной сертификации.

ISO 27001:2005 является стандартом, по которому проводится официальная сертификация СУИБ. Стандарт представляет собой перечень требований, обязательных для сертификации.

Под сертификацией системы управления информационной безопасностью (СУИБ) организации по требованиям стандарта ISO 27001:2005 понимается комплекс организационно-технических мероприятий, проводимых независимыми экспертами, в результате чего подтверждается наличие и надлежащее функционирование всех рекомендуемых стандартом механизмов контроля, применимых в данной организации.

Хотя без этого можно и обойтись, в большинстве случаев сертификация полностью оправдывает вложенные средства и время.

Во-первых, официальная регистрация СУИБ организации в реестре авторитетных органов, таких как служба аккредитации Великобритании (UKAS), что укрепляет имидж компании, повышает интерес со стороны потенциальных клиентов, инвесторов, кредиторов и спонсоров.

Во-вторых, в результате успешной сертификации расширяется сфера деятельности компании за счет получения возможности участия в тендерах и развития бизнеса на международном уровне. В наиболее чувствительных к уровню информационной безопасности областях, такой, например, как финансы, наличие сертификата соответствия ISO 27001 начинает выступать как обязательное требование для осуществления деятельности. Некоторые российские компании уже сталкиваются с этими ограничениями.

Также очень важно, что процедура сертификации оказывает серьезное мотивирующее и мобилизующее воздействие на персонал компании: повышается уровень осведомленности сотрудников, эффективнее выявляются и устраняются недостатки и несоответствия в системе управления информационной безопасностью, что в перспективе означает для организации снижение средне-статистического ущерба от инцидентов безопасности, а также сокращение накладных расходов на эксплуатацию информационных систем. Вполне возможно, наличие сертификата позволит застраховать информационные риски организации на более выгодных условиях.

Как свидетельствует текущая практика, расходы на сертификацию в большинстве случаев несопоставимо малы в сравнении с затратами организации на обеспечение информационной безопасности, а получаемые преимущества многократно их компенсируют.

Следует подчеркнуть, что все перечисленные преимущества организация получает только в том случае, если речь идет о системе сертификации,

имеющей международное признание, в рамках которой обеспечивается надлежащее качество проведения работ и достоверность результатов.

Для получения сертификата система управления информационной безопасности предприятия оценивается аудитором. Аудит состоит из анализа документации по системе управления информационной безопасностью, а также выборочного контроля в организации, который позволяет удостовериться, что реальная практика отвечает описанию системы.

Аккредитованную сертификацию могут осуществлять лишь те сертификационные общества, которые прошли аккредитацию ISO. Сертификат, выданный такой организацией, признается на международном уровне.

Сертификация на соответствие стандарту ISO 27001:2005 позволяет наглядно показать деловым партнерам, инвесторам и клиентам, что в компании налажено эффективное управление информационной безопасностью. В свою очередь это обеспечивает компании конкурентное преимущество, демонстрируя способность управлять информационными рисками, при этом также увеличивается капитализация компании.

Выгоды внедрения системы управления информационной безопасностью по требованиям стандарта ISO/IEC 27001:2005

Система управления информационной безопасностью на основе стандарта ISO 27001 позволит:

Сделать большинство информационных активов наиболее понятными для управления компании.

Выявлять основные угрозы безопасности для существующих бизнес-процессов.

Рассчитывать риски и принимать решения на основе бизнес-целей компании.

Обеспечить эффективное управление системой в критичных ситуациях.

Проводить процесс выполнения политики безопасности (находить и исправлять слабые места в системе информационной безопасности).

Четко определить личную ответственность.

Достигнуть снижения и оптимизации стоимости поддержки системы безопасности.

Продемонстрировать клиентам, партнерам, владельцам бизнеса свою приверженность к информационной безопасности.

Получить международное признание и повышение авторитета компании, как на внутреннем рынке, так и на внешних рынках.

Подчеркнуть прозрачность и чистоту бизнеса перед законом благодаря соответствию стандарту.

Тема 5: "Создание СУИБ на предприятии"

5.1. Этапы создания системы управления ИБ

Для начала отметим, что создание СУИБ на предприятии и подготовка к ее сертификации на соответствие требованиям стандарта ISO27001, как правило, делится на два основных этапа:

- разработку системы управления (и всех необходимых процедур);
- внедрение системы управления.

Для выполнения первого этапа рекомендуется приглашать консультантов. Второй этап (внедрение) выполняется самой компанией (специалисты компании должны ознакомиться с необходимыми процедурами, наладить их четкое выполнение, проверять и контролировать их эффективность и пр.).

Можно выделить следующие **основные этапы разработки** системы управления ИБ:

- 1) инвентаризация активов;
- 2) категорирование активов;
- 3) оценка защищенности информационной системы;
- 4) оценка информационных рисков;
- 5) обработка информационных рисков (в том числе определение конкретных мер для защиты ценных активов);
- 6) внедрение выбранных мер обработки рисков;
- 7) контроль выполнения и эффективности выбранных мер.

Роль руководства компании в системе управления ИБ

Одним из основных условий эффективного функционирования системы управления ИБ является вовлеченность руководства компании в процесс управления ИБ. Все сотрудники должны понимать, что, во-первых, вся деятельность по обеспечению ИБ инициирована руководством и обязательна для выполнения, во-вторых, руководство компании лично контролирует функционирование системы управления ИБ, в-третьих, само руководство выполняет те же правила по обеспечению ИБ, что и все сотрудники компании.

Выбор области сертификации

Систему управления ИБ, как правило, целесообразно разрабатывать для всей компании в целом. Другими словами, процедуры системы управления в большинстве случаев необходимы для выполнения во всей компании. Однако внедрить систему управления сразу во все бизнес-процессы часто непросто, поэтому лучше, если ее внедрение будет осуществляться последовательно. Таким образом, внедрив систему управления в каком-то одном бизнес-процессе компании, мы можем получить сертификат на нее в рамках данного бизнес-процесса, а затем расширять область сертификации по мере внедрения в остальные процессы компании. Следовательно, при подготовке к сертификации требуется определить область сертификации (описать, в какой конкретно под-

системе компании будет внедрена система управления). Аудиторы сертификационных органов проверяют выполнение всех процедур системы управления только в рамках выбранной области сертификации.

Важно иметь в виду, что описание области сертификации необходимо выполнить максимально подробно, то есть требуется точно определить активы, входящие в область сертификации.

2. Содержание этапов разработки и внедрения системы управления ИБ.

1. Инвентаризация активов компании

Прежде всего, следует определить, что является ценным активом компании с точки зрения информационной безопасности. Стандарт ISO 17799, подробно описывающий процедуры системы управления ИБ, выделяет следующие виды активов:

- информационные ресурсы (базы и файлы данных, контракты и соглашения, системная документация, научно-исследовательская информация, документация, обучающие материалы и пр.);
- программное обеспечение,
- материальные активы (компьютерное оборудование, средства телекоммуникаций и пр.);
- сервисы (поддерживающая инфраструктура);
- сотрудники компании, их квалификация и опыт,
- нематериальные ресурсы (репутация и имидж компании).

Следует определить, нарушение информационной безопасности, каких активов может нанести ущерб компании. В этом случае актив будет считаться ценным, и его необходимо будет учитывать при анализе информационных рисков.

Инвентаризация заключается в составлении перечня ценных активов компании. Как правило, данный процесс выполняют владельцы активов.

5.2 Категорирование активов компании

В процессе категорирования активов необходимо оценить их критичность для бизнес-процессов компании или, другими словами, определить, какой ущерб понесет компания в случае нарушения информационной безопасности активов.

Данный процесс вызывает наибольшую сложность, так как ценность активов определяется на основе экспертных оценок их владельцев. В процессе данного этапа часто проводятся обсуждения между консультантами по разработке системы управления и владельцами активов. Это помогает последним понять, каким образом следует определять ценность активов с точки зрения информационной безопасности (как правило, процесс определения критичности активов является для владельца новым и нетривиальным). Кроме этого, для владельцев активов разрабатываются различные методики оценки. В частно-

сти, такие методики могут содержать конкретные критерии (актуальные для данной компании), которые следует учитывать при оценке критичности.

Оценка критичности активов выполняется по трем параметрам: конфиденциальности, целостности и доступности (следует оценить ущерб, который понесет компания при нарушении конфиденциальности, целостности или доступности активов).

Оценку критичности активов можно выполнять в денежных единицах и в уровнях. Однако, учитывая тот факт, что для анализа информационных рисков необходимы значения в денежных единицах, в случае оценки критичности активов в уровнях, следует определить оценку каждого уровня в деньгах. Например, для базовой оценки рисков достаточно 3-уровневой шкалы оценки критичности - низкий, средний и высокий уровни. В этом случае оценка каждого уровня в деньгах будет выполняться на основе принципов, отображенных в табл. 1.

При выборе шкалы важно учитывать следующее:

- чем меньше количество уровней, тем ниже точность оценки;
- чем больше количество уровней, тем выше сложность оценки (то есть сложно определить разницу между, скажем, 7-м и 8-м уровнем 10-ти уровневой шкалы).

Следовательно, в этом вопросе нужно найти «золотую середину», чтобы и точность не очень пострадала, и сложность не превышала допустимых пределов.

Кроме этого, следует иметь в виду, что для расчета информационных рисков достаточно примерных значений критичности активов: не обязательно оценивать их с точностью до денежной единицы. Однако денежное выражение критичности все равно необходимо.

Рассмотрим подробнее принципы оценки критичности каждого указанного актива.

- Информационные активы (или виды информации) оцениваются с точки зрения нанесения компании ущерба от их раскрытия, модификации или недоступности в течение определенного времени.
- Программное обеспечение, материальные ресурсы и сервисы оцениваются, как правило, с точки зрения их доступности или работоспособности. То есть требуется определить, какой ущерб понесет компания при нарушении функционирования данных активов. Например, нарушение системы кондиционирования в течение трех суток приведет к отказу серверов компании, к ним будет нарушен доступ, и вследствие этого компания понесет убытки.
- Сотрудники компании с точки зрения конфиденциальности и целостности оцениваются, учитывая их доступ к информационным ресурсам с правами на чтение и на модификацию. Доступность сотрудников оценивается с точки зрения их отсутствия на рабочем месте. Другими словами, оценивается, какой ущерб понесет компания при отсутствии сотрудника в течение определенного периода времени. Здесь важно учесть опыт сотрудника, его квалификацию, выполнение им каких-либо специфических операций.

- Репутация компании оценивается в связи с информационными ресурсами: какой ущерб репутации компании будет нанесен в случае нарушения безопасности информации компании.

Заметим, что процесс категорирования активов должен подчиняться четким документированным процедурам компании. Аудиторам сертификационного органа будет недостаточно формального документа, отражающего результаты категорирования. От владельцев активов требуется, чтобы они могли объяснить, какие методики они использовали при оценке, на основании каких данных были получены результаты оценки.

5.3 Оценка защищенности информационной системы компании

Очевидно, что для анализа информационных рисков необходимо оценить не только критичность активов, но и уровень их защищенности.

В процессе оценки защищенности информационной системы определяются угрозы, действующие на активы, а также уязвимости информационной системы, в которой обрабатываются активы и которые могут привести к реализации угроз. Угрозы и уязвимости рассматриваются только во взаимосвязи друг с другом. Уязвимость, через которую невозможно реализовать ни одну из угроз, не имеет смысла. Аналогично, угроза, которую невозможно реализовать ввиду отсутствия уязвимости, также неактуальна.

Не вызывает сомнения, что различные угрозы и уязвимости имеют разное значение (разный вес) для информационной системы. Например, злоумышленник скорее решит воспользоваться открытой дверью, чем открытым окном, если офис компании расположен на семнадцатом этаже 34-этажного здания (однако совсем исключать вторую возможность не стоит). Следовательно, необходимо определить, какие угрозы и уязвимости наиболее актуальны, а какие менее значимы, или, другими словами, определить вероятность реализации угрозы через уязвимость. Вероятность реализации уязвимостей (как и любая другая вероятность) определяется в пределах от 0 до 1 (или от 0 до 100 %).

Угрозы, уязвимости, а также их вероятности определяются в результате проведения технологического аудита защищенности информационной системы компании. Такой аудит может быть выполнен как специалистами компании (так называемый, внутренний аудит), так и сторонними консультантами (внешний аудит).

5.4 Оценка информационных рисков

Оценка информационных рисков заключается в расчете рисков, который выполняется с учетом сведений о критичности активов, а также вероятностей реализации уязвимостей.

Классическая формула оценки рисков:

$$R=D \times P(V)$$

где R - информационный риск;

D - критичность актива (ущерб);

$P(V)$ - вероятность реализации уязвимости.

Результаты оценки рисков, как правило, представляются в «Отчете об оценке информационных рисков компании».

5.Обработка информационных рисков

Обработка информационных рисков - это этап, в процессе которого определяется, какие действия по отношению к рискам требуется выполнить в компании.

Основными способами обработки рисков являются:

- принятие рисков;
- уклонение от рисков;
- передача рисков;
- снижение рисков.

Принятие рисков осуществляется в том случае, если уровень рисков признается приемлемым, то есть компания не считает целесообразным применять какие-либо меры по отношению к этим рискам и готова понести ущерб.

Уклонение от рисков - это полное устранение источника риска.

Передача рисков — перенесение ответственности за риск на третьи лица (например, поставщика оборудования или страховую компанию) без устранения источника риска.

Снижение рисков - это выбор и внедрение мер по снижению вероятности нанесения ущерба.

В процессе обработки рисков сначала требуется определить, какие из них требуют дальнейшей обработки, а какие можно принять. Как правило, это решается с помощью оценки приемлемого уровня риска. Риски, равные или ниже приемлемого, можно принять. Очевидно, что для рисков, превышающих приемлемый уровень, требуется выбрать дальнейшие меры по обработке. Приемлемый уровень риска определяется руководством компании или специальной группой, в которую входят руководители и главные финансисты компании. Например, если руководство компании декларирует, что низкий уровень риска считается приемлемым, то дальнейшие действия по обработке рисков определяются только для средних и высоких уровней риска. Причем, средний и высокий уровни риска требуется снизить до низкого (то есть до приемлемого) уровня.

В случае, когда в компании наблюдается большой разброс значений риска (как правило, это может возникнуть, если критичность активов была определена в денежных единицах, а не уровнях), информационные риски можно разбить на категории и определять приемлемый уровень для каждой из них отдельно. Это вызвано тем, что снижать различные значения рисков до одного заданного значения не всегда целесообразно (часто для снижения высоких рисков до заданного уровня необходимы неоправданно большие затраты).

По результатам данного этапа требуется составить «Отчет об обработке информационных рисков компании», который подробно описывает способы обработки рисков. Кроме этого, составляется «План снижения рисков», где

четко описываются конкретные меры по снижению рисков, сотрудники, ответственные за выполнение каждого положения плана, сроки выполнения плана.

Положение о применимости

По результатам оценки и обработки рисков разрабатывается Положение о применимости. Наличие этого документа обязательно для прохождения сертификации. Положение о применимости содержит все требования приложения А к стандарту ISO27001 с описанием, выполняются ли данные требования в компании. Если требования не выполняются, необходимо описать причину невыполнения (такой причиной могут быть результаты оценки рисков). Если требования выполняются, следует перечислить документы, которым должно соответствовать их выполнение.

В приложении А к стандарту ISO27001 перечислены все требования к обеспечению безопасности, которые должны выполняться в компании. Следовательно, Положение о применимости является итоговым решением относительно снижения информационных рисков компании.

Документированные процедуры

Стандарт требует, чтобы все меры по снижению рисков были документально зафиксированы. То есть для эффективного управления ИБ необходимо наличие процедур, которые будут поддерживаться определенными документами (инструкциями, политиками, регламентами), выполняться определенными людьми. Причем каждая процедура должна быть отражена в соответствующем документе. Документированные процедуры являются обязательным элементом системы управления информационной безопасностью. Следовательно, в рамках системы управления необходимо разработать базу нормативных документов, описывающих все процедуры в области ИБ.

Основными документами по управлению ИБ являются Политика управления информационной безопасностью и Политика информационной безопасности. Политика управления ИБ описывает общий подход к управлению ИБ. Политика ИБ описывает основные процедуры обеспечения ИБ с указанием ссылок на конкретные документы системы управления ИБ.

Кроме этого, разрабатываются методики и инструкции, описывающие процедуры обеспечения ИБ и управления ею.

В качестве примеров можно привести следующие методики:

- Методика инвентаризации активов;
- Методика категорирования активов;
- Методика оценки информационных рисков;
- Методика обработки информационных рисков.

Инструкции следует разработать для каждой процедуры обеспечения информационной безопасности. Примерный перечень может содержать следующие инструкции:

- Инструкция по обеспечению сохранности конфиденциальной инфор-

мации (соглашение о конфиденциальности);

- Инструкция пользователя по обеспечению информационной безопасности;
- Инструкция системного администратора по обеспечению информационной безопасности;
- Инструкция администратора безопасности;
- Инструкция по управлению доступом пользователей к информационной системе;
- Инструкция по защите от вредоносного программного обеспечения;
- Инструкция по выполнению резервного копирования;
- Инструкция по обращению со съемными носителями информации;
- Инструкция по использованию мобильных компьютеров;
- Инструкция по использованию средств криптографической защиты информации;
- Инструкция по внесению изменений в информационную систему;
- Инструкция по управлению инцидентами информационной безопасности;
- План непрерывности ведения бизнеса;
- Регламент обеспечения физической безопасности.

Обучение сотрудников компании как способ снижения рисков ИБ

В настоящей лекции, наверное, нет смысла говорить обо всех способах снижения информационных рисков, поскольку, во-первых, они могут сильно различаться в зависимости от особенностей информационных систем, а, во-вторых, как правило, системные администраторы и администраторы безопасности знают, какие средства защиты требуется внедрить в их информационную систему.

Остановимся подробнее на одном из способов снижения рисков, на который стандарт обращает особое внимание и который часто вызывает сложности при реализации - обучении пользователей информационной системы.

В настоящее время внутренний нарушитель уверенно занимает лидирующие позиции среди основных угроз ИБ. Это связано, прежде всего, с тем, что внешний периметр в большинстве компаний защищен достаточно надежно. Кроме этого, сотрудники компании являются легитимными пользователями информационной системы - им необходимо иметь доступ к ценной информации компании для выполнения своих должностных обязанностей. Следовательно, средства защиты в гораздо меньшей степени обеспечивают безопасность информации от внутреннего нарушителя. Основными способами воздействия на сотрудников компании являются нормативные документы, устанавливающие их ответственность за выполняемые действия, и информирование сотрудников по вопросам ИБ. С целью повышения осведомленности сотрудников компании в области ИБ проводятся различные виды тренингов и обучения.

Обучение сотрудников можно выполнять в форме очных и заочных курсов с последующим тестированием. Однако в больших компаниях проведение курсов часто вызывает сложности, так как, во-первых, сложно организовать курсы для большого количества сотрудников, а во-вторых, часто руководителям не хочется отрывать сотрудников от работы для участия в многочасовых семинарах. В таком случае, целесообразно организовать обучение сотрудников с помощью системы дистанционного обучения, в рамках которой могут быть представлены различные курсы (как для пользователей, так и для специалистов), игровые методики обучения, тестирование.

Управление ИБ

Управление информационной безопасностью заключается в четком выполнении всех процедур по обеспечению ИБ и по управлению ИБ, координации и регулированию процедур, контроле их правильного, а также эффективного выполнения.

Стандарт декларирует два основных принципа управления.

1. Процессный подход к управлению безопасностью, который рассматривает управление как процесс набор взаимосвязанных непрерывных действий, акцентирует внимание на достижении поставленных целей, а также на ресурсах, затраченных для достижения целей.

2. Применение PDCA-модели как основы для всех процедур управления ИБ.

PDCA-модель (или модель Шухарта-Деминга) определяет четыре этапа, которые должны выполняться последовательно для каждого процесса (рисунок и табл. 3).

Таким образом, для каждой процедуры системы управления информационной безопасностью определяются правила выполнения, необходимые ресурсы, график выполнения, процедуры контроля, критерии оценки эффективности. При этом для каждой процедуры последовательно и непрерывно выполняются следующие этапы:

- планирование процедуры;
- внедрение процедуры;
- проверка правильности и эффективности выполнения процедуры;
- внесение необходимых изменений в ход выполнения процедуры.

Далее через определенный период времени требуется заново пересматривать цели и задачи выполнения процедуры, то есть заново приступить к выполнению первого этапа модели PDCA.

Основная сложность может заключаться в проверке эффективности процедур системы управления ИБ. Для каждой процедуры необходимо разработать критерии, по которым будет проверяться ее эффективность, и, кроме этого, такие критерии требуется разработать для всей системы управления в целом.

Критериями оценки эффективности системы управления ИБ могут быть, например, изменение количества инцидентов ИБ, квалификация пользователей в области ИБ и пр.

6. Внедрение процедур системы управления ИБ

Внедрение процедур, как правило, заключается в информировании соответствующих сотрудников о правилах и сроках выполнения процедуры, регулярном контроле выполнения процедуры, а также оценке ее эффективности, внесении корректирующих и превентивных действий, то есть, по сути, во внедрении всего цикла PDCA-модели для каждой процедуры.

Как правило, консультанты по разработке и внедрению системы управления ИБ разрабатывают «План внедрения системы управления», в котором описывают четкую последовательность действий при внедрении процедур, методы контроля и осуществления проверок выполнения процедуры.

Заключение

Систему управления ИБ можно считать внедренной и эффективно функционирующей на практике тогда, когда все ее процедуры хотя бы один раз пройдут этапы модели PDCA, когда будут найдены и решены проблемы, возникающие при внедрении процедур.

Обеспечение ИБ и управление ею - достаточно трудоемкие процессы. Однако если к ним подойти комплексно и своевременно, а также выполнять все рекомендации международных стандартов в области управления ИБ - ISO/IEC 27001:2005 и ISO/IEC 17799:2005, они станут прозрачными, а защита от угроз безопасности эффективной.

Тема 6: "Методика оценки рисков информационной безопасности компании"

6.1 Управление рисками. Основные понятия.

При внедрении системы управления информационной безопасностью (СУИБ) в организации одной из основных точек преткновения обычно становится система управления рисками.

Система управления рисками (СУР) является главным, базовым элементом СУИБ.

СУР позволяет получить ответ на главный вопрос:

На каком направлении информационной безопасности требуется сосредоточить внимание?

Вообще говоря, управление рисками, равно как и выработка собственной политики безопасности, актуально только для тех организаций, которые рабо-

тают с большими объемами ценной информации или если компания обрабатывает или хранит ценную информацию своих клиентов (банк).

Обычную организацию вполне устроит типовой набор защитных мер, выбранный на основе представления о типичных рисках или вообще без всякого анализа рисков.

Использование информационных систем связано с риском. (Если ИС не использовать вообще, то риск будет связан с другими факторами).

Говоря о рисках для бизнеса, мы имеем в виду возможность с определенной вероятностью понести определенный ущерб. Это может быть как прямой материальный ущерб, так и косвенный ущерб, выражающийся, например, в упущенной выгоде, вплоть до выхода из бизнеса, ведь, если риском не управлять, то бизнес можно потерять.

Если возможный ущерб неприемлемо велик, необходимо принять экономически оправданные меры защиты. Периодическая переоценка рисков необходима для контроля эффективности защитных мер и для учета изменений обстановки.

С количественной точки зрения уровень риска является произведением вероятности реализации определенной угрозы (использующей некоторые уязвимые места), на величину возможного ущерба: $R = P(V) \times D$.

Таким образом, суть мероприятий по управлению рисками состоит в том, чтобы оценить их размер, выработать эффективные и экономичные меры снижения рисков, а затем убедиться, что риски заключены в приемлемые рамки (и остаются таковыми).

Следовательно, управление рисками включает в себя два вида деятельности, которые чередуются циклически:

- оценка и переоценка (измерение) рисков;
- выбор эффективных и **экономически оправданных** защитных мер и средств для уменьшения или нейтрализации рисков.

Процесс управления рисками можно разделить на следующие этапы:

1. Выбор анализируемых объектов и уровня детализации их рассмотрения.
2. Выбор методики оценки рисков.
3. Инвентаризация активов.
4. Анализ угроз и их последствий, выявление уязвимых мест в защите.
5. Оценка рисков.
6. Обработка рисков.
7. Выбор защитных мер.
8. Реализация и проверка выбранных мер.
9. Оценка остаточного риска.

Этапы 6 и 7 относятся к выбору защитных средств (нейтрализации рисков), остальные к оценке рисков.

Уже перечисление этапов показывает, что управление рисками — процесс циклический. По существу, последний этап — это оператор конца цикла,

предписывающий вернуться к началу. Риски нужно контролировать постоянно, периодически проводя их переоценку. Отметим, что добросовестно выполненная и тщательно документированная первая оценка может существенно упростить последующую работу.

На сегодняшний день существует две основные методики оценки рисков информационной безопасности: метод оценки рисков, основанный на построении **модели угроз и уязвимостей** и метод оценки рисков, основанный на построении **модели информационных потоков**.

Разработка методики оценки риска - достаточно трудоемкая задача. Во-первых, такая методика должна **всесторонне описывать информационную систему, ее ресурсы, ее угрозы и уязвимости**. Задача заключается в том, чтобы построить максимально гибкую модель информационной системы, которую можно было бы настраивать в соответствии с реальной системой. Во-вторых, методика оценки рисков должна быть предельно прозрачна, чтобы владелец информации, использующий ее, мог адекватно оценить ее эффективность и применимость к своей конкретной системе.

Остановимся подробнее на методах оценки информационного риска.

6.2 Метод оценки рисков на основе модели угроз и уязвимостей.

Для того, чтобы оценить риск информации, анализируются все угрозы, действующие на информационную систему, и уязвимости, через которые возможна реализация угроз.

Исходя из введенных владельцем информационной системы данных, строится модель угроз и уязвимостей, актуальных для информационной системы компании.

На основе полученной модели проводится анализ вероятности реализации угроз информационной безопасности на каждый ресурс и, исходя из этого, рассчитываются риски.

Основные понятия и допущения модели

Базовые угрозы информационной безопасности – нарушение конфиденциальности, нарушение целостности и отказ в обслуживании.

Ресурс – любой контейнер, предназначенный для хранения информации, подверженный угрозам информационной безопасности (сервер, рабочая станция, переносной компьютер).

Свойствами ресурса являются: перечень угроз, воздействующих на него, и критичность ресурса.

Угроза – действие, которое потенциально может привести к нарушению безопасности.

Свойством угрозы является перечень уязвимостей, при помощи которых может быть реализована угроза.

Уязвимость – это слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы.

Свойствами уязвимости являются: вероятность (простота) реализации угрозы через данную уязвимость и критичность реализации угрозы через данную уязвимость.

Критичность ресурса (D) – ущерб, который понесет компания от потери ресурса. Задается в уровнях (количество уровней может быть в диапазоне от 2 до 100) или в деньгах. В зависимости от выбранного режима работы, может состоять из критичности ресурса по конфиденциальности, целостности и доступности (D_c, D_i, D_a).

Критичность реализации угрозы (ER) – степень влияния реализации угрозы на ресурс, т.е. как сильно реализация угрозы повлияет на работу ресурса. Задается в процентах. Состоит из критичности реализации угрозы по конфиденциальности, целостности и доступности (ER_c, ER_i, ER_a).

Вероятность реализации угрозы через данную уязвимость в течение года ($P(V)$) – степень возможности реализации угрозы через данную уязвимость в тех или иных условиях. Указывается в процентах.

Максимальное критичное время простоя (T_{max}) – значение времени простоя, которое является критичным для организации. Т.е. ущерб, нанесенный организации при простаивании ресурса в течение критичного времени простоя, максимальный. При простаивании ресурса в течение времени, превышающего критичное, ущерб, нанесенный организации, не увеличивается.

Принцип работы алгоритма

Исходные данные:

- Ресурсы;
- Критичность ресурса;
- Отделы, к которым относятся ресурсы;
- Угрозы, действующие на ресурсы;
- Уязвимости, через которые реализуются угрозы;
- Вероятность реализации угрозы через данную уязвимость;
- Критичность реализации угрозы через данную уязвимость.

С точки зрения базовых угроз информационной безопасности существует два режима работы алгоритма:

- Одна базовая угроза (суммарная);
- Три базовые угрозы.

Расчет рисков по угрозе информационной безопасности

1. На первом этапе рассчитывается **уровень угрозы по уязвимости** T_h на основе критичности и вероятности реализации угрозы через данную уязвимость. Уровень угрозы показывает, насколько критичным является воздействие данной угрозы на ресурс с учетом вероятности ее реализации

$$Th_{c,I,a} = \frac{ER_{c,i,a}}{100} \times \frac{P(V)_{c,i,a}}{100},$$

где $ER_{c,I,a}$ – критичность реализации угрозы (указывается в %);

$P(V)_{c,I,a}$ – вероятность реализации угрозы через данную уязвимость (указывается в %).

Вычисляется одно или три значения в зависимости от количества базовых угроз. Получается значение *уровня угрозы по уязвимости* в интервале от 0 до 1.

2. Для расчета *уровня угрозы по всем уязвимостям* CTh, через которые возможна реализация данной угрозы на ресурсе, суммируются полученные уровни угроз через конкретные уязвимости по следующей формуле:

Для режима с одной базовой угрозой:

$$CTh = 1 - \prod_{i=1}^n (1 - Th)$$

Для режима с тремя базовыми угрозами:

$$CTh_c = 1 - \prod_{i=1}^n (1 - Th_c)$$

$$CTh_i = 1 - \prod_{i=1}^n (1 - Th_i)$$

$$CTh_a = 1 - \prod_{i=1}^n (1 - Th_a)$$

Значения *уровня угрозы по всем уязвимостям* получаются в интервале от 0 до 1.

3. Аналогично рассчитывается *общий уровень угроз* по ресурсу CThR (учитывая все угрозы, действующие на ресурс):

Для режима с одной базовой угрозой:

$$CThR = 1 - \prod_{i=1}^n (1 - CTh)$$

Для режима с тремя базовыми угрозами:

$$CThR_c = 1 - \prod_{i=1}^n (1 - CTh_c)$$

$$CThR_i = 1 - \prod_{i=1}^n (1 - CTh_i)$$

$$CThR_a = 1 - \prod_{i=1}^n (1 - CTh_a)$$

Значение *общего уровня угрозы* получается в интервале от 0 до 1.

4. Риск по ресурсу R рассчитывается следующим образом:

Для режима с одной базовой угрозой:

$$R = CThR \times D,$$

где D – критичность ресурса. Задается в деньгах или уровнях.

В случае угрозы доступность (отказ в обслуживании) критичность ресурса в год вычисляется по следующей формуле:

$$D_{a/год} = D_{a/час} \times T$$

Для остальных угроз критичность ресурса задается в год.

Для режима с тремя базовыми угрозами:

$$R_c = CThR_c \times D_c$$

$$R_i = CThR_i \times D_i$$

$$R_a = CThR_a \times D_a$$

$$R = (1 - \prod_{i=1}^3 (1 - \frac{R_i}{100})) \times 100$$

$D_{a,c,i}$ – критичность ресурса по трем угрозам. Задается в деньгах или уровнях.

R - суммарный риск по трем угрозам.

Таким образом, получается значение *риска по ресурсу* в уровнях (заданных пользователем) или деньгах.

5. Риск по информационной системе CR рассчитывается по формуле:

Для режима с одной базовой угрозой:

- для режима работы в деньгах:

$$CR = \sum_{i=1}^n R_i$$

- для режима работы в уровнях:

$$CR = (1 - \prod_{i=1}^n (1 - \frac{R_i}{100})) \times 100$$

Для режима работы с тремя угрозами:

- для режима работы в деньгах:

$$CR_{a,c,i} = \sum_{i=1}^n R_i$$

$$CR = \sum_{i=1}^n CR_{a,c,i}$$

$CR_{a,c,i}$ - риск по системе по каждому виду угроз

CR - риск по системе суммарно по трем видам угроз

$$CR_{a,c,i} = (1 - \prod_{i=1}^n (1 - \frac{R_i}{100})) \times 100$$

$$CR = (1 - \prod_{i=1}^3 (1 - \frac{R_{a,c,i}}{100})) \times 100$$

- для режима работы в уровнях:

Задание контрмер

Для расчета эффективности введенной контрмеры необходимо пройти последовательно по всему алгоритму с учетом заданной контрмеры. Т.е. на выходе пользователь получает значение двух рисков – риска без учета контрмеры (**Rold**) и риск с учетом заданной контрмеры (**Rnew**) (или с учетом того, что уязвимость закрыта).

Эффективность введения контрмеры рассчитывается по следующей формуле (**E**):

$$E = \frac{R_{old} - R_{new}}{R_{old}}$$

В результате работы алгоритма пользователь системы получает следующие данные:

- Риск по трем базовым угрозам (или по одной суммарной угрозе) для ресурса;
- Риск суммарно по всем угрозам для ресурса;
- Риск по трем базовым угрозам (или по одной суммарной угрозе) для информационной системы;
- Риск по всем угрозам для информационной системы;
- Риск по всем угрозам для информационной системы после задания контрмер;
- Эффективность контрмеры;

- Эффективность комплекса контрмер.

Пример расчета риска информационной безопасности на основе модели угроз и уязвимостей

(Расчет рисков приведен только для одной угрозы информационной безопасности, т.к. для остальных угроз риск рассчитывается аналогично).

1. Угрозы и уязвимости

Ресурс	Угрозы	Уязвимости
Сервер (критичность ресурса 100 у.е.)	Угроза 1 Неавторизованное проникновение нарушителя внутрь охраняемого периметра (одного из периметров)	Уязвимость 1 Отсутствие регламента доступа в помещения с ресурсами, содержащими ценную информацию
		Уязвимость 2 Отсутствие системы наблюдения (видео-наблюдение, сенсоры и т.д.) за объектом (или существующая система наблюдения охватывает не все важные объекты)
	Угроза 2 Неавторизованная модификация информации в системе электронной почты, хранящейся на ресурсе	Уязвимость 1 Отсутствие авторизации для внесения изменений в систему электронной Почты
		Уязвимость 2 Отсутствие регламента работы с системой криптографической защиты электронной корреспонденции
	Угроза 3 Разглашение конфиденциальной информации сотрудниками компании	Уязвимость 1 Отсутствие соглашений о конфиденциальности
		Уязвимость 2 Распределение атрибутов безопасности (ключи доступа, шифрования) между несколькими доверенными сотрудниками

1.1 Вероятность реализации

Угроза/Уязвимость	Вероятность реализации угрозы через данную уязвимость в течение года (%), P(V)	Критичность реализации угрозы через уязвимость (%), ER
Угроза 1/Уязвимость 1	50	60
Угроза 1/Уязвимость 2	20	60
Угроза 2/Уязвимость 1	60	40
Угроза 2/Уязвимость 2	10	40
Угроза 3/Уязвимость 1	10	80
Угроза 3/Уязвимость 2	80	80

2. Уровень угрозы

Угроза/Уязвимость	Уровень угрозы (%), Th $Th = \frac{ER}{100} \times \frac{P(V)}{100}$	Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза (%), CTh $CTh = 1 - \prod_{i=1}^n (1 - Th)$
Угроза 1/Уязвимость 1	0,3	0,384
Угроза 1/Уязвимость 2	0,12	
Угроза 2/Уязвимость 1	0,24	0,270
Угроза 2/Уязвимость 2	0,04	
Угроза 3/Уязвимость 1	0,08	0,669
Угроза 3/Уязвимость 2	0,64	

3. Общий уровень угроз, действующих на ресурс

Угроза/Уязвимость	Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза (%), CTh $CTh = 1 - \prod_{i=1}^n (1 - Th)$	Общий уровень угроз по ресурсу (%), CThR $CThR = 1 - \prod_{i=1}^n (1 - CTh)$
Угроза 1/Уязвимость 1	0,384	0,8511
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1	0,270	
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1	0,669	
Угроза 3/Уязвимость 2		

4. Риск ресурса

Критичность ресурса (ущерб, который понесет Компания от потери ресурса) – 100 у.е.

Для угрозы доступность, критичность ресурса задается в час (а не в год, как для остальных угроз). Поэтому, чтобы получить критичность ресурса в год, необходимо умножить критичность ресурса в час на максимально критичное время простоя ресурса за год.

Угроза/Уязвимость	Общий уровень угроз по ресурсу (%), CThR $CThR = 1 - \prod_{i=1}^n (1 - CTh_i)$	Риск ресурса (у.е.), R $R = CThR \times D$
Угроза 1/Уязвимость 1	0,8511	85,11
Угроза 1/Уязвимость 2		
Угроза 2/Уязвимость 1		
Угроза 2/Уязвимость 2		
Угроза 3/Уязвимость 1		
Угроза 3/Уязвимость 2		

Тема 7: "Методика оценки рисков информационной безопасности компании Digital Security"

7.1 Метод оценки рисков на основе модели информационных потоков.

Анализ рисков информационной безопасности осуществляется с помощью построения модели информационной системы организации.

Данная модель позволяет оценить защищенность каждого вида информации.

Алгоритм позволяет получить следующие данные:

- Реестр ресурсов;
- Значения риска для каждого ценного ресурса организации;
- Значения риска для ресурсов после задания контрмер (остаточный риск);
- Эффективность контрмер;
- Рекомендации экспертов.

7.2. Описание архитектуры ИС.

Для того, чтобы построить модель ИС, необходимо проанализировать защищенность и архитектуру построения информационной системы.

Специалист по ИБ, привлекая владельца (менеджера) информационной системы (используя вопросники, интервью, документацию, инструменты автоматического сканирования), должен подробно *описать архитектуру сети*:

- все аппаратные (компьютерные) ресурсы, на которых хранится ценная информация;

- сетевые группы, в которых находятся ресурсы системы (т.е. физические связи ресурсов друг с другом);
- отделы, к которым относятся ресурсы;
- виды ценной информации;
- ущерб для каждого вида ценной информации по трем видам угроз;
- бизнес-процессы, в которых обрабатывается информация;
- пользователей (группы пользователей), имеющих доступ к ценной информации;
- класс группы пользователей;
- доступ группы пользователей к информации;
- характеристики этого доступа (вид и права);
- средства защиты информации;
- средства защиты рабочего места группы пользователей.

Исходя из введенных данных, можно построить полную модель информационной системы компании, на основе которой будет проведен анализ защищенности каждого вида информации на ресурсе.

Целесообразно составить карту ИС на которой отобразить все указанные характеристики. Иными словами, необходимо:

1. Изобразить ИС в виде структурной схемы, на которой отобразить:
 - 1) все ресурсы (сервер, РС и т.д.);
 - 2) отделы, к которым относятся ресурсы;
 - 3) сетевые группы (локальные сети), физические связи ресурсов между собой и их подключения к Интернет;
 - 4) виды ценной информации, хранящейся на ресурсах;
 - 5) пользователей (группы пользователей), имеющих доступ к ценной (конфиденциальной) информации.

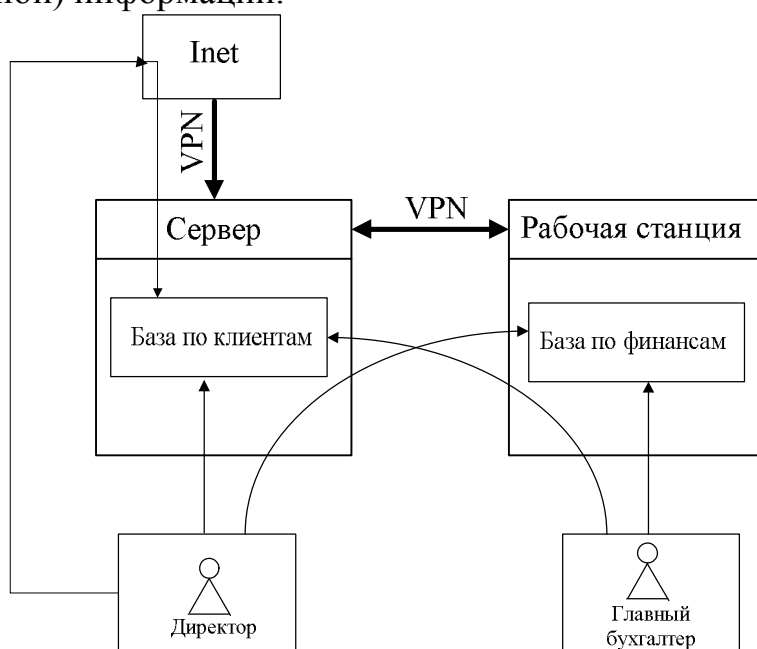


Рис. 5 ИС в виде структурной схемы

2. Описать в виде таблиц средства защиты каждого аппаратного ресурса, средства защиты каждого вида информации, хранящегося на нем с указанием веса каждого средства, например:

Средства защиты сервера	Вес
Средства физической защиты	
Контроль доступа в помещение, где расположен ресурс (физическая охрана, дверь с замком, специальный пропускной режим в помещении)	25
Средства локальной защиты	
Отсутствие дисководов и USB портов	10
Средства корпоративной сетевой защиты	
Межсетевой экран	10
Обманная система	2
Система антивирусной защиты на сервере	10
Средства резервирования и контроля целостности	
Аппаратная система контроля целостности	20
Средства защиты информации (информация №1)	Вес
Средства локальной защиты	
Средства криптографической защиты (криптозащита данных на ПК)	20
Средства резервирования и контроля целостности	
Резервное копирование	10
Программная система контроля целостности	10

Средства защиты рабочей станции	Вес
Средство физической защиты	
Контроль доступа в помещение, где расположен ресурс (дверь с замком, видеонаблюдение)	10
Средства локальной защиты	
Средства антивирусной защиты (антивирусный монитор)	10
Отсутствие дисководов и USB портов	10
Средства персональной сетевой защиты	
Наличие персонального межсетевого экрана	3
Система криптозащиты электронной почты	10

3. Описать в виде таблицы вид доступа (локальный, удаленный) и права доступа (чтение, запись, удаление) для каждого пользователя (групп пользователей), а так же наличие соединения через VPN, количество человек в группе для каждого информационного потока:

Информационный поток	Вид доступа	Права доступа	Наличие VPN-соединения	Количество человек в группе
----------------------	-------------	---------------	------------------------	-----------------------------

(Наименование)	(Локальный, удаленный)	(Чтение, запись, удаление)	(Да, нет)	(1,2,...n)
----------------	------------------------	----------------------------	-----------	------------

4. Указать наличие у пользователей выхода в Интернет

Пользователь (группа пользователей.)	Доступ в Интернет
(Наименование)	(Есть, нет, не анализируется)

5. Указать ущерб компании от реализации угроз ИБ для каждого информационного потока:

Информационный поток	Конфиденциальность	Целостность	Доступность
(Наименование)	(у.е. в год)	(у.е. в год)	(у.е. в час)

Ущерб определяется с участием владельца ИС, либо им самим непосредственно.

На этом описание архитектуры ИС завершается.

Далее производится расчет рисков для **каждого вида ценной информации хранящейся в ИС** по угрозе «нарушение конфиденциальности».

7.3 Расчет рисков по угрозе конфиденциальность

1. Расчет коэффициентов защищенности.

Для каждого информационного потока рассчитывается коэффициент локальной либо удаленной защищенности информации, хранящейся на ресурсе, в зависимости от типа доступа. Если доступ локальный, то рассчитывается только коэффициент локальной защищенности информации. Если доступ удаленный, то рассчитывается коэффициент удаленной защищенности информации, хранящейся на ресурсе и коэффициент локальной защищенности рабочего места пользователя.

Коэффициент локальной защищенности информации рассчитывается, если доступ к информации в данном информационном потоке **локальный**. Он равен сумме весов средств физической и локальной защиты информации. Учитываются все средства физической защиты и средства локальной защиты информации, обеспечивающие защиту информации по угрозе **конфиденциальность**:

средства физической защиты: (охрана, замок, пропускной режим в **помещение**) (25);

средства локальной защиты:

отсутствие дисководов и USB портов (10);

криптозащита данных на ПК (20).

Коэффициент удаленной защищенности информации на ресурсе рассчитывается, если доступ к информации в данном информационном потоке **удаленный**. Он необходим для того, чтобы учесть сетевые средства защиты, и равен сумме весов средств корпоративной сетевой защиты информации.

Эти средства (межсетевой экран, серверная антивирусная защита) находятся **на сервере**.

Коэффициент локальной защищенности рабочего места пользователя (группы пользователей) рассчитывается только при удаленном доступе к информации. Он равен сумме весов средств **физической, локальной и персональной сетевой защиты** информации.

Средства физической защиты – те же.

Средства локальной защиты: антивирус, отсутствие дисководов и USB-портов.

Средства персональной сетевой защиты: межсетевой экран (брандмауэр), средства криптозащиты электронной почты.

Эти средства (персональный межсетевой экран – брандмауэр, средства криптозащиты электронной почты) находятся на рабочей станции (на компьютере, подключенном к локальной сети).

Этот коэффициент не определяется для анонимных и авторизованных Интернет-пользователей, т.к. рабочее место пользователя в данном случае не является частью ИС.

Для дальнейших расчетов по каждому потоку из трех коэффициентов выбирается **наименьший коэффициент защищенности (НК)**.

Информационный поток	Коэффициент локальной защищенности информации	Коэффициент удаленной защищенности информации	Коэффициент локальной защищенности рабочего места	Наименьший коэффициент
(Наименование)	$(\Phi + Л)$	$(СКСЗ)$	$(\Phi + Л + ПСЗ)$	(НК) min

2. Учет наличия доступа при помощи VPN.

При локальном доступе VPN не учитывается, поскольку локальная сеть не используется для передачи информации.

При удаленном доступе через VPN к наименьшему коэффициенту защищенности потока прибавляется вес VPN шлюза (20). Это сетевое устройство повышает защищенность информации.

При этом от наименьшего коэффициента переходят к результирующему: **РК=НК+20 (или +0)**

Информационный поток	Наименьший коэффициент	Вес VPN соединения	Результирующий коэффициент
(Наименование)	(НК)	(20 либо 0)	(РК)

3. Далее от результирующего коэффициента (РК) переходят к итоговому коэффициенту (ИК) защищенности.

Если количество пользователей 1, и у группы нет доступа в Интернет, то:
ИК=1/РК.

Учет количества человек N в группе пользователей: **ИК=N/РК.**

Если группа пользователей имеет доступ в Интернет, то ИК увеличивается в 2 раза:

ИК=2 N/РК.

Если при удаленном доступе Интернет-пользователей VPN-соединение не используется (Интернет заведен на компьютер, а не на сервер), то для них **итоговый** коэффициент защищенности (ИК) умножается на 4, **в силу отсутствия защиты шлюза ИК=(4 N)/РК**

Результаты расчетов сводятся в таблицу.

Информационный поток	Результирующий коэффициент	Количество человек в гр.	Наличие Интернет	Итоговый коэффициент
Главный бухгалтер –бухгалтерский отчет	(РК)	(N)	I=2,1	ИК=(N I)/РК

4. Расчет итоговой вероятности (ИВ).

Чтобы получить **ИВ**, необходимо сначала определить **базовую вероятность (БВ)** реализации угрозы нарушения конфиденциальности и умножить ее на **ИК**:

ИВ=БВ·ИК.

БВ реализации угрозы «К» определяется на основе метода экспертных оценок. Группа экспертов определяет БВ для каждой информации (для каждого потока). БВ может задать владелец информации.

Информационный поток	Базовая вероятность (БВ)	Итоговая базовая вероятность (ИБВ)	Итоговый коэффициент (ИК)	Промежуточная вероятность (ПВ)	Итоговая вероятность (ИВ)
Главный бух-	0,2	0,5	0,036	0,018	0,018

галтер – бухгалтерский отчет					
Бухгалтер – база клиентов Компании	0,2	0,5	0,024	0,012	0,024
Финансовый директор- база клиентов Компании	0,5	0,5	0,024	0,012	
Бухгалтер-база данных наименований товаров Компании	0,2	0,5	0,033	0,0165	0,0165

Итоговая базовая вероятность (**ИБВ**) одинакова для всех потоков, поскольку к информации «база клиентов Компании» имеется доступ через Интернет (Финансовый директор имеет права «запись, чтение»). Базовая вероятность реализации угрозы конфиденциальности для потока «Финансовый директор – база клиентов Компании» самая большая (0,7) и она распространяется на все информации, хранящиеся на всех ресурсах, входящих в локальную сеть (сетевую группу).

Это так называемое **наследование коэффициентов защищенности**. Если на ресурсе расположены несколько видов информации, причем к некоторым из них осуществляется доступ через Интернет (группами анонимных, авторизованных или мобильных Интернет-пользователей), то угрозы, исходящие от этих групп пользователей могут повлиять и на другие виды информации. Следовательно, это необходимо учесть. Если на одном из ресурсов, находящемся в сетевой группе, хранится информация, к которой осуществляют доступ указанные группы пользователей, то это учитывается аналогично для всех видов информации, хранящихся на всех ресурсах, входящих в сетевую группу. В реальной информационной системе все ресурсы, взаимосвязанные между собой, оказывают друг на друга влияние. Т.е. злоумышленник, проникнув на один ресурс информационной системы (например, получив доступ к информации ресурса), может без труда получить доступ к ресурсам, физически связанным со взломанным.

Промежуточная вероятность (**ПВ**) вычисляется, как: **ПВ=ИБВ·ИК**.

Итоговая вероятность **ИБ1=ПВ1; ИВ3=ПВ3**.

Итоговая вероятность **ИВ2=1-(1-ПВ21) (1-ПВ22)**, как суммарная по двум группам пользователей.

5. Расчет риска по угрозе конфиденциальность для каждой информации (1,2,3)

Риск по угрозе конфиденциальность для каждой информации (1-бух. отчет, 2-база клиентов, 3-база наименований товаров) рассчитывается, как произведение итоговой вероятности на ущерб:

$$R1=IB1*D1=0,018*100=1,8;$$

$$R2=IB2*D2=0,024*100=2,4;$$

$$R3=IB3*D3=0,0165*100=1,65.$$

где У – ущерб от реализации угрозы.

6. Расчет риска по угрозе конфиденциальность для ресурса.

Риск для ресурса, на котором хранится несколько видов информации (несколько БД) равен сумме рисков по всем видам информации.

Расчет рисков по угрозе целостность

1. Расчет коэффициентов защищенности.

Выполняется аналогично расчету по угрозе конфиденциальность. Фактически берутся наименьшие коэффициенты НК из предыдущего расчета.

2. Учет средств резервирования и контроля целостности.

Информационный поток	Наименьший коэффициент (НК)	Вес VPN-соединения	Вес средств резервирования и контроля целостности	Результирующий коэффициент (РК)
Главный бухгалтер – бухгалтерский отчет	55	-	40 АСКЦ-20 РК-10 ЦП-10	95 55+40
Бухгалтер – база клиентов Компании	22	20	20 РК-10 ЦП-10	62 22+20+20
Финансовый директор – база клиентов Компании	22	20	20 АСКЦ-20	62 22+20+20
Бухгалтер-база данных наименований товаров Компании	30	-	20 РК-10 ЦП-10	50 30+20

3. Учет резервного копирования, количества человек в группе пользователей и наличия у группы пользователей доступа в Интернет:

Информационный поток	Результующий коэффициент (РК)	Наличие резервного копирования	Кол-во человек в группе	Наличие у группы доступа в Интернет	Итоговый коэффициент (ИК)
Главный бухгалтер – бухгалтерский отчет	95	1	1	2	0,021 (1/95)*2
Бухгалтер – база клиентов Компании	62	1	1	1	0,016 1/62
Финансовый директор – база клиентов Компании	62	4	1	-	0,065 (1/62)*4
Бухгалтер-база данных наименований товаров Компании	50	1	1	1	0,02 1/50

Наличие резервного копирования учитывается следующим образом: если у информации на ресурсе осуществляется резервное копирование, то вес резервного копирования (10) прибавляется к коэффициенту защищенности (п.2). Если резервное копирование не осуществляется, и в группе пользователей, имеющей доступ к информации, разрешены **запись** или **удаление**, то итоговый коэффициент увеличивается в 4 раза.

4. Расчет итоговой вероятности.

Информационный поток	Базовая вероятность (БВ)	Итоговая базовая вероятность (ИБВ)	Итоговый коэффициент (ИК)	Промежуточная вероятность	Итоговая вероятность
Главный бухгалтер – бухгалтерский отчет	0,25	0,7	0,021	0,0147 0,7*0,021	0,0147

Бухгалтер – база клиентов Компании	0,1	0,7	0,016	0,0112 0,7*0,016	0,05619
Финансовый директор- база клиентов Компании	0,7	0,7	0,065	0,0455 0,7*0,065	
Бухгалтер- база данных наименований товаров Компании	0,25	0,7	0,02	0,014 0,7*0,02	0,014

Базовая вероятность определяется на основе метода экспертных оценок. Ее значения по данной угрозе **целостность** отличаются от значений в расчете по угрозе **конфиденциальность**. Группа экспертов, исходя из классов групп пользователей, получающих доступ к ресурсу, видов и прав их доступа к информации, рассчитывает базовую вероятность для каждой информации. Владелец информационной системы, при желании, может задать этот параметр самостоятельно.

Итоговая базовая вероятность. Базовая вероятность реализации угрозы конфиденциальности для потока «Финансовый директор- база клиентов Компании» самая большая (0,7) и она распространяется на все информации, хранящиеся на всех ресурсах, входящих в локальную сеть (сетевую группу).

Перемножив итоговую базовую вероятность и итоговый коэффициент защищенности, получим итоговую вероятность реализации угрозы. Напомним, что для каждой из трех угроз информационной безопасности мы отдельно рассчитываем вероятность реализации.

Итоговая вероятность по второй информации:

ИБ2=1-(1-ПВ21)*(1-ПВ22), как суммарная по двум группам пользователей.

6. Расчет риска по угрозе целостность.

На завершающем этапе значение полученной итоговой вероятности умножаем на ущерб от реализации угрозы и получаем риск угрозы информационной безопасности для связи <вид информации - группа пользователей>.

$$R1=ИБ1*D1=0,0147*100=1,47;$$

$$R2=ИБ2*D2=0,05619*100=5,61;$$

$$R3=ИБ3*D3=0,014*100=1,4.$$

- Чтобы получить риск для вида информации (с учетом всех групп пользователей, имеющих к ней доступ), необходимо сначала просуммировать итоговые вероятности реализации угрозы по следующей формуле:

$$P_{\text{inf}} = 1 - \prod_{i=1}^n (1 - P_{\text{уг},n})$$

А затем полученную итоговую вероятность для информации умножаем на ущерб от реализации угрозы, получая, таким образом, риск от реализации угрозы для данной информации.

- Чтобы получить риск для аппаратного ресурса (с учетом всех видов информации, хранимой и обрабатываемой на ресурсе), необходимо просуммировать риски по всем видам информации.

Тема 8: "Методики и технологии управления рисками"

В настоящее время управление информационными рисками представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента в области защиты информации. **Его основная задача — объективно идентифицировать и оценить наиболее значимые для бизнеса информационные риски компании, а также адекватность используемых средств контроля рисков для увеличения эффективности и рентабельности экономической деятельности компании.**

Поэтому под термином «управление информационными рисками» обычно понимается *системный процесс идентификации, контроля и уменьшения информационных рисков компаний в соответствии с определенными ограничениями нормативно-правовой базы в области защиты информации и собственной корпоративной политики безопасности.*

Считается, что качественное управление рисками позволяет использовать оптимальные по эффективности и затратам средства контроля рисков и средства защиты информации, адекватные текущим целям и задачам бизнеса компании.

Не секрет, что сегодня наблюдается повсеместное усиление **зависимости** успешной бизнес деятельности отечественных компаний от используемых организационных мер и технических средств контроля и уменьшения риска.

Для эффективного управления информационными рисками разработаны специальные методики, например методики международных стандартов ISO 15408, ISO 17799 (BS7799), BSI; а также национальных стандартов NIST 80030, SAC, COSO, SAS 55/78 и некоторые другие, аналогичные им.

В соответствие с этими методиками управление информационными рисками любой компании предполагает следующее.

Во-первых, определение основных целей и задач защиты информационных активов компании.

Во-вторых, создание эффективной системы оценки и управления информационными рисками.

В-третьих, расчет совокупности детализированных не только качественных, но и количественных оценок рисков, адекватных заявленным целям бизнеса.

В-четвертых, применение специального инструментария оценивания и управления рисками. Давайте рассмотрим некоторые качественные и количественные международные методики управления информационными рисками, обращая основное внимание на возможность их адаптации и применения в отечественных условиях.

8.1 Качественные методики управления рисками

Качественные методики управления рисками приняты на вооружение в технологически развитых странах многочисленной армией внутренних и внешних ИТ-аудиторов. Эти методики достаточно популярны и относительно просты, и разработаны, как правило, на основе требований международного стандарта ISO 17799. В сентябре 2002 года основные положения ISO 17799 были пересмотрены и дополнены с учетом развития современных информационных технологий и требований к организации режима ИБ. Сегодня это наиболее распространенный стандарт во всем мире среди организаций и предприятий, которые используют подобные стандарты на добровольной основе.

К качественным методикам управления рисками на основе требований ISO 17999 относятся методики COBRA и RA Software Tool (Инструмент Программного Обеспечения). Давайте кратко рассмотрим названные методики.

COBRA

Во второй половине 90х годов компания C & A Systems Security Ltd. разработала одноименные методику и соответствующий инструментарий для анализа и управления информационными рисками под названием COBRA. Эта методика позволяет выполнить в автоматизированном режиме простейший вариант оценивания информационных рисков любой компании. Для этого предлагается использовать специальные электронные базы знаний и процедуры логического вывода, ориентированные на требования ISO 17799. Существенно, что при желании перечень учитываемых требований можно дополнить различными требованиями отечественных нормативно-регулирующих органов, например, требованиями НД ТЗИ.

Методика COBRA представляет требования стандарта ISO 17799 в виде тематических вопросников (check list's), на которые следует ответить в ходе оценки рисков информационных активов и электронных бизнес транзакций компании.

Далее введенные ответы автоматически обрабатываются, и с помощью соответствующих правил логического вывода формируется итоговый отчет с текущими оценками информационных рисков компании и рекомендациями по их управлению.

Достоинство методики - в ее простоте. Необходимо ответить на несколько десятков вопросов, затем автоматически формируется отчет.

Этот программный продукт может применяться при проведении аудита ИБ или для работы специалистов служб, ответственных за обеспечение информационной безопасности.

Простота, соответствие международному стандарту, сравнительно небольшое число вопросов позволяют легко адаптировать этот метод для работы в отечественных условиях.

RA Software Tool

Методика и одноименное инструментальное средство RA Software Tool основаны на требованиях международных стандартов ISO 17999 и ISO 13335 (части 3 и 4), а также на требованиях некоторых руководств Британского национального института стандартов (BSI), например, PD 3002 (Руководство по оценке и управлению рисками), PD 3003 (Оценка готовности компании к аудиту в соответствии с BS 7799), PD 3005 (Руководство по выбору системы защиты) и пр.

Эта методика позволяет выполнять оценку информационных рисков (модули 4 и 5) в соответствии с требованиями ISO 17799, а при желании в соответствии с более детальными спецификациями руководства PD 3002 Британского института стандартов.

8.2 Количественные методики управления рисками. Метод CRAMM

Вторую группу методик управления рисками составляют количественные методики, актуальность которых обусловлена необходимостью решения различных оптимизационных задач, которые часто возникают в реальной жизни. **Суть этих задач сводится к поиску единственного оптимального решения, из множества существующих.** Например, необходимо ответить на следующие вопросы: «Как, оставаясь в рамках утвержденного годового (квартального) бюджета на информационную безопасность, достигнуть максимального уровня защищенности информационных активов компании?» или «Какую из альтернатив построения корпоративной защиты информации (защищенного WWW сайта или корпоративной Email) выбрать с учетом известных ограничений бизнес ресурсов компании?» Для решения этих задач и разрабатываются методы и методики количественной оценки и управления рисками на основе структурных и реже объектно-ориентированных методов системного анализа и проектирования (SSADM — Structured Systems Analysis and Design). На практике такие методики управления рисками позволяют:

- Создавать модели информационных активов компании с точки зрения безопасности;
- Классифицировать и оценивать ценности активов;

- Составлять списки наиболее значимых угроз и уязвимостей безопасности;
- Ранжировать угрозы и уязвимости безопасности;
- Обосновывать средства и меры контроля рисков;
- Оценивать эффективность/стоимость различных вариантов защиты;
- Формализовать и автоматизировать процедуры оценивания и управления рисками.

Одной из наиболее известных методик этого класса является методика CRAMM.

Метод CRAMM

В 1985 году Центральное агентство по компьютерам и телекоммуникациям (ССТА) Великобритании начало исследования существующих методов управления информационной безопасностью для выдачи рекомендаций по их использованию в правительственных организациях, обрабатывающих конфиденциальную информацию. Ни один из рассмотренных методов не подошел. Поэтому сначала был создан метод, а затем одноименная методика CRAMM (анализа и контроля рисков), соответствующая требованиям ССТА. Затем появилось несколько версий методики, ориентированных на требования различных государственных и коммерческих организаций и структур. Одна из версий «коммерческого профиля» широко распространилась на рынке средств защиты информации.

Основными целями методики CRAMM являются:

- Формализация и автоматизация процедур анализа и управления рисками;
- Оптимизация расходов на средства контроля и защиты;
- Комплексное планирование и управление рисками на всех стадиях жизненного цикла информационных систем;
- Сокращение времени на разработку и сопровождение корпоративной системы защиты информации;
- Обоснование эффективности предлагаемых мер защиты и средств контроля;
- Управление изменениями и инцидентами;
- Поддержка непрерывности бизнеса;
- Оперативное принятие решений по вопросам управления безопасностью и пр.

Управление рисками в методике CRAMM осуществляется в несколько этапов (рис. 6).

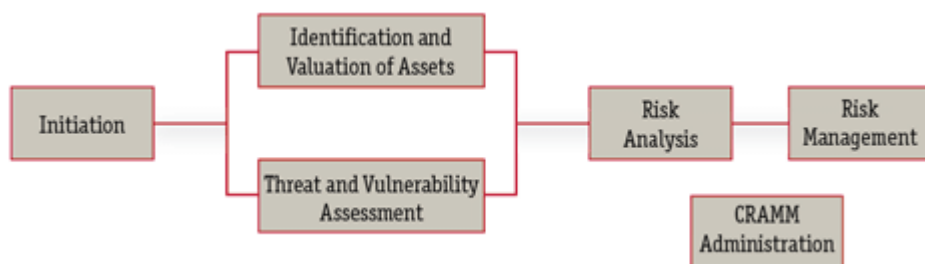


Рис. 6 Управление рисками в методике CRAMM

На первом этапе инициации — «Initiation» — определяются границы исследуемой информационной системы компании, состав и структура ее основных информационных активов и транзакций.

На этапе идентификации и оценки ресурсов — «Identification and Valuation of Assets» — четко идентифицируются активы, и определяется их стоимость. Расчет стоимости информационных активов однозначно позволяет определить необходимость и достаточность предлагаемых средств контроля и защиты.

На этапе оценивания угроз и уязвимостей — «Threat and Vulnerability Assessment» — идентифицируются и оцениваются угрозы и уязвимости информационных активов компании.

Этап анализа рисков — «Risk Analysis» — позволяет получить качественные и количественные оценки рисков.

На этапе управления рисками — «Risk management» — предлагаются меры и средства уменьшения или уклонения от риска.

Давайте рассмотрим возможности CRAMM на следующем примере. Пусть проводится оценка информационных рисков следующей корпоративной информационной системы (рис. 7).



Рис.7 оценка информационных рисков информационной системы

В этой схеме условно выделим следующие элементы системы:

- рабочие места, на которых операторы вводят информацию, поступающую из внешнего мира;
- почтовый сервер, на который информация поступает с удаленных узлов сети через Интернет;
- сервер обработки, на котором установлена СУБД;
- сервер резервного копирования;
- рабочие места группы оперативного реагирования;
- рабочее место администратора безопасности;
- рабочее место администратора БД.

Функционирование системы осуществляется следующим образом. Данные, введенные с рабочих мест пользователей и поступившие на почтовый сервер, направляются на сервер корпоративной обработки данных. Затем данные поступают на рабочие места группы оперативного реагирования и там принимаются соответствующие решения.

Давайте теперь проведем анализ рисков с помощью методики CRAMM и предложим некоторые средства контроля и управления рисками, адекватные целям и задачам бизнеса компании.

Определение границ исследования. Этап начинается с решения задачи определения границ исследуемой системы. Для этого собирается следующая информация: ответственные за физические и программные ресурсы; кто является пользователем и как пользователи применяют или будут использовать систему; конфигурация системы. Первичная информация собирается в процессе бесед с менеджерами проектов, менеджером пользователей или другими сотрудниками.

Идентификация ресурсов и построение модели системы с точки зрения ИБ. Проводится идентификация ресурсов: материальных, программных и информационных, содержащихся внутри границ системы. Каждый ресурс необходимо отнести к одному из predetermined классов. Классификация физических ресурсов приводится в приложении. Затем строится модель информационной системы с точки зрения ИБ. Для каждого информационного процесса, имеющего самостоятельное значение с точки зрения пользователя и называемого пользовательским сервисом (EndUserService), строится дерево связей используемых ресурсов. В рассматриваемом примере будет единственный подобный сервис (рис. 8). Построенная модель позволяет выделить критичные элементы.

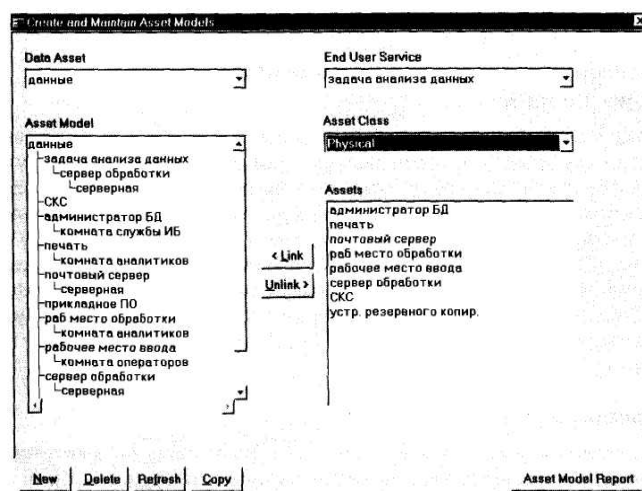


Рис.8 дерево связей используемых ресурсов

Ценность ресурсов. Методика позволяет определить ценность ресурсов. Этот шаг является обязательным в полном варианте анализа рисков. Ценность физических ресурсов в данном методе определяется ценой их восстановления в случае разрушения.

Ценность данных и программного обеспечения определяется в следующих ситуациях:

- недоступность ресурса в течение определенного периода времени;
- разрушение ресурса — потеря информации, полученной со времени последнего резервного копирования или ее полное разрушение;
- нарушение конфиденциальности в случаях несанкционированного доступа штатных сотрудников или посторонних лиц;
- модификация рассматривается для случаев мелких ошибок персонала (ошибки ввода), программных ошибок, преднамеренных ошибок;
- ошибки, связанные с передачей информации: отказ от доставки, недоставка информации, доставка по неверному адресу.

Для оценки возможного ущерба предлагается использовать следующие критерии:

- ущерб репутации организации;
- нарушение действующего законодательства;

- ущерб для здоровья персонала;
- ущерб, связанный с разглашением персональных данных отдельных лиц;

- финансовые потери от разглашения информации;
- финансовые потери, связанные с восстановлением ресурсов;
- потери, связанные с невозможностью выполнения обязательств;
- дезорганизация деятельности.

Приведенная совокупность критериев используется в коммерческом варианте метода (профиль Standard). В других версиях совокупность будет иной, например, в версии, используемой в правительственных учреждениях, добавляются параметры, отражающие такие области, как национальная безопасность и международные отношения.

Для данных и программного обеспечения выбираются применимые к данной ИС критерии, дается оценка ущерба по шкале со значениями от 1 до 10.

К примеру, если данные содержат подробности коммерческой конфиденциальной (критичной) информации, эксперт, проводящий исследование, задает вопрос: как может повлиять на организацию несанкционированный доступ посторонних лиц к этой информации?

Возможен такой ответ: провал сразу по нескольким параметрам из перечисленных выше, причем каждый аспект следовало бы рассмотреть подробнее и присвоить самую высокую из возможных оценок.

Затем разрабатываются шкалы для выбранной системы параметров. Они могут выглядеть следующим образом.

Ущерб репутации организации:

- 2 — негативная реакция отдельных чиновников, общественных деятелей;
- 4 — критика в средствах массовой информации, не имеющая широкого общественного резонанса;
- 6 — негативная реакция отдельных депутатов Верховной Рады Украины;
- 8 — критика в средствах массовой информации, имеющая последствия в виде крупных скандалов, парламентских слушаний, широкомасштабных проверок и т. п.;
- 10 — негативная реакция на уровне Президента и Правительства.

Ущерб для здоровья персонала:

- 2 — минимальный ущерб (последствия не связаны с госпитализацией или длительным лечением);
- 4 — ущерб среднего размера (необходимо лечение для одного или нескольких сотрудников, но длительных отрицательных последствий нет);
- 6 — серьезные последствия (длительная госпитализация, инвалидность одного или нескольких сотрудников);
- 10 — гибель людей.

Финансовые потери, связанные с восстановлением ресурсов:

- 2 — менее \$1000;
- 6 — от \$1000 до \$10 000;
- 8 — от \$10 000 до \$100 000;
- 10 — свыше \$100 000.

Дезорганизация деятельности в связи с недоступностью данных:

- 2 — отсутствие доступа к информации до 15 минут;
- 4 — отсутствие доступа к информации до 1 часа;
- 6 — отсутствие доступа к информации до 3 часов;
- 8 — отсутствие доступа к информации от 12 часов;
- 10 — отсутствие доступа к информации более суток.

Далее рассматриваются основные сценарии, приводящие к различным негативным последствиям, описываемым в терминах выбранных параметров (рис.9. - Оценка ценности информационных ресурсов).

Impact	Guideline	Scale	Cost	Scenario Descriptive
UNAVAIL-3H		0		
UNAVAIL-12H	Commercial and Economic Interests	4	\$1,000	Восстановление I
UNAVAIL-1D		0		
UNAVAIL-2D	Commercial and Economic Interests	6	\$50,000	Неиспр. оборудо
UNAVAIL-1W	Financial Loss	8	\$1,000,000	Авария с тяжелы

Рис.9 Оценка ценности информационных ресурсов

На этом этапе может быть подготовлено несколько типов отчетов (границы системы, модель, определение ценности ресурсов). Если ценности ресурсов низкие, можно использовать базовый вариант защиты. В таком случае исследователь может перейти от этой стадии сразу к стадии анализа рисков. Однако

для адекватного учета потенциального воздействия какой-либо угрозы, уязвимости или комбинации угроз и уязвимостей, которые имеют высокие уровни, следует использовать сокращенную версию стадии оценки угроз и уязвимостей. Это позволяет разработать более эффективную систему защиты информации компании.

На этапе оценивания угроз и уязвимостей оцениваются зависимости пользовательских сервисов от определенных групп ресурсов и существующий уровень угроз и уязвимостей.

Далее активы компании группируются с точки зрения угроз и уязвимостей. Например, в случае наличия угрозы пожара или кражи, в качестве группы ресурсов разумно рассмотреть все ресурсы, находящиеся в одном месте (серверный зал, комната средств связи и т. д.).

Программное обеспечение CRAMM для каждой группы ресурсов и каждого из 36 типов угроз генерирует список вопросов, допускающих однозначный ответ. Уровень угроз оценивается, в зависимости от ответов, как очень высокий, высокий, средний, низкий и очень низкий. Уровень уязвимости оценивается, в зависимости от ответов, как высокий, средний и низкий.

На основе этой информации рассчитываются уровни рисков в дискретной шкале с градациями от 1 до 7. Полученные уровни угроз, уязвимостей и рисков анализируются и согласовываются с заказчиком.

CRAMM объединяет угрозы и уязвимости в матрице риска. Рассмотрим, как получается эта матрица, и что каждый из уровней риска означает.

Основной подход, для решения этой проблемы состоит в рассмотрении:

- уровня угрозы (шкала приведена в табл. 1);
- уровня уязвимости (шкала приведена в табл. 2);
- размера ожидаемых финансовых потерь (пример на рис. 10).

Таблица 1. Шкала оценки уровней угрозы (частота возникновения).

Описание	Значение
инцидент происходит в среднем, не чаще, чем каждые 10 лет	очень низкий
инцидент происходит в среднем один раз в 3 года	низкий
инцидент происходит в среднем раз в год	средний
инцидент происходит в среднем один раз в четыре месяца	высокий
инцидент происходит в среднем раз в месяц	очень высокий

Таблица 2. Шкала оценки уровня уязвимости (вероятность успешной реализации угрозы).

Описание	Значение
В случае возникновения инцидента, вероятность развития событий по наихудшему сценарию меньше 0,33	низкий
В случае возникновения инцидента, вероятность развития событий по наихудшему сценарию от 0,33 до 0,66	средний
В случае возникновения инцидента, вероятность развития событий по наихудшему сценарию выше 0,66	высокий

Исходя из оценок стоимости ресурсов защищаемой ИС, оценок угроз и уязвимостей, определяются "ожидаемые годовые потери". На рис. 10 приведен пример матрицы оценки ожидаемых потерь. В ней второй столбец слева содержит значения стоимости ресурса, верхняя строка заголовка таблицы - оценку частоты возникновения угрозы в течение года (уровня угрозы), нижняя строка заголовка - оценку вероятности успеха реализации угрозы (уровня уязвимости).

		0.1	0.1	0.1	0.34	0.34	0.34	1	1	1	3.33	3.33	3.33	10	10	10
		0.1	0.5	1	0.1	0.5	1	0.1	0.5	1	0.1	0.5	1	0.1	0.5	1
1	1000	1.0E+01	5.0E+01	1.0E+02	3.4E+01	1.7E+02	3.4E+02	1.0E+02	5.0E+02	1.0E+03	3.3E+02	1.7E+03	3.3E+03	5.0E+03	5.0E+03	1.0E+04
2	10000	1.0E+02	5.0E+02	1.0E+03	3.4E+02	1.7E+03	3.4E+03	1.0E+03	5.0E+03	1.0E+04	3.3E+03	1.7E+04	3.3E+04	5.0E+04	5.0E+04	1.0E+05
3	30000	3.0E+02	1.5E+03	3.0E+03	1.0E+03	5.1E+03	1.0E+04	3.0E+03	1.5E+04	3.0E+04	1.0E+04	5.0E+04	1.0E+05	1.5E+05	1.5E+05	3.0E+05
4	100000	1.0E+03	5.0E+03	1.0E+04	3.4E+03	1.7E+04	3.4E+04	1.0E+04	5.0E+04	1.0E+05	3.3E+04	1.7E+05	3.3E+05	5.0E+05	5.0E+05	1.0E+06
5	300000	3.0E+03	1.5E+04	3.0E+04	1.0E+04	5.1E+04	1.0E+05	3.0E+04	1.5E+05	3.0E+05	1.0E+05	5.0E+05	1.0E+06	1.5E+06	1.5E+06	3.0E+06
6	1000000	1.0E+04	5.0E+04	1.0E+05	3.4E+04	1.7E+05	3.4E+05	1.0E+05	5.0E+05	1.0E+06	3.3E+05	1.7E+06	3.3E+06	5.0E+06	5.0E+06	1.0E+07
7	3000000	3.0E+04	1.5E+05	3.0E+05	1.0E+05	5.1E+05	1.0E+06	3.0E+05	1.5E+06	3.0E+06	1.0E+06	5.0E+06	1.0E+07	1.5E+07	1.5E+07	3.0E+07
8	1E+07	1.0E+05	5.0E+05	1.0E+06	3.4E+05	1.7E+06	3.4E+06	1.0E+06	5.0E+06	1.0E+07	3.3E+06	1.7E+07	3.3E+07	5.0E+07	5.0E+07	1.0E+08
9	3E+07	3.0E+05	1.5E+06	3.0E+06	1.0E+06	5.1E+06	1.0E+07	3.0E+06	1.5E+07	3.0E+07	1.0E+07	5.0E+07	1.0E+08	1.5E+08	1.5E+08	3.0E+08
10	1E+08	1.0E+06	5.0E+06	1.0E+07	3.4E+06	1.7E+07	3.4E+07	1.0E+07	5.0E+07	1.0E+08	3.3E+07	1.7E+08	3.3E+08	5.0E+08	5.0E+08	1.0E+09

Рис. 10. Матрица ожидаемых годовых потерь

Значения ожидаемых годовых потерь (англ. Annual Loss of Expectancy) переводятся в CRAMM в баллы, показывающие уровень риска, согласно шкале, представленной на рис. 11 (в этом примере размер потерь приводится в фунтах стерлингов).

CRAMM Measure of Risk	"Annual Loss of Expectancy"
1	<£1,000
2	<£10,000
3	<£100,000
4	<£1,000,000
5	<£10,000,000
6	<£100,000,000
7	<£1,000,000,000

Рис. 11 Шкала оценки уровня рисков

В соответствии с приведенной ниже матрицей, выводится оценка риска (рис. 12) уровни рисков рассчитываются в дискретной шкале с градациями от 1 до 7 (этап анализа рисков). Полученные уровни угроз, уязвимостей и рисков

анализируются и согласовываются с заказчиком. Только после этого можно переходить к заключительной стадии метода.

Threat Vuln.	Very Low Low	Very Low Medium	Very Low High	Low Low	Low Medium	Low High	Medium Low	Medium Medium	Medium High	High Low	High Medium	High High	Very High Low	Very High Medium	Very High High
Asset Value															
1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
2	1	1	2	1	2	2	2	3	3	2	3	3	3	3	4
3	1	2	2	2	2	3	2	3	3	3	3	4	3	4	4
4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

Рис. 13 Матрица оценки риска

Третья стадия исследования заключается в поиске адекватных контрмер. По существу, это поиск варианта системы безопасности, наилучшим образом удовлетворяющей требованиям заказчика.

На этом этапе CRAMM генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням. Контрмеры разбиваются на группы и подгруппы по следующим категориям:

- Обеспечение безопасности на сетевом уровне.
- Обеспечение физической безопасности.
- Обеспечение безопасности поддерживающей инфраструктуры.
- Меры безопасности на уровне системного администратора.

В результате выполнения данного этапа формируется несколько видов отчетов.

Таким образом, рассмотренная методика анализа и управления рисками полностью применима и в наших условиях, несмотря на то, что показатели защищенности от НСД к информации и требования по защите информации различаются в украинских нормативных документах и зарубежных стандартах. Особенно полезным представляется использование инструментальных средств типа метода CRAMM при проведении анализа рисков информационных систем с повышенными требованиями в области ИБ. Это позволяет получать обоснованные оценки существующих и допустимых уровней угроз, уязвимостей, эффективности защиты.

CRAMM как инструментальный аудитор

CRAMM имеет средства генерации отчетов, необходимые при проведении аудита информационной безопасности в соответствии с BS 7799 (ISO 17799).

Это следующие отчеты:

- политика информационной безопасности;
- система управления информационной безопасностью;
- план обеспечения бесперебойной работы;
- ведомость соответствия.

Метод CRAMM в настоящее время применяется наиболее часто, если требуется провести аудит в соответствии с требованиями Британского стандарта.

Его достоинства заключаются в использовании технологии оценки угроз и уязвимостей по косвенным факторам с возможностью верификации результатов, удобной системе моделирования информационной системы с позиции безопасности, обширной базе данных по контрмерам. Этот метод - самый «мощный» и самый трудоемкий из рассмотренных в настоящем обзоре, он позволяет весьма детально оценить риски и различные варианты контрмер.

Его недостаток с позиции отечественного потребителя состоит в сложности русификации и большом объеме выходных документов (сотни страниц). Аналитик (аудитор) обычно вынужден на основе полученных документов сам писать отчет для заказчика.

Таким образом, CRAMM - пример методики расчета, при которой первоначальные оценки даются на качественном уровне, и потом производится переход к количественной оценке (в баллах).

Тема 9: "Разработка корпоративной методики анализа рисков"

9.1 Постановка задачи

Анализ информационных рисков позволяет эффективно управлять информационной безопасностью предприятия. Для этого в начале работ по анализу рисков необходимо определить, что именно подлежит защите на предприятии и воздействию каких угроз оно подвержено, а затем выработать рекомендации по практике защиты. Обсудим теперь, как разработать **свою собственную** методику анализа и управления информационными рисками компании.

Такой анализ производится исходя из непосредственных целей и задач по защите конкретного вида информации конфиденциального характера. Одна из важнейших задач в рамках такой защиты информации - обеспечение ее целостности и доступности. Часто забывают, что нарушение целостности может произойти не только вследствие преднамеренных действий, но и по ряду других причин: сбоев оборудования, ведущих к потере или искажению информации; физических воздействий, в частности в результате стихийных бедствий; ошибок в программном обеспечении (в том числе из-за недокументированных возможностей). Поэтому под термином «атака» будем понимать воздействия на информационные ресурсы не только человеческие, но и окружающей среды, в которой функционирует система обработки информации предприятия.

Анализ риска можно проводить согласно методике по сценарию, представленному на рис. 14.

Каждый из шести этапов анализа риска должен быть конкретизирован.

На первом и втором этапах выявляются сведения, составляющие для предприятия коммерческую тайну, которые предстоит защищать.

Понятно, что такие сведения хранятся в установленных местах и на конкретных носителях, передаются по каналам связи и обрабатываются в соответствии с принятым регламентом. При этом основным фактором в технологии обращения с информацией является архитектура КИС, от которой во многом зависит защищенность информационных ресурсов предприятия.

В связи с этим необходимо еще раз подчеркнуть, что степень информационной безопасности определяется не только (а может быть и не столько) средствами и способами защиты, но и особенностями построения КИС. И когда говорят о КИС в защищенном исполнении, речь идет прежде всего о выборе такой архитектуры (топологии) системы обработки информации, расположения средств обработки конфиденциальной информации и способов ее хранения и передачи, которые существенно уменьшают число возможных точек доступа к информации.

Третий этап анализа риска - построение схем каналов доступа, утечки или воздействия на информационные ресурсы основных узлов КИС.



Рис.14. Сценарий анализа информационных рисков компании

Каждый канал доступа характеризуется множеством точек, с которых можно «снять» информацию. Именно они представляют собой уязвимости и требуют применения средств недопущения нежелательных воздействий на информацию.

Анализ способов защиты всех возможных точек атак соответствует целям защиты, и его результатом должна быть характеристика возможных брешей в обороне, в том числе за счет неблагоприятного стечения обстоятельств (четвертый этап).

На пятом этапе исходя из известных на данный момент способов и средств преодоления оборонительных рубежей находятся вероятности реализации угроз по каждой из возможных точек атак.

На заключительном этапе производится оценка ущерба организации в случае реализации каждой из атак. Эти данные вместе с оценками уязвимости позволяют получить ранжированный список угроз информационным ресурсам.

Результаты работы представляются в виде, удобном для их восприятия и выработки решений о коррекции существующей системы защиты информации. При этом важно, что каждый информационный ресурс может быть подвержен воздействию нескольких потенциальных угроз. Принципиальное же значение имеет суммарная вероятность доступа к информационным ресурсам, которая складывается из элементарных вероятностей доступа к отдельным точкам прохождения информации.

Величина информационного риска по каждому ресурсу - это произведение вероятности нападения на ресурс, вероятности реализации угрозы и ущерба от информационного вторжения. В данном произведении могут быть использованы различные способы взвешивания составляющих.

Объединение рисков по всем ресурсам дает общую величину риска при принятой архитектуре КИС и внедренной в нее системы защиты информации.

Таким образом, варьируя варианты построения системы защиты информации и архитектуры КИС, можно (за счет изменения вероятности реализации угроз) представить и рассмотреть различные значения риска. Здесь весьма важным шагом является выбор одного из вариантов в соответствии с заданным критерием принятия решения. Таким критерием может быть допустимая величина риска или отношение затрат на обеспечение информационной безопасности к остаточному риску.

При построении систем обеспечения информационной безопасности также нужно определить **стратегию управления рисками** на предприятии.

На сегодня известно несколько подходов к управлению рисками. Один из наиболее распространенных - уменьшение риска путем принятия комплексной системы контрмер, включающей программно-технические и организационные меры защиты. Близким является подход, связанный с уклонением от риска. От некоторых классов рисков можно уклониться, например: вынесение Web-сервера организации за пределы локальной сети позволяет избежать риска несанкционированного доступа в локальную сеть со стороны Web-клиентов.

Наконец, в ряде случаев допустимо принятие риска. В этой ситуации важно определиться со следующей дилеммой: что для предприятия выгоднее - бороться с рисками или же с их последствиями. Здесь приходится решать оптимизационную задачу.

После того как стратегия управления рисками выбрана, проводится окончательная оценка мероприятий по обеспечению информационной безопасности с подготовкой экспертного заключения о защищенности информационных ресурсов. В экспертное заключение входят все материалы анализа рисков и рекомендации по их снижению.

Отметим, что выполнение анализа рисков и оценки потерь требует глубоких системных знаний и аналитического мышления во многих областях, смежных с проблемой защиты информации.

9.2 Методы оценивания информационных рисков

В настоящее время используются различные методы оценки информационных рисков отечественных компаний и управления ими. Оценка информационных рисков компании может быть выполнена в соответствии со следующим планом:

- 1) Идентификация и количественная оценка информационных ресурсов компании, значимых для бизнеса.
- 2) Оценивание возможных угроз.
- 3) Оценивание существующих уязвимостей.
- 4) Оценивание эффективности средств обеспечения информационной безопасности.

Предполагается, что значимые для бизнеса уязвимые информационные ресурсы компании подвергаются риску, если по отношению к ним существуют какие-либо угрозы. Другими словами, риски характеризуют опасность, которая может угрожать компонентам корпоративной информационной системы. При этом информационные риски компании зависят от:

- показателей ценности информационных ресурсов;
- вероятности реализации угроз для ресурсов;
- эффективности существующих или планируемых средств обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков корпоративной информационной системы и ее ресурсов. После оценки рисков можно выбрать средства, обеспечивающие желаемый уровень информационной безопасности компании. При оценивании рисков учитываются такие факторы, как ценность ресурсов, значимость угроз и уязвимостей, эффективность имеющихся и планируемых средств защиты. Сами показатели ресурсов, значимости угроз и уязвимостей, эффективность средств защиты могут быть установлены как количественными методами (например, при нахождении стоимостных характеристик), так и качественными, скажем, с учетом штатных или чрезвычайно опасных нештатных воздействий внешней среды.

Возможность реализации угрозы для некоторого ресурса компании оценивается вероятностью ее реализации в течение заданного отрезка времени. При этом вероятность того, что угроза реализуется, определяется следующими основными факторами:

- привлекательностью ресурса (учитывается при рассмотрении угрозы от умышленного воздействия со стороны человека);
- возможностью использования ресурса для получения дохода (также в случае угрозы от умышленного воздействия со стороны человека);
- техническими возможностями реализации угрозы при умышленном воздействии со стороны человека;
- степенью легкости, с которой уязвимость может быть использована.
-

9.3 Табличные методы оценки рисков

В настоящее время известно множество табличных методов оценки информационных рисков компании. Важно, чтобы компания выбрала для себя подходящий метод, который обеспечивал бы корректные и достоверные воспроизводимые результаты. Рассмотрим несколько примеров подобных методов, рекомендованных стандартами в области информационной безопасности [209, 291], и методические рекомендации к ним [189, 200, 210, 284, 285]. Важно, что в этих методах количественные показатели имеющихся или предлагаемых физических ресурсов компании оцениваются с точки зрения стоимости их замены или восстановления работоспособности ресурса. А существующие или предполагаемые программные ресурсы оцениваются так же, как и физические, то есть путем определения затрат на их приобретение или восстановление. Если обнаружится, что к какому-либо прикладному программному обеспечению предъявляются особые требования к конфиденциальности или целостности, например исходный текст ПО обладает высокой коммерческой ценностью, то оценка этого ресурса производится в стоимостном выражении по той же схеме, что и для информационных ресурсов.

Количественные показатели информационных ресурсов рекомендуется оценивать по результатам опросов сотрудников компании - владельцев информации, то есть должностных лиц компании, которые в состоянии определить ценность информации, ее характеристики и степень критичности исходя из фактического положения дел. На основе результатов опроса оцениваются показатели и степень критичности информационных ресурсов в случае несанкционированного ознакомления с конфиденциальной информацией, нарушения ее целостности или доступности.

Пример оценки рисков по двум факторам

В таблице можно наглядно отразить связь факторов негативного воздействия (показателей ресурсов) и вероятностей реализации угрозы с учетом показателей уязвимостей.

На первом шаге оценивается негативное воздействие по заранее определенной шкале, например от 1 до 5, для каждого ресурса, которому угрожает опасность (колонка В в табл. 1).

На втором шаге по заданной шкале, например от 1 до 5, оценивается вероятность реализации каждой угрозы.

На третьем шаге вычисляется показатель риска. В простейшем варианте методики это делается путем умножения ($B \times C$). Необходимо помнить, что операция умножения определена для количественных шкал. Для ранговых (качественных) шкал измерения показатель риска, соответствующий ситуации $B = 1$, $C = 3$, совсем не обязательно эквивалентен случаю $B = 3$, $C = 1$. Соответственно, должна быть разработана методика оценивания показателей рисков применительно к конкретной организации.

На четвертом шаге угрозы ранжируются по значениям их фактора риска.

В рассматриваемом примере для наименьшего негативного воздействия и для наименьшей возможности реализации угрозы выбран показатель 1.

Таблица 1. Ранжирование рисков

Дескриптор угрозы	Показатель	Возможность негативного воздействия (ресурса)	Показатель риска реализации угрозы (субъективная оценка)	Ранг риска
Угроза А	5	2	10	2
Угроза В	2	4	8	3
Угроза С	3	5	15	1
Угроза D	1	3	3	5
Угроза Е	4	1	4	4
Угроза F	2	4	8	3

Данная процедура позволяет сравнивать и ранжировать угрозы с различными негативными воздействиями и вероятностями реализации. В случае необходимости дополнительно могут приниматься во внимание стоимостные показатели.

Разделение рисков на приемлемые и неприемлемые

Другой способ оценивания рисков состоит в разделении их только на приемлемые и неприемлемые риски. Подход основывается на том, что количественные показатели рисков служат лишь для того, чтобы их упорядочить и определить, какие действия необходимы в первую очередь. Но этого можно достичь и с меньшими затратами.

Матрица, используемая в данном подходе, содержит не числа, а только символы Д (риск допустим) и Н (риск недопустим). Например, матрица может иметь вид табл. 2.

Таблица 2. Разделение рисков на приемлемые и неприемлемые

Показатель ценности ресурса	Показатель возможности реализации угрозы				
	0	1	2	3	4
0	Д	Д	Д	Д	Н

1	Д	Д	Д	Н	Н
2	Д	Д	Н	Н	Н
3	Д	Н	Н	Н	Н
4	Н	Н	Н	Н	Н

Вопрос о том, как провести границу между приемлемыми и неприемлемыми рисками, остается на усмотрение аналитика, подготавливающего данную таблицу, и руководящих специалистов в области информационной безопасности.

Пример оценки рисков по трем факторам

По каждой группе ресурсов, связанной с данной угрозой, оценивается уровень угрозы (вероятность реализации) и уровень уязвимости (степень легкости, с которой реализованная угроза способна привести к негативному воздействию). Оценивание производится в качественных шкалах.

Сначала определим уровни угроз, уязвимостей, тяжести последствий и рисков.

Уровни угроз:

- низкий (Н) - реализация данной угрозы маловероятна, за последние два года подобных случаев не зафиксировано;
- средний (С) - угроза может реализоваться в течение одного года с вероятностью около 0,3;
- высокий (В) - угроза, скорее всего, реализуется в течение года и, возможно, не один раз.

Уровни уязвимостей:

- низкий (Н) - защищенность системы очень высока, реализация угроз почти никогда не приводит к происшествию;
- средний (С) - защищенность системы средняя, реализация около 30% угроз приводит к происшествию;
- высокий (В) - защищенность системы низкая, реализация угрозы практически всегда приводит к происшествию.

Показатель негативного воздействия (тяжесть последствий)

Используем введенную в главе 2 классификацию последствий:

- 1) Незначительные (менее \$100).
- 2) Маленькие (менее \$1000).
- 3) Умеренные (менее \$10 000).
- 4) Серьёзные (существенное негативное влияние на бизнес).

5) Критические (катастрофическое воздействие, возможно прекращение функционирования системы).

Уровни рисков

Показатель риска измеряется по шкале от 0 до 8, уровни риска определяются следующим образом:

1 - риск пренебрежимо мал. Ситуации, при которых событие наступает, практически исключены, а последствия незначительны, потери менее 100 долларов;
2 - риск незначителен. Событие наступает редко, последствия (потери) находятся в допустимых пределах (не более 1000 долларов);

8 - риск очень высок. Событие, скорее всего, наступит, и последствия будут катастрофическими (возможно полное прекращение деятельности организации).

Примером таблицы, с помощью которой задается значение уровня риска в зависимости от уровней угроз и уязвимостей при фиксированной стоимости потерь (Умеренные), является табл. 3.

Таблица 3. Определение уровня риска в зависимости от уровней угроз и уязвимостей

Уровень угрозы								
низкий			средний			высокий		
Уровни уязвимости			Уровни уязвимости			Уровни уязвимости		
Н	С	В	Н	С	В	Н	С	В
2	3	4	3	4	5	4	5	6

Далее строится таблица для различных уровней потерь. Пример такой таблицы представлен ниже.

Таблица 4. Определение риска в зависимости от трех факторов

Степень серьезности происшествя (цена потери)	Уровень угрозы								
	низкий			средний			высокий		
	Уровни уязвимостей			Уровни уязвимостей			Уровни уязвимостей		
	Н	С	В	Н	С	В	Н	С	В
Незначительные	0	1	2	1	2	3	2	3	4
Маленькие	1	2	3	2	3	4	3	4	5
Умеренные	2	3	4	3	4	5	4	5	6
Серьезные	3	4	5	4	5	6	5	6	7
Критические	4	5	6	5	6	7	6	7	8

9.4 Методика анализа рисков Microsoft

В качестве возможного примера корпоративной методики анализа рисков рассмотрим методику компании Microsoft.

В методике риск определяется как возможность понести убытки из-за нарушения безопасности сети изнутри или извне. Управление рисками предприятия в сфере информационной безопасности требует выполнения четырех этапов:

- 1) Распознавание (идентификация) рисков.
- 2) Определение размера риска.
- 3) Разработка плана управления рисками.
- 4) Текущий контроль и управление рисками.

При ограниченном времени для идентификации рисков рекомендуется применять методики получения сведений от экспертов, в частности метод

«мозгового штурма». Для каждого выявленного риска требуется оценить его стоимость (то есть определить ущерб в том случае, если рассматриваемое нежелательное событие произошло) и вероятность возникновения риска.

Оценка для каждой из угроз может производиться следующими способами:

- с использованием группы нападения - имитируется атака на систему группой специалистов;
- методом накопления идей - создается группа сотрудников и/или консультантов, которые обсуждают возможные риски и предлагают контрмеры;
- путем применения формальных оценок угроз, методов управления рисками и интеграции защитных мер.

Предлагаемая Microsoft стратегия оценки рисков включает следующие этапы:

- определение допустимого уровня рисков (то есть того уровня рисков, который приемлем);
- оценка вероятности возникновения каждого риска;
- присвоение стоимости каждому риску;
- расстановка приоритетов.

В процессе оценки для каждого риска вычисляется вероятность его возникновения и размер связанных с ним потерь. Далее используется одна из разновидностей табличной оценки рисков - строится матрица следующего вида (см. табл. 3.7).

Таблица 5. Табличная оценка риска в зависимости от факторов

Вероятность	Стоимость		
	высокая	средняя	низкая
Высокая	Красная	Красная	Синяя
Средняя	Желтая	Желтая	Зеленая
Низкая	Синяя	Синяя	Зеленая

В зависимости от полученных оценок риск относится к одной из следующих групп:

- высокий риск (красная область). Предполагается, что без снижения таких рисков обращение к информационной системе предприятия может оказать отрицательное влияние на бизнес;
- существенный риск (желтая область). Здесь требуется эффективная стратегия управления рисками, которая позволит уменьшить или полностью исключить отрицательные последствия нападения;
- умеренный риск (синяя область). В отношении рисков, попавших в эту область, достаточно применить основные процедуры управления рисками;
- незначительный риск (зеленая область). Усилия по управлению рисками в данном случае не будут играть важной роли.

На основании уровня допуска (уровня допустимых рисков), размера потенциальных потерь и вероятности их возникновения рискам назначаются приоритеты. Они служат для того, чтобы определить те риски, которые в первую очередь надо предотвратить (рекомендуется создать список десяти основных рисков, которым в первую очередь уделяется внимание), после чего составляется план по управлению рисками.

Планирование заключается в следующем:

- идентификации триггеров для каждого риска (*триггер*, или пусковое событие -идентификатор риска, реализованного или ожидаемого в скором времени);
- подготовке плана превентивных мероприятий, планов реагирования на непредвиденные ситуации и планов по уменьшению последствий каждого риска.

Выделяются четыре составные части планирования управления рисками:

- исследование;
- принятие (можно ли принять данный риск?);
- управление (можно ли сделать что-то, чтобы уменьшить риск?);
- исключение (что можно сделать, чтобы предотвратить риск или блокировать его?).

При этом исследование применяется по отношению к каждому риску, а остальные стадии могут комбинироваться. Предположим, исследование системы показало, что на предприятии установлено потенциально уязвимое приложение, причем полностью отказаться от работы с ним в данный момент невозможно. Допустим, далее данное приложение удалили на всех узлах, где это было допустимо, а на остальных, соответственно, оставили. Получается, что в отношении этого риска были выполнены следующие этапы: исследование, исключение (частичное), принятие (частичное).

Не менее важна и задача контроля рисков (отслеживания рисков), которая заключается в том, чтобы при изменении внешних или внутренних условий скорректировать сделанные ранее оценки рисков.

Тема 10: " Современные методы и средства анализа и управление рисками информационных систем компаний"

10.1 Обоснование необходимости инвестиций в информационную безопасность компании

Сегодня не вызывает сомнений необходимость вложений в обеспечение информационной безопасности современного крупного бизнеса. Основной вопрос современного бизнеса - как оценить необходимый уровень вложений в ИБ для обеспечения максимальной эффективности инвестиций в данную сферу. Для решения этого вопроса существует только один способ - применять систе-

мы анализа рисков, позволяющие оценить существующие в системе риски и выбрать оптимальный по эффективности вариант защиты (по соотношению существующих в системе рисков к затратам на ИБ).

Для подтверждения факта актуальности задачи обеспечения безопасности бизнеса, воспользуемся отчетом ФБР за 2005 год. Данные были собраны на основе опроса 530 американских компаний (средний и крупный бизнес).

Статистика инцидентов области ИТ-секьюрити неумолима. Согласно данным ФБР в 2005 году 56 % опрошенных компаний подвергались атаке.

По статистике, самым большим препятствием на пути принятия каких-либо мер по обеспечению информационной безопасности в компании являются две причины:

- 1) ограничение бюджета;
- 2) отсутствие поддержки со стороны руководства.

Обе причины возникают из-за непонимания руководством серьезности вопроса и сложности задачи для ИТ-менеджера обосновать, зачем необходимо вкладывать деньги в информационную безопасность. Часто считается, что основная проблема заключается в том, что ИТ-менеджеры и руководители разговаривают на разных языках - техническом и финансовом, но ведь и самим ИТ-специалистам часто трудно оценить, на что потратить деньги и сколько их требуется для обеспечения большей защищенности системы компании, чтобы эти расходы не оказались напрасными или чрезмерными.

Если ИТ-менеджер четко представляет, сколько компания может потерять денег в случае реализации угроз, какие места в системе наиболее уязвимы, какие меры можно предпринять для повышения уровня защищенности и при этом не потратить лишних денег, и всё это подтверждено документально, то решение задачи убедить руководство обратить внимание и выделить средства на обеспечение информационной безопасности становится значительно более реальным.

Для решения данной задачи были разработаны методики и программные комплексы анализа и контроля информационных рисков.

Среди наиболее распространенных методик анализируются: CRAMM; Microsoft; FRAP; OCTAVE; Risk Watch. Первые две методики нами уже рассмотрены. Сегодня мы рассмотрим методики FRAP; OCTAVE; Risk Watch.

Методики FRAP, OCTAVE использует оценку риска на качественном уровне (например, по шкале "высокий", "средний", "низкий"). Количественные методики (риск оценивают через числовое значение, например размер ожидаемых годовых потерь). К этому классу относится методика RiskWatch;

10.2 Методика FRAP

Методика "Facilitated Risk Analysis Process (FRAP) (Облегченный Процесс Анализа Риска)" предложена консалтинговой компанией Пелтиер Ассокиетз, специализирующейся на оценке потерь от наличия уязвимых мест в системе безопасности и выработке рекомендаций по их предотвращению. Методика

разработана Томасом Пелтиером. В методике, обеспечение ИБ ИС предлагается рассматривать в рамках процесса управления рисками.

Управление рисками в сфере ИБ - процесс, позволяющий компаниям найти баланс между затратами средств и сил на средства защиты и получаемым эффектом.

Управление рисками должно начинаться с оценки рисков: должным образом оформленные результаты оценки станут основой для принятия решений в области повышения безопасности системы.

После завершения оценки, проводится анализ соотношения затрат и получаемого эффекта, который позволяет определить те средства защиты, которые нужны, для снижения риска до приемлемого уровня.

Ниже приведены основные этапы оценки рисков. Данный список во многом повторяет аналогичный перечень из других методик, но во FRAP более подробно раскрываются пути получения данных о системе и ее уязвимостях.

Основные этапы оценки риска

1. Определение защищаемых активов. Производится с использованием опросных листов, изучения документации на систему, использования инструментов автоматизированного анализа (сканирования) сетей.

2. Идентификация угроз. При составлении списка угроз могут использоваться разные подходы:

- заранее подготовленные экспертами перечни угроз (checklists), из которых выбираются актуальные для данной системы;
- анализ статистики происшествий в данной ИС и в подобных ей - оценивается частота их возникновения; по ряду угроз, например, угрозе возникновения пожара, подобную статистику можно получить у соответствующих государственных организаций;
- "мозговой штурм", проводимый сотрудниками компании.

3. Когда список угроз закончен, каждой из них сопоставляют вероятность возникновения. После чего **оценивают ущерб**, который может быть нанесен данной угрозой. Исходя из полученных значений, **оценивается уровень угрозы.**

При проведении анализа, как правило, принимают, что на начальном этапе в системе отсутствуют средства и механизмы защиты. Таким образом оценивается уровень риска для незащищенной ИС, что в последствии позволяет показать эффект от внедрения средств защиты информации (СЗИ).

Оценка производится для вероятности возникновения угрозы и ущерба от нее по следующим шкалам.

Вероятность (Probability):

- Высокая (High Probability) - очень вероятно, что угроза реализуется в течение следующего года;
- Средняя (Medium Probability) - возможно угроза реализуется в течение следующего года;

- Низкая (Low Probability) - маловероятно, что угроза реализуется в течение следующего года.

Ущерб (Impact) - мера величины потерь или вреда, наносимого активу:

- Высокий (High Impact): остановка критически важных бизнес-подразделений, которая приводит к существенному ущербу для бизнеса, потере имиджа или неполучению существенной прибыли;

- Средний (Medium Impact): кратковременное прерывание работы критических процессов или систем, которое приводит к ограниченным финансовым потерям в одном бизнес-подразделении;

- Низкий (Low Impact): перерыв в работе, не вызывающий ощутимых финансовых потерь.

Оценка риска определяется в соответствии с правилом, задаваемым матрицей рисков, изображенной на рис 15. Полученная оценка уровня риска может интерпретироваться следующим образом:

- уровень А - связанные с риском действия (например, внедрение СЗИ) должны быть выполнены немедленно и в обязательном порядке;

- уровень В - связанные с риском действия должны быть предприняты;

- уровень С - требуется мониторинг ситуации (но непосредственных мер по противодействию угрозе принимать, возможно, не надо);

- уровень D - никаких действий в данный момент предпринимать не требуется.

		ИМПАКТ		
P R O B A B I L I T Y		High	Medium	Low
	High	A	B	C
	Medium	B	B	C
	Low	B	C	D

A - Corrective action must be implemented
 B - Corrective action should be implemented
 C - Requires monitor
 D - No action required at this time

Рис. 15. Матрица рисков FRAP

4. После того как угрозы идентифицированы и дана оценка риска, должны быть **определены контрмеры**, позволяющие устранить риск или свести его до приемлемого уровня.

При этом должны приниматься во внимание законодательные ограничения, делающие невозможным или, наоборот, предписывающие в обязательном порядке, использование тех или иных средств и механизмов защиты.

Чтобы определить ожидаемый эффект, можно провести оценку того же риска, но при условии внедрения предлагаемого СЗИ. Если риск снижен недостаточно, возможно, надо применить другое СЗИ.

Вместе с определением средства защиты, надо определить **какие затраты повлечет его приобретение и внедрение** (затраты могут быть как прямые, так и косвенные - см. ниже). Кроме того, необходимо оценить, безопасно ли само это средство, не создает ли оно новых уязвимостей в системе.

Чтобы использовать экономически эффективные средства защиты, нужно проводить анализ соотношения затрат и получаемого эффекта. При этом надо оценивать не только стоимость приобретения решения, но и стоимость поддержания его работы. В затраты могут включаться:

- стоимость реализации проекта, включая дополнительное программное и аппаратное обеспечение;
- снижение эффективности выполнения системой своих основных задач;
- внедрение дополнительных политик и процедур для поддержания средства;
- затраты на найм дополнительного персонала или переобучение имеющегося.

5. **Документирование.** Когда оценка рисков закончена, ее результаты должны быть подробно документированы в стандартизованном формате. Полученный отчет может быть использован при определении политик, процедур, бюджета безопасности и т.д.

6.

10.3 Методика OCTAVE (октэйв)

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) - методика поведения оценки рисков в организации. Разработана Инженерным Институтом Программного Обеспечения (SEI) при университете Карнеги Меллон (университет и исследовательский центр, расположенный в Питтсбурге, штат Пенсильвания, США).

Особенность данной методики заключается в том, что весь процесс анализа производится силами сотрудников организации, без привлечения внешних консультантов. Для этого создается смешанная группа, включающая как технических специалистов, так и руководителей разного уровня, что позволяет все-сторонне оценить последствия для бизнеса возможных инцидентов в области безопасности и разработать контрмеры.

OCTAVE предполагает три фазы анализа:

1. разработка **профиля угроз**, связанных с активом;
2. идентификация инфраструктурных уязвимостей;
3. разработка стратегии и планов безопасности.

Профиль угрозы включает в себя указания на актив (asset), тип доступа к активу (access), источник угрозы (actor), тип нарушения или мотив (motive), результат (outcome) и ссылки на описания угрозы в общедоступных каталогах. По типу источника, угрозы в OSTAVE делятся на:

1. угрозы, исходящие от человека-нарушителя, действующего через сеть передачи данных;
2. угрозы, исходящие от человека-нарушителя, использующего физический доступ;
3. угрозы, связанные со сбоями в работе системы;
4. прочие.

Результатом может быть раскрытие (disclosure), изменение (modification), потеря или разрушение (loss/destruction) информационного ресурса или разрыв подключения. Отказ в обслуживании (interruption).

Методика OSTAVE предлагает при описании профиля использовать "деревья вариантов", пример подобного дерева для угроз класса 1) приведен на Рис 2. При создании профиля угроз рекомендуется избегать обилия технических деталей - это задача второго этапа исследования. Главная задача первой стадии - стандартизованным образом описать сочетание угрозы и ресурса.

Предположим, что на предприятии имеется информационный ресурс (актив) - база данных (БД) отдела кадров (HR Database). Профиль, соответствующий угрозе кражи информации сотрудником предприятия представлен в таблице 1.

Таблица1. Пример профиля угрозы.

Ресурс (Asset)	БД отдела кадров (HR Database)
Тип доступа (Access)	Через сеть передачи данных (Network)
Источник угрозы (Actor)	Внутренний (Inside)
Тип нарушения (Motive)	Преднамеренное (Deliberate)
Уязвимость (Vulnerability)	-
Результат (Outcome)	Раскрытие данных (Disclosure)
Ссылка на каталог уязвимостей (Catalog reference)	-



Human Actors - Network Access



©2001 Carnegie Mellon University

S4-14

Рис. 16 Дерево вариантов, использующееся при описании профиля.

Вторая фаза исследования системы в соответствии с методикой - **идентификация инфраструктурных уязвимостей**. В ходе этой фазы определяется инфраструктура, поддерживающая существование выделенного ранее актива.

Например, если это БД отдела кадров, то нам для работы с ней нужен сервер, на котором база размещена, рабочая станция служащего отдела кадров и то окружение, которое может позволить получить к ней доступ (например, соответствующий сегмент локальной сети).

Рассматриваются компоненты следующих классов: серверы; сетевое оборудование; СЗИ; персональные компьютеры; домашние персональные компьютеры "надомных" пользователей, работающих удаленно, но имеющих доступ в сеть организации; мобильные компьютеры; системы хранения; беспроводные устройства; прочее.

Группа, проводящая анализ для каждого сегмента сети, отмечает, какие компоненты в нем проверяются на наличие уязвимостей. Уязвимости проверяются сканерами безопасности уровня операционной системы, сетевыми сканерами безопасности, специализированными сканерами (для конкретных web-серверов, СУБД и проч.), с помощью списков уязвимостей (checklists), тестовых скриптов.

Для каждого компонента определяется:

- список уязвимостей, которые надо устранить немедленно (high-severity vulnerabilities);
- список уязвимостей, которые надо устранить в ближайшее время (middle-severity vulnerabilities);
- список уязвимостей, в отношении которых не требуется немедленных действий (low-severity vulnerabilities).

По результатам стадии готовится отчет, в котором указывается, какие уязвимости обнаружены, какое влияние они могут оказать на выделенные ранее активы, какие меры надо предпринять для устранения уязвимостей.

Разработка стратегии и планов безопасности - третья стадия исследования системы. Она начинается с оценки рисков, которая проводится на базе отчетов по двум предыдущим этапам.

В OSTATE *при оценке риска дается только оценка ожидаемого ущерба, без оценки вероятности. Шкала: высокий (high), средний (middle), низкий (low)*. Оценивается финансовый ущерб, ущерб репутации компании, жизни и здоровью клиентов и сотрудников, ущерб, который может вызвать судебное преследование в результате того или иного инцидента. Описываются значения, соответствующие каждой градации шкалы (например, для малого предприятия финансовый ущерб в \$10000 - высокий, для более крупного - средний).

Далее, разрабатывают планы снижения рисков нескольких типов:

- долговременные;
- на среднюю перспективу;
- списки задач на ближайшее время.

Для определения мер противодействия угрозам в методике предлагаются каталоги средств.

Хотелось бы еще раз подчеркнуть, что в отличие от прочих методик, OSTATE не предполагает привлечения для исследования безопасности ИС сторонних экспертов, а вся документация по OSTATE общедоступна и бесплатна, что делает методику особенно привлекательной для предприятий с жестко ограниченным бюджетом, выделяемым на цели обеспечения ИБ.

10.4 Методика RiskWatch (пуск вэтч)

Компания RiskWatch разработала собственную методику анализа рисков и семейство программных средств, в которых она в той либо иной мере реализуется

В семейство RiskWatch входят программные продукты для проведения различных видов аудита безопасности:

- RiskWatch for Physical Security - для анализа физической защиты ИС;
- RiskWatch for Information Systems - для информационных рисков;
- HIPAA-WATCH for Healthcare Industry - для оценки соответствия требованиям стандарта HIPAA (US Healthcare Insurance Portability and Accountability Act), актуальных в основном для медицинских учреждений, работающих на территории США;
- RiskWatch RW17799 for ISO 17799 - для оценки соответствия ИС требованиям стандарта международного стандарта ISO 17799.

В методе RiskWatch в качестве критериев для оценки и управления рисками используются **ожидаемые годовые потери** (Annual Loss Expectancy, ALE) и **оценка возврата инвестиций** (Return on Investment, ROI).

RiskWatch ориентирована на точную **количественную оценку** соотношения потерь от угроз безопасности и затрат на создание системы защиты. В основе продукта RiskWatch находится методика анализа рисков, которая состоит из четырех этапов.

Первый этап - определение предмета исследования. Здесь описываются такие параметры, как тип организации, состав исследуемой системы (в общих чертах), базовые требования в области безопасности.

Для облегчения работы аналитика, в шаблонах, соответствующих типу организации ("коммерческая информационная система", "государственная/военная информационная система" и т.д.), есть списки категорий защищаемых ресурсов, потерь, угроз, уязвимостей и мер защиты. Из них нужно выбрать те, что реально присутствуют в организации (рис. 3).

Например, категории потерь:

- Задержки и отказ в обслуживании;
- Раскрытие информации;
- Прямые потери (например, от уничтожения оборудования огнем);
- Жизнь и здоровье (персонала, заказчиков и т.д.);
- Изменение данных;
- Косвенные потери (например, затраты на восстановление);
- Репутация.

Второй этап - ввод данных, описывающих конкретные характеристики системы. Данные могут вводиться вручную или импортироваться из отчетов, созданных инструментальными средствами исследования уязвимости компьютерных сетей. На этом этапе, в частности, подробно описываются ресурсы, потери и классы инцидентов. Классы инцидентов получаются путем сопоставления категории потерь и категории ресурсов.

Для выявления возможных уязвимостей используется вопросник, база которого содержит более 600 вопросов. Вопросы связаны с категориями ресурсов.

Также задается частота возникновения каждой из выделенных угроз, степень уязвимости и ценность ресурсов. Если для выбранного класса угроз в системе есть среднегодовые оценки возникновения (LAFE и SAFE), то используются они. Все это используется в дальнейшем для расчета эффекта от внедрения средств защиты.

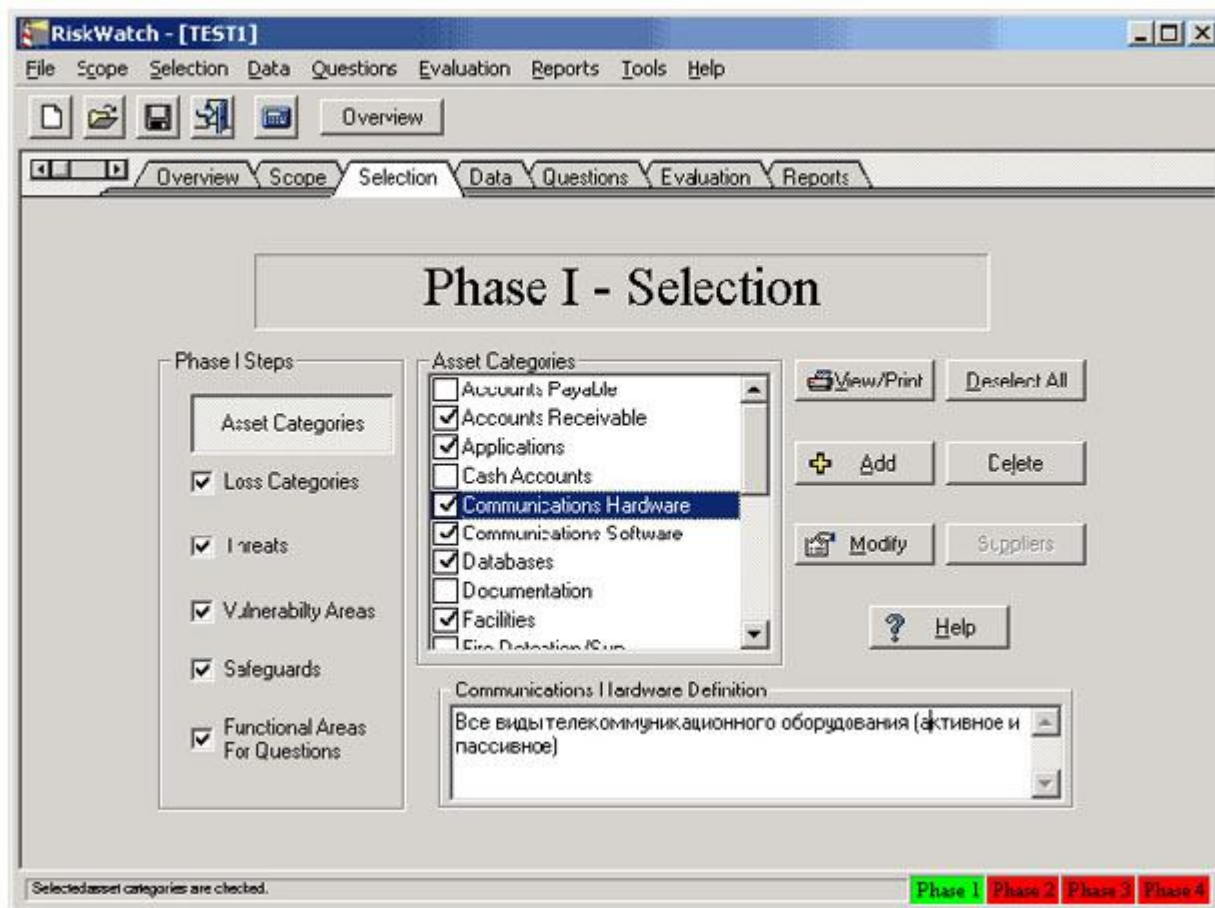


Рис. 17 Определение категорий защищаемых ресурсов

Третий этап - количественная оценка риска. На этом этапе рассчитывается профиль рисков, и выбираются меры обеспечения безопасности. Сначала устанавливаются связи между ресурсами, потерями, угрозами и уязвимостями, выделенными на предыдущих шагах исследования. По сути, риск оценивается с помощью математического ожидания потерь за год. Например, если стоимость сервера \$150000, а вероятность того, что он будет уничтожен пожаром в течение года, равна 0.01, то ожидаемые потери составят \$1500.

Формула расчета ($m=p*v$, где m -математическое ожидание, p - вероятность возникновения угрозы, v - стоимость ресурса) претерпела некоторые изменения, в связи с тем, что RiskWatch использует определенные американским институтом стандартов NIST оценки, называемые LAFE и SAFE.

LAFE (Local Annual Frequency Estimate) - показывает, сколько раз в год в среднем данная угроза реализуется в данном месте (например, в городе). SAFE (Standard Annual Frequency Estimate) - показывает, сколько раз в год в среднем данная угроза реализуется в этой "части мира" (например, в Северной Америке). Вводится также поправочный коэффициент, который позволяет учесть, что в результате реализации угрозы защищаемый ресурс может быть уничтожен не полностью, а только частично.

Формулы (1) и (2) показывают варианты расчета показателя ALE:

$$ALE = AssetValue \times ExposureFactor \times Frequency \quad (1)$$

где:

- Asset Value - стоимость рассматриваемого актива (данных, программ, аппаратуры и т.д.);
- Exposure Factor - коэффициент воздействия - показывает, какая часть (в процентах) от стоимости актива, подвергается риску;
- Frequency - частота возникновения нежелательного события;
- ALE - это оценка ожидаемых годовых потерь для одного конкретного актива от реализации одной угрозы.

Когда все активы и воздействия идентифицированы и собраны вместе, то появляется возможность оценить общий риск для ИС, как сумму всех частных значений.

Можно ввести показатели "ожидаемая годовая частота происшествия" (Annualized Rate of Occurrence - ARO) и "ожидаемый единичный ущерб" (Single Loss Expectancy - SLE), который может рассчитываться как разница первоначальной стоимости актива и его остаточной стоимости после происшествия (хотя подобный способ оценки применим не во всех случаях, например, он не подходит для оценки рисков, связанных с нарушением конфиденциальности информации). Тогда, для отдельно взятого сочетания угроза-ресурс применима формула (2)

$$ALE = ARO \times SLE \quad (2)$$

ополнительно рассматриваются сценарии "что если:", которые позволяют описать аналогичные ситуации при условии внедрения средств защиты. Сравнивая ожидаемые потери при условии внедрения защитных мер и без них можно оценить эффект от таких мероприятий.

RiskWatch включает в себя базы с оценками LAFE и SAFE, а также с обобщенным описанием различных типов средств защиты.

Эффект от внедрения средств защиты количественно описывается с помощью показателя ROI (Return on Investment - возврат инвестиций), который показывает отдачу от сделанных инвестиций за определенный период времени. Рассчитывается он по формуле:

$$ROI = \sum_i NPV(Benefits_i) - \sum_j NPV(Costs_j) \quad (3)$$

где:

- $Costs_j$ - затраты на внедрение и поддержание j -меры защиты;
- $Benefits_i$ - оценка той пользы (т.е. ожидаемого снижения потерь), которую приносит внедрение данной меры защиты;
- NPV (Net Present Value) - чистая текущая стоимость.

Четвертый этап - генерация отчетов.

Типы отчетов:

- Краткие итоги.
- Полные и краткие отчеты об элементах, описанных на стадиях 1 и 2.
- Отчет от стоимости защищаемых ресурсов и ожидаемых потерях от реализации угроз.
- Отчет об угрозах и мерах противодействия.
- Отчет о ROI (фрагмент - на рис. 18).
- Отчет о результатах аудита безопасности.

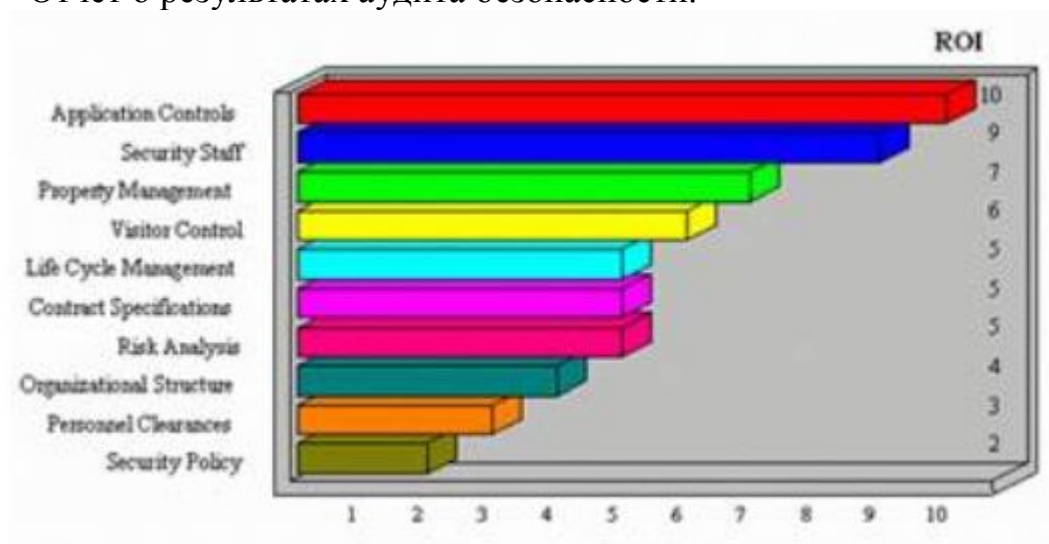


Рис. 18 Пример графика показателя ROI для различных мер защиты

Таким образом, рассматриваемое средство позволяет оценить не только те риски, которые сейчас существуют у предприятия, но и ту выгоду, которую может принести внедрение физических, технических, программных и прочих средств и механизмов защиты.

Подготовленные отчеты и графики дают материал, достаточный для принятия решений об изменении системы обеспечения безопасности предприятия.

Для отечественных пользователей проблема заключается в том, что получить используемые в RiskWatch оценки (такие как LAFE и SAFE) для наших условий достаточно проблематично. Хотя сама методология может с успехом применяться и у нас.

Подводя итог, можно отметить, что конкретную методику проведения анализа рисков на предприятии и инструментальные средства, поддерживающие ее, нужно выбирать, учитывая следующие факторы:

Наличие экспертов, способных дать достоверные оценки объема потерь от угроз информационной безопасности;

Наличие на предприятии достоверной статистики по инцидентам в сфере информационной безопасности;

Нужна ли точная количественная оценка последствий реализации угроз или достаточно оценки на качественном уровне.

К недостаткам RiskWatch можно отнести:

Такой метод подходит, если требуется провести анализ рисков на программно-техническом уровне защиты, без учета организационных и административных факторов.

Полученные оценки рисков (математическое ожидание потерь) далеко не исчерпывает понимание риска с системных позиций - метод не учитывает комплексный подход к информационной безопасности.

Программное обеспечение RiskWatch существует только на английском языке.

Высокая стоимость лицензии (от 10 000 долл. за одно рабочее место для небольшой компании).

Тема 11: "Правовые меры обеспечения информационной безопасности"

11.1 Основные направления обеспечения информационной безопасности

Высокая степень информатизации современных предприятий, учреждений и организаций обуславливает необходимость всестороннего комплексного подхода к обеспечению защиты информации, как от внутренних, так и от внешних угроз.

С учетом практики, что сложилась на настоящее время, выделяют следующие направления защиты информации:

- **правовая защита** — это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, которые обеспечивают защиту информации на правовой основе;
- **организационная защита** — это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, которая исключает или ослабляет нанесение каких-либо убытков предприятию;
- **инженерно-техническая защита** — это использование разнообразных технических средств, которые препятствуют нанесению убытков предприятию.

Кроме того, меры защиты, ориентированные на обеспечение безопасности информации, могут быть охарактеризованы целым рядом параметров, которые отображают, кроме направлений, ориентацию на объекты защиты, характер угроз, способы действий, их распространение, размах и масштабность.

Так, по характеру угроз защитные мероприятия ориентированы на защиту информации от разглашения, утечки и несанкционированного доступа.

По способу действия их можно разделить на предупреждение, выявление, прекращение и возмещение убытков или других потерь.

По охвату защитные мероприятия могут распространяться на территорию, здание, помещение, аппаратуру или отдельные элементы аппаратуры.

Масштабность мероприятий защиты характеризуется как объектовая, групповая или индивидуальная защита.

11.2 Законодательно-правовая база обеспечения информационной безопасности на предприятии

Правовая защита информации на межгосударственном и государственном уровне определяется межгосударственными договорами, конвенциями, декларациями и реализуется патентами, авторским правом и лицензиями на их защиту. На государственном уровне правовая защита регулируется государственными и ведомственными актами (рис. 1).

В нашем государстве такими правилами (актами, нормами) является Конституция Украины, законы Украины, гражданское, административное, уголовное право, изложенное в соответствующих кодексах. (Л 4)

Что же касается ведомственных нормативных актов, то они определяются приказами, руководствами, положениями и инструкциями, которые издаются ведомствами, организациями и предприятиями, и действуют в пределах определенных структур (например, в пределах министерства или отдельного предприятия).

При этом ведомственные документы по информационной безопасности не должны противоречить законам и правовым актам Украины. Требования информационной безопасности должны разрабатываться на основе Конституции Украины, общих и специальных законов и кодексов, которые включают

нормы по вопросам информационной безопасности, а так же на основе подзаконных актов по защите информации.

В их составе особое место занимают Законы "Об информации", "О государственной тайне" и "О защите информации в информационно-телекоммуникационных системах", рассмотренные ранее.

Правовая защита информации на предприятии обеспечивается нормативно законодательными актами, совокупность которых представляет собой систему от Конституции Украины до функциональных обязанностей и контракта конкретного исполнителя, которые, с одной стороны, определяют перечень сведений, подлежащих охране, и с другой стороны – ответственность за их разглашение.

Опираясь на государственные правовые акты и учитывая ведомственные интересы на уровне конкретного предприятия (фирмы, организации), разрабатываются собственные нормативно-правовые документы, ориентированные на обеспечение информационной безопасности.

11.3 Нормативные акты предприятия по информационной безопасности

Основным документом по информационной безопасности современного коммерческого предприятия является документ под названием "Политика информационной безопасности предприятия (компании, организации и т.д.)".

Политика безопасности организации — совокупность руководящих принципов, правил, процедур и практических приёмов в области безопасности, которые регулируют управление, защиту и распределение ценной информации.

"Политика безопасности" включает в себя комплекс превентивных мер по защите информации на предприятии и содержит требования в адрес персонала, менеджеров и технических служб.

Основные направления разработки политики безопасности:

- определение, какие данные и насколько серьезно необходимо защищать,
- определение кто и какой ущерб может нанести фирме в информационном аспекте,
- вычисление рисков и определение схемы уменьшения их до приемлемой величины.

Целью политики информационной безопасности является обеспечение развития организации в области ИБ в соответствии с целями бизнеса и требованиями, предъявляемыми различными регулирующими органами.

Данный документ регламентирован международными стандартами по информационной безопасности ISO 27001 и ISO 27002.

Стандарт ISO 27002 определяет, что политика информационной безопасности должна быть одобрена руководством компании, опубликована и доведена до сведения всех сотрудников и заинтересованных сторонних организаций.

Политика информационной безопасности должна включать следующее:

Определение понятия информационная безопасность;
Цели обеспечения информационной безопасности;
Признание важности обеспечения информационной безопасности;
Заявление о намерении руководства компании поддерживать цели и принципы обеспечения информационной безопасности, соответствующим целям бизнеса;

Подход к управлению рисками и выбора контрмер для минимизации рисков информационной безопасности;

Краткое объяснение принципов информационной безопасности, требования информационной безопасности (выполнение требований регуляторов, обучение в области информационной безопасности, обеспечение непрерывности бизнеса, последствия нарушения положений политики информационной безопасности);

Определение общих и специфических обязанностей по обеспечению информационной безопасности;

Ссылки на более детальные политики и процедуры поддерживающие политику информационной безопасности.

Политика информационной безопасности должна пересматриваться через определенные интервалы времени и в случае значительных изменений (изменения структуры компании, стратегических целей бизнеса) для того, чтобы оставаться актуальной и эффективной.

Помимо того, что политика информационной безопасности должна быть утверждена руководством и должна определять принципы информационной безопасности, подход к выбору мер по снижению рисков информационной безопасности, учитывать требования законодательства и закрепленные в контрактах, не противоречить подходу к управлению рисками, принятом в компании, она должна также определять критерии для оценки рисков.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы, и стратегия защиты определена, составляется программа обеспечения информационной безопасности, которая должна реализовать принятую политику безопасности.

Пример высокоуровневой политики информационной безопасности:

Политика информационной безопасности.

Настоящая политика определяет цели и принципы обеспечения информационной безопасности в Компании.

Политика распространяется на главный офис Компании и все филиалы. Политика обязательна для исполнения всеми сотрудниками, а также лицами, работающими с информацией, принадлежащей Компании, в рамках заключенных контрактов.

Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности. Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам, целостность – в случае внесения в данные исключительно авторизованных изменений, доступность – при обеспечении возможности получения доступа к данным авторизованным лицам в нужное для них время.

Целями обеспечения информационной безопасности являются минимизация ущерба от реализации угроз информационной безопасности и улучшение деловой репутации и корпоративной культуры Компании.

Информация является важным активом Компании и ее защита является обязанностью каждого сотрудника.

Доступ к информации предоставляется только лицам, которым он необходим для выполнения должностных или контрактных обязательств в минимально возможном объеме.

Для каждого информационного ресурса определяется владелец, отвечающий за предоставление к нему доступа и эффективное функционирование мер защиты информации.

Сотрудники Компании проходят регулярное обучение в области информационной безопасности.

В Компании ежегодно проводится независимый аудит информационной безопасности.

Генеральный директор Компании утверждает политики информационной безопасности.

Отдел информационной безопасности отвечает за определение детальных требований информационной безопасности и контролирует их исполнение в Компании.

Система управления информационной безопасностью в Компании строится на основе международных стандартов ISO 27001 и ISO 27002.

Меры защиты информации внедряются по результатам проведения оценки рисков информационной безопасности.

Оценка рисков информационной безопасности проводится ежегодно, а также в случае значительных изменений в структуре Компании и ее бизнес-процессах.

При оценке рисков учитывается влияние реализации угроз информационной безопасности на финансовое положение Компании и ее репутацию на рынке.

Стоимость принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз.

Успешное достижение целей настоящей политики возможно только при выполнении положений следующих детальных политик информационной безопасности:

Политика использования паролей;

Политика использования сети Интернет;

Политика использования электронной почты;

...

Несоблюдение политик информационной безопасности сотрудниками Компании может повлечь дисциплинарные меры взыскания вплоть до увольнения.

Кроме политики и программы информационной безопасности на предприятии разрабатываются следующие документы:

- положение о сохранении конфиденциальной информации;
- перечень сведений, которые составляют конфиденциальную информацию;
- инструкция о порядке допуска сотрудников к сведениям, которые составляют конфиденциальную информацию;
- положение о специальном делопроизводстве и документообороте;
- перечень сведений, которые разрешены к опубликованию в открытой печати;
- положение о работе с иностранными фирмами и их представителями;
- обязательство сотрудника о сохранении конфиденциальной информации;
- памятка сотруднику о сохранении коммерческой тайны.

Приведенные выше нормативные акты направлены на предупреждение случаев неправомерного разглашения секретов. В случае их нарушения должны приниматься соответствующие меры воздействия.

11.4 Формы правовой защиты информации на предприятии

В зависимости от характера информации, ее доступности для заинтересованных потребителей, а также экономической целесообразности конкретных защитных мероприятий, могут быть избраны следующие формы защиты информации:

- патентование;
- признание сведений коммерческой тайной ("ноу-хау");
- авторское право;
- товарные знаки;
- применения норм обязательного права.

Существует определенная разница между авторским правом и коммерческой тайной.

К **авторскому праву** прибегают при широкой публикации своей информации, в то время как коммерческую тайну держат в секрете. Очевидно, что по сравнению с патентом и авторским правом коммерческая тайна и производственная тайна являются наиболее удобными, надежными и гибкими формами защиты информации.

Коммерческая тайна — это сведения, которые не являются государственными секретами и связаны с производством, технологией, управлением, финансами и другой деятельностью, разглашение, утечка и несанкционирован-

ный доступ к которой может привести к убыткам их владельцев (упущенная выгода).

К коммерческой тайне не относятся:

- сведения, которые охраняются государством;
- сведения, которые являются общеизвестными на законном основании;
- сведения о негативных сторонах деятельности;
- учредительные документы и сведения о хозяйственной деятельности.

Кроме вышеизложенных форм правовой защиты информации находит широкое распространение официальная передача права на пользование информацией в виде *лицензии*.

Лицензия — это разрешение, выданное государством на проведение некоторых видов хозяйственной деятельности, включая внешнеторговые операции (ввоз и вывоз) и предоставления права использовать защищенные патентами изобретения, технологии, методики. Лицензионные разрешения предоставляются на определенное время и на определенные виды товаров.

Создавая систему информационной безопасности, необходимо четко понимать, что **без правового обеспечения** защиты информации какие-либо претензии к недобросовестному сотруднику, клиенту, конкуренту и должностному лицу будут просто безосновательными.

Если перечень сведений конфиденциального характера не доведен своевременно до каждого сотрудника (естественно, если от допущен к выполнению должностных обязанностей) в письменном виде, то сотрудник, который похитил важную информацию при нарушении установленного порядка работы с ней скорее всего не будет наказан.

11.5 Другие документы предприятия, в которых отражаются вопросы обеспечения информационной безопасности

Правовые нормы обеспечения безопасности и защиты информации на конкретном предприятии (фирме, организации) отображаются в совокупности ***учредительных, организационных и функциональных*** документов.

Требования обеспечения безопасности и защиты информации отображаются в Уставе предприятия (учредительном договоре) в виде следующих положений:

- предприятие имеет право определять состав, объемы и порядок защиты конфиденциальных сведений, требовать от своих сотрудников обеспечения их сохранения и защиты от внутренних и внешних угроз;
- предприятие обязано обеспечивать сохранность конфиденциальной информации.

Такие требования дают администрации предприятия следующие права:

- создавать организационные структуры по защите конфиденциальной информации ("Служба защиты информации");

- издавать нормативные и предписывающие документы, которые определяют порядок выделения сведений конфиденциального характера и механизмы их защиты;

- включать требования по защите информации в соглашения по всем видам хозяйственной деятельности;

- требовать защиты интересов предприятия со стороны государственных и судебных инстанций;

- распоряжаться информацией, которая является собственностью предприятия, с целью получения выгоды и недопущения экономических убытков коллективу предприятия и его владельцу;

- разрабатывать "Перечень сведений конфиденциальной информации".

Требования правового обеспечения защиты информации предусматриваются в **коллективном договоре**. Коллективный договор должен содержать следующие требования.

- Раздел "Предмет договора". Администрация предприятия (в том числе и администрация самостоятельных подразделений) обязывается обеспечить разработку и осуществление мероприятий по определению и защите конфиденциальной информации. Трудовой коллектив принимает на себя обязательства по соблюдению установленных на предприятии требований по защите конфиденциальной информации. Администрация обязана учитывать требования защиты конфиденциальной информации в правилах внутреннего распорядка.

- Раздел "Кадры. Обеспечение дисциплины труда". Администрация обязывается привлекать нарушителей требований по защите коммерческой тайны к административной и криминальной ответственности в соответствии с действующим законодательством.

Правила внутреннего трудового распорядка для рабочих и служащих предприятия целесообразно дополнить следующими требованиями.

- Раздел "Порядок приема и увольнения рабочих и служащих".

При приеме рабочего или служащего на работу или переводе его в установленном порядке на другую работу, связанную с конфиденциальной информацией предприятия, а также при увольнении его с работы администрация обязана проинструктировать рабочего или служащего относительно правил сохранения коммерческой тайны с оформлением письменного обязательства о ее неразглашении. Администрация предприятия вправе принимать решения об отстранении от работ лиц, которые нарушают установленные требования по защите конфиденциальной информации.

- Раздел "Основные обязанности рабочих и служащих". Рабочие и служащие обязаны придерживаться требований нормативных документов по защите конфиденциальной информации на предприятии.

- Раздел "Основные обязанности администрации". Администрация предприятия, руководители подразделений обязаны:

- обеспечивать сохранность конфиденциальной информации, постоянно осуществлять организационную и воспитательно-профилактическую работу, направленную на защиту секретов предприятия;

- включать в должностные инструкции и положения обязанности по сохранению конфиденциальной информации;
- неуклонно выполнять требования Устава, коллективного договора, трудовых договоров, правил внутреннего распорядка и других организационных и хозяйственных документов в части обеспечения экономической и информационной безопасности.

Обязанности конкретного сотрудника, рабочего или служащего относительно защиты информации обязательно должны быть оговорены в трудовом договоре (контракте). В соответствии с КЗоТ при заключении трудового договора работник обязывается выполнять определенные требования, которые действуют на данном предприятии. Независимо от формы заключения договора (устного, письменного ли) подпись работника на приказе о приеме на работу подтверждает его согласие с условиями договора.

Требования по защите конфиденциальной информации могут быть оговорены в тексте договора, если договор заключается в письменной форме. Если же договор заключается в устной форме, то действуют требования по защите информации, которые вытекают из нормативно-правовых документов предприятия. При заключении трудового договора и оформлении приказа о приеме на работу нового сотрудника делается отметка об осведомленности его с порядком защиты информации предприятия. Это создает необходимый элемент привлечения данного лица в механизм обеспечения информационной безопасности.

Не следует считать, что после подписания такого соглашения с новым сотрудником тайна будет сохранена. Это только предупреждение сотруднику, что в дело вступает система мероприятий по защите информации, и правовая основа для того, чтобы прекратить его неверные или противоправные действия. Следующая задача — не допустить потери коммерческих секретов.

Вопросы соблюдения конфиденциальности отражаются отдельным пунктом в договорах, соглашениях и других документах, которые заключаются между различными предприятиями.

Правовая регуляция на предприятии необходима для совершенствования механизма предупреждения противоправных действий по отношению к информационным ресурсам, для уточнения и закрепления заданий и правомочия отдельных субъектов в сфере предупредительной деятельности, охраны прав и законных интересов граждан и организации.

Правовые мероприятия обеспечения безопасности и защиты информации являются основой порядка деятельности и поведения сотрудников предприятия и определяют меру их ответственности за нарушение установленных норм.

Тема 12: "Организационные меры обеспечения безопасности компьютерных информационных систем"

12.1 Общие положения организационной защиты

Организационная защита — это регламентация производственной деятельности и взаимоотношений исполнителей на нормативной основе, что исключает или существенно осложняет неправомерное овладение конфиденциальной информацией и проявления внутренних и внешних угроз.

Организационная защита обеспечивает:

- организацию режима, охраны, работу с кадрами, с документами;
- использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз деятельности предприятия (организации).

Организационные мероприятия играют существенную роль в создании надежного механизма защиты информации, поскольку возможности несанкционированного использования конфиденциальных сведений в значительной мере обуславливаются не техническими аспектами, а злоумышленными действиями и небрежностью пользователей или персонала. Именно люди являются главной угрозой, поэтому "человеческий фактор" заслуживает особого внимания.

Угрозы информационной безопасности, связанные с людьми, практически невозможно предотвратить с помощью технических мероприятий.

Для этого необходима совокупность организационно-правовых и организационно-технических мероприятий, которые исключали бы (или сводили к минимуму) возможность возникновения опасности утечки конфиденциальной информации.

К основным организационным мероприятиям обычно относят следующие:

1. Организация режима и охраны.

Цель:

- исключение возможности тайного проникновения на территорию и в помещение посторонних лиц;
- обеспечение удобства прохода и перемещения сотрудников и посетителей;
- создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа;
- контроль и соблюдение временного режима труда и пребывания на территории персонала предприятия;
- организация и поддержка надежного пропускного режима и контроля сотрудников и посетителей;
- организация работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерой ответственности за нарушение правил защиты информации;

2. Организация работы с документами и документируемой информацией, включая организацию разработки и использование документов и носителей конфиденциальной информации, их учет, использование, возврат, хранение и уничтожение.

3. Организация использования технических средств сбора, обработки и хранения конфиденциальной информации.

4. Организация работы по анализу внутренних и внешних угроз конфиденциальной информации и разработка мероприятий по обеспечению ее защиты.

5. Организация работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

В каждом конкретном случае организационные мероприятия носят специфическую для данной организации форму и содержание, которые направлены на обеспечение безопасности информации в конкретных условиях.

12.2. Особенности организационной защиты компьютерных информационных систем и сетей

Организация защиты компьютерных информационных систем и сетей определяет порядок и схему функционирования их основных подсистем, использования устройств и ресурсов, взаимоотношения пользователей между собой в соответствии с нормативно-правовыми требованиями и правилами.

Защита информации на основе организационных мероприятий играет значительную роль в обеспечении надежности и эффективности, поскольку несанкционированный доступ и утечка информации чаще всего обусловлены злоумышленными действиями, небрежностью пользователей или персонала. Эти факторы практически невозможно исключить или локализовать с помощью аппаратных и программных средств, криптографии и физических средств защиты, поэтому совокупность организационных, организационно-правовых и организационно-технических мероприятий, которые применяются вместе с техническими методами, имеют целью исключить, уменьшить или полностью устранить потери при действии разнообразных деструктивных факторов.

Организационные средства защиты компьютерных информационных систем и сетей чаще всего применяются в следующих случаях:

- при проектировании, строительстве и оборудовании помещений, узлов сети и других объектов информационной системы, исключая влияние стихийных бедствий, возможность недозволенного проникновения в помещения и др.;
- при подборе и подготовке персонала — в этом случае предусматривается проверка лиц, которые принимаются на работу, создание условий, при которых персонал был бы заинтересован в сохранности информации, обучение правилам работы с закрытой информацией, ознакомление с мерой ответственности за нарушение правил защиты и т.д.;

- при хранении и использовании документов и других носителей (маркировка, регистрация, определение правил выдачи и возвращения, ведение документации и др.);

- при соблюдении надежного пропускного режима к техническим средствам, к ПЭВМ и информационным системам при сменной работе (выделение ответственных за защиту информации в сменах, контроль за работой персонала, ведение (возможно и автоматизированное) журналов работы, уничтожение в установленном порядке закрытых производственных документов);

- при внесении изменений в программное обеспечение (строгое санкционирование, рассмотрение и утверждение проектов изменений, проверка их на удовлетворение требований защиты, документальное оформление изменений и т.п.);

- при подготовке и контроле работы пользователей.

Основными нормативными документами, регламентирующими организационные мероприятия по защите информации в информационных системах, являются:

– Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах, затверджене постановою Кабінету Міністрів України від 16.02.98 р. № 180;

– Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, що затверджені постановою Кабінету Міністрів України від 29.03.2006 р. № 373.

В соответствии с требованиями этого Положения и порядка обеспечения режима секретности, организации разрабатывают отдельные инструкции, правила выполнения работ по обеспечению режима секретности в ИС, а так же нормативные документы, которые используются в пределах организации и учитывают особенности и условия обработки информации в конкретной ИС.

К их числу относятся:

Положення про службу захисту інформації в ИС;

План захисту інформації в ИС;

Посібник користувача КСЗІ;

Інструкція про порядок введення в експлуатацію КСЗІ;

Інструкція про порядок модернізації КСЗІ;

Порядок розробки, впровадження та модернізації програмного забезпечення ИС;

Правила видачі, вилучення та обліку персональних ідентифікаторів;

Правила управління паролями в ИС;

Правила класифікації та класифікатор інформації і користувачів ИС;

Інструкція про порядок резервування інформації;

Порядок обліку і супроводження архівів та ротації носіїв інформації;

Інструкція про порядок оперативного відновлення функціонування ИС;

Інструкція про порядок використання криптографічних засобів;

Інструкція про порядок опрацювання секретних документів з використанням ИС;

Інструкція про організацію контролю за функціонуванням КСЗІ;
Інструкція про порядок проведення ремонтних робіт,
інші документи.

Обязательными документами являются Положения о службе защиты информации в ИС и План защиты информации в ИС.

Положение о службе защиты информации в ИС определяет задачи, функции, штатную структуру службы защиты информации, обязанности, права и ответственность работников службы, взаимодействие с другими подразделениями организации.

План защиты информации в ИС определяет: задачи защиты, классификацию информации, описание технологии обработки секретной информации, а так же календарный план работ по защите информации в ИС.

План защиты определяет перечень организационных мероприятий по защите информации в ИС.

Организационные мероприятия по защите информации в ИС.

Для обеспечения режима секретности во время обработки в ИС информации, что составляет государственную тайну, и надлежащего функционирования комплексной системы защиты информации создается служба защиты информации. Состав и функции службы защиты информации определяются в соответствии с документом "Положения о службе защиты информации".

Полномочия пользователей устанавливаются руководителем предприятия и согласовываются с РСО. Учет пользователей информационных систем осуществляется с помощью учетных карточек, на основании которых администратор безопасности вводит, изменяет или удаляет информацию о пользователе ИС. Учетные карточки заполняются и хранятся в РСО.

Учетная карточка обычного пользователя содержит такие данные:

- имя пользователя для регистрации в ОС;
- фамилию и инициалы, подразделение и должность пользователя;
- уровень допуска пользователя;
- перечень ролей пользователя.

Выполнение работ в ИС допускается работникам, которые имеют оформленный в установленном порядке допуск к государственной тайне.

РСО предприятия обеспечивает выполнение требований нормативных документов относительно обеспечения режима секретности во время работы с информацией, что составляет государственную тайну, а именно:

- контроль за процессом печати информации и копированием на съемные носители;
- учет печатных документов;
- учет съемных носителей (дискет, накопителей USB Flash и др.);
- учет технических средств, что прошли спецобследования;
- ведение учетных карточек пользователей.

Основные функции относительно обеспечения защиты информации в ИС

возлагаются на администратора безопасности. К его основным функциям относятся такие:

- ведение учетных карточек пользователей;
- ведение базы данных защиты;
- установление параметров работы системы;
- изменение, в случае необходимости, владельца документов;
- отслеживание потенциально опасных событий;
- архивация данных защиты.

Системный администратор должен выполнять такие функции:

- сопровождение программного обеспечения ИС;
- обеспечение антивирусной защиты.
- сопровождение аппаратного обеспечения (вместе с ответственным за безопасность информации).

Ответственный за безопасность информации должен выполнять такие функции:

- организация печати и учета носителей, что содержат ИзОД;
- наблюдение за работой системы;
- настройка аппаратного обеспечения.

За организацию работ с документами отвечает администратор документов. К его функциям относятся такие:

- создание баз документов;
- управление доступом к документам.

Все действия, которые прямо или опосредствовано могут повлиять на защищенность информации (изменения разрешений на доступ к файлам и папкам, очистки журналов ОС, изменения настроек BIOS Setup и тому подобное), системный администратор выполняет с разрешения администратора безопасности, что фиксируется в “Журнале обслуживания системы ЛОЗА-1”.

Контроль за соблюдением персоналом и пользователями ИС положений политики безопасности возлагается на РСО и службу защиты информации.

Ответственность за обеспечение режима секретности в ИС, своевременная разработка и внедрение необходимых мер возлагается на руководителя организации и руководителей ее структурных подразделений.

12.3 Служба безопасности предприятия

Одним из важнейших организационных мероприятий является создание специальных штатных служб защиты информации в закрытых информационных системах в виде администратора безопасности сети и администратора безопасности распределенных баз и банков данных, которые содержат сведения конфиденциального характера.

Вполне очевидно, что организационные мероприятия должны четко планироваться, направляться и осуществляться определенной организационной структурой, определенным специально созданным для этих целей структурным

подразделением, укомплектованным соответствующими специалистами по безопасности деятельности и защиты информации.

Чаще всего таким структурным подразделением является служба безопасности предприятия (фирмы, организации), на которую возлагаются следующие функции:

- организация и обеспечение охраны персонала, материальных и финансовых ценностей и защиты конфиденциальной информации;
- обеспечение пропускного и внутриобъектового режима на территории, в зданиях и помещениях, контроль соблюдения требований режима сотрудниками, смежниками, партнерами и посетителями;
- руководство работами по правовой и организационной регуляции отношений по защите информации;
- участие в разработке основополагающих документов с целью закрепления в них требований обеспечения безопасности и защиты информации, а также положений о подразделениях, трудовых договорах, соглашениях, подрядах, должностных инструкциях и обязанностях руководства, специалистов, рабочих и служащих;
- разработка и осуществление вместе с другими подразделениями мероприятий по обеспечению работы с документами, которые содержат конфиденциальные сведения; при всех видах работ организация и контроль выполнения требований "Инструкции по защите конфиденциальной информации";
- изучение всех сторон производственной, коммерческой, финансовой и другой деятельности для выявления и следующего противодействия каким-нибудь попыткам нанесения ущерба, ведение учета и анализ нарушений режима безопасности, накопление и анализ данных о злоумышленных стремлениях конкурентной и других организаций, о деятельности предприятия и его клиентов, партнеров, смежников;
- разработка, ведение, обновление и пополнение "Перечня сведений, что носят конфиденциальный характер" и других нормативных актов, которые регламентируют порядок обеспечения и защиты информации;
- обеспечение строгого выполнения требований нормативных актов по защите производственных секретов предприятия;
- осуществление руководства службами и подразделениями безопасности подведомственных предприятий, организаций, заведений и другими структурами в части оговоренных в договорах условий по защите информации;
- организация и регулярное проведение учета сотрудников предприятия и службы безопасности по всем направлениям защиты информации и обеспечения безопасности производственной деятельности;
- ведения учета и строгого контроля выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации и каналами проникновения к источникам информации, которые находятся под охраной;

- обеспечение проведения всех необходимых мероприятий по пресечению попыток нанесения морального и материального ущерба со стороны внутренних и внешних угроз;

- поддержка контактов с правоохранительными органами и службами безопасности соседних предприятий для изучения криминогенной обстановки в районе, (зоне) и предоставление взаимной помощи в кризисных ситуациях.

Служба безопасности является самостоятельной организационной единицей предприятия, которая подчиняется непосредственно руководителю предприятия. Возглавляет службу безопасности начальник службы безопасности в должности заместителя руководителя предприятия по безопасности.

Организационно служба безопасности может состоять из следующих структурных единиц:

- подразделения режима и охраны;
- специального подразделения по обработке документов конфиденциального характера (Служба защиты информации);
- инженерно-технических подразделений;
- информационно-аналитических подразделений.

В таком составе служба безопасности способна обеспечить защиту конфиденциальной информации от каких-либо угроз.

На службу безопасности возлагаются следующие задачи:

- определение круга лиц, которые в соответствии с положением, которое они занимают на предприятии, прямо или косвенно имеют доступ к сведениям конфиденциального характера;

- определение участков сосредоточения конфиденциальных сведений;
- определение круга посторонних предприятий, связанных с данным предприятием кооперативными связями, на которых в силу производственных отношений возможен выход из-под контроля сведений конфиденциального характера;

- выявление круга лиц, не допущенных к конфиденциальной информации, но которые проявляют повышенный интерес к таким сведениям;

- выявление круга предприятий, в том числе иностранных, что заинтересованы в доступе к сведениям, которые охраняются, с целью нанесения экономического ущерба данному предприятию, устранения экономического конкурента или его компрометации;

- разработка системы защиты документов, которые содержат сведения экономического характера;

- определение на предприятии участков, уязвимых в аварийном отношении, выход из строя которых может нанести материальный ущерб предприятию и сорвать поставки готовой продукции или комплектующих предприятиям, связанных с ним кооперацией;

- определение на предприятии технологического оборудования, выход (или выводение) которого из строя может привести к большим экономическим потерям;

- определение уязвимых мест в технологии производственного цикла, несанкционированное изменение в котором может привести к потере качества продукции и нанести материальный или моральный ущерб предприятию (потеря конкурентоспособности);

- определение на предприятии мест, несанкционированное посещение которых может привести к изъятию (хищению) готовой продукции или полуфабрикатов, заготовок и т.п. та организация их физической защиты;

- определение и обоснование мероприятий правовой, организационной и инженерно-физической защиты предприятия, персонала, продукции и информации;

- разработка необходимых мер, направленных на совершенствование системы экономической, социальной и информационной безопасности;

- внедрение в деятельность предприятия новейших достижений науки и техники, передового опыта в области обеспечения экономической и информационной безопасности;

- организация обучения сотрудников службы безопасности в соответствии с их функциональными обязанностями;

- изучение, анализ и оценка состояния обеспечения экономической и информационной безопасности предприятия и разработка предложений и рекомендаций для его усовершенствования;

- разработка технико-экономических обоснований, направленных на приобретение технических средств, получения консультации у специалистов, разработку необходимой документации с целью усовершенствования системы мероприятий по обеспечению экономической и информационной безопасности.

Организационные мероприятия являются решающим звеном формирования и реализации комплексной защиты информации и создания системы безопасности предприятия.

Тема 13: "Программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация, управление доступом"

13.1 Основные программно-технические меры.

По данным статистики главную угрозу информационным системам представляют легальные пользователи, а точнее их некомпетентность и неаккуратность при выполнении служебных обязанностей. Физическая защита в данном случае малоэффективна, и только программно-технические меры способны им противостоять.

Программно-технические меры обеспечения информационной безопасности ИС – это меры, направленные на защиту аппаратных, программных ресурсов и данных, хранящихся в ИС. В данном случае эта задача возлагается на саму информационную систему. Компьютеры помогли автоматизировать многие

области человеческой деятельности. Почему бы не возложить на них обеспечение собственной безопасности.

В рамках современных информационных систем известны следующие меры или **сервисы безопасности**:

- идентификация и аутентификация;
- управление доступом;
- протоколирование и аудит;
- шифрование;
- контроль целостности;
- экранирование;
- анализ защищенности;
- обеспечение высокой доступности;
- туннелирование;
- управление.

Среди этих мер можно выделить меры, направленные на:

- предупреждение нарушений ИБ;
- обнаружение нарушений ИБ;
- меры по локализации зоны действия нарушений;
- меры по выявлению нарушителя;
- меры по восстановлению режима безопасности.

Задачи сервисов безопасности

Большинство сервисов безопасности направлено на **предупреждение нарушений**. Это идентификация, аутентификация, управление доступом, шифрование, экранирование.

Протоколирование, аудит и контроль целостности помогут в **обнаружении нарушений**, (о которых, часто даже не знают). Активный аудит позволяет обеспечить **реакцию системы на нарушения** и отследить его.

Анализ защищенности необходим для **выявления уязвимых мест** ИС с целью их оперативной ликвидации.

Меры обеспечения высокой доступности направлены на **повышение отказоустойчивости системы и обеспечение безопасного восстановления** (например «откат операционной системы»).

Туннелирование – это конвертирование одних протоколов передачи пакетов через сеть, в другие протоколы. Оно позволяет реализовать такое защитное средство, как **частные виртуальные сети (VPN)** поверх других сетей, например, сети Интернет.

И, наконец, задача управления – **обеспечение нормальной работы** всех компонентов и средств безопасности.

Далее мы рассмотрим несколько подробнее основные сервисы безопасности.

13.2 Идентификация и аутентификация. Основные понятия

Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности. Идентификация и аутентификация — это первая линия обороны, «проходная» информационного пространства организации.

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством **аутентификации** вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова «аутентификация» иногда используют словосочетание «проверка подлинности».

(В обыденной жизни средством аутентификации личности является фотокарточка в паспорте или в каком-либо другом документе.)

Рассмотрим конкретный пример. Перед началом интерактивного сеанса работы большинство операционных систем запрашивают у пользователя его имя (логин) и пароль. Введенное имя является **идентификатором** пользователя, а его пароль - **аутентификатором**. Это пример односторонней аутентификации, когда клиент доказывает свою подлинность серверу. Аутентификация бывает и двусторонней (взаимной).

Существуют различные варианты реализации данного сервиса безопасности. Их разнообразие определяется 2-мя аспектами:

- 1) аутентификатором (то есть что используется для подтверждения подлинности субъекта);
- 2) организацией обмена данными идентификации/аутентификации.

Субъект может подтвердить свою подлинность, предъявив, один из следующих аутентификаторов:

- нечто, **что он знает** (пароль, личный идентификационный номер, криптографический ключ и т.д.)
- нечто, **чем он владеет** (личную карточку или иное устройство аналогичного назначения);
- нечто, **что есть часть его самого** (голос, отпечатки пальцев и т.п., то есть свои биометрические характеристики).

Существуют некоторые особенности, которые необходимо учесть.

1. В открытой сетевой среде между сторонами идентификации/аутентификации не существует доверенного маршрута. Это значит, что данные, переданные субъектом, могут быть искажены злоумышленником. Необходимо обеспечить защиту от пассивного и активного прослушивания сети, то есть от перехвата, изменения или воспроизведения данных. Передача паролей в открытом виде, очевидно, недопустима. Не спасает положение и шифрование паролей, так как оно не защищает от воспроизведения. Нужны более сложные протоколы аутентификации.

2. Надежная идентификация и аутентификация затруднена не только из-за сетевых угроз, но и по целому ряду других причин. Во-первых, почти все ау-

тентификаторы можно узнать, украсть или подделать. Во-вторых, имеется противоречие между надежностью аутентификации, с одной стороны, и удобствами пользователя и системного администратора с другой. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить аутентификационную информацию (ведь на его место мог сесть другой человек), а это не только хлопотно, но и повышает вероятность того, что кто-то может подсмотреть за вводом данных. В-третьих, чем надежнее средство защиты, тем оно дороже.

3. Современные средства идентификации/аутентификации должны поддерживать концепцию единого входа в сеть. Единый вход в сеть - это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная идентификация/аутентификация становится слишком обременительной. К сожалению, пока нельзя сказать, что единый вход в сеть стал нормой, доминирующие решения пока не сформировались.

Таким образом, необходимо искать компромисс между надежностью, доступностью по цене и удобством использования и администрирования средств идентификации и аутентификации.

Любопытно отметить, что сервис идентификации/аутентификации может стать **объектом атак на доступность**. Если система сконфигурирована так, что после определенного числа неудачных попыток устройство ввода идентификационной информации (такое, например, как терминал) блокируется, то злоумышленник может остановить работу легального пользователя буквально несколькими нажатиями клавиш.

Парольная аутентификация

Главное достоинство парольной аутентификации — простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать **самым слабым средством проверки подлинности**.

Чтобы пароль был запоминающимся, его зачастую делают простым (имя подруги, название спортивной команды и т.п.). Однако простой пароль нетрудно угадать, особенно если знать пристрастия данного пользователя. Известна классическая история про советского разведчика Рихарда Зорге, объект внимания которого через слово говорил «карамба» — разумеется, этим же словом открывался сверхсекретный сейф.

Иногда пароли с самого начала не хранятся в тайне, так как имеют стандартные значения, указанные в документации, и далеко не всегда после установки системы производится их смена.

Ввод пароля можно подсмотреть. Иногда для подглядывания используются даже оптические приборы.

Пароли нередко сообщают коллегам, чтобы те могли, например, подменить на некоторое время владельца пароля. Теоретически в подобных случаях более правильно задействовать средства управления доступом, но на практике так никто не поступает; а тайна, которую знают двое, это уже не тайна.

Пароль можно угадать «методом грубой силы», используя, скажем, словарь. Если файл паролей зашифрован, но доступен для чтения, его можно скачать к себе на компьютер и попытаться подобрать пароль, запрограммирован полный перебор (предполагается, что алгоритм шифрования известен).

Тем не менее, ***следующие меры позволяют значительно повысить надежность парольной защиты:***

- наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.);
- управление сроком действия паролей, их периодическая смена;
- ограничение доступа к файлу паролей;
- ограничение числа неудачных попыток входа в систему (это затруднит применение «метода грубой силы»);
- обучение пользователей;
- использование программных генераторов паролей (такая программа, основываясь на несложных правилах, может порождать только благозвучные и, следовательно, запоминающиеся пароли).

Перечисленные меры целесообразно применять всегда, даже если наряду с паролями используются другие методы аутентификации.

Одноразовые пароли

Рассмотренные выше пароли можно назвать многоразовыми; их раскрытие позволяет злоумышленнику действовать от имени легального пользователя. Гораздо более сильным средством, устойчивым к пассивному прослушиванию сети, являются одноразовые пароли.

Наиболее известным программным генератором одноразовых паролей является система S/KEY компании Bellcore. Идея этой системы состоит в следующем. Пусть имеется односторонняя функция f (то есть функция, вычислить обратную которой за приемлемое время не представляется возможным). Эта функция известна и пользователю, и серверу аутентификации. Пусть, далее, имеется секретный ключ K , известный только пользователю.

На этапе начального администрирования пользователя функция применяется к ключу K n раз, после чего результат сохраняется на сервере. После этого процедура проверки подлинности пользователя выглядит следующим образом:

- сервер присылает на пользовательскую систему число $(n-1)$;
- пользователь применяет функцию к секретному ключу K $(n-1)$ раз и отправляет результат по сети на сервер аутентификации;
- сервер применяет функцию f к полученному от пользователя, значению и сравнивает результат с ранее сохраненной величиной. В случае совпадения подлинность пользователя считается установленной, сервер запоминает новое значение (присланное пользователем) и уменьшает на единицу счетчик (n) .

Поскольку функция необратима, перехват пароля, равно как и получение доступа к серверу аутентификации, не позволяют узнать секретный ключ *K* и предсказать следующий одноразовый пароль.

Другой подход к надежной аутентификации состоит в генерации нового пароля через небольшой промежуток времени (например, каждые 60 секунд), для чего могут использоваться программы или специальные интеллектуальные карты (с практической точки зрения такие пароли можно считать одноразовыми). Серверу аутентификации должен быть известен алгоритм генерации паролей и ассоциированные с ним параметры; кроме того, часы клиента и сервера должны быть синхронизированы.

Сервер аутентификации Kerberos

Kerberos — это программный продукт, разработанный в середине 1980-х годов в Массачусетском технологическом институте и претерпевший с тех пор ряд принципиальных изменений. Клиентские компоненты Kerberos присутствуют в большинстве современных операционных систем.

Kerberos предназначен для решения следующей задачи. Имеется открытая (незащищенная) сеть, в узлах которой сосредоточены субъекты — пользователи, а также клиентские и серверные программные системы. Каждый пользователь *C* обладает секретным ключом. Чтобы пользователь *C* мог доказать свою подлинность серверу *S* (без этого *S* не станет обслуживать *C*), он должен не только назвать себя, но и продемонстрировать знание секретного ключа. Пользователь *C* не может просто послать *S* свой секретный ключ, во-первых, потому, что сеть открыта (доступна для пассивного и активного прослушивания), а, во-вторых, потому, что *S* не знает (и не должен знать) секретный ключ *C*. Требуется менее прямолинейный способ демонстрации знания секретного ключа.

Система Kerberos представляет собой доверенную третью сторону (то есть сторону, которой доверяют все), владеющую секретными ключами обслуживаемых субъектов и помогающую им в попарной проверке подлинности.

Чтобы с помощью Kerberos получить доступ к серверу *S*, пользователь *C* посылает Kerberos запрос, содержащий сведения о нем (клиенте) и о запрашиваемой услуге. В ответ Kerberos возвращает так называемый билет, зашифрованный секретным ключом *сервера*, и копию части информации из билета, зашифрованную секретным ключом *клиента*. Клиент должен расшифровать вторую порцию данных и переслать ее вместе с билетом серверу. Сервер, расшифровав билет, может сравнить его содержимое с дополнительной информацией, присланной клиентом. Совпадение свидетельствует о том, что клиент смог расшифровать предназначенные ему данные (ведь содержимое билета никому, кроме сервера и Kerberos, недоступно), то есть продемонстрировал знание секретного ключа. Значит, клиент — именно тот, за кого себя выдает. Подчеркнем, что секретные ключи в процессе проверки подлинности не передавались по сети (даже в зашифрованном виде) — они только использовались для шифрования. Как организован первоначальный обмен ключами между Kerberos и субъектами и как субъекты хранят свои секретные ключи — вопрос отдельный.

Проиллюстрируем описанную процедуру.

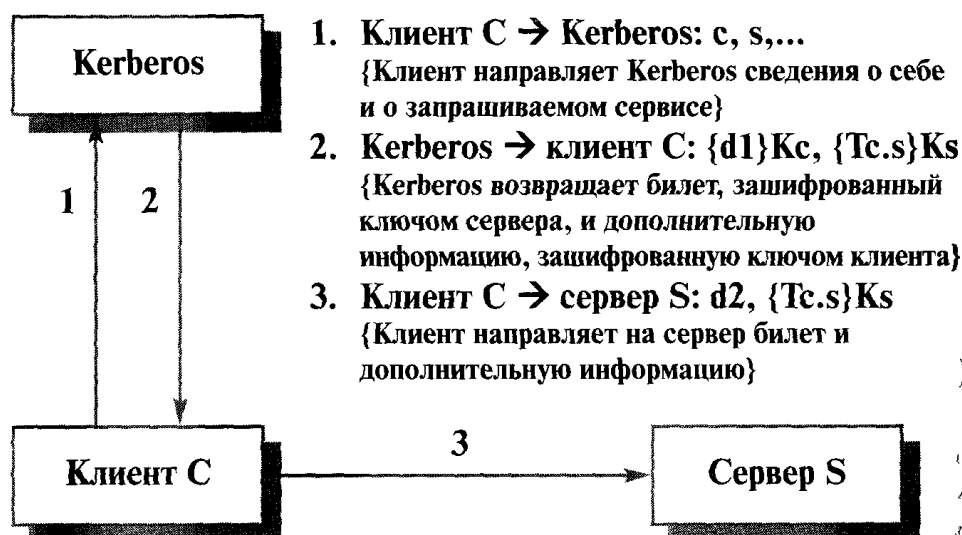


Рис. 19 Проверка сервером S подлинности клиента С

Здесь c и s — сведения (например, имя), соответственно, о клиенте и сервере, $d1$ и $d2$ — дополнительная (по отношению к билету) информация, $Tc.s$ — билет для клиента С на обслуживание у сервера S, Kc и Ks — секретные ключи клиента и сервера.

Идентификация/аутентификация с помощью биометрических данных

Биометрия представляет собой совокупность автоматизированных методов идентификации и/или аутентификации людей на основе их физиологических и поведенческих характеристик.

К числу физиологических характеристик принадлежат особенности отпечатков пальцев, сетчатки и роговицы глаз, геометрия руки и лица и т.п. К поведенческим характеристикам относятся динамика подписи (ручной). На стыке физиологии и поведения находятся анализ особенностей голоса и распознавание речи.

Биометрией во всем мире занимаются очень давно, однако долгое время все, что было связано с ней, отличалось сложностью и дороговизной. В последнее время спрос на биометрические продукты, в первую очередь в связи с развитием электронной коммерции, постоянно и весьма интенсивно растет. Это понятно, поскольку с точки зрения пользователя гораздо удобнее предъявить себя самого (свой палец или глаз), чем что-то запоминать. Спрос рождает предложение, и на рынке появились относительно недорогие аппаратно-программные продукты, ориентированные в основном на распознавание отпечатков пальцев.

В общем виде работа с биометрическими данными организована следующим образом. Сначала создается и поддерживается **база данных характеристик потенциальных пользователей**. Для этого биометрические характеристики пользователя снимаются, обрабатываются, и результат обработки (на-

зываемый биометрическим шаблоном) заносится в базу данных (исходные данные, такие как результат сканирования пальца или роговицы, обычно не хранятся).

В дальнейшем для идентификации (и одновременно аутентификации) пользователя процесс снятия и обработки повторяется, после чего производится поиск в базе данных шаблонов. В случае успешного поиска личность пользователя и ее подлинность считаются установленными. Для аутентификации достаточно произвести сравнение с одним биометрическим шаблоном, выбранным на основе предварительно введенных данных (имя пользователя).

Иногда биометрическая аутентификация является лишь первым рубежом защиты и служит для активизации интеллектуальных карт, хранящих криптографические секреты. В таком случае биометрический шаблон хранится на той же карте.

На наш взгляд, к биометрии следует относиться весьма осторожно. Необходимо учитывать, что она подвержена тем же угрозам, что и другие методы аутентификации. Во-первых, биометрический шаблон сравнивается не с результатом первоначальной обработки характеристик пользователя, а с тем, что пришло к месту сравнения. А, как известно, за время пути... много чего может произойти. Во-вторых, биометрические методы не более надежны, чем база данных шаблонов. В-третьих, следует учитывать разницу между применением биометрии на контролируемой территории, под бдительным оком охраны, и в «полевых» условиях, когда, например, к устройству сканирования роговицы могут поднести муляж и т.п. В-четвертых, биометрические данные человека меняются, так что база шаблонов нуждается в сопровождении, что создает определенные проблемы и для пользователей, и для администраторов.

Но главная опасность состоит в том, что любая «пробоина» для биометрии оказывается **фатальной**. Пароли, при всей их ненадежности, в крайнем случае, можно сменить. Утерянную аутентификационную карту можно аннулировать и завести новую. Палец же, глаз или голос сменить нельзя. Если биометрические данные окажутся скомпрометированы, придется, как минимум производить существенную модернизацию всей системы.

13.3 Управление доступом. Основные понятия

С традиционной точки зрения средства управления доступом позволяют контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над объектами (информацией и другими компьютерными ресурсами). В данном разделе речь идет о логическом управлении доступом, которое, в отличие от физического, реализуется программными средствами. Логическое управление доступом — это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность (путем запрещения обслуживания неавторизованных пользователей).

Рассмотрим формальную постановку задачи в традиционной трактовке. Имеется совокупность субъектов и набор объектов. Задача логического управ-

ления доступом состоит в том, чтобы для каждой пары «субъект-объект» определить множество допустимых операций и контролировать выполнение установленного порядка.

Отношение «субъекты-объекты» можно представить в виде матрицы доступа, в строках которой перечислены субъекты, в столбцах — объекты, а в клетках, расположенных на пересечении строк и столбцов, записаны дополнительные условия (например, время и место действия) и разрешенные виды доступа.

К объектам относятся файлы, устройства и процессы. Применительно к файлам и устройствам обычно рассматриваются права на чтение, запись, выполнение (для программных файлов), иногда на удаление и добавление. Отдельным правом может быть возможность передачи полномочий доступа другим субъектам (так называемое право владения).

Права (профили) пользователей задаются системным администратором.

Контроль прав доступа производится разными компонентами программной среды — ядром операционной системы, сервисами безопасности, системой управления базами данных, программным обеспечением промежуточного слоя (таким, как монитор транзакций) и т.д.

При принятии решения о предоставлении доступа обычно анализируется следующая информация:

- идентификатор пользователя;
- атрибуты пользователя (метка безопасности, группа пользователя и т.п.).

Метки безопасности — основа принудительного (мандатного) управления доступом.

Матрицу доступа обычно хранят по столбцам, то есть для каждого объекта поддерживается список «допущенных» пользователей вместе с их правами.

Списки доступа — исключительно гибкое средство. Посредством списков системный администратор может добавить права или явным образом запретить доступ (например, чтобы наказать нескольких членов группы пользователей). Безусловно, списки являются лучшим средством **произвольного управления доступом**.

Подавляющее большинство операционных систем и систем управления базами данных реализуют именно произвольное управление доступом. Основное достоинство произвольного управления — гибкость. Вообще говоря, для каждой пары «субъект-объект» можно независимо задавать права доступа, если используются списки управления доступом.

Удобной надстройкой над средствами логического управления доступом является ограничивающий интерфейс, когда пользователя лишают самой возможности попытаться совершить несанкционированные действия, включив в число видимых ему объектов только те, к которым он имеет доступ. Например, у каждого пользователя может храниться на общем накопителе своя информация, доступ к которой имеет только он один. Файлы других пользователей он просто не видит.

Тема 14: "Протоколирование и аудит, шифрование, контроль целостности"

14.1 Протоколирование и аудит

Под протоколированием понимается сбор и накопление информации о событиях, происходящих в информационной системе.

У каждого сервиса свой набор возможных событий. Их можно разделить на внешние (вызванные действиями других сервисов), внутренние (вызванные действиями самого сервиса) и клиентские (вызванные действиями пользователей и администраторов).

Аудит — это анализ накопленной информации. Он проводится оперативно, в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Реализация протоколирования и аудита решает следующие задачи:

- обеспечение подотчетности пользователей и администраторов;
- обеспечение возможности реконструкции последовательности событий;
- обнаружение попыток нарушений информационной безопасности;
- предоставление информации для выявления и анализа проблем.

Протоколирование требует для своей реализации здравого смысла. Какие события регистрировать? С какой степенью детализации? На подобные вопросы невозможно дать универсальные ответы. Необходимо следить за тем, чтобы, с одной стороны, достигались перечисленные выше цели, а, с другой, расход ресурсов оставался в пределах допустимого. Слишком обширное или подробное протоколирование не только снижает производительность сервисов (что отрицательно сказывается на доступности), но и затрудняет аудит, то есть не увеличивает, а уменьшает информационную безопасность.

Применительно к операционным системам в «Оранжевой книге» предлагается протоколировать следующие события:

- вход в систему (успешный или нет);
- выход из системы;
- обращение к удаленной системе;
- операции с файлами (открыть, закрыть, переименовать, удалить);
- смена привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и тп.).

При протоколировании события рекомендуется записывать, по крайней мере, следующую информацию:

- дата и время события;
- уникальный **идентификатор пользователя** — инициатора действия;
- тип события;
- результат действия (успех или неудача);
- источник запроса (например, имя терминала);

- имена затронутых объектов (например, открываемых или удаляемых файлов);
- описание изменений, внесенных в базы данных защиты (например, новая метка безопасности объекта).

Еще одно важное понятие, фигурирующее в «Оранжевой книге», — **выборочное протоколирование**, как в отношении пользователей (внимательно следить только за подозрительными), так и в отношении событий.

Реализация протоколирования и аудита — зависит от других средств безопасности. Идентификация и аутентификация является обязательным условием регистрации действий пользователей, (иначе все действия будут записаны на «гостя»). Логическое управление доступом защищает конфиденциальность и целостность регистрационной информации. Возможно, для защиты привлекаются и криптографические методы.

Возвращаясь к целям протоколирования и аудита, отметим, что обеспечение подотчетности важно в первую очередь как **сдерживающее средство**. Если пользователи и администраторы знают, что все их действия фиксируются, они, возможно, воздержатся от незаконных операций. Очевидно, если есть основания подозревать какого-либо пользователя в нечестности, можно регистрировать все его действия, вплоть до каждого нажатия клавиши. При этом обеспечивается не только возможность расследования случаев нарушения режима безопасности, но и откат некорректных изменений (если в протоколе присутствуют данные до и после модификации). Тем самым защищается целостность информации.

Реконструкция последовательности событий позволяет выявить слабые места в защите сервисов, найти виновника вторжения, оценить масштабы причиненного ущерба и вернуться к нормальной работе.

Обнаружение попыток нарушений информационной безопасности — функция активного аудита, о котором пойдет речь в следующем разделе. Обычный аудит позволяет выявить подобные попытки с опозданием, но и это оказывается полезным. В свое время поимка немецких хакеров, действовавших по заказу КГБ, началась с выявления подозрительного расхождения в несколько центов в ежедневном отчете крупного вычислительного центра.

Выявление и анализ проблем могут помочь улучшить такой параметр безопасности, как доступность. Обнаружив узкие места, можно попытаться переконфигурировать или перенастроить систему (увеличить оперативную память), снова измерить производительность и т.д.

Непросто осуществить организацию согласованного протоколирования и аудита в распределенной разнородной системе. Во-первых, некоторые компоненты, важные для безопасности (например, маршрутизаторы), могут не обладать своими ресурсами протоколирования; в таком случае их нужно экранировать другими сервисами, которые возьмут протоколирование на себя. Во-вторых, необходимо увязывать между собой события в разных сервисах.

14.2 Активный аудит

Под подозрительной активностью понимается поведение пользователя или компонента информационной системы, являющееся злоумышленным (в соответствии с заранее определенной политикой безопасности) или нетипичным (согласно принятым критериям).

Задача активного аудита — оперативно выявлять подозрительную активность и предоставлять средства для автоматического реагирования на нее.

Активность, не соответствующую политике безопасности, целесообразно разделить на **атаки**, направленные на незаконное получение полномочий, и на действия, выполняемые в рамках имеющихся полномочий, но нарушающие политику безопасности.

Атаки нарушают любую осмысленную политику безопасности. Иными словами, активность атакующего является разрушительной независимо от политики. Следовательно, для описания и выявления атак можно применять универсальные методы, инвариантные относительно политики безопасности, такие как **сигнатуры** и их обнаружение во входном потоке событий с помощью аппарата экспертных систем.

Сигнатура атаки — это совокупность условий (действий), при выполнении которых атака считается имеющей место, что вызывает заранее определенную реакцию. Простейший пример сигнатуры — «зафиксированы три последовательные неудачные попытки входа в систему с одного терминала», пример ассоциированной реакции — блокирование терминала до прояснения ситуации.

Действия, выполняемые в рамках имеющихся полномочий, но нарушающие политику безопасности, мы будем называть **злоупотреблением полномочиями**. Злоупотребления полномочиями возможны из-за неправильного разграничения доступа, не соответствующего выбранной политике безопасности. Простейшим примером злоупотреблений является неэтичное поведение суперпользователя, просматривающего личные файлы других пользователей. Анализируя регистрационную информацию, можно обнаружить подобные события и сообщить о них администратору безопасности.

Выделение злоупотреблений полномочиями в отдельную группу неправомерных действий, выявляемых средствами активного аудита, не является общепринятым, однако, на наш взгляд, подобный подход имеет право на существование, и мы будем его придерживаться, хотя наиболее радикальным решением было бы правильное разграничение доступа.

Нетипичное поведение выявляется статистическими методами. В простейшем случае применяют систему порогов, превышение которых является подозрительным. (Впрочем, «пороговый» метод можно трактовать и как вырожденный случай сигнатуры атаки).

Применительно к средствам активного аудита различают ошибки первого и второго рода: **пропуск атаки** и **ложные тревоги**, соответственно. Нежелательность ошибок первого рода очевидна: ошибки второго рода не менее не-

приятны, поскольку отвлекают администратора безопасности от действительно важных дел, косвенно способствуя пропуску атак.

Достоинства сигнатурного метода высокая производительность, малое число ошибок второго рода, обоснованность решений. Основной недостаток — неумение обнаруживать неизвестные атаки и вариации известных атак.

Основные достоинства статистического подхода — универсальность и обоснованность решений, потенциальная способность обнаруживать неизвестные атаки, то есть минимизация числа ошибок первого рода. Минусы заключаются в относительно высокой доле ошибок второго рода, плохой работе в случае, когда неправомерное поведение является типичным, когда типичное поведение плавно меняется от легального к неправомерному, а также в случаях, когда типичного поведения нет (как показывает статистика, таких пользователей примерно 5-10%).

Средства активного аудита могут располагаться на всех линиях обороны информационной системы. На границе контролируемой зоны они могут обнаруживать подозрительную активность в точках подключения к внешним сетям (не только попытки нелегального проникновения, но и действия по «прощупыванию» сервисов безопасности). В корпоративной сети, в рамках информационных сервисов и сервисов безопасности, активный аудит в состоянии обнаружить и пресечь подозрительную активность внешних и внутренних пользователей, выявить проблемы в работе сервисов, вызванные как нарушениями безопасности, так и аппаратнопрограммными ошибками. Важно отметить, что активный аудит, в принципе, способен обеспечить защиту от атак на доступность.

К сожалению, формулировка «в принципе, способен обеспечить защиту» не случайна. Активный аудит развивается более десяти лет, и первые результаты казались весьма многообещающими. Довольно быстро удалось реализовать распознавание простых типовых атак, однако затем было выявлено множество проблем, связанных с обнаружением заранее неизвестных атак, атак распределенных, растянутых во времени и т.п. Было бы наивно ожидать полного решения подобных проблем в ближайшее время. (Оперативное пополнение базы сигнатур атак таким решением, конечно, не является.) Тем не менее, и на нынешней стадии развития активный аудит полезен как один из рубежей (вернее, как набор прослоек) эшелонированной обороны.

14.3 Шифрование

Мы приступаем к рассмотрению криптографических сервисов безопасности. Поскольку криптография изучается в отдельном курсе, мы рассмотрим только основные принципы компьютерной криптографии.

Криптография необходима для реализации, по крайней мере, трех сервисов безопасности:

- шифрование;
- контроль целостности;

- аутентификация (этот сервис был рассмотрен нами ранее).

Шифрование — наиболее мощное средство обеспечения конфиденциальности. Во многих отношениях этот сервис занимает центральное место среди программно-технических регуляторов безопасности. Шифрование является основой реализации других сервисов безопасности, в частности средств контроля целостности. Оно иногда бывает единственным средством. Например, для портативных компьютеров только шифрование позволяет обеспечить конфиденциальность данных даже в случае кражи.

В большинстве случаев и шифрование, и контроль целостности играют обеспечивающую роль, являясь доступным и для приложений, и для пользователей. Типичное место этих сервисов безопасности — на сетевом и транспортном уровнях реализации компьютерных сетей.

Различают два основных метода шифрования: *симметричный* и *асимметричный*. В первом из них один и тот же ключ (хранящийся в секрете) используется и для зашифрования, и для расшифрования данных. Разработаны весьма эффективные (быстрые и надежные) методы симметричного шифрования (DES, AES).

Рис. 20 иллюстрирует использование симметричного шифрования. Для определенности мы будем вести речь о защите сообщений, хотя события могут развиваться не только в пространстве, но и во времени, когда зашифровываются и расшифровываются никуда не перемещающиеся файлы.

Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю. С одной стороны, это создает новую проблему распространения ключей. С другой стороны, получатель на основании наличия зашифрованного и расшифрованного сообщения не может доказать, что он получил это сообщение от конкретного отправителя, поскольку такое же сообщение он мог сгенерировать самостоятельно.

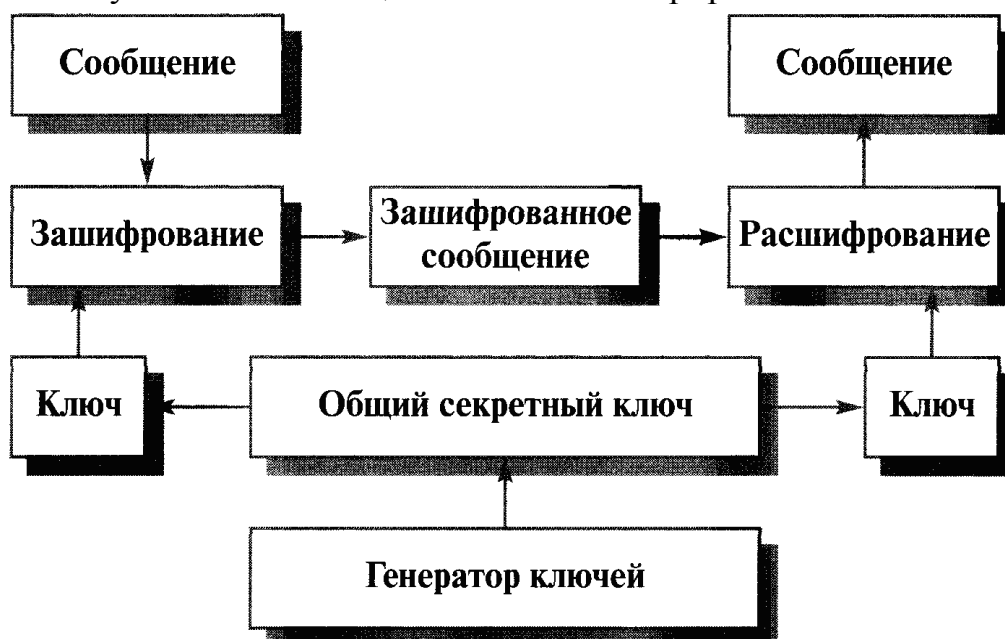


Рис.20. Использование симметричного метода шифрования.

В асимметричных методах используются два ключа. Один из них, не-секретный (он может публиковаться вместе с другими открытыми сведениями о пользователе), применяется для шифрования, другой (секретный, известный только получателю) — для расшифрования. Самым популярным из асимметричных является метод RSA (Райнест, Шамир, Адлеман), основанный на операциях с большими (скажем, 100-значными) простыми числами и их произведениями.

Проиллюстрируем использование асимметричного шифрования (см. рис.21).

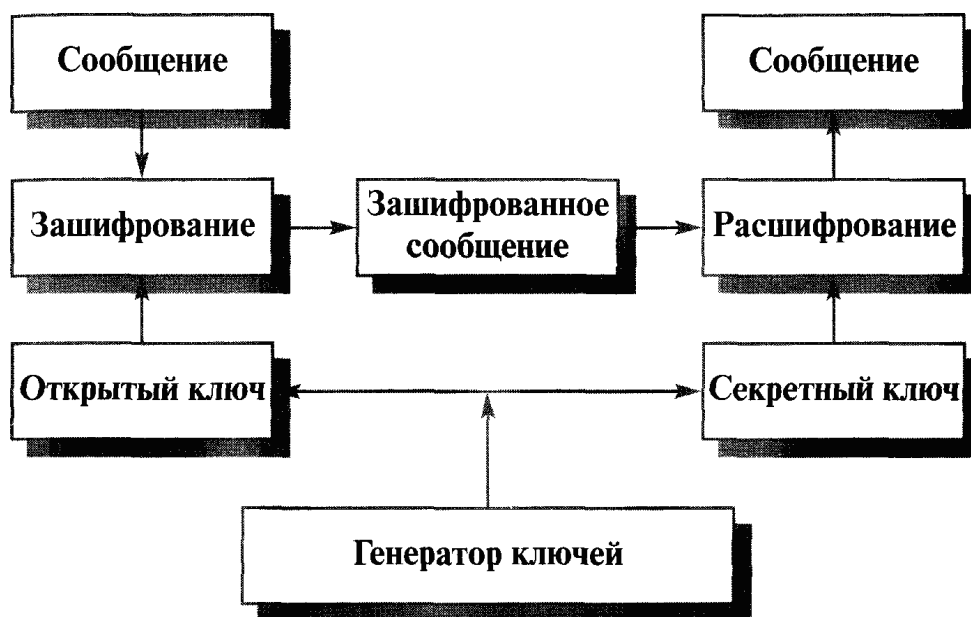


Рис.21. Использование асимметричного метода шифрования.

Существенным недостатком асимметричных методов шифрования является их **низкое быстродействие**, поэтому данные методы приходится сочетать с симметричными (асимметричные методы на 3-4 порядка медленнее). Так, для решения задачи эффективного шифрования с передачей секретного ключа, использованного отправителем, сообщение сначала симметрично зашифровывают случайным ключом, затем этот ключ зашифровывают открытым асимметричным ключом получателя, после чего сообщение и ключ отправляются по сети.

Рис.21 иллюстрирует эффективное шифрование, реализованное путем сочетания симметричного и асимметричного методов.

На рис.22 показано расшифрование эффективно зашифрованного сообщения.

Отметим, что асимметричные методы позволили решить важную задачу совместной выработки секретных ключей (это существенно, если стороны не доверяют друг другу), обслуживающих сеанс взаимодействия, при изначальном отсутствии общих секретов. Для этого используется алгоритм Диффи-Хелмана.

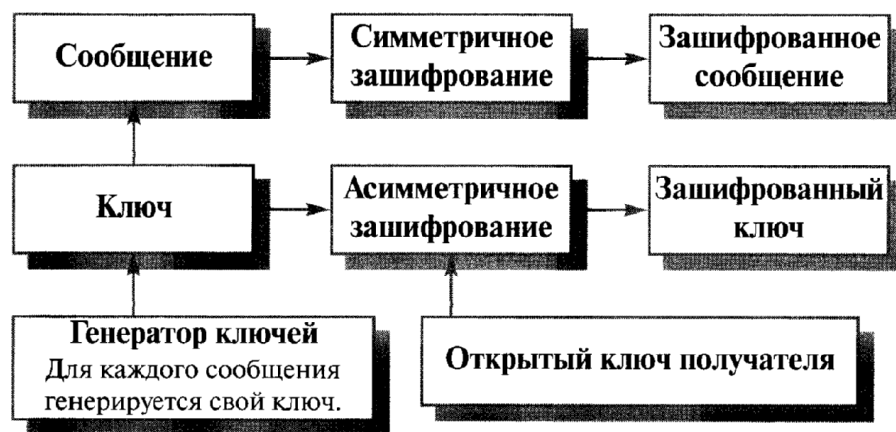


Рис. 11.3. Эффективное шифрование сообщения.

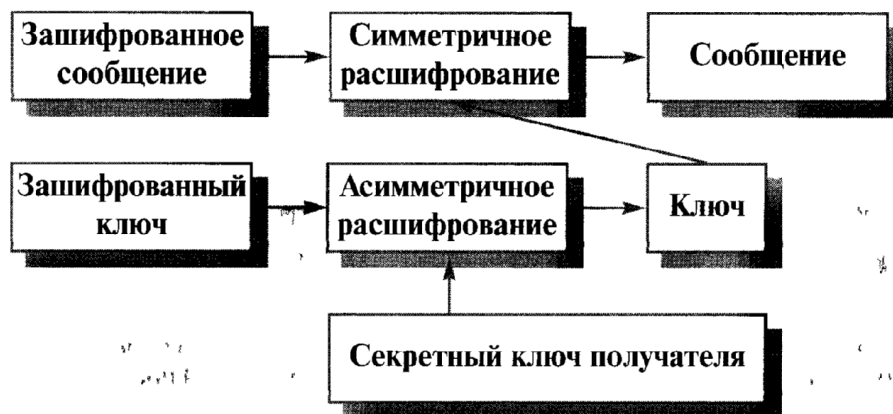


Рис. 22 Расшифрование зашифрованного сообщения

14.4 Контроль целостности

Криптографические методы позволяют надежно контролировать целостность, как отдельных порций данных, так и их наборов (таких как поток сообщений); определять подлинность источника данных, гарантировать невозможность отказаться от совершенных действий («неотказуемость»).

В основе криптографического контроля целостности лежат два понятия:

- хэш-функция;
- электронная цифровая подпись (ЭЦП).

Хэш-функция — это труднообратимое преобразование данных (одно-сторонняя функция), реализуемое, как правило, средствами симметричного шифрования со связыванием блоков. Результат шифрования последнего блока (зависящий от всех предыдущих) и служит результатом хэш-функции.

Пусть имеются данные, целостность которых нужно проверить, хэш-функция и ранее вычисленный результат ее применения к исходным данным (так называемый **дайджест** или **цифровой отпечаток**). Обозначим хэш-функцию через h , исходные данные — через T , проверяемые данные — через T' . Контроль целостности данных сводится к проверке равенства $h(T') = h(T)$. Если оно выполнено, считается, что $T' = T$. Совпадение дайджестов для различных данных называется коллизией. В принципе, коллизии, конечно, возможны, поскольку мощность множества дайджестов меньше, чем мощность множества

хэшируемых данных, однако то, что h есть функция односторонняя, означает, что за приемлемое время специально организовать коллизию невозможно.

Рассмотрим теперь применение асимметричного шифрования для выработки и проверки электронной цифровой подписи. Пусть $E(T)$ обозначает результат зашифрования текста T с помощью открытого ключа, а

$D(T)$ — результат расшифрования текста T (как правило, зашифрованного) с помощью секретного ключа.

На рис.23, 24 показана процедура выработки и проверки электронной цифровой подписи, состоящая в шифровании преобразованием E дайджеста $h(T)$.

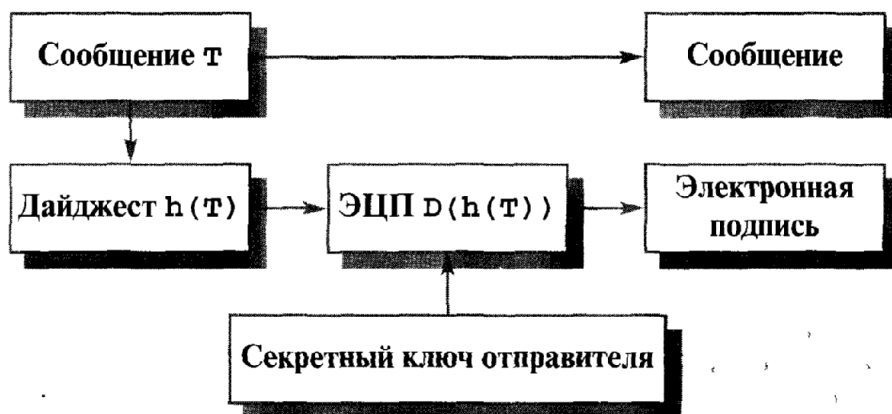


Рис. 23 Выработка электронной цифровой подписи

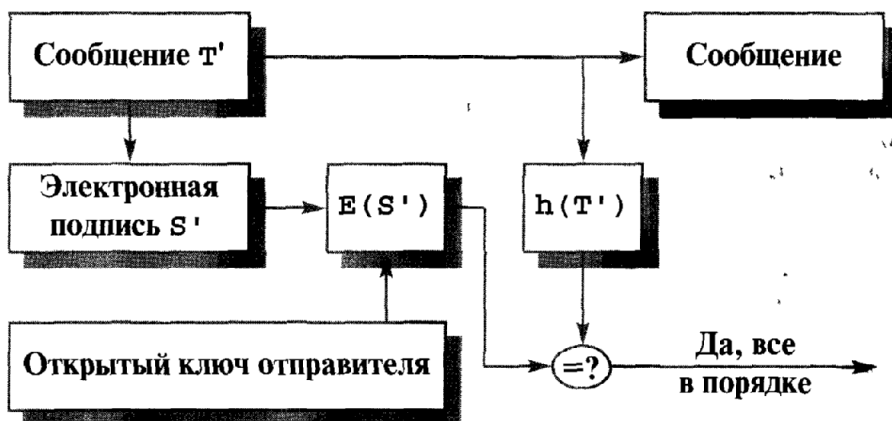


Рис. 24 Проверка электронной цифровой подписи

Таким образом, электронная цифровая подпись защищает целостность сообщения и удостоверяет личность отправителя, то есть защищает целостность источника данных и служит основой неотказуемости.

Для контроля целостности последовательности сообщений (то есть для защиты от кражи, дублирования и переупорядочения сообщений) применяют временные метки и нумерацию элементов последовательности, при этом метки и номера включают в подписываемый текст.

14.5 Цифровые сертификаты

При использовании **асимметричных** методов шифрования (и, в частности, электронной цифровой подписи) необходимо иметь гарантию подлинности пары (имя пользователя, открытый ключ пользователя). Для решения этой задачи в спецификациях X.509 вводятся **понятия цифрового сертификата и удостоверяющего центра**.

Удостоверяющий центр - это компонент глобальной службы каталогов, отвечающий за управление криптографическими ключами пользователей. Открытые ключи и другая информация о пользователях хранится удостоверяющими центрами в виде цифровых сертификатов, имеющих следующую структуру:

- порядковый номер сертификата;
- идентификатор алгоритма электронной подписи;
- имя удостоверяющего центра;
- срок годности;
- имя владельца сертификата (имя пользователя, которому принадлежит сертификат);
- открытые ключи владельца сертификата (ключей может быть несколько),
- идентификаторы алгоритмов, ассоциированных с открытыми ключами владельца сертификата;
- электронная подпись, сгенерированная с использованием секретного ключа удостоверяющего центра (подписывается результат хэширования всей информации, хранящейся в сертификате).

Цифровые сертификаты обладают следующими свойствами:

- любой пользователь, знающий открытый ключ удостоверяющего центра, может узнать открытые ключи других клиентов центра и проверить целостность сертификата;
- никто, кроме удостоверяющего центра, не может модифицировать информацию о пользователе без нарушения целостности сертификата.

В спецификациях X.509 не описывается конкретная процедура генерации криптографических ключей и управления ими, однако даются некоторые общие рекомендации. В частности, оговаривается, что пары ключей могут порождаться любым из следующих способов.

- ключи может генерировать сам пользователь. В таком случае секретный ключ не попадает в руки третьих лиц, однако нужно решать задачу безопасной связи с удостоверяющим центром;
- ключи генерирует доверенное лицо. В таком случае приходится решать задачи безопасной доставки секретного ключа владельцу и предоставления доверенных данных для создания сертификата;
- ключи генерируются удостоверяющим центром. В таком случае остается только задача безопасной передачи ключей владельцу. Цифровые сертификаты в формате X.509 версии 3 стали не только формальным, но и фактиче-

ским стандартом, поддерживаемым многочисленными удостоверяющими центрами.

Тема 15: «Управление информационной безопасностью на государственном уровне. Общие принципы и российская практика»

15.1 Организационно-правовые формы управления безопасностью

Законом Российской Федерации от 5 марта 1992 года «О безопасности» безопасность определяется как состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. В нее включаются государственная, экономическая, общественная, оборонная, информационная, экологическая и иные виды безопасности. Такое широкое понимание безопасности предполагает функционирование большого числа органов и организаций, обеспечивающих ее, а также использование в целях достижения безопасности соответственно мер экономического, политического, военного, организационного, экологического и иного характера.

Обеспечение безопасности достигается деятельностью сил обеспечения безопасности Российской Федерации, в которые входят Вооруженные Силы. Федеральная служба безопасности. Служба внешней разведки, органы внутренних дел, налоговая служба, служба ликвидации последствий чрезвычайных ситуаций, формирования гражданской обороны; пограничные, внутренние войска: органы, обеспечивающие безопасное ведение работ в промышленности, энергетике и в сельском хозяйстве; службы обеспечения безопасности средств связи и информации; органы охраны здоровья населения и другие органы обеспечения безопасности.

В целях непосредственного выполнения функций по обеспечению безопасности государством образуются специальные органы обеспечения безопасности.

В соответствии с Конституцией Российской Федерации и Законом «О безопасности» общее руководство органами обеспечения безопасности возложено на Президента Российской Федерации. Он контролирует и координирует деятельность органов обеспечения безопасности, принимает в случае необходимости оперативные решения в этой области.

Правительство Российской Федерации в пределах своей компетенции обеспечивает руководство государственными органами безопасности. Оно организует разработку и реализацию мероприятий по обеспечению безопасности министерствами, государственными комитетами и другими подведомственными ему органами, а также субъектами Российской Федерации.

Важное место в системе органов обеспечения безопасности занимает Совет безопасности Российской Федерации, руководство деятельностью которого осуществляет Президент Российской Федерации.

Положением о Совете безопасности на него возложена подготовка проектов решений Президента Российской Федерации по основным направлениям

внутренней, внешней и военной политики в области обеспечения безопасности Российской Федерации.

Являясь совещательным органом при Президенте Российской Федерации. Совет безопасности на своих заседаниях рассматривает вопросы внутренней, внешней и военной политики Российской Федерации в области обеспечения безопасности, стратегические проблемы государственной, экономической, общественной, оборонной, экологической, информационной и иных видов безопасности.

Совет безопасности разрабатывает основные направления стратегии безопасности Российской Федерации, рекомендации Президенту Российской Федерации по вопросам внутренней, внешней и военной политики в области обеспечения безопасности, предложения по совершенствованию системы обеспечения безопасности.

На него возложено создание надежно действующей системы обеспечения Президента Российской Федерации достоверной, объективной и качественной информацией о состоянии безопасности Российской Федерации: организация разработки федеральных программ в данной области, а также оценка их эффективности.

Решения Совета безопасности по важнейшим вопросам претворяются в жизнь указами Президента Российской Федерации.

В систему специальных органов обеспечения безопасности входит Федеральная служба безопасности Российской Федерации (ФСБ России), основы организации и деятельности которой закреплены в Законе Российской Федерации от 22 февраля 1995 года «Об органах федеральной службы безопасности в Российской Федерации» и в Положении о Федеральной службе безопасности Российской Федерации, утвержденном Указом Президента Российской Федерации от 23 июня 1995 года.

Являясь федеральным органом исполнительной власти. ФСБ России возглавляет единую централизованную систему органов федеральной службы безопасности, в которую входят управления (отделы) ФСБ России по отдельным регионам и субъектам Российской Федерации (территориальные органы безопасности); управления (отделы) ФСБ России в Вооруженных Силах Российской Федерации, войсках и иных воинских формированиях, а также в их органах управления (органы безопасности в войсках), которые непосредственно подчиняются в своей деятельности ФСБ России.

Основными направлениями деятельности органов федеральной службы безопасности являются контрразведывательная деятельность и борьба с организованной преступностью.

К основным задачам ФСБ России относится: информирование Президента Российской Федерации, Председателя Правительства Российской Федерации и по их поручениям федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации об угрозах безопасности Российской Федерации; выявление, предупреждение и пресечение разведывательной и иной деятельности спецслужб и организаций иностранных госу-

дарств, отдельных лиц, направленной на нанесение ущерба безопасности Российской Федерации; добывание разведывательной информации в целях обеспечения безопасности Российской Федерации, повышения ее экономического, научно-технического, оборонного потенциала; обеспечение в пределах своей компетенции защиты сведений, составляющих государственную тайну; организация и осуществление во взаимодействии с другими государственными органами борьбы с организованной преступностью, коррупцией, контрабандой, незаконным оборотом оружия и наркотических средств, а также с деятельностью незаконных вооруженных формирований, преступных групп, отдельных лиц и общественных объединений, ставящих своей целью насильственное изменение конституционного строя Российской Федерации и др.

Выполняя свои задачи, ФСБ России участвует в разработке и реализации государственных программ обеспечения безопасности Российской Федерации; на основе прогнозов развития внутривнутриполитической, социально-экономической и криминогенной обстановки в стране разрабатывает предложения по предупреждению и нейтрализации угроз безопасности Российской Федерации и т.д.

На ФСБ России и ее органы возложены и другие функции, которые осуществляются ими во взаимодействии с государственными органами и организациями, общественными объединениями и гражданами.

Составной частью системы обеспечения безопасности являются **органы внешней разведки Российской Федерации**, основы организации и деятельности которых закреплены в Законе Российской Федерации от 8 декабря 1995 года «О внешней разведке».

В систему органов внешней разведки входит Служба внешней разведки Российской Федерации, органы внешней разведки Минобороны России, органы внешней разведки Федерального агентства правительственной связи и информации (ФАПСИ) при Президенте Российской Федерации, органы внешней разведки Федеральной пограничной службы (ФПС) Российской Федерации. Перечисленные органы осуществляют свою деятельность путем добывания и обработки информации о затрагивающих жизненно важные интересы Российской Федерации реальных и потенциальных возможностях, действиях, планах и намерениях иностранных государств, организаций и лиц, а также оказания содействия в реализации мер, осуществляемых государством в интересах обеспечения безопасности Российской Федерации.

Обработанная органами внешней разведки информация направляется Президенту Российской Федерации, Федеральному Собранию и Правительству Российской Федерации, которая необходима им для принятия решений в политической, экономической, оборонной, научно-технической и экологических областях; обеспечения условий, способствующих успешной реализации политики Российской Федерации в сфере безопасности; содействия экономическому развитию, научно-техническому прогрессу и военно-техническому обеспечению безопасности Российской Федерации.

Разведывательная информация в отдельных случаях, определяемых Президентом Российской Федерации, может предоставляться федеральным орга-

нам исполнительной и судебной власти, федеральным органам исполнительной власти, входящим в состав сил обеспечения безопасности Российской Федерации, а также предприятиям, учреждениям и организациям.

Органы внешней разведки имеют свои сферы разведывательной деятельности. Так, Служба внешней разведки осуществляет свою деятельность в политической, экономической, военно-стратегической, научно-технической и экологической сферах, а также в сфере обеспечения безопасности учреждений Российской Федерации, находящихся за пределами ее территории, и командированных за пределы территории Российской Федерации граждан Российской Федерации, имеющих по роду своей деятельности допуск к сведениям, составляющим государственную тайну, орган внешней разведки Минобороны России в военной, военно-политической, военно-технической, военно-экономической и экологической сферах; орган внешней разведки ФАПСИ при Президенте Российской Федерации — в политической, экономической, военной и научно-технической сферах; орган внешней разведки ФПС Российской Федерации — в сфере охраны Государственной границы Российской Федерации, исключительной экономической зоны Российской Федерации и ее континентального шельфа.

Специальным органом обеспечения безопасности является **Федеральная служба охраны Российской Федерации**, задачи и полномочия которой закреплены в Законе Российской Федерации от 24 апреля 1991 года «О государственной охране», а также Служба безопасности Президента Российской Федерации, задачи которой определены названным Законом, а также Положением о Службе безопасности Президента Российской Федерации.

К органам обеспечения безопасности относится Межведомственная комиссия по защите государственной тайны, основной функцией которой является координация деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации по защите государственной тайны.

Перечисленные органы в соответствии с Законом от 21 июля 1992 года «О государственной тайне» в пределах своей компетенции обеспечивают защиту сведений, составляющих государственную тайну, перечень которых утвержден Указом Президента Российской Федерации от 30 ноября 1995 года.

15.2 Предпосылки развития государственного управления в сфере информационной безопасности

Основные задачи государственных органов в сфере информационной безопасности, также как и во многих других сферах, связаны с охраной общественных интересов, предотвращением противоправной деятельности, а также с защитой информации, имеющей государственную важность (военных сведений, информации о космических и ядерных технологиях и т.п.). При этом решение вопросов информационной безопасности в частном секторе экономики, как правило, является прерогативой самих частных компаний и организаций, а

вмешательство государства в эту сферу должно быть минимизировано. Таким образом, на практике деятельность органов власти, как правило, концентрируется на решении вопросов информационной безопасности внутри отдельных сфер, которые считаются наиболее важными для обеспечения государственной безопасности и достижения политических целей: вооруженные силы, внешняя разведка, стратегические технологии (например, космические, атомные и военные), государственные финансы, общественная стабильность и некоторые другие. Решению вопросов информационной безопасности в других областях государственными органами, как правило, уделяется меньше внимания. Государственные органы могут решать определенные задачи информационной безопасности, не относящиеся напрямую к защите государственных информационных систем, в тех случаях, когда выгоды от государственного вмешательства существенно превышают затраты и решения, предлагаемые государством, не составляют конкуренции альтернативным решениям (услугам, технологиям, методикам и т.п.), которые предлагаются (или потенциально могут быть предложены) частными компаниями.

Деятельность государства в сфере информационной безопасности, как правило, строится на более общих задачах государственной власти, таких как:

- сохранение суверенитета государства;
- сохранение государственной и политической стабильности в стране;
- сохранение и развитие демократических институтов общества, а также обеспечение прав и свобод граждан;
- укрепление законности и правопорядка;
- обеспечение социально-экономического развития страны и устойчивости финансовой системы;
- участие в жизни международного сообщества.

По своей природе факторы, определяющие состояние информационной безопасности и, соответственно, деятельность государства в этой сфере, подразделяются на:

- политические;
- социально-экономические;
- организационно-технические.

Организационная деятельность государства в сфере информационной безопасности, как правило, сводится к противодействию различным угрозам:

- внешним, таким как деятельность иностранных спецслужб и вооруженных сил, враждебная экономическая и техническая политика отдельных государств, агрессивные рыночные стратегии крупных международных корпораций и финансово-промышленных групп, незаконная деятельность международных преступных и террористических группировок и т.п.;

- внутренним, таким как деятельность криминальных структур в сфере обращения информации, неправомерные действия государственных структур, халатность или целенаправленные нарушения, допускаемые гражданами и организациями при использовании информационных систем и обращении информации, нарушения в работе информационных и телекоммуникационных систем и т.п.

Таким образом, деятельность государства в этой сфере направлена на нейтрализацию существующих угроз информационной безопасности с учетом всех факторов, воздействующих как на сами управляющие государственные структуры, так и на информационные системы.

15.3 Общая методология и структура организационного обеспечения информационной безопасности на уровне государств

Для решения основных задач в сфере информационной безопасности действуют все основные органы государственной власти и управления: судебные, органы исполнительной власти, правоохранительные органы, организации и предприятия, которые контролируются государством и имеют доступ к информации, составляющей государственную тайну, и другие.

Для обеспечения информационной безопасности государственные органы выполняют следующие основные функции:

- создают законодательную базу, обеспечивающую защиту базовых прав частных лиц, предприятий и государства, таких как право на защиту частной информации, право на защиту коммерческой и банковской тайны, право на беспрепятственный доступ к информации и т.п. Данная функция осуществляется законодательными органами в сотрудничестве с органами исполнительной власти, общественными организациями, научно-исследовательскими учреждениями и другими заинтересованными участниками;

- осуществляют правоприменительную деятельность, непосредственно реализуют меры по защите информационных ресурсов государственного управления, а также выполняют все функции, необходимые для реализации требований законодательства;

- выполняют судебные функции в отношении лиц, которые допустили правонарушения, связанные с использованием информационных ресурсов, и участвуют в хозяйственных спорах, связанных с нарушениями информационной безопасности.

Функции создания и постоянного совершенствования законодательно-правовой базы, обеспечивающей защиту законных частных, коммерческих, общественных и государственных интересов, реализуются законодательными органами (парламентами) государств. Как правило, все законодательные функции в данной сфере в большинстве стран осуществляются центральными (федеральными) органами законодательной власти, а местные (региональные) органы таких полномочий не имеют. Для создания и поддержания в актуальном состоянии законодательства в сфере информационной безопасности в законодательных органах могут создаваться профильные комитеты и комиссии, которые состоят из членов данного законодательного органа, имеющих некоторые базовые знания и навыки в сфере информационных технологий и правового регулирования вопросов информационного обмена. Кроме того, вопросы совершенствования законодательства в сфере обеспечения информационной безопасности также могут решаться в различных профильных комитетах, подкомитетах и рабочих группах, специализирующихся на смежных проблемах государственного управления и социально-экономического регулирования, таких как:

- оборона;
- национальная безопасность;
- политика в сфере связи, информации и информатизации;
- промышленная и экономическая политика;
- наука и образование
- и других.

Для разработки соответствующих нормативно-правовых актов подразделения (комитеты и подкомитеты) органов законодательной власти могут привлекать для совместной работы ответственных специалистов, руководителей, аналитиков и экспертов, работающих в:

- органах исполнительной власти (министерствах, отвечающих за научное и техническое развитие, т.н. "силовых" министерствах и ведомствах, юридических ведомствах и т.п.);
- частных компаниях, а также общественных и профессиональных организациях, которые занимаются оказанием информационных услуг, поставкой информационно-технических продуктов, специализирующихся на развитии информационных технологий и т.п.;

- научно-исследовательских организациях, специализирующихся на соответствующих проблемах информационных технологий и управления.

Процедуры согласования, принятия и утверждения законодательных актов, а также процедуры контроля за действиями органов исполнительной власти в каждой стране определяются в соответствии с действующим законодательством (конституцией).

Деятельность исполнительных органов государственной власти в сфере обеспечения информационной безопасности направлена на реализацию действующих в государстве законов и непосредственную защиту интересов государственной власти, гражданских прав и прав компаний, осуществляющих хозяйственную деятельность.

Конкретная работа органов исполнительной власти в сфере информационной безопасности, как правило, осуществляется по нескольким относительно самостоятельным направлениям.

- Установление конкретных правил производства, продажи, экспорта, импорта и использования средств защиты информации, а также организация системы контроля за соблюдением действующих законов и установленных правил.
- Лицензирование и сертификация предприятий и организаций, занимающихся производством, продажей установкой и настройкой программных и аппаратных средств защиты информации.
- Осуществление правоохранительной деятельности в сфере защиты информации (уголовного преследования лиц и преступных группировок, совершающих противоправные действия, содержащие признаки уголовных преступлений в соответствии с действующим уголовным законодательством).
- Непосредственное осуществление функций защиты информации в государственных учреждениях и службах (правительство, вооруженные силы, органы внутренних дел и т.п.).
- Разработка государственных стандартов, относящихся к организации и технологиям защиты информации (программным и аппаратным средствам, средствам криптографии и т.п.).
- Поддержка образования и подготовки кадров, а также регулирование деятельности образовательных учреждений (включая установку образовательных стандартов).
- Поддержка научных исследований в сфере информационной безопасности.

- Осуществление международного сотрудничества в сфере защиты информации (взаимодействие с правительствами и правоохранительными органами других стран) как в целях общего развития инфраструктуры информационной безопасности, так и для разрешения отдельных инцидентов (раскрытия преступлений и т.п.).

Судебные функции, как правило, реализуются судами общей юрисдикции, так же как и для всех остальных гражданских и уголовных дел. Специальных судебных инстанций, которые были бы предназначены для рассмотрения дел, связанных с информационной безопасностью (таких как, например, суды по правам человека или военные суды), не существует. При этом могут создаваться судебные лаборатории, специализирующиеся на проведении экспертиз, анализов и исследований различных элементов информационных систем в связи с расследованиями и судебными разбирательствами по делам о нарушениях в сфере информационной безопасности.

Основой организации государственной деятельности в сфере информационной безопасности является национальная политика (доктрина, национальный план, национальная стратегия) информационной безопасности. Этот документ, издаваемый, как правило, главой исполнительной ветви власти (президентом страны) отражает:

- признание государственной властью существенной значимости проблем защиты информации для общества, личности, экономики и самого государства;
- современное понимание общего ландшафта информационной безопасности на национальном уровне: потенциально уязвимые информационные объекты, источники угроз и др.;
- основные направления, в которых государство намерено осуществлять активные действия с целью повышения уровня информационной безопасности на национальном уровне (создание систем безопасности, упорядочивание взаимоотношений различных субъектов, пресечение правонарушений, развитие инфраструктуры и технологий безопасности и т.п.).

В рамках утвержденной государственной доктрины информационной безопасности:

- создаются специализированные правительственные организации, отвечающие за реализацию политики информационной безопасности и решение отдельных задач в этой сфере;
- отдельные правительственные учреждения наделяются специфическими функциями и полномочиями, связанными с управлением информационной безопасностью (как в общегосударственном масштабе,

так и в рамках определенных сфер ответственности), а также создаются специальные структурные подразделения, отвечающие за решение вопросов защиты информации и информационной инфраструктуры;

- создается система локальных правовых актов, регулирующих отношения в сфере защиты информации, а также система государственных стандартов, относящихся к технологиям и организации защиты информации.

Специализированные органы, создаваемые в структуре исполнительной власти для решения задач информационной безопасности на государственном уровне, как правило, подчиняются непосредственно главе исполнительной ветви власти, носят статус федеральных агентств, комитетов или комиссий и наделены правом самостоятельно издавать нормативные акты в рамках имеющихся полномочий, установленных действующим законодательством. Издаваемые таким образом локальные нормативные акты (указы, постановления, инструкции, порядки, правила и т.п.) непосредственно регулируют отношения в сфере создания, распространения и использования средств автоматизации и защиты информации.

Государственная стандартизация технологий и методов, используемых в процессах защиты информации, осуществляется уполномоченными государственными органами с целью упорядочивания знаний о современном состоянии технологий и методов защиты и установления универсальных критериев надежности и функциональности для определенных технологий. Государственная стандартизация позволяет достичь универсальности при оценке используемых технологий и методов и, таким образом, до определенной степени упорядочить многие взаимоотношения, связанные с использованием таких технологий и методов. Стандартизация, осуществляемая отдельными государственными органами, как правило, опирается на существующую систему имеющихся международных стандартов, а национальные органы, занимающиеся стандартизацией, могут принимать участие в разработке международных стандартов. Основными объектами государственной и международной стандартизации могут выступать:

- методы шифрования и криптографической защиты данных;
- технологии идентификации пользователей информационных систем;
- методы аутентификации;
- методы тестирования (проверки) и оценки информационных систем на предмет их защищенности;

а также некоторые другие элементы систем обеспечения информационной безопасности.

15.4 Общая политика России в сфере информационной безопасности

Основой современной политики Российской Федерации в сфере информационной безопасности можно считать "Доктрину информационной безопасности РФ", утвержденную Президентом РФ Владимиром Путиным 9 сентября 2000г. Этот документ:

- описывает основные предпосылки формирования государственной политики в данной сфере (потребность в безопасности, существующие интересы, угрозы, источники угроз и т.п.);
- формулирует базовые задачи государства и общества, основанные непосредственно на необходимости выполнения требований Конституции, обеспечения суверенитета страны и т.п.;
- описывает состояние дел в сфере общегосударственного регулирования процессов информационной безопасности на момент утверждения Доктрины (основные достижения и недостатки);
- перечисляет приоритетные направления деятельности государства (задачи, требующие безотлагательного решения) по обеспечению информационной безопасности;
- формулирует основные методики, которые государство должно использовать для обеспечения информационной безопасности, а также специфику применения этих методов в отдельных областях общественной жизни;
- перечисляет основные информационные объекты (в различных сферах), на охрану которых должна быть направлена государственная политика;
- описывает основные направления международного сотрудничества в сфере информационной безопасности;
- перечисляет основные организационные инструменты, используемые для реализации государственной политики и осуществления государственного управления в сфере информационной безопасности;
- описывает распределение ответственности между основными органами государственной власти, решающими задачи в сфере информационной безопасности.

В соответствии с Доктриной государство должно уделять внимание информационной безопасности в таких основных сферах, как:

- экономика;
- внутренняя политика;

- внешняя политика;
- наука и техника;
- духовная жизнь;
- информационные системы государственного управления;
- оборона.

К числу первоочередных мероприятий, которые должны быть реализованы на государственном уровне, Доктрина относит:

- совершенствование законодательной базы в сфере информационных отношений;
- разработку механизмов управления государственными средствами массовой информации и реализации государственной информационной политики;
- подготовку кадров для работы в сфере информационной безопасности;
- совершенствование и развитие системы государственных стандартов в сфере информатизации и обеспечения информационной безопасности;
- принятие и реализацию федеральных программ, решающих определенные задачи информатизации и обеспечения информационной безопасности: создание информационных архивов и информационно-телекоммуникационных систем органов власти, развитие информационной культуры населения и т.п.

Как можно видеть из этого перечня, а также в целом из текста Доктрины, она предполагает определенное расширение понятия "информационная безопасность" и включение в него некоторых вопросов, которые связаны с деятельностью средств массовой информации и другими аспектами информационной политики, не имеющими прямого отношения к категории "информационная безопасность" в ее первоначальном понимании.

Помимо Доктрины также важным основополагающим документом, в значительной мере определяющим политику государства в сфере информатизации и обеспечения защиты информации, можно считать Федеральную целевую программу "Электронная Россия", реализация которой планируется в три этапа в период с 2002 по 2010 год. В частности, одной из заявленных целей реализации данной Программы является обеспечение реализации прав на "обеспечение конфиденциальности любой охраняемой законом информации, имеющейся в информационных системах". В целом предполагается, что весь комплекс меро-

приятий, предусмотренных Программой, должен обеспечить принципиально более высокий уровень надежности ключевых информационных потоков на государственном уровне.

Кроме того, важными организующими документами, действующими в этой сфере на государственном уровне, являются:

- Федеральный Закон "О государственной тайне";
- Федеральный Закон "Об информации, информационных технологиях и о защите информации";
- Федеральный Закон "Об участии в международном информационном обмене".
-

15.5 Структура органов государственной власти, обеспечивающих информационную безопасность в РФ

Основным государственным органом, определяющим политику РФ в сфере безопасности страны в целом и информационной безопасности в частности, является **Совет безопасности РФ**.

Ведущим государственным учреждением, непосредственно ответственным за реализацию государственной политики в сфере информационной безопасности и защиту государственных интересов на общенациональном уровне, является **Федеральная служба по техническому и экспортному контролю – ФСТЭК**. Важную роль в системе органов государственной власти, отвечающих за решение задач информационной безопасности, играет также **Служба специальной связи и информации ("Спецсвязь России")**, с 2004 года входящая в состав Федеральной службы охраны. Вопросы повышения качества информационной работы и информационной безопасности решают также другие федеральные органы (в пределах своей компетенции):

- Министерство связи и массовых коммуникаций РФ;
- Министерство внутренних дел РФ.

Также отдельные государственные ведомства, предъявляющие особые требования к уровню защищенности информации, реализуют собственные мероприятия по обеспечению защиты информации:

- ФСБ (Управление компьютерной и информационной безопасности, а также Центр по лицензированию, сертификации и защите государственной тайны, Управление специальной связи и НИИ информационных технологий);

- Минатом РФ и система подведомственных ему предприятий (в составе которого функционирует Центр "Атомзащитаинформ");
- Центральный банк РФ (в составе которого функционирует Главное управление безопасности и защиты информации)
- и некоторые другие.

Совет Безопасности РФ, возглавляемый Президентом РФ, состоит из ключевых министров и рассматривает вопросы внутренней и внешней политики Российской Федерации в области обеспечения безопасности, стратегические проблемы государственной, экономической, общественной, оборонной, **информационной**, экологической и иных видов безопасности. Основными функциями Совета Безопасности являются:

- подготовка решений Президента РФ по соответствующим вопросам, в т.ч. по вопросам информационной безопасности;
- рассмотрение законопроектов, в рамках своей компетенции;
- организация и координация разработки стратегии в области внутренней, внешней и военной политики, военно-технического сотрудничества и информационной безопасности РФ, осуществление контроля за реализацией этой стратегии органами власти, оценка внутренних и внешних угроз жизненно важным интересам объектов безопасности и выявление их источников и др.

Для решения задач, связанных с обеспечением информационной безопасности, в составе СБ функционирует созданное в 1997 году Управление информационной безопасности (одно из восьми профильных управлений), а также Межведомственная комиссия по информационной безопасности. Функциями Управления информационной безопасности являются:

- подготовка предложений Совету Безопасности по выработке и реализации основных направлений политики государства в области обеспечения информационной безопасности РФ;
- анализ и прогнозирование ситуации в области информационной безопасности РФ;
- выявление источников опасности, оценка внешних и внутренних угроз информационной безопасности и подготовка предложений Совету Безопасности по их предотвращению;
- рассмотрение в установленном порядке проектов федеральных целевых программ, направленных на обеспечение информационной безопасности РФ, подготовка соответствующих предложений;

- участие в подготовке материалов по вопросам обеспечения информационной безопасности РФ для ежегодного послания Президента РФ Федеральному Собранию и для докладов Президента РФ;
- подготовка предложений по проектам решений Совета Безопасности и информационно-аналитических материалов к его заседаниям по вопросам обеспечения информационной безопасности РФ;
- подготовка предложений Совету Безопасности по разработке проектов нормативных правовых актов, направленных на обеспечение информационной безопасности РФ.

Федеральная служба по техническому и экспортному контролю (ФСТЭК), до августа 2004 года известная как **Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия РФ)**, была создана в январе 1992 года на базе Гостехкомиссии СССР по противодействию иностранным технологическим разведкам, которая, в свою очередь ведет отсчет своего существования с декабря 1973 года. Произошедшее в 1992 году преобразование было связано со сменой политических приоритетов, интенсивным развитием электронных коммуникаций и средств вычислительной техники, отменой государственной монополии на многие сферы экономической и технической деятельности, развитием рыночных отношений, расширением международных связей и другими факторами. ФСТЭК, ранее подчинявшаяся напрямую Президенту РФ, в процессе административной реформы была подчинена Министерству обороны. ФСТЭК является коллегиальным органом – в состав Коллегии входят около двадцати представителей различных министерств и ведомств (главным образом, в ранге заместителей министров и директоров департаментов), таких как МВД, МИД, ФСБ, Минатом, ФСО, СВР и других.

Основными функциями ФСТЭК являются:

- проведение единой технической политики и координация работ по защите информации;
- организация и контроль за проведением работ по защите информации в органах государственного управления, объединениях, концернах, на предприятиях, в организациях и учреждениях (независимо от форм собственности) от утечки по техническим каналам, от несанкционированного доступа к информации, обрабатываемой техническими средствами, и от специальных воздействий на информацию с целью ее уничтожения и искажения;
- поддержание системы лицензирования деятельности предприятий, организаций и учреждений по осуществлению мероприятий и (или) оказанию услуг в области защиты информации и сертификации средств защиты информации.

Для реализации функций по лицензированию в составе ФСТЭК функционируют 7 региональных управлений (по федеральным округам), а также 20 отраслевых аттестационных (лицензионных) центров.

Служба специальной связи и информации (Спецсвязь России), созданная в марте 2003 года в рамках Федеральной службы охраны на базе упраздненного Федерального агентства правительственной связи и информации (ФАПСИ), в целом призвана обеспечивать функционирование президентской связи, организацию, эксплуатацию и развитие специальной связи для государственных органов и решать другие аналогичные задачи.

При этом задачами Спецсвязи также являются:

- проведение работ по защите технических средств специальной связи, устанавливаемых в категорированных помещениях государственных органов, включая особо важные;
- организация в системе специальной связи шифровальной деятельности, отнесенной к компетенции Спецсвязи России;
- участие в разработке нормативной технической документации по вопросам защиты информации в системах специальной связи;
- участие в разработке и реализации мер по обеспечению информационной безопасности Российской Федерации, защите сведений, составляющих государственную тайну;
- участие в создании, обеспечении и развитии системы электронного документооборота государственных органов с использованием удостоверяющих центров;
- организация и проведение мероприятий по предотвращению утечки по техническим каналам информации в системах специальной связи, информационно-технологических, информационно-аналитических и информационно-телекоммуникационных системах, находящихся в ведении Спецсвязи России;
- выполнение требований обеспечения информационной безопасности объектов государственной охраны.

Министерство связи и массовых коммуникаций РФ в лице подчиняющегося ему Федерального агентства по информационным технологиям (Росинформтехнологии) осуществляет и организует следующие виды работ в сфере информационной безопасности:

- подтверждение подлинности электронных цифровых подписей уполномоченных лиц удостоверяющих центров в выданных ими сертификатах ключей подписей;

- ведение единого государственного реестра сертификатов ключей подписей удостоверяющих центров и реестра сертификатов ключей подписей уполномоченных лиц федеральных органов государственной власти, а также обеспечение доступа к ним граждан, организаций, органов государственной власти и органов местного самоуправления;
- выполнение функции государственного заказчика научно-технических и инвестиционных программ и проектов в сфере информационных технологий.

Уполномоченным органом по ведению реестра доверенных удостоверяющих центров является ФГУП НИИ "Восход".

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является уполномоченным федеральным органом исполнительной власти по защите прав субъектов персональных данных. В полномочия данного органа входит пресечение нарушений, которые могут возникать при обработке персональных данных граждан РФ.

В системе законодательной власти основным структурным подразделением, призванным решать вопросы формирования и реализации государственной политики в сфере информационной безопасности, является **Комитет по безопасности Государственной думы Федерального собрания Российской Федерации**. В составе этого Комитета функционирует **Подкомитет по информационной безопасности**. В законодательной работе в рамках этого Комитета принимают участие:

- специалисты и руководители профильных подразделений ФСБ, СВР, ФСТЭК, МВД и других ведомств;
- руководители Совета безопасности РФ и других правительственных органов;
- представители общественных организаций, фондов и профессиональных объединений;
- представители крупных коммерческих компаний – лидеров в развитии организации и технологий информационной безопасности (в том числе банков, технологических компаний и др.);
- представители ведущих научно-исследовательских учреждений и учебных заведений.

15.6 Государственная граница и ее охрана

Российская Федерация, как и любое государство в мире, имеет свою государственную границу, охрана и обеспечение неприкосновенности которой является одной из функций государства.

Основным законодательным актом, непосредственно закрепляющим и регулирующим вопросы охраны границы, ее режима, пограничного режима и т.д., является Закон Российской Федерации от 1 апреля 1993 года «О Государственной границе Российской Федерации». Данный Закон определяет государственную границу Российской Федерации как линию и проходящую по этой линии вертикальную поверхность, определяющие пределы государственной территории (суши, воды, недр и воздушного пространства) Российской Федерации. Государственной границей Российской Федерации на море является линия внешнего предела территориальных вод).

К территориальным водам Российской Федерации относятся прибрежные морские воды шириной в 12 морских миль. Они отсчитываются от линии наибольшего отлива как на материке, так и вокруг островов, принадлежащих Российской Федерации. Если береговая линия глубоко изрезана, имеет много извилин, то линия границы определяется от прямых исходных линий, соединяющих соответствующие точки и географические координаты.

Таким образом, граница Российской Федерации представляет собой пространственный предел, в рамках которого определяется ее государственный суверенитет.

Охрана государственной границы является одной из важнейших функций государства по обеспечению безопасности Российской Федерации, которая включает в себя осуществление политических, экономических, правовых, военных, технических, санитарных и других мер по обеспечению режима государственной границы, пограничного режима, защите на границе интересов личности, общества, государства и внутренних угроз.

Охрана государственной границы подразделяется на политическую, экономическую, санитарную.

Политическая охрана призвана обеспечивать неприкосновенность государственной границы Российской Федерации; неукоснительное соблюдение существующих правил пересечения границы гражданами Российской Федерации и иностранными гражданами, перемещения средств и грузов; пресечение попыток незаконного пересечения границы людьми, всеми видами транспорта (наземного, воздушного, морского, речного и др.), вооруженными группами и т.п.

В современных условиях исключительно важное значение приобретает *экономическая охрана* государственной границы. Это обусловлено тем, что, во-первых, становление и развитие рыночных отношений в Российской Федерации привело к резкому увеличению числа предприятий, организаций различных форм собственности, имеющих право непосредственного выхода на внешний рынок. Однако это право нередко используется для незаконного вывоза за пре-

делы Российской Федерации стратегического сырья, материальных и культурных ценностей, валюты и т.п., а также ввоз в Российскую Федерацию различных товаров, оружия, наркотиков и др. Во-вторых, в последние годы резко обострилась проблема незаконного лова морских животных в прибрежных водах Российской Федерации как иностранными, так и российскими рыболовецкими судами. Все это наносит невосполнимый ущерб хозяйству, экономике, культуре Российской Федерации. Поэтому важной задачей экономической охраны государственной границы является борьба с перечисленными выше и другими подобными действиями.

Санитарная охрана государственной границы призвана обеспечивать предупреждение заноса инфекционных заболеваний из-за границы в пределы территории Российской Федерации и из ее пределов. Ее разновидностями является ветеринарная охрана, имеющая целью предупреждение заноса на территорию Российской Федерации заразных заболеваний животных и птиц, а также внешний карантин, состоящий в предупреждении ввоза и вывоза семян, растений, сельскохозяйственных продуктов, зараженных болезнями.

Охрана государственной границы предполагает функционирование соответствующих правовых режимов. Законом закрепляются следующие режимы:

а) режим государственной границы; б) пограничный режим; в) режим в пунктах пропуска через государственную границу.

Режим государственной границы — совокупность правил, устанавливающих порядок ее содержания, пересечения гражданами и транспортными средствами; перемещения через границу товаров и животных; ведения на ней хозяйственной, промысловой и иной деятельности; разрешения с иностранными государствами инцидентов, связанных с нарушением режима границы.

Пограничный режим — совокупность правил въезда (прохода), временного пребывания лиц и транспортных средств в пограничной полосе; осуществление в ее пределах хозяйственной, промысловой и *иной деятельности; проведение массовых общественно-политических, культурных и других мероприятий* в пограничной полосе и т.п.

Пограничная полоса — часть территории Российской Федерации, непосредственно прилегающей к государственной границе на всем ее протяжении. Ширина полосы устанавливается до 5 километров.

В соответствии с требованиями режима государственной границы ее пересечение осуществляется через пункты пропуска, под которыми понимается территория в пределах железнодорожного, автомобильного вокзала, станции, морского, речного порта, аэродрома, открытого для международных сообщений, а также иное, специально оборудованное место, где осуществляется пограничный, а при необходимости и другие виды контроля и пропуск через государственную границу лиц, транспортных средств, товаров и животных.

Режим в пунктах пропуска через государственную границу есть совокупность правил въезда в названные пункты, пребывания и выезда из них лиц, транспортных средств, ввоза, нахождения и вывоза товаров и животных. Этот

режим необходим для осуществления пограничного, таможенного, ветеринарного и других видов контроля.

Охрана государственной границы Российской Федерации на суше, море, реках, озерах и других водоемах возложена на **Пограничные войска Федеральной пограничной службы Российской Федерации (ФПС России)**; воздушного пространства — на войска противовоздушной обороны; участков границы в подводной среде — на Военно-Морской Флот.

Организация охраны государственной границы, территориального моря, континентального шельфа и исключительной экономической зоны Российской Федерации возложена на Федеральную пограничную службу Российской Федерации, Положение о которой утверждено Указом Президента Российской Федерации от 2 марта 1995 года. Являясь федеральным органом исполнительной власти, она возглавляет систему органов пограничной службы Российской Федерации, в которую входят Пограничные войска, органы пограничного и иных видов контроля, оперативные органы, органы обеспечения безопасности, учебные заведения, предприятия, учреждения и организации, находящиеся в подчинении ФПС России; осуществляет координацию деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления по вопросам своей компетенции.

Основными задачами ФПС России являются: руководство органами пограничной службы; организация охраны государственной границы Российской Федерации и государств-участников СНГ на основе двусторонних договоров (соглашений); организация пропуска лиц, транспортных средств, грузов, товаров и животных через государственную границу Российской Федерации; организация разведывательной, контрразведывательной и оперативно-розыскной деятельности органов пограничной службы и др.

Выполняя возложенные на нее задачи, ФПС России участвует в разработке и реализации государственной пограничной политики, пограничных программ Российской Федерации, подготовке законодательных актов и других правовых актов по вопросам охраны государственной границы.

ФПС России разрабатывает меры по предупреждению и пресечению незаконного изменения прохождения государственной границы Российской Федерации, по поддержанию режима государственной границы, соблюдению пограничного режима и режима в пунктах пропуска через государственную границу Российской Федерации.

Являясь составной частью сил обеспечения безопасности, ФПС России добывает и обрабатывает информацию об угрозах безопасности Российской Федерации в сфере охраны государственной границы, представляя ее Президенту Российской Федерации, Правительству Российской Федерации, а также заинтересованным федеральным органам государственной власти и органам государственной власти субъектов Российской Федерации и т.д.

ФПС России осуществляет руководство пограничными представителями, которые назначаются на определенные участки государственной границы Рос-

сийской Федерации в соответствии с международными договорами Российской Федерации. Основное назначение пограничных представителей заключается в осуществлении контроля за соблюдением режима государственной границы Российской Федерации, в принятии мер для недопущения нарушений порядка содержания государственной границы, ее пересечения лицами и транспортными средствами, перемещения через государственную границу грузов, товаров и животных, ведения на государственной границе Российской Федерации хозяйственной, промысловой и иной деятельности, для обеспечения выполнения международных договоров о государственной границе Российской Федерации и ее режиме. На пограничных представителей возложена разработка и осуществление мер по предупреждению и урегулированию пограничных инцидентов, а также проведение в одностороннем порядке или совместно с пограничными представителями сопредельных с Российской Федерацией государств расследования пограничных инцидентов.

Основная нагрузка по охране государственной границы ложится на Пограничные войска. Они призваны обеспечивать всеми имеющимися у них средствами недопущение противоправного изменения прохождения границы на местности, отражать вооруженные вторжения на территорию Российской Федерации; проводить оперативно-розыскную деятельность. На них возложен непосредственный контроль за соблюдением правил режима государственной границы, пограничного режима, режима в пунктах пропуска через государственную границу.

Пограничные войска наделены широким кругом полномочий. В частности, они вправе проверять документы у граждан, а также документы транспортных средств; в случае необходимости осуществлять; задержание и личный досмотр граждан, досмотр транспортных средств и перевозимых грузов на них; осуществлять в пределах своей компетенции производство по делам об административных правонарушениях и т.п.

Закон Российской Федерации «О Государственной границе Российской Федерации» предусматривает возможность граждан участвовать на добровольной основе в охране государственной границы.

Эту деятельность они осуществляют в составе добровольных народных дружин по охране государственной границы Российской Федерации либо в качестве внештатных сотрудников Пограничных войск Их задачи и полномочия определены в правовом акте «Порядок привлечения граждан к охране государственной границы Российской Федерации», который был утвержден постановлением Правительства Российской Федерации от 15 апреля 1995 года.

В определенных законодательством случаях в охране государственной границы участвуют ФСБ России, федеральные органы внешней разведки, войска Минобороны России, внутренние войска Министерства внутренних дел Российской Федерации и др.

граждан, досмотр транспортных средств и перевозимых грузов на них; осуществлять в пределах своей компетенции производство по делам об административных правонарушениях и т.п.

Закон Российской Федерации «О Государственной границе Российской Федерации» предусматривает возможность граждан участвовать на добровольной основе в охране государственной границы. Эту деятельность они осуществляют в составе добровольных народных дружин по охране государственной границы Российской Федерации либо в качестве внештатных сотрудников Пограничных войск. Их задачи и полномочия определены в правовом акте «Порядок привлечения граждан к охране государственной границы Российской Федерации», который был утвержден постановлением Правительства Российской Федерации от 15 апреля 1995 года.

В определенных законодательством случаях в охране государственной границы участвуют ФСБ России, федеральные органы внешней разведки, войска Минобороны России, внутренние войска Министерства внутренних дел Российской Федерации и др.

Библиографический список

1. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика. Электронинформ, 1997.
2. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации. – М.: ИНФРА-М, 2001.
3. Закон Российской Федерации «Об информации, информатизации и защите информации», от 25 января 1995г. №24-ФЗ.
4. О Правительстве Российской Федерации : федер. конституционный закон от 17.12.1997 г. № 2-ФКЗ // СЗ РФ. 1997. № 51. Ст. 5712; 1998. № 1. Ст. 1; 2004. № 25. Ст. 2478, № 45. Ст. 4376; 2005. № 23. Ст. 2197.
5. О безопасности : закон РФ от 05.03.1992 г. № 2446-1 // Ведомости СНД и ВС РФ. 1992. № 15. Ст. 769; 1993. № 2. Ст. 77; СЗ РФ. 2002. № 30. Ст. 3033; 2005. № 10. Ст. 763.
6. О федеральной службе безопасности : ФЗ от 03.04.1995 г. № 40-ФЗ // СЗ РФ. 1995. № 15. Ст. 1269; 2000. № 1 (ч. 1). Ст. 9; № 46. Ст. 4537; 2002. № 19. Ст. 1794; № 30. Ст. 3033; 2003. № 2. Ст. 156; № 27 (ч. 1). Ст. 2700; 2004. № 35. Ст. 3607; 2005. № 10. Ст. 763; 2006. № 17 (ч. 1). Ст. 1779.
7. О внешней разведке : ФЗ от 10.01.1996 г. № 5-ФЗ // СЗ РФ. 1996. № 3. Ст. 143; 2000. № 46. Ст. 4537; 2003. № 27 (ч. 1). Ст. 2700; 2004. № 35. Ст. 3607.
8. Концепция национальной безопасности Российской Федерации : утв. указом Президента Российской Федерации от 10.01.2000 г. № 24 // СЗ РФ. 2000. № 2. Ст. 170.
9. Об утверждении положений о Совете Безопасности Российской Федерации и Аппарате Совета Безопасности Российской Федерации, а также об изменении и признании утратившими силу отдельных актов Президента Российской Федерации : указ Президента Российской Федерации от 07.06.2004 г. № 726 // СЗ РФ. 2004. № 24. Ст. 2392.
10. Вопросы Федеральной службы безопасности Российской Федерации : указ Президента Российской Федерации от 11.08.2003 г. № 960 // СЗ РФ. 2003. № 33. Ст. 3254; 2004. № 28. Ст. 2883; 2005. № 36. Ст. 3665.
11. Вопросы Федеральной службы охраны Российской Федерации : указ Президента Российской Федерации от 07.08.2004 г. № 1013 // СЗ РФ. 2004. № 32. Ст. 3314; 2005. № 1 (ч. 1). Ст. 67; № 13. Ст. 1137.
12. Вишняков В. Г. О методологических основах правового регулирования проблем безопасности Российской Федерации // Журнал российского права. 2005. № 9.
13. Гончаров И. В. К вопросу о понятии конституционной безопасности федеративного государства // Государство и право. 2003. № 12.

- 14.Дмитриев Ю. А., Петров С. М., Идрисов Р. Ф. Государство как субъект обеспечения национальной безопасности России // Право и политика. 2001. № 11.
- 15.Кардашова И. Б. Механизм обеспечения национальной безопасности Российской Федерации: сущность, задачи и пути совершенствования // Право и политика. 2005. № 2.
- 16.Кетов Ю. Роль органов исполнительной власти в обеспечении национальной безопасности // Государственная служба. 2005. № 3.
- 17.Кириянов А. Ю. Региональная безопасность в системе национальной безопасности // Российский судья. 2005. № 9.
- 18.Полянский И. А. Военная доктрина: понятие, содержание и значение для обеспечения военной безопасности // Вестник Хабаровской государственной академии экономики и права. 2006. № 1.
- 19.Полянский И. А., Трофимов Е. В. Военная доктрина России и ее роль в обеспечении военной безопасности и строительстве Вооруженных Сил // Право и политика. 2006. № 1.
- 20.Прокудин И. И. Полномочия Президента и Правительства Российской Федерации по осуществлению контроля в области обеспечения национальной безопасности // Право и политика. 2003. № 9.
- 21.Стахов А. Концепция национальной безопасности России: административно-правовой аспект // Российская юстиция. 2003. № 3.
- 22.Тропин С. А. Экономическая безопасность России // Законодательство и экономика. 2004. № 5.
- 23.Устинов В. В. Государственная антитеррористическая стратегия: общая концепция и правовые аспекты // Государство и право. 2003. № 3.
- 24.Государственная тайна и её защита. Серия «Закон и право» М.: Ось-89, 2004 г.
- 25.Краковский Ю.М. Информационная безопасность и защита информации: Уч. пособие, изд-во Март, 2008
- 26.Скиба В. Ю., Курбатов В. А Руководство по защите от внутренних угроз информационной безопасности. Издательство: Питер, 2008
- 27.Белов Е.Б., Лось В.П. Основы информационной безопасности. Учебное пособие для вузов, Гелиос АРВ, 2006.
- 28.Д.П. Зегжда, А.М. Ивашко. Основы безопасности информационных систем. М., Горячая линия-Телеком, 2005.
- 29.Казанцев С.Я., Згадзай О.Э., Оболенский Р.М. и др. Правовое обеспечение информационной безопасности: Учебное пособие для студентов высш. учеб. заведений. – М.: Издательский центр «Академия», 2005.
- 30.В.Н. Лопатин. Правовые основы информационной безопасности. Курс лекций. М., МИФИ, 2000.

Роман Александрович Васильев

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Курс лекций для студентов специальности 090900 – Информационная
безопасность

Редактор

603155, г. Нижний Новгород, ул. Минина, д. 31а, НГЛУ им. Н.А. Добролюбова
Редакционно-издательский отдел

Подписано в печать

Бумага писчая №1 Формат 60х84 1/16 Усл.п.л. 4,9 Уч.-изд.л. 4,3

Тираж экз. Цена договорная Заказ