Қазақстан Республикасы білім және ғылым министрлігі
Қостанай облысы әкімдігінің білім басқармасы
«Қостанай жоғары политехникалық колледжі» КМҚК

Министерство образования и науки Республики Казахстан
КГКП «Костанайский политехнический высший колледж»
Управления образования акимата Костанайской области

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ПО МОДУЛЮ
ТОМ 1

КМ 08 «Ақпараттық қауіпсіздік бойынша шараларды қамтамасыз ету, тораптық есептеу желісі мен Internet-ті пайдалану және икемдеу»

ПМ 08 «Обеспечение мер по информационной безопасности, использование и настройка локальных вычислительных сетей и Interneta»

модуль атауы/ наименование модуля

Мамандық/Специальность:

1304000 «Есептеу техникасы және бағдарламалық қамтамасыз ету (түрлері бойынша)»

1304000 «Вычислительная техника и программное обеспечение (по видам)»

Біліктілік/Квалификация:

130404 3 техник-бағдармалашы

130404 3 техник-программист

Костанай 2021

СОДЕРЖАНИЕ

1. Глоссарий…….…….3
2. Введение……7
3. Методы защиты информации…….…….8
4. Заключение……...….159

ГЛОССАРИЙ

1. *Алфавит* – набор знаков, в котором установлен порядок их следования (лексикографический порядок).
2. *Анализ* – метод исследования, основанный на выделении отдельных компонентов системы и рассмотрении их свойств и связей.
3. *Аналоговая форма представления информации* – представление сообщения, содержащего информацию, посредством сигналов, информационный параметр которых является непрерывной функцией времени
4. *Бит* – единица измерения энтропии при двух возможных равновероятных исходах опыта.
5. *Вес кодовой комбинации* – число ненулевых (единичных) разрядов в данной кодовой комбинации
6. *Внешние запоминающие устройства (ВЗУ)* – устройства, выполняющие операции, связанные с сохранения и считывания данных на материальном носителе.
7. *Данные* – это сведения, характеризующие какую-то систему, явление, процесс или объект, представленные в определенной форме и предназначенные для дальнейшего использования.
8. *Декодер* – устройство, обеспечивающее выполнение операции декодирования
9. *Декодирование* – операция, обратная кодированию, т.е. восстановление информации в первичном алфавите по полученной последовательности кодов.
10. *Дискретный канал* – канал связи, используемый для передачи дискретных сообщений
11. *Дискретные устройства* – те, у которых дискретны множества внутренних состояний, входных и выходных сигналов, а также множество моментов времени, в которые поступают входные сигналы, меняются внутренние состояния и выдаются выходные сигналы.
12. *Дискретная форма представления информации* – представление сообщения, содержащего информацию, посредством конечного числа знаков (алфавита)
13. *Документ* – продукт, сформированный в результате исполнения некоторой программы.
14. *Запись логическая* – поименованная совокупность элементарных данных, имеющая смысловую завершенность.
15. *Запись физическая* – элемент поверхности носителя, на котором в соответствии с физическими принципами функционирования носителя размещаются данные, составляющие логическую запись.
16. *Запоминающие устройства с произвольным доступом* – те, в которых доступ к данным осуществляется по адресу ячейки, где они хранятся.
17. *Знак* – элемент некоторого конечного множества отличных друг от друга сущностей, используемого для представления дискретных сигналов.
18. *Избыточность кода относительная* – характеристика, показывающая, во сколько раз требуется удлинить сообщение, чтобы обеспечить его надежную (безошибочную) передачу (хранение).

19. *Информация* (статистическое определение) – это содержание сообщения, понижающего неопределенность некоторого опыта с неоднозначным исходом; убыль связанной с ним энтропии является количественной мерой информации.

20. *Информационный процесс* – это изменение с течением времени содержания информации или представляющего его сообщения.

21. *Источник информации* – это субъект или объект, порождающий информацию и представляющий ее в виде сообщения.

22. *Канал связи* – это материальная среда, а также физический или иной процесс, посредством которого осуществляется передача сообщения, т.е. распространение сигналов в пространстве с течением времени

23. *Класс* – это множество объектов, обладающих одним или несколькими одинаковыми атрибутами; эти атрибуты называются *полем свойств класса.*

24. *Классификация* – это распределение однотипных объектов в соответствии с выделенными свойствами (признаками, категориями, классами).

25. *Кодер* – устройство, обеспечивающее выполнение операции кодирования

26. *Код* – (1) правило, описывающее соответствие знаков или их сочетаний одного алфавита знакам или их сочетаниям другого алфавита. (2) знаки вторичного алфавита, используемые для представления знаков или их сочетаний первичного алфавита.

27. *Кодирование* – перевод информации, представленной посредством первичного алфавита, в последовательность кодов.

28. *Конечным автомат* – система $<X,Y,Q,\Psi,\Theta>$, в которой X и Y являются конечными входным и выходным алфавитами, Q – конечным множеством внутренних состояний, $\Psi(x,q)$ – функцией переходов и $\Theta(x,q)$ – функцией выходов.

29. *Линия связи* – это совокупность средств связи и канала связи, посредством которых осуществляется передача информации от источника к приемнику

30. *Массив* – упорядоченная линейная совокупность однородных данных.

31. *Материальный носитель информации* – материальный объект или среда, которые служат для представления или передачи информации.

32. *Машинное слово* – (1) совокупность двоичных элементов, обрабатываемая как единое целое в устройствах и памяти компьютера; (2) данные, содержащиеся в одной ячейке памяти компьютера.

33. *Моделирование* – построение упрощенного варианта прототипа, обеспечивающего приемлемую для данной задачи точность описания его строения или поведения.

34. *Моделирование имитационное* – метод исследования, основанный на том, что изучаемый прототип заменяется ее имитатором – натурной или информационной моделью – с которым и проводятся эксперименты с целью получения информации об особенностях прототипа.

35. *Модель* – это объединение составных частей (элементов) и связей между ними, отражающая существенные для данной задачи свойства прототипа.

36. *Модель математическая* – это множество элементов произвольной природы, на которых определено конечное множество отношений.

37. *Модель проверяемая* – та, у которой результат ее использования может быть соотнесен (сравнен) с прототипом.

38. *Набор знаков* – дискретное множество знаков.

39. *Объект* – простейшая составляющая сложного объединения, обладающая следующими качествами:

a. в рамках данной задачи он не имеет внутреннего устройства и рассматривается как единое целое;

b. у него имеется набор свойств (атрибутов), которые изменяются в результате внешних воздействий;

c. он идентифицирован, т.е. имеет имя (название).

40. *Оптимальный (n,k)-код* – код, который обеспечивает минимальную вероятность ошибочного декодирования среди всех иных кодов с теми же n и k.

41. *Помехоустойчивый код* – код, позволяющий обнаружить и при необходимости исправить ошибки в принятом сообщении.

42. *Правило интерпретации сообщения* – соотношение (закон), устанавливающий соответствие между сообщением и содержащейся в нем информацией.

43. *Приемник информации* – это субъект или объект, способный принять сообщение и правильно его интерпретировать.

44. *Пропускная способность канала связи* – максимальное количество информации, передаваемое по каналу за единицу времени.

45. *Свойство (атрибут)* – качество объекта, для которого установлена мера.

46. *Сигнал* – изменение характеристики материального носителя, которое используется для представления информации.

47. *Сигнал непрерывный (аналоговый)* – его параметр может принимать любое значение в пределах некоторого интервала.

48. *Сигнал дискретным* – его параметр может принимать конечное число значений в пределах некоторого интервала.

49. *Синтез* – (1) метод исследования (изучения) системы в целом (т.е. компонентов в их взаимосвязи), сведение в единое целое данных, полученных в результате анализа;
(2) создание системы путем соединения отдельных компонентов на основании законов, определяющих их взаимосвязь.

50. *Система* – совокупность взаимодействующих компонентов, каждый из которых в отдельности не обладает свойствами системы в целом, но является ее неотъемлемой частью.

51. *Систематический код* – (n,k)-код), в котором значения всех проверочных бит (p_j) определяются линейными комбинациями информационных бит (u_i)

52. *Система счисления* – это правило записи чисел с помощью заданного набора специальных знаков – цифр.

53. *Система счисления позиционная* – те, в которых значение каждой цифры в изображении числа определяется ее положением (позицией) в ряду других цифр.

54. *Сообщения (источники) марковские (с памятью)* – те, в которых в которых существуют статистические связи (корреляции) между знаками или их сочетаниями

55. *Сообщения (источники) шенноновские (без памяти)* – те, в которых вероятность появления каждого отдельного знака не меняется со временем.

56. *Средства связи* – совокупность устройств, обеспечивающих преобразование первичного сообщения от источника информации в сигналы заданной физической природы, их передачу и прием.

57. *Структура данных* – перечень объединяемых одиночных данных, их характеристики, а также особенности связей между ними образуют.

58. *Схема* – это комбинация базисных элементов, в которой выходы одних элементов присоединяются к входам других.

59. *Условие Фано:* неравномерный код может быть однозначно декодирован, если никакой из кодов не совпадает с началом какого–либо иного более длинного кода.

60. *Файл* – определенным образом оформленная совокупность физических записей, рассматриваемая как единое целое и имеющая описание в системе хранения информации.

61. *Формальная грамматика* – система правил, описывающая множество конечных последовательностей символов формального алфавита.

62. *Формальный исполнитель* – субъект или устройство, способные воспринимать и анализировать указания алгоритма, изменять в соответствии с ним свое состояние, а также обладающие механизмом исполнения, способным производить пошаговую обработку информации.

63. *Формальная система* – это математическая модель, задающая множество дискретных компонентов путем описания исходных объектов и правил построения новых компонентов из исходных и уже построенных.

64. *Функциональный блок* – часть алгоритма, организованная как простое действие, т.е. имеющая один вход (выполнение начинается всегда с одного и того же действия) и один выход.

65. *Черный ящик* – это система, строение которой неизвестно пользователю, однако, известна ее реакция на определенные внешние воздействия.

66. *Ширина полосы пропускания* – интервал частот, используемый данным каналом связи для передачи сигналов.

67. *Экономичность системы счисления* – то количество чисел, которое можно записать в данной системе с помощью определенного количества цифр.

68. *Энтропия* - есть мера неопределенности опыта, в котором проявляются случайные события, равная средней неопределенности всех возможных его исходов.

ВВЕДЕНИЕ

В курс включены сведения, необходимые всем специалистам в области информационной безопасности (ИБ).

Рассматриваются основные понятия ИБ, структура мер в области ИБ, кратко описываются меры законодательного, административного, процедурного и программно-технического уровней.

Информационная безопасность (ИБ) - сравнительно молодая, быстро развивающаяся область информационных технологий (ИТ), для успешного освоения которой важно с самого начала усвоить современный, согласованный с другими ветвями ИТ базис. Это - первая задача курса, для решения которой привлекается объектно-ориентированный подход.

Успех в области ИБ может принести только комплексный подход. Описание общей структуры и отдельных уровней такого подхода - вторая задача курса. Для ее решения рассматриваются меры законодательного, административного, процедурного и программно-технического уровней. Приводятся сведения о зарубежном законодательстве в области ИБ, о проблемах, существующих в настоящее время в законодательстве. На административном уровне рассматриваются политика и программа безопасности, их типовая структура, меры по выработке и сопровождению. На процедурном уровне описываются меры безопасности, имеющие дело с людьми. Формулируются основные принципы, помогающие успеху таких мер. Программно-технический уровень, в соответствии с объектным подходом, трактуется как совокупность сервисов. Дается описание каждого сервиса.

Предполагается, что большинство понятий, введенных в данном курсе, станет предметом более детального рассмотрения в других, специальных курсах.

Цель

Цель курса - заложить методически правильные основы знаний, необходимые будущим специалистам-практикам в области информационной безопасности.

Предварительные знания

Требуется знание основ объектно-ориентированного подхода, основ современной технологии программирования, стандартов и технологии программирования распределенных систем, структуры и функций современных операционных систем, организации семейства протоколов TCP/IP.

РАЗДЕЛ 1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСТНОСТИ, ОСНОВЫ ПРОЕКТИРОВАНИЯ И СОЗДАНИЯ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ. МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ.

Тема1: Введение. Понятие национальной безопасности; виды безопасности; роль и место системы обеспечения информационной безопасности в системе национальной безопасности РК

Понятие информационной безопасности. Основные составляющие. Важность проблемы

Под информационной безопасностью (ИБ) следует понимать защиту интересов субъектов информационных отношений. Ниже описаны основные ее составляющие – конфиденциальность, целостность, доступность. Приводится статистика нарушений ИБ, описываются наиболее характерные случаи.

1.1. Понятие информационной безопасности

Словосочетание *"информационная безопасность"* в разных контекстах может иметь различный смысл. В Доктрине информационной безопасности термин *"информационная безопасность"* используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В Законе "Об участии в международном информационном обмене" *информационная безопасность* определяется аналогичным образом – как 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, на каком языке (русском или каком-либо ином) она закодирована, кто или что является ее источником и какое психологическое воздействие она оказывает на людей. Поэтому термин *"информационная безопасность"* будет использоваться в узком смысле, так, как это принято, например, в англоязычной литературе.

Под ***информационной безопасностью*** мы будем понимать защищенность информации и *поддерживающей инфраструктуры* от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести *неприемлемый ущерб* субъектам информационных отношений, в том числе владельцам и пользователям информации и *поддерживающей инфраструктуры*. (Чуть дальше мы поясним, что следует понимать под *поддерживающей инфраструктурой*.)

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

Таким образом, правильный с методологической точки зрения подход к проблемам *информационной безопасности* начинается с выявления *субъектов информационных отношений* и интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы *информационной безопасности* – это оборотная сторона использования информационных технологий.

Из этого положения можно вывести два важных следствия:

1. Трактовка проблем, связанных с *информационной безопасностью*, 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".

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.

Возвращаясь к вопросам терминологии, отметим, что термин "компьютерная безопасность" (как эквивалент или заменитель *ИБ*) представляется нам слишком узким. Компьютеры – только одна из составляющих информационных систем, и хотя наше внимание будет сосредоточено в первую очередь на информации, которая хранится, обрабатывается и передается с помощью компьютеров, ее безопасность определяется всей совокупностью составляющих и, в первую очередь, самым слабым звеном, которым в подавляющем большинстве случаев оказывается человек (записавший, например, свой пароль на "горчичнике", прилепленном к монитору).

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.

1.2. Основные составляющие информационной безопасности

Информационная безопасность – многогранная, можно даже сказать, многомерная область деятельности, в которой успех может принести только систематический, комплексный подход.

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение **доступности**, **целостности** и **конфиденциальности** информационных ресурсов и *поддерживающей инфраструктуры*.

Иногда в число основных составляющих *ИБ* включают защиту от несанкционированного копирования информации, но, на наш взгляд, это слишком специфический аспект с сомнительными шансами на успех, поэтому мы не станем его выделять.

Поясним понятия доступности, целостности и конфиденциальности.

Доступность – это возможность за приемлемое время получить требуемую информационную услугу. Под целостностью подразумевается актуальность и непротиворечивость информации, 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 финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений.

Целостность оказывается важнейшим аспектом *ИБ* в тех случаях, когда информация служит "руководством к действию". Рецептура лекарств, 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 Web-сервера какой-либо правительственной организации. Конфиденциальность – самый проработанный у нас в стране аспект *информационной безопасности*. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы.

Если вернуться к анализу интересов различных категорий *субъектов информационных отношений*, то 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).

1.3. 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** (здесь, подчеркнем, термин *"информационная безопасность"* используется в широком смысле) защита от несанкционированного доступа к информационным ресурсам, обеспечение безопасности информационных и телекоммуникационных систем выделены в качестве важных составляющих национальных интересов в информационной сфере.
- По распоряжению президента США Клинтона (от 15 июля 1996 года, номер 13010) была создана Комиссия по защите критически важной инфраструктуры как от физических нападений, так и от атак, предпринятых с помощью информационного оружия. В начале октября 1997 года при подготовке доклада президенту глава вышеупомянутой комиссии Роберт Марш заявил, что в настоящее время ни правительство, ни частный сектор не располагают средствами защиты от компьютерных атак, способных вывести из строя коммуникационные сети и сети энергоснабжения.
- Американский ракетный крейсер "Йорктаун" был вынужден вернуться в порт из-за многочисленных проблем с программным обеспечением, функционировавшим на платформе Windows NT 4.0 (Government Computer News, 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 сообщил, что хакеры с 1994 по 1996 год предприняли почти 500 попыток проникновения в компьютерную сеть Центрального банка. В 1995 году ими было похищено 250 миллиардов рублей (ИТАР-ТАСС, АР, 17 сентября 1996 года).
- Как сообщил журнал Internet Week 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 середине июля 1996 года корпорация General Motors отозвала 292860 автомобилей марки Pontiac, Oldsmobile и Buick моделей 1996 и 1997 годов, поскольку ошибка в программном обеспечении двигателя могла привести к пожару.
- В феврале 2001 года двое бывших сотрудников компании Commerce One, 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. Чего стоит одна только "Проблема 2000" – стыд и позор программистского сообщества!

При анализе проблематики, связанной с *информационной безопасностью*, необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что *информационная безопасность* есть составная часть информационных технологий – области, развивающейся беспрецедентно высокими темпами. Здесь важны не столько отдельные решения (законы, учебные курсы, программно-технические изделия), находящиеся на современном уровне, сколько механизмы генерации новых решений, позволяющие жить в темпе технического прогресса.

К сожалению, современная технология программирования не позволяет создавать безошибочные программы, что не способствует быстрому развитию средств обеспечения *ИБ*. Следует исходить из того, что необходимо конструировать надежные системы (*информационной безопасности*) с привлечением ненадежных компонентов (программ). В принципе, это возможно, но требует соблюдения определенных архитектурных принципов и контроля состояния защищенности на всем протяжении **жизненного цикла ИС**.

Приведем еще несколько цифр. В марте 1999 года был опубликован очередной, четвертый по счету, годовой отчет "Компьютерная преступность и безопасность-1999: проблемы и тенденции" (Issues and Trends: 1999 CSI/FBI Computer Crime and Security Survey). 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 Internet подвергались 57% опрошенных; в 55% случаях отмечались нарушения со стороны собственных сотрудников. Примечательно, что 33% респондентов на вопрос "были ли взломаны ваши Web-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 InformationWeek, 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 (National Infrastructure Protection Center, NIPC) 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 Unix, Windows, MacOS, 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. Распространение объектно-ориентированного подхода на информационную безопасность

В этой лекции закладываются методические основы курса. Кратко формулируются необходимые понятия объектно-ориентированного подхода, в соответствии с ним выделяются уровни мер в области ИБ с небольшим числом сущностей на каждом из них.

2.1. О необходимости объектно-ориентированного подхода к информационной безопасности

В настоящее время информационная безопасность является относительно замкнутой дисциплиной, развитие которой не всегда синхронизировано с изменениями в других областях информационных технологий. В частности, в ИБ пока не нашли отражения основные положения *объектно-ориентированного подхода*, ставшего основой при построении современных информационных систем. Не учитываются в ИБ и достижения в технологии программирования, основанные на накоплении и многократном использовании программистских знаний. На наш взгляд, это очень серьезная проблема, затрудняющая прогресс в области ИБ.

Попытки создания больших систем еще в 60-х годах вскрыли многочисленные проблемы программирования, главной из которых является сложность создаваемых и сопровождаемых систем. Результатами исследований в области технологии программирования стали сначала структурированное программирование, затем *объектно-ориентированный подход*.

Объектно-ориентированный подход является основой современной технологии программирования, испытанным методом борьбы со сложностью систем. Представляется естественным и, более того, необходимым, стремление распространить этот подход и на системы информационной безопасности, для которых, как и для программирования в целом, имеет место упомянутая проблема сложности.

Сложность эта имеет двоякую природу. Во-первых, сложны не только аппаратно-программные системы, которые необходимо защищать, но и сами средства безопасности. Во-вторых, быстро нарастает сложность семейства нормативных документов, таких, например, как профили защиты на основе "Общих критериев", речь о которых впереди. Эта сложность менее очевидна, но ею также нельзя пренебрегать; необходимо изначально строить семейства документов по объектному принципу.

Любой разумный метод борьбы со сложностью опирается на *принцип "divide et impera" - "разделяй и властвуй"*. В данном контексте этот ***принцип*** означает, что *сложная*

система (информационной безопасности) на верхнем уровне должна состоять из небольшого числа относительно независимых *компонентов*. Относительная независимость здесь и далее понимается как минимизация числа связей между *компонентами*. Затем *декомпозиции* подвергаются выделенные на первом этапе *компоненты*, и так далее до заданного *уровня детализации*. В результате система оказывается представленной в виде иерархии с несколькими уровнями абстракции.

Важнейший вопрос, возникающий при реализации *принципа "разделяй и властвуй"*, - как, собственно говоря, разделять. Упоминавшийся выше *структурный подход* опирается на алгоритмическую *декомпозицию*, когда выделяются функциональные элементы системы. Основная проблема *структурного подхода* состоит в том, что он неприменим на ранних этапах анализа и моделирования предметной области, когда до алгоритмов и функций дело еще не дошло. Нужен подход "широкого спектра", не имеющий такого концептуального разрыва с анализируемыми системами и применимый на всех этапах разработки и реализации *сложных систем*. Мы постараемся показать, что *объектно-ориентированный подход* удовлетворяет таким требованиям.

2.2. Основные понятия объектно-ориентированного подхода

Объектно-ориентированный подход использует объектную *декомпозицию*, то есть поведение системы описывается в терминах взаимодействия *объектов*.

Что же понимается под *объектом* и каковы другие основополагающие понятия данного подхода?

Прежде всего, введем понятие *класса*. ***Класс*** - это абстракция множества сущностей реального мира, объединенных общностью структуры и поведения.

Объект - это элемент *класса*, то есть абстракция определенной сущности.

Подчеркнем, что *объекты* активны, у них есть не только внутренняя структура, но и поведение, которое описывается так называемыми *методами объекта*. Например, может быть определен *класс* "пользователь", характеризующий "пользователя вообще", то есть ассоциированные с пользователями данные и их поведение (*методы*). После этого может быть создан *объект* "пользователь Иванов" с соответствующей конкретизацией данных и, возможно, *методов*.

К активности *объектов* мы еще вернемся.

Следующую группу важнейших понятий объектного подхода составляют *инкапсуляция*, *наследование* и *полиморфизм*.

Основным инструментом борьбы со сложностью в *объектно-ориентированном подходе* является ***инкапсуляция*** - сокрытие реализации *объектов* (их внутренней структуры и деталей реализации *методов*) с предоставлением вовне только строго определенных интерфейсов.

Понятие "***полиморфизм***" может трактоваться как способность *объекта* принадлежать более чем одному *классу*. Введение этого понятия отражает необходимость смотреть на *объекты* под разными углами зрения, выделять при построении абстракций разные аспекты сущностей моделируемой предметной области, не нарушая при этом целостности *объекта*. (Строго говоря, существуют и другие виды *полиморфизма*, такие как перегрузка и параметрический *полиморфизм*, но нас они сейчас не интересуют.)

Наследование означает построение новых *классов* на основе существующих с возможностью добавления или переопределения данных и *методов*. *Наследование* является важным инструментом борьбы с размножением сущностей без необходимости.

Общая информация не дублируется, указывается только то, что меняется. При этом *класс*-потомок помнит о своих "корнях".

Очень важно и то, что *наследование* и *полиморфизм* в совокупности наделяют объектно-ориентированную систему способностью к относительно безболезненной эволюции. Средства информационной безопасности приходится постоянно модифицировать и обновлять, и если нельзя сделать так, чтобы это было экономически выгодно, ИБ из инструмента защиты превращается в обузу.

Мы еще вернемся к механизму *наследования* при рассмотрении ролевого управления доступом. Пополним рассмотренный выше классический набор понятий *объектно-ориентированного подхода* еще двумя понятиями: *грани объекта* и *уровня детализации*.

Объекты реального мира обладают, как правило, несколькими относительно независимыми характеристиками. Применительно к объектной модели будем называть такие характеристики ***гранями***. Мы уже сталкивались с тремя основными *гранями* ИБ - доступностью, целостностью и конфиденциальностью. Понятие *грани* позволяет более естественно, чем *полиморфизм*, смотреть на *объекты* с разных точек зрения и строить разноплановые абстракции.

Понятие *уровня детализации* важно не только для визуализации *объектов*, но и для систематического рассмотрения *сложных систем*, представленных в иерархическом виде. Само по себе оно очень простое: если очередной уровень иерархии рассматривается с *уровнем детализации* n > 0, то следующий - с *уровнем* (n - 1). *Объект* с *уровнем детализации* 0 считается атомарным.

Понятие *уровня детализации* показа позволяет рассматривать иерархии с потенциально бесконечной высотой, варьировать детализацию как *объектов* в целом, так и их *граней*.

Весьма распространенной конкретизацией *объектно-ориентированного подхода* являются ***компонентные объектные среды***, к числу которых принадлежит, например, JavaBeans. Здесь появляется два новых важных понятия: *компонент* и *контейнер*.

Неформально ***компонент*** можно определить как многократно используемый *объект*, допускающий обработку в графическом инструментальном окружении и сохранение в долговременной памяти.

Контейнеры могут включать в себя множество *компонентов*, образуя общий контекст взаимодействия с другими *компонентами* и с окружением. *Контейнеры* могут выступать в роли *компонентов* других *контейнеров*.

Компонентные объектные среды обладают всеми достоинствами, присущими *объектно-ориентированному подходу*:

инкапсуляция объектных *компонентов* скрывает сложность реализации, делая видимым только предоставляемый вовне интерфейс;

наследование позволяет развивать созданные ранее *компоненты*, не нарушая целостность объектной оболочки;

полиморфизм по сути дает возможность группировать *объекты*, характеристики которых с некоторой точки зрения можно считать сходными.

Понятия же *компонента* и *контейнера* необходимы нам потому, что с их помощью мы можем естественным образом представить защищаемую ИС и сами защитные средства. В частности, *контейнер* может определять границы контролируемой зоны (задавать так называемый "периметр безопасности").

На этом мы завершаем описание основных понятий *объектно-ориентированного подхода*.

2.3. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем

Попытаемся применить *объектно-ориентированный подход* к вопросам информационной безопасности.

Проблема обеспечения информационной безопасности - комплексная, защищать приходится *сложные системы*, и сами защитные средства тоже сложны, поэтому нам понадобятся все введенные понятия. Начнем с понятия *грани*.

Фактически три *грани* уже были введены: это доступность, целостность и конфиденциальность. Их можно рассматривать относительно независимо, и считается, что если все они обеспечены, то обеспечена и ИБ в целом (то есть субъектам информационных отношений не будет нанесен неприемлемый ущерб).

Таким образом, мы структурировали нашу цель. Теперь нужно структурировать средства ее достижения. Введем следующие *грани*:

- законодательные меры обеспечения информационной безопасности;
- административные меры (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);
- процедурные меры (меры безопасности, ориентированные на людей);
- программно-технические меры.

В дальнейшей части курса мы поясним подробнее, что понимается под каждой из выделенных *граней*. Здесь же отметим, что, в принципе, их можно рассматривать и как результат варьирования *уровня детализации* (по этой причине мы будем употреблять словосочетания "законодательный уровень", "процедурный уровень" и т.п.). Законы и нормативные акты ориентированы на всех субъектов информационных отношений независимо от их организационной принадлежности (это могут быть как юридические, так и физические лица) в пределах страны (международные конвенции имеют даже более широкую область действия), административные меры - на всех субъектов в пределах организации, процедурные – на отдельных людей (или небольшие категории субъектов), программно-технические – на оборудование и программное обеспечение. При такой трактовке в переходе с уровня на уровень можно усмотреть применение *наследования* (каждый следующий уровень не отменяет, а дополняет предыдущий), а также *полиморфизма* (субъекты выступают сразу в нескольких ипостасях - например, как инициаторы административных мер и как обычные пользователи, обязанные этим мерам подчиняться).

Очевидно, для всех выделенных, относительно независимых *граней* действует принцип *инкапсуляции* (это и значит, что *грани* "относительно независимы"). Более того, эти две совокупности *граней* можно назвать *ортогональными*, поскольку для фиксированной *грани* в одной совокупности (например, доступности) *грани* в другой совокупности должны пробегать все множество возможных значений (нужно рассмотреть законодательные, административные, процедурные и программно-технические меры). *Ортогональных совокупностей* не должно быть много; думается, двух совокупностей с числом элементов, соответственно, 3 и 4 уже достаточно, так как они дают 12 комбинаций.

Продемонстрируем теперь, как можно рассматривать защищаемую ИС, варьируя *уровень детализации*.

Пусть интересы субъектов информационных отношений концентрируются вокруг ИС некой организации, располагающей двумя территориально разнесенными производственными площадками, на каждой из которых есть серверы, обслуживающие своих и внешних пользователей, а также пользователи, нуждающиеся во внутренних и внешних сервисах. Одна из площадок оборудована внешним подключением (то есть имеет выход в Internet).

При взгляде с нулевым *уровнем детализации* мы увидим лишь то, что у организации есть информационная система (см. рис. 2.1).

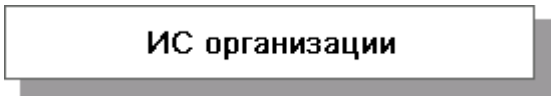


Рис. 2.1. ИС при рассмотрении с уровнем детализации 0.

Подобная точка зрения может показаться несостоятельной, но это не так. Уже здесь необходимо учесть законы, применимые к организациям, располагающим информационными системами. Возможно, какую-либо информацию нельзя хранить и обрабатывать на компьютерах, если ИС не была аттестована на соответствие определенным требованиям. На административном уровне могут быть декларированы цели, ради которых создавалась ИС, общие правила закупок, внедрения новых *компонентов*, эксплуатации и т.п. На процедурном уровне нужно определить требования к физической безопасности ИС и пути их выполнения, правила противопожарной безопасности и т.п. На программно-техническом уровне могут быть определены предпочтительные аппаратно-программные платформы и т.п.

По каким критериям проводить *декомпозицию* ИС – в значительной степени дело вкуса. Будем считать, что на первом *уровне детализации* делаются видимыми сервисы и пользователи, точнее, разделение на клиентскую и серверную часть (рис. 2.2).

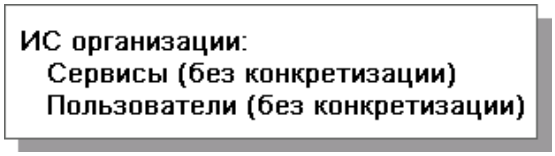


Рис. 2.2. ИС при рассмотрении с уровнем детализации 1.

На этом уровне следует сформулировать требования к сервисам (к самому их наличию, к доступности, целостности и конфиденциальности предоставляемых информационных услуг), изложить способы выполнения этих требований, определить общие правила поведения пользователей, необходимый уровень их предварительной подготовки, методы контроля их поведения, порядок поощрения и наказания и т.п. Могут быть сформулированы требования и предпочтения по отношению к серверным и клиентским платформам.

На втором *уровне детализации* мы увидим следующее (см. рис. 2.3).

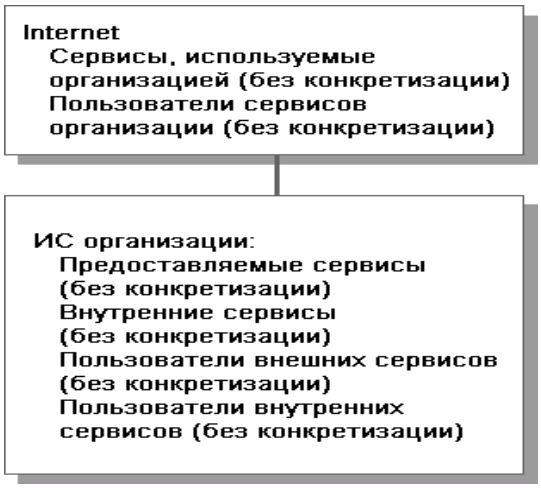


Рис. 2.3. ИС при рассмотрении с уровнем детализации 2.

На этом уровне нас все еще не интересует внутренняя структура ИС организации, равно как и детали Internet. Констатируется только существование связи между этими сетями, наличие в них пользователей, а также предоставляемых и внутренних сервисов. Что это за сервисы, пока неважно.

Находясь на *уровне детализации* 2, мы должны учитывать законы, применимые к организациям, ИС которых снабжены внешними подключениями. Речь идет о допустимости такого подключения, о его защите, об ответственности пользователей, обращающихся к внешним сервисам, и об ответственности организаций, открывающих свои сервисы для внешнего доступа. Конкретизация аналогичной направленности, с учетом наличия внешнего подключения, должна быть выполнена на административном, процедурном и программно-техническом уровнях.

Обратим внимание на то, что *контейнер* (в смысле *компонентной объектной среды*) "ИС организации" задает границы контролируемой зоны, в пределах которых организация проводит определенную политику. Internet живет по другим правилам, которые организация должна принимать, как данность.

Увеличивая *уровень детализации*, можно разглядеть две разнесенные производственные площадки и каналы связи между ними, распределение сервисов и пользователей по этим площадкам и средства обеспечения безопасности внутренних коммуникаций, специфику отдельных сервисов, разные категории пользователей и т.п. Мы, однако, на этом остановимся.

2.4. Недостатки традиционного подхода к информационной безопасности с объектной точки зрения

Исходя из основных положений *объектно-ориентированного подхода*, следует в первую очередь признать устаревшим традиционное **деление на** активные и пассивные сущности (**субъекты** и *объекты* в привычной для дообъектной ИБ терминологии). Подобное деление устарело, по крайней мере, по двум причинам.

Во-первых, в объектном подходе пассивных *объектов* нет. Можно считать, что все *объекты* активны одновременно и при необходимости вызывают *методы* друг друга. Как реализованы эти *методы* (и, в частности, как организован доступ к переменным и их значениям) - внутреннее дело вызываемого *объекта*; детали реализации скрыты, инкапсулированы. Вызывающему *объекту* доступен только предоставляемый интерфейс.

Во-вторых, нельзя сказать, что какие-то программы (*методы*) выполняются от имени пользователя. Реализации *объектов* сложны, так что последние нельзя

рассматривать всего лишь как инструменты выполнения воли пользователей. Скорее можно считать, что пользователь прямо или (как правило) косвенно, на свой страх и риск, "просит" некоторый *объект* об определенной информационной услуге. Когда активизируется вызываемый *метод, объект* действует скорее от имени (во всяком случае, по воле) своего создателя, чем от имени вызвавшего его пользователя. Можно считать, что *объекты* обладают достаточной "свободой воли", чтобы выполнять действия, о которых пользователь не только не просил, но даже не догадывается об их возможности. Особенно это справедливо в сетевой среде и для программного обеспечения (ПО), полученного через Internet, но может оказаться верным и для коммерческого ПО, закупленного по всем правилам у солидной фирмы.

Для иллюстрации приведем следующий гипотетический пример. Банк, ИС которого имеет соединение с Internet, приобрел за рубежом автоматизированную банковскую систему (АБС). Только спустя некоторое время в банке решили, что внешнее соединение нуждается в защите, и установили межсетевой экран.

Изучение регистрационной информации экрана показало, что время от времени за рубеж отправляются IP-пакеты, содержащие какие-то непонятные данные (наверное, зашифрованные, решили в банке). Стали разбираться, куда же пакеты направляются, и оказалось, что идут они в фирму, разработавшую АБС. Возникло подозрение, что в АБС встроена закладка, чтобы получать информацию о деятельности банка. Связались с фирмой; там очень удивились, поначалу все отрицали, но в конце концов выяснили, что один из программистов не убрал из поставленного в банк варианта отладочную выдачу, которая была организована через сеть (как передача IP-пакетов специфического вида, с явно заданным IP-адресом рабочего места этого программиста). Таким образом, никакого злого умысла не было, однако некоторое время информация о платежах свободно гуляла по сетям.

В дальнейшей части курса, в лекции, посвященной разграничению доступа, мы обсудим, как можно кардинальным образом решить подобные проблемы. Здесь отметим лишь, что при определении допустимости доступа важно не только (и не столько), кто обратился к *объекту*, но и то, какова **семантика** действия. Без привлечения семантики нельзя определить так называемые **"троянские программы"**, выполняющие, помимо декларированных, некоторые скрытые (обычно негативные) действия.

По-видимому, следует признать устаревшим и положение о том, что разграничение доступа направлено на защиту от злоумышленников. Приведенный выше пример показывает, что внутренние ошибки распределенных ИС представляют не меньшую опасность, а гарантировать их отсутствие в *сложных системах* современная технология программирования не позволяет.

В дообъектной ИБ одним из важнейших требований является **безопасность повторного использования** пассивных сущностей (таких, например, как динамически выделяемые области памяти). Очевидно, подобное требование вступает в конфликт с таким фундаментальным принципом, как *инкапсуляция*. *Объект* нельзя очистить внешним образом (заполнить нулями или случайной последовательностью бит), если только он сам не предоставляет соответствующий *метод*. При наличии такого *метода* надежность очистки зависит от корректности его реализации и вызова.

Одним из самых прочных стереотипов среди специалистов по ИБ является трактовка **операционной системы** как доминирующего **средства безопасности**. На разработку

защищенных ОС выделяются значительные средства, зачастую в ущерб остальным направлениям защиты и, следовательно, в ущерб реальной безопасности. В современных ИС, выстроенных в многоуровневой архитектуре клиент/сервер, ОС не контролирует *объекты*, с которыми работают пользователи, равно как и действия самих пользователей, которые регистрируются и учитываются прикладными средствами. Основной функцией безопасности ОС становится защита возможностей, предоставляемых привилегированным пользователям, от атак пользователей обычных.

Это важно, но безопасность такими мерами не исчерпывается. Далее мы рассмотрим подход к построению программно-технического уровня ИБ в виде совокупности сервисов безопасности.

Тема 3. Наиболее распространенные угрозы

Знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности.

3.1. Основные определения и критерии классификации угроз

Угроза - это потенциальная возможность определенным образом нарушить информационную безопасность.

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

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).

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 использования 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. Иметь представление о возможных *угрозах*, а также об *уязвимых* местах, которые эти *угрозы* обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности. Слишком много мифов существует в сфере информационных технологий (вспомним все ту же "Проблему 2000"), поэтому 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.

Подчеркнем, что само понятие "*угроза*" в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнуто 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 (и от того, какой ущерб является для них неприемлемым).

Мы попытаемся взглянуть на предмет с точки зрения типичной (на наш взгляд) организации. Впрочем, многие *угрозы* (например, пожар) опасны для всех.

Угрозы можно классифицировать по нескольким критериям:

- по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого *угрозы* направлены в первую очередь;
- по компонентам информационных систем, на которые *угрозы* нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);
- по расположению *источника угроз* (внутри/вне рассматриваемой ИС).

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

3.2. Наиболее распространенные угрозы доступности

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

Иногда такие ошибки и являются собственно *угрозами* (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают *уязвимые* места, которыми могут воспользоваться *злоумышленники* (таковы обычно ошибки администрирования). 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.

Другие *угрозы* доступности классифицируем по компонентам ИС, на которые нацелены *угрозы*:

- *отказ пользователей*;
- *внутренний отказ* информационной системы;

• *отказ поддерживающей инфраструктуры*.

Обычно применительно к пользователям рассматриваются следующие *угрозы*:

• нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);

• невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);

• невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

Основными источниками *внутренних отказов* являются:

• отступление (случайное или умышленное) от установленных правил эксплуатации;

• выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);

• ошибки при (пере)конфигурировании системы;

• отказы программного и аппаратного обеспечения;

• разрушение данных;

• разрушение или *повреждение аппаратуры*.

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие *угрозы*:

• нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;

• разрушение или повреждение помещений;

• невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его *угроза*, забастовка и т.п.).

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.

Опасны, разумеется, *стихийные бедствия* и события, воспринимаемые как *стихийные бедствия*,- пожары, наводнения, землетрясения, ураганы. По статистике, на долю огня, воды и тому подобных "*злоумышленников*" (среди которых самый опасный - перебой электропитания) приходится 13% потерь, нанесенных информационным системам.

3.3. 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 питания 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. Автору курса довелось быть свидетелем ситуации, когда прорвало трубу с горячей водой, и системный блок компьютера (это была рабочая станция производства Sun Microsystems) оказался заполнен кипятком. Когда кипяток вылили, а компьютер просушили, он возобновил нормальную работу, но лучше таких опытов не ставить...

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 будут похитрее засоров канализации. Речь пойдет о программных *атаках* на доступность.

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 широковещательными 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. Временем начала "моды" на подобные *атаки* можно считать февраль 2000 года, когда жертвами оказались несколько крупнейших систем электронной коммерции (точнее - владельцы и пользователи систем). Отметим, что если

имеет место архитектурный просчет в виде разбалансированности между пропускной способностью сети и производительностью сервера, то защититься от распределенных *атак* на доступность крайне трудно.

Для выведения систем из штатного режима эксплуатации могут использоваться *уязвимые* места в виде программных и аппаратных ошибок. Например, известная ошибка в процессоре Pentium I дает возможность локальному пользователю путем выполнения определенной команды "подвесить" компьютер, так что помогает только аппаратный RESET.

Программа "Teardrop" удаленно "подвешивает" компьютеры, эксплуатируя ошибку в сборке фрагментированных IP-пакетов.

3.4. Вредоносное программное обеспечение

Одним из опаснейших способов проведения *атак* является внедрение в *атакуемые* системы *вредоносного программного обеспечения*.

Мы выделим следующие грани *вредоносного ПО*:

- вредоносная функция;
- способ распространения;
- внешнее представление.

Часть, осуществляющую разрушительную функцию, будем называть ***"бомбой"*** (хотя, возможно, более удачными терминами были бы "заряд" или "боеголовка"). Вообще говоря, спектр вредоносных функций неограничен, поскольку *"бомба"*, как и любая другая программа, может обладать сколь угодно сложной логикой, но обычно *"бомбы"* предназначаются для:

- внедрения другого *вредоносного ПО*;
- получения контроля над *атакуемой* системой;
- *агрессивного потребления ресурсов*;
- изменения или разрушения программ и/или данных.

По механизму распространения различают:

- ***вирусы*** - код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;
- ***"черви"*** - код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации *вируса* требуется запуск зараженной программы).

Вирусы обычно распространяются локально, в пределах узла сети; для передачи по сети им требуется внешняя помощь, такая как пересылка зараженного файла. *"Черви"*, напротив, ориентированы в первую очередь на путешествия по сети.

Иногда само распространение *вредоносного ПО* вызывает *агрессивное потребление ресурсов* и, следовательно, является вредоносной функцией. Например, *"черви"* "съедают" полосу пропускания сети и ресурсы почтовых систем. По этой причине для *атак* на доступность они не нуждаются во встраивании специальных *"бомб"*.

Вредоносный код, который выглядит как функционально полезная программа, называется *троянским*. Например, обычная программа, будучи пораженной *вирусом*, становится ***троянской***; порой *троянские программы* изготавливают вручную и подсовывают доверчивым пользователям в какой-либо привлекательной упаковке.

Отметим, что данные нами определения и приведенная классификация *вредоносного ПО* отличаются от общепринятых. Например, в ГОСТ Р 51275-99 "Защита информации.

Объект информатизации. Факторы, воздействующие на информацию. Общие положения" содержится следующее определение:

"Программный *вирус* - это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах".

На наш взгляд, подобное определение неудачно, поскольку в нем смешаны функциональные и транспортные аспекты.

Окно опасности для *вредоносного ПО* появляется с выпуском новой разновидности *"бомб", вирусов* и/или *"червей"* и перестает существовать с обновлением базы данных антивирусных программ и наложением других необходимых заплат.

По традиции из всего *вредоносного ПО* наибольшее внимание общественности приходится на долю *вирусов*. Однако до марта 1999 года с полным правом можно было утверждать, что "несмотря на экспоненциальный рост числа известных *вирусов*, аналогичного роста количества инцидентов, вызванных ими, не зарегистрировано. Соблюдение несложных правил "компьютерной гигиены" практически сводит риск заражения к нулю. Там, где работают, а не играют, число зараженных компьютеров составляет лишь доли процента".

В марте 1999 года, с появлением *вируса* "Melissa", ситуация кардинальным образом изменилась. "Melissa" - это макро*вирус* для файлов MS-Word, распространяющийся посредством электронной почты в присоединенных файлах. Когда такой (зараженный) присоединенный файл открывают, он рассылает свои копии по первым 50 адресам из адресной книги Microsoft Outlook. В результате почтовые серверы подвергаются *атаке* на доступность.

В данном случае нам хотелось бы отметить два момента.

1. Как уже говорилось, пассивные объекты отходят в прошлое; так называемое ***активное содержимое*** становится нормой. Файлы, которые по всем признакам должны были бы относиться к данным (например, документы в форматах MS-Word или Postscript, тексты почтовых сообщений), способны содержать интерпретируемые компоненты, которые могут запускаться неявным образом при открытии файла. Как и всякое в целом прогрессивное явление, такое "повышение активности данных" имеет свою оборотную сторону (в рассматриваемом случае - отставание в разработке механизмов безопасности и ошибки в их реализации). Обычные пользователи еще не скоро научатся применять интерпретируемые компоненты "в мирных целях" (или хотя бы узнают об их существовании), а перед *злоумышленниками* открылось по существу неограниченное поле деятельности. Как ни банально это звучит, но если для стрельбы по воробьям выкатывается пушка, то пострадает в основном стреляющий.

2. Интеграция разных сервисов, наличие среди них сетевых, всеобщая связность многократно увеличивают потенциал для *атак* на доступность, облегчают распространение *вредоносного ПО* (*вирус* "Melissa" - классический тому пример). Образно говоря, многие информационные системы, если не принять защитных мер, оказываются "в одной лодке" (точнее - в корабле без переборок), так что достаточно одной пробоины, чтобы "лодка" тут же пошла ко дну.

Как это часто бывает, вслед за "Melissa" появилась на свет целая серия *вирусов*, *"червей"* и их комбинаций: "Explorer.zip" (июнь 1999), "Bubble Boy" (ноябрь 1999), "ILOVEYOU" (май 2000) и т.д. Не то что бы от них был особенно большой ущерб, но общественный резонанс они вызвали немалый.

Активное содержимое, помимо интерпретируемых компонентов документов и других файлов данных, имеет еще одно популярное обличье - так называемые ***мобильные агенты***. Это программы, которые загружаются на другие компьютеры и там выполняются. Наиболее известные примеры *мобильных агентов* - Java-апплеты, загружаемые на пользовательский компьютер и интерпретируемые Internet-навигаторами. Оказалось, что разработать для них модель безопасности, оставляющую достаточно возможностей для полезных действий, не так-то просто; еще сложнее реализовать такую модель без ошибок. В августе 1999 года стали известны недочеты в реализации технологий ActiveX и Java в рамках Microsoft Internet Explorer, которые давали возможность размещать на Web-серверах вредоносные апплеты, позволяющие получать полный контроль над системой-визитером.

Для внедрения *"бомб"* часто используются ошибки типа *"переполнение буфера"*, когда программа, работая с областью памяти, выходит за границы допустимого и записывает в нужные *злоумышленнику* места определенные данные. Так действовал еще в 1988 году знаменитый *"червь* Морриса"; в июне 1999 года хакеры нашли способ использовать аналогичный метод по отношению к Microsoft Internet Information Server (IIS), чтобы получить контроль над Web-сервером. *Окно опасности* охватило сразу около полутора миллионов серверных систем...

Не забыты современными *злоумышленниками* и испытанные *троянские программы*. Например, *"троянцы"* Back Orifice и Netbus позволяют получить контроль над пользовательскими системами с различными вариантами MS-Windows.

Таким образом, действие *вредоносного ПО* может быть направлено не только против доступности, но и против других основных аспектов информационной безопасности.

3.5. Основные угрозы целостности

На втором месте по размерам ущерба (после *непреднамеренных ошибок* и упущений) стоят *кражи* и *подлоги*. 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.

Ранее мы проводили различие между *статической* и *динамической целостностью*. 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 Oracle (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 привела 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 рассмотренного выше *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.

Основные угрозы конфиденциальности

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 многоразовые 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 пределах 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 нетехнической *угрозой* конфиденциальности являются *методы морально-психологического воздействия*, такие как ***маскарад*** - выполнение действий под видом лица, обладающего полномочиями для доступа к данным (см., например, статью Айрэ Винклера "Задание: шпионаж" в Jet Info, 1996, 19).

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.

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

Тема 4. Стандарты и спецификации в области информационной безопасности

4.1. Оценочные стандарты и технические спецификации. "Оранжевая книга" как оценочный стандарт.

Основные понятия

Мы приступаем к обзору стандартов и спецификаций двух разных видов:

- оценочных стандартов, направленных на классификацию информационных систем и средств защиты по требованиям безопасности;
- технических спецификаций, регламентирующих различные аспекты *реализации* средств защиты.

Важно отметить, что между этими видами нормативных документов нет глухой стены. Оценочные стандарты выделяют важнейшие, с точки зрения ИБ, аспекты ИС, играя роль архитектурных спецификаций. Другие технические спецификации определяют, как строить ИС предписанной архитектуры.

Исторически первым оценочным стандартом, получившим широкое распространение и оказавшим огромное влияние на базу стандартизации ИБ во многих странах, стал стандарт Министерства обороны США "Критерии оценки *доверенных* компьютерных *систем*".

Данный труд, называемый чаще всего по цвету обложки "Оранжевой книгой", был впервые опубликован в августе 1983 года. Уже одно его название требует комментария. Речь идет не о безопасных, а о *доверенных системах*, то есть системах, которым можно оказать определенную *степень доверия*.

"Оранжевая книга" поясняет понятие *безопасной системы*, которая "управляет, с помощью соответствующих средств, доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, записывать, создавать и удалять информацию".

Очевидно, однако, что абсолютно *безопасных систем* не существует, это абстракция. Есть смысл оценивать лишь *степень доверия*, которое можно оказать той или иной системе.

В "Оранжевой книге" ***доверенная система*** определяется как "система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа".

Обратим внимание, что в рассматриваемых Критериях и безопасность, и доверие оцениваются исключительно с точки зрения управления доступом к данным, что является

одним из средств обеспечения конфиденциальности и целостности (статической). Вопросы доступности "Оранжевая книга" не затрагивает.

Степень доверия оценивается по двум основным критериям.

1. ***Политика безопасности*** - набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь может оперировать конкретными наборами данных. Чем выше *степень доверия* системе, тем строже и многообразнее должна быть *политика безопасности*. В зависимости от сформулированной политики можно выбирать конкретные механизмы обеспечения безопасности. *Политика безопасности* - это активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.

2. ***Уровень гарантированности*** - мера доверия, которая может быть оказана архитектуре и *реализации* ИС. Доверие безопасности может проистекать как из анализа результатов *тестирования*, так и из проверки (формальной или нет) общего замысла и *реализации* системы в целом и отдельных ее компонентов. *Уровень гарантированности* показывает, насколько корректны механизмы, отвечающие за *реализацию политики безопасности*. Это пассивный аспект защиты.

Важным средством обеспечения безопасности является механизм *подотчетности* (протоколирования). *Доверенная система* должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться аудитом, то есть *анализом регистрационной информации*.

Концепция *доверенной вычислительной базы* является центральной при оценке *степени доверия* безопасности. ***Доверенная вычислительная база*** - это совокупность защитных механизмов ИС (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь *политики безопасности*. Качество вычислительной базы определяется исключительно ее *реализацией* и корректностью исходных данных, которые вводит системный администратор.

Вообще говоря, компоненты вне вычислительной базы могут не быть доверенными, однако это не должно влиять на безопасность системы в целом. В результате, для оценки доверия безопасности ИС достаточно рассмотреть только ее вычислительную базу, которая, как можно надеяться, достаточно компактна.

Основное назначение *доверенной вычислительной базы* - выполнять функции *монитора обращений*, то есть контролировать допустимость выполнения субъектами (активными сущностями ИС, действующими от имени пользователей) определенных операций над объектами (пассивными сущностями). Монитор проверяет каждое обращение пользователя к программам или данным на предмет согласованности с набором действий, допустимых для пользователя.

Монитор обращений должен обладать тремя качествами:

1. *Изолированность*. Необходимо предупредить возможность отслеживания работы монитора.

2. *Полнота*. Монитор должен вызываться при каждом обращении, не должно быть способов обойти его.

3. *Верифицируемость*. Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в *полноте тестирования*.

Реализация монитора обращений называется *ядром безопасности*. *Ядро безопасности* - это основа, на которой строятся все защитные механизмы. Помимо перечисленных выше свойств *монитора обращений*, ядро должно гарантировать собственную неизменность.

Границу *доверенной вычислительной базы* называют ***периметром безопасности***. Как уже указывалось, компоненты, лежащие вне *периметра безопасности*, вообще говоря, могут не быть доверенными. С развитием распределенных систем понятию *"периметр безопасности"* все чаще придают другой смысл, имея в виду границу владений определенной организации. То, что находится внутри владений, считается доверенным, а то, что вне, - нет.

Механизмы безопасности

Согласно "Оранжевой книге", *политика безопасности* должна обязательно включать в себя следующие элементы:

- *произвольное управление доступом*;
- *безопасность повторного использования объектов*;
- *метки безопасности*;
- *принудительное управление доступом*.

Произвольное управление доступом (называемое иногда дискреционным) - это метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению предоставлять другим субъектам или отбирать у них права доступа к объекту.

Безопасность повторного использования объектов - важное дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения конфиденциальной информации из "мусора". *Безопасность повторного использования* должна гарантироваться для областей оперативной памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т.п.), для дисковых блоков и магнитных носителей в целом.

Как мы указывали ранее, современный объектно-ориентированный подход резко сужает область действия данного элемента безопасности, затрудняет его *реализацию*. То же верно и для интеллектуальных устройств, способных буферизовать большие объемы данных.

Для *реализации принудительного управления доступом* с субъектами и объектами ассоциируются *метки безопасности*. Метка субъекта описывает его благонадежность, метка объекта - степень конфиденциальности содержащейся в нем информации.

Согласно "Оранжевой книге", *метки безопасности* состоят из двух частей - уровня секретности и списка категорий. Уровни секретности образуют упорядоченное множество, категории - неупорядоченное. Назначение последних - описать предметную область, к которой относятся данные.

Принудительное (или мандатное) управление доступом основано на сопоставлении *меток безопасности* субъекта и объекта.

Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в *метке безопасности* объекта, присутствуют в метке субъекта. В таком случае говорят, что метка субъекта доминирует

над меткой объекта. Смысл сформулированного правила понятен - читать можно только то, что положено.

Субъект может записывать информацию в объект, если *метка безопасности* объекта доминирует над меткой субъекта. В частности, "конфиденциальный" субъект может записывать данные в секретные файлы, но не может - в несекретные (разумеется, должны также выполняться ограничения на набор категорий).

Описанный способ управления доступом называется *принудительным*, поскольку он не зависит от воли субъектов (даже системных администраторов). После того, как зафиксированы *метки безопасности* субъектов и объектов, оказываются зафиксированными и права доступа.

Если понимать *политику безопасности* узко, то есть как правила разграничения доступа, то механизм *подотчетности* является дополнением подобной политики. Цель *подотчетности* - в каждый момент времени знать, кто работает в системе и что делает. Средства *подотчетности* делятся на три категории:

- *идентификация* и *аутентификация*;
- *предоставление доверенного пути*;
- *анализ регистрационной информации*.

Обычный способ *идентификации* - ввод имени пользователя при входе в систему. Стандартное средство проверки подлинности (*аутентификации*) пользователя - пароль.

Доверенный путь связывает пользователя непосредственно с *доверенной вычислительной базой*, минуя другие, потенциально опасные компоненты ИС. Цель *предоставления доверенного пути* - дать пользователю возможность убедиться в подлинности обслуживающей его системы.

Анализ регистрационной информации (аудит) имеет дело с действиями (событиями), так или иначе затрагивающими безопасность системы.

Если фиксировать все события, объем регистрационной информации, скорее всего, будет расти слишком быстро, а ее эффективный анализ станет невозможным. "Оранжевая книга" предусматривает наличие средств выборочного протоколирования, как в отношении пользователей (внимательно следить только за подозрительными), так и в отношении событий.

Переходя к пассивным аспектам защиты, укажем, что в "Оранжевой книге" рассматривается два вида гарантированности - операционная и технологическая. *Операционная гарантированность* относится к архитектурным и реализационным аспектам системы, в то время как *технологическая* - к методам построения и *сопровождения*.

Операционная гарантированность включает в себя проверку следующих элементов:

- архитектура системы;
- целостность системы;
- проверка *тайных каналов передачи информации*;
- доверенное администрирование;
- доверенное *восстановление после сбоев*.

Операционная гарантированность - это способ убедиться в том, что архитектура системы и ее *реализация* действительно реализуют избранную *политику безопасности*.

Технологическая гарантированность охватывает весь *жизненный цикл ИС*, то есть периоды *проектирования*, *реализации*, *тестирования*, *продажи* и *сопровождения*. Все

перечисленные действия должны выполняться в соответствии с жесткими стандартами, чтобы исключить утечку информации и нелегальные "закладки".

Тема 5. Классы безопасности

"Критерии ..." Министерства обороны США открыли путь к ранжированию информационных систем по *степени доверия* безопасности.

В "Оранжевой книге" определяется четыре уровня доверия - D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. По мере перехода от уровня C к A к системам предъявляются все более жесткие требования. Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3) с постепенным возрастанием *степени доверия*.

Всего имеется шесть *классов безопасности* - C1, C2, B1, B2, B3, A1. Чтобы в результате процедуры сертификации систему можно было отнести к некоторому классу, ее *политика безопасности* и *уровень гарантированности* должны удовлетворять заданным требованиям, из которых мы упомянем лишь важнейшие.

Класс C1:

- *доверенная вычислительная база* должна управлять доступом именованных пользователей к именованным объектам;
- пользователи должны идентифицировать себя, прежде чем выполнять какие-либо иные действия, контролируемые *доверенной вычислительной базой*. Для *аутентификации* должен использоваться какой-либо защитный механизм, например пароли. Аутентификационная информация должна быть защищена от несанкционированного доступа;
- *доверенная вычислительная база* должна поддерживать область для собственного выполнения, защищенную от внешних воздействий (в частности, от изменения команд и/или данных) и от попыток слежения за ходом работы;
- должны быть в наличии аппаратные и/или программные средства, позволяющие периодически проверять корректность функционирования аппаратных и микропрограммных компонентов *доверенной вычислительной базы*;
- защитные механизмы должны быть протестированы на предмет соответствия их поведения системной документации. *Тестирование* должно подтвердить, что у неавторизованного пользователя нет очевидных способов обойти или разрушить средства защиты *доверенной вычислительной базы*;
- должны быть описаны подход к безопасности, используемый производителем, и применение этого подхода при *реализации доверенной вычислительной базы*.

Класс C2 (в дополнение к C1):

- права доступа должны гранулироваться с точностью до пользователя. Все объекты должны подвергаться контролю доступа;
- при выделении хранимого объекта из пула ресурсов *доверенной вычислительной базы* необходимо ликвидировать все следы его использования;
- каждый пользователь системы должен уникальным образом идентифицироваться. Каждое регистрируемое действие должно ассоциироваться с конкретным пользователем;
- *доверенная вычислительная база* должна создавать, поддерживать и защищать журнал регистрационной информации, относящейся к доступу к объектам, контролируемым базой;

• *тестирование* должно подтвердить отсутствие очевидных недостатков в механизмах изоляции ресурсов и защиты регистрационной информации.

Класс B1 (в дополнение к C2):

• *доверенная вычислительная база* должна управлять *метками безопасности*, ассоциируемыми с каждым субъектом и хранимым объектом;

• *доверенная вычислительная база* должна обеспечить *реализацию принудительного управления доступом* всех субъектов ко всем хранимым объектам;

• *доверенная вычислительная база* должна обеспечивать взаимную *изоляцию процессов* путем *разделения* их *адресных пространств*;

• группа специалистов, полностью понимающих *реализацию доверенной вычислительной базы*, должна подвергнуть описание архитектуры, исходные и объектные коды тщательному анализу и *тестированию*;

• должна существовать неформальная или формальная модель *политики безопасности*, поддерживаемой *доверенной вычислительной базой*.

Класс B2 (в дополнение к B1):

• снабжаться метками должны все ресурсы системы (например, ПЗУ), прямо или косвенно доступные субъектам;

• к *доверенной вычислительной базе* должен поддерживаться доверенный коммуникационный путь для пользователя, выполняющего операции начальной *идентификации* и *аутентификации*;

• должна быть предусмотрена возможность регистрации событий, связанных с организацией тайных каналов обмена с памятью;

• *доверенная вычислительная база* должна быть внутренне структурирована на хорошо определенные, относительно независимые модули;

• системный архитектор должен тщательно проанализировать возможности организации тайных каналов обмена с памятью и оценить максимальную пропускную способность каждого выявленного канала;

• должна быть продемонстрирована относительная устойчивость *доверенной вычислительной базы* к попыткам проникновения;

• модель *политики безопасности* должна быть формальной. Для *доверенной вычислительной базы* должны существовать описательные спецификации верхнего уровня, точно и полно определяющие ее интерфейс;

• в процессе разработки и *сопровождения доверенной вычислительной базы* должна использоваться система конфигурационного управления, обеспечивающая контроль изменений в описательных спецификациях верхнего уровня, иных архитектурных данных, реализационной документации, исходных текстах, работающей версии объектного кода, тестовых данных и документации;

• тесты должны подтверждать действенность мер по уменьшению пропускной способности *тайных каналов передачи информации*.

Класс B3 (в дополнение к B2):

• для *произвольного управления доступом* должны обязательно использоваться *списки управления доступом* с указанием разрешенных режимов;

• должна быть предусмотрена возможность регистрации появления или накопления событий, несущих угрозу *политике безопасности* системы. *Администратор безопасности* должен немедленно извещаться о попытках нарушения *политики*

безопасности, а система, в случае продолжения попыток, должна пресекать их наименее болезненным способом;

- *доверенная вычислительная база* должна быть спроектирована и структурирована таким образом, чтобы использовать полный и концептуально простой защитный механизм с точно определенной семантикой;
- процедура анализа должна быть выполнена для временных тайных каналов;
- должна быть специфицирована роль *администратора безопасности*. Получить права *администратора безопасности* можно только после выполнения явных, протоколируемых действий;
- должны существовать процедуры и/или механизмы, позволяющие произвести *восстановление после сбоя* или иного нарушения работы без ослабления защиты;
- должна быть продемонстрирована устойчивость *доверенной вычислительной базы* к попыткам проникновения.

Класс А1 (в дополнение к В3):

- *тестирование* должно продемонстрировать, что *реализация доверенной вычислительной базы* соответствует *формальным спецификациям верхнего уровня*;
- помимо описательных, должны быть представлены *формальные спецификации верхнего уровня*. Необходимо использовать современные методы формальной спецификации и *верификации* систем;
- механизм конфигурационного управления должен распространяться на весь *жизненный цикл* и все компоненты системы, имеющие отношение к обеспечению безопасности;
- должно быть описано соответствие между *формальными спецификациями верхнего уровня* и исходными текстами.

Такова классификация, введенная в "Оранжевой книге". Коротко ее можно сформулировать так:

- уровень С - *произвольное управление доступом*;
- уровень В - *принудительное управление доступом*;
- уровень А - верифицируемая безопасность.

Конечно, в адрес "Критериев ..." можно высказать целый ряд серьезных замечаний (таких, например, как полное игнорирование проблем, возникающих в распределенных системах). Тем не менее, следует подчеркнуть, что публикация "Оранжевой книги" без всякого преувеличения стала эпохальным событием в области информационной безопасности. Появился общепризнанный понятийный базис, без которого даже обсуждение проблем ИБ было бы затруднительным.

Отметим, что огромный идейный потенциал "Оранжевой книги" пока во многом остается невостребованным. Прежде всего это касается концепции *технологической гарантированности*, охватывающей весь *жизненный цикл системы* - от выработки спецификаций до фазы эксплуатации. При современной технологии программирования результирующая система не содержит информации, присутствующей в исходных спецификациях, теряется информация о семантике программ. Важность данного обстоятельства мы планируем продемонстрировать далее, в лекции об управлении доступом.

5.1 Информационная безопасность распределенных систем. Рекомендации X.800

Сетевые сервисы безопасности

Следуя скорее исторической, чем предметной логике, мы переходим к рассмотрению технической спецификации X.800, появившейся немногим позднее "Оранжевой книги", но весьма полно и глубоко трактующей вопросы информационной безопасности распределенных систем.

Рекомендации X.800 - документ довольно обширный. Мы остановимся на специфических сетевых функциях (сервисах) безопасности, а также на необходимых для их *реализации* защитных механизмах.

Выделяют следующие сервисы безопасности и исполняемые ими роли:

Аутентификация. Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. **Аутентификация партнеров по общению** используется при установлении соединения и, быть может, периодически во время сеанса. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. *Аутентификация* бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной).

Управление доступом. Обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.

Конфиденциальность данных. Обеспечивает защиту от несанкционированного получения информации. Отдельно упомянем **конфиденциальность трафика** (это защита информации, которую можно получить, анализируя сетевые потоки данных).

Целостность данных подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры - с установлением соединения или без него, защищаются ли все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.

Неотказуемость (невозможность отказаться от совершенных действий) обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки. Побочным продуктом неотказуемости является **аутентификация источника данных**.

В следующей таблице указаны уровни **эталонной семиуровневой модели** OSI, на которых могут быть реализованы функции безопасности. Отметим, что прикладные процессы, в принципе, могут взять на себя поддержку всех защитных сервисов.

Таблица 5.1. Распределение функций безопасности по уровням эталонной семиуровневой модели OSI

Функции безопасности	**Уровень**						
Аутентификация							
Управление доступом							
Конфиденциальность соединения							
Конфиденциальность вне соединения							
Избирательная конфиденциальность							
Конфиденциальность трафика							
Целостность с восстановлением							

Целостность без восстановления							
Избирательная целостность							
Целостность вне соединения							
Неотказуемость							

"+" данный уровень может предоставить функцию безопасности;

"-" данный уровень не подходит для предоставления функции безопасности.

Сетевые механизмы безопасности

Для *реализации* сервисов (функций) безопасности могут использоваться следующие механизмы и их комбинации:

- **шифрование**;
- **электронная цифровая подпись**;
- механизмы управления доступом. Могут располагаться на любой из участвующих в общении сторон или в промежуточной точке;
- механизмы контроля целостности данных. В рекомендациях X.800 различаются два аспекта целостности: целостность отдельного сообщения или поля информации и целостность потока сообщений или полей информации. Для проверки целостности потока сообщений (то есть для защиты от кражи, переупорядочивания, дублирования и вставки сообщений) используются порядковые номера, временные штампы, криптографическое связывание или иные аналогичные приемы;
- механизмы *аутентификации*. Согласно рекомендациям X.800, *аутентификация* может достигаться за счет использования паролей, личных карточек или иных устройств аналогичного назначения, криптографических методов, устройств измерения и анализа биометрических характеристик;
- механизмы **дополнения трафика**;
- механизмы **управления маршрутизацией**. Маршруты могут выбираться статически или динамически. Оконечная система, зафиксировав неоднократные атаки на определенном маршруте, может отказаться от его использования. На выбор маршрута способна повлиять *метка безопасности*, ассоциированная с передаваемыми данными;
- механизмы **нотаризации**. Служат для заверения таких коммуникационных характеристик, как целостность, время, личности отправителя и получателей. Заверение обеспечивается надежной третьей стороной, обладающей достаточной информацией. Обычно нотаризация опирается на механизм электронной подписи.

В следующей таблице сведены сервисы (функции) и механизмы безопасности. Таблица показывает, какие механизмы (по отдельности или в комбинации с другими) могут использоваться для *реализации* той или иной функции.

Таблица 5.2. Взаимосвязь функций и механизмов безопасности

Функции	**Механизмы**						
	Ш ифрование	**Э лектронная подпись**	**У правление доступом**	**Ц елостность**	**Аутентификация**	**Дополнение трафика**	**Управление маршрутизация**	**Н отаризация**

		пись					ией	
Аутентификация партнеров	+	+	-	-	+	-	-	-
Аутентификация источника	+	+	-	-	-	-	-	-
Управление доступом	-	-	+	-	-	-	-	-
Конфиденциальность	+	-	+	-	-	-	+	-
Избирательная конфиденциальность	+	-	-	-	-	-	-	-
Конфиденциальность трафика	+	-	-	-	-	+	+	-
Целостность соединения	+	-	-	+	-	-	-	-
Целостность вне соединения	+	+	-	+	-	-	-	-
Неотказуемость	-	+	-	+	-	-	-	+

"+" механизм пригоден для *реализации* данной функции безопасности;

"-" механизм не предназначен для *реализации* данной функции безопасности.

Администрирование средств безопасности

Администрирование средств безопасности включает в себя распространение информации, необходимой для работы сервисов и механизмов безопасности, а также сбор и анализ информации об их функционировании. Примерами могут служить распространение **криптографических ключей**, установка значений параметров защиты, ведение регистрационного журнала и т.п.

Концептуальной основой администрирования является информационная база управления безопасностью. Эта база может не существовать как единое (распределенное) хранилище, но каждая из оконечных систем должна располагать информацией, необходимой для *реализации* избранной *политики безопасности*.

Согласно рекомендациям X.800, усилия администратора средств безопасности должны распределяться по трем направлениям:

- администрирование информационной системы в целом;
- администрирование сервисов безопасности;
- администрирование механизмов безопасности.

Среди действий, относящихся к ИС в целом, отметим обеспечение актуальности *политики безопасности*, взаимодействие с другими административными службами, **реагирование** на происходящие события, **аудит** и **безопасное восстановление**.

Администрирование сервисов безопасности включает в себя определение защищаемых объектов, выработку правил подбора механизмов безопасности (при наличии альтернатив), комбинирование механизмов для *реализации* сервисов, взаимодействие с другими администраторами для обеспечения согласованной работы.

Обязанности администратора механизмов безопасности определяются перечнем задействованных механизмов. Типичный список таков:

- **управление ключами (генерация и распределение)**;
- **управление шифрованием** (установка и синхронизация криптографических параметров).

К управлению шифрованием можно отнести и администрирование механизмов электронной подписи. Управление целостностью, если оно обеспечивается криптографическими средствами, также тяготеет к данному направлению;

- администрирование управления доступом (распределение информации, необходимой для управления - паролей, списков доступа и т.п.);
- управление *аутентификацией* (распределение информации, необходимой для *аутентификации* - паролей, ключей и т.п.);
- управление дополнением трафика (выработка и поддержание правил, задающих характеристики дополняющих сообщений - частоту отправки, размер и т.п.);
- управление маршрутизацией (выделение доверенных путей);
- управление нотаризацией (распространение информации о нотариальных службах, администрирование этих служб).

Мы видим, что администрирование средств безопасности в распределенной ИС имеет много особенностей по сравнению с централизованными системами.

5.3. Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий"

Основные понятия

Мы возвращаемся к теме оценочных стандартов, приступая к рассмотрению самого полного и современного среди них - "Критериев оценки безопасности информационных технологий" (издан 1 декабря 1999 года). Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран, он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба.

По историческим причинам данный стандарт часто называют "Общими критериями" (или даже ОК). Мы также будем использовать это сокращение.

"Общие критерии" на самом деле являются метастандартом, определяющим инструменты оценки безопасности ИС и порядок их использования. В отличие от "Оранжевой книги", ОК не содержат предопределенных *"классов безопасности"*. Такие классы можно строить, исходя из **требований безопасности**, существующих для конкретной организации и/или конкретной информационной системы.

С программистской точки зрения ОК можно считать набором библиотек, помогающих писать содержательные "программы" - **задания по безопасности**, типовые **профили защиты** и т.п. Программисты знают, насколько хорошая библиотека упрощает разработку программ, повышает их качество. Без библиотек, "с нуля", программы не пишут уже очень давно; оценка безопасности тоже вышла на сопоставимый уровень сложности, и "Общие критерии" предоставили соответствующий инструментарий.

Важно отметить, что **требования могут быть параметризованы**, как и полагается библиотечным функциям.

Как и "Оранжевая книга", ОК содержат два основных вида **требований** безопасности:

• **функциональные**, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности и реализующим их механизмам;

• **требования доверия**, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации.

Требования безопасности предъявляются, а их выполнение проверяется для определенного **объекта оценки** - аппаратно-программного продукта или информационной системы.

Очень важно, что безопасность в ОК рассматривается не статично, а в привязке к жизненному циклу объекта оценки. Выделяются следующие этапы:

• определение назначения, условий применения, целей и требований безопасности;

• *проектирование* и разработка;

• испытания, оценка и сертификация;

• внедрение и эксплуатация.

В ОК объект оценки рассматривается в контексте **среды безопасности**, которая характеризуется определенными условиями и угрозами.

В свою очередь, угрозы характеризуются следующими параметрами:

• источник угрозы;

• метод воздействия;

• уязвимые места, которые могут быть использованы;

• ресурсы (активы), которые могут пострадать.

Уязвимые места могут возникать из-за недостатка в:

• требованиях безопасности;

• *проектировании*;

• эксплуатации.

Слабые места по возможности следует устранить, минимизировать или хотя бы постараться ограничить возможный ущерб от их преднамеренного использования или случайной активизации.

С точки зрения технологии программирования в ОК использован устаревший библиотечный (не объектный) подход. Чтобы, тем не менее, структурировать пространство требований, в "Общих критериях" введена иерархия **класс-семейство-компонент-элемент**.

Классы определяют наиболее общую, "предметную" группировку требований (например, функциональные требования *подотчетности*).

Семейства в пределах класса различаются по строгости и другим нюансам требований.

Компонент - минимальный набор требований, фигурирующий как целое.

Элемент - неделимое требование.

Как и между библиотечными функциями, между компонентами ОК могут существовать зависимости. Они возникают, когда компонент сам по себе недостаточен для достижения **цели безопасности**. Вообще говоря, не все комбинации компонентов имеют смысл, и понятие зависимости в какой-то степени компенсирует недостаточную выразительность библиотечной организации, хотя и не заменяет объединение функций в содержательные объектные интерфейсы.

Как указывалось выше, с помощью библиотек могут формироваться два вида нормативных документов: профиль защиты и задание по безопасности.

Профиль защиты (ПЗ) представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса (например, операционные системы на компьютерах в правительственных организациях).

Задание по безопасности содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности.

Выше мы отмечали, что в ОК нет готовых классов защиты. Сформировать классификацию в терминах "Общих критериев" - значит определить несколько иерархически упорядоченных (содержащих усиливающиеся требования) профилей защиты, в максимально возможной степени использующих стандартные функциональные требования и требования **доверия безопасности**.

Выделение некоторого подмножества из всего множества профилей защиты во многом носит субъективный характер. По целому ряду соображений (одним из которых является желание придерживаться объектно-ориентированного подхода) целесообразно, на наш взгляд, сформировать сначала отправную точку классификации, выделив базовый (минимальный) ПЗ, а дополнительные требования компоновать в функциональные пакеты.

Функциональный пакет - это неоднократно используемая совокупность компонентов, объединенных для достижения определенных целей безопасности. "Общие критерии" не регламентируют структуру пакетов, процедуры *верификации*, регистрации и т.п., отводя им роль технологического средства формирования ПЗ.

Базовый профиль защиты должен включать требования к основным (обязательным в любом случае) возможностям. Производные профили получаются из базового путем добавления необходимых пакетов расширения, то есть подобно тому, как создаются производные классы в объектно-ориентированных языках программирования.

Функциональные требования

Функциональные требования сгруппированы на основе выполняемой ими роли или обслуживаемой цели безопасности. Всего в "Общих критериях" представлено 11 функциональных классов, 66 семейств, 135 компонентов. Это, конечно, значительно больше, чем число аналогичных сущностей в "Оранжевой книге".

Перечислим классы функциональных требований ОК:

- *идентификация* и *аутентификация*;
- **защита данных пользователя**;
- **защита функций безопасности** (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов);
- **управление безопасностью** (требования этого класса относятся к управлению атрибутами и параметрами безопасности);
- **аудит безопасности** (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности);
- **доступ к объекту оценки**;
- **приватность** (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных);
- **использование ресурсов** (требования к доступности информации);
- **криптографическая поддержка** (управление ключами);

• **связь** (*аутентификация* сторон, участвующих в обмене данными);

• **доверенный маршрут/канал** (для связи с сервисами безопасности).

Опишем подробнее два класса, демонстрирующие особенности современного подхода к ИБ.

Класс "Приватность" содержит 4 семейства функциональных требований.

Анонимность. Позволяет выполнять действия без раскрытия идентификатора пользователя другим пользователям, субъектам и/или объектам. Анонимность может быть полной или выборочной. В последнем случае она может относиться не ко всем операциям и/или не ко всем пользователям (например, у уполномоченного пользователя может оставаться возможность выяснения идентификаторов пользователей).

Псевдонимность. Напоминает анонимность, но при применении псевдонима поддерживается ссылка на идентификатор пользователя для обеспечения *подотчетности* или для других целей.

Невозможность ассоциации. Семейство обеспечивает возможность неоднократного использования информационных сервисов, но не позволяет ассоциировать случаи использования между собой и приписать их одному лицу. Невозможность ассоциации защищает от построения профилей поведения пользователей (и, следовательно, от получения информации на основе подобных профилей).

Скрытность. Требования данного семейства направлены на то, чтобы можно было использовать информационный сервис с сокрытием факта использования. Для *реализации* скрытности может применяться, например, широковещательное распространение информации, без указания конкретного адресата. Годятся для *реализации* скрытности и методы стеганографии, когда скрывается не только содержание сообщения (как в криптографии), но и сам факт его отправки.

Еще один показательный (с нашей точки зрения) класс функциональных требований - "Использование ресурсов", содержащий требования доступности. Он включает три семейства.

Отказоустойчивость. Требования этого семейства направлены на сохранение доступности информационных сервисов даже в случае сбоя или отказа. В ОК различаются активная и пассивная отказоустойчивость. Активный механизм содержит специальные функции, которые активизируются в случае сбоя. Пассивная отказоустойчивость подразумевает наличие избыточности с возможностью нейтрализации ошибок.

Обслуживание по приоритетам. Выполнение этих требований позволяет управлять использованием ресурсов так, что низкоприоритетные операции не могут помешать высокоприоритетным.

Распределение ресурсов. Требования направлены на защиту (путем применения механизма квот) от несанкционированной монополизации ресурсов.

Мы видим, что "Общие критерии" - очень продуманный и полный документ с точки зрения функциональных требований. В то же время, хотелось бы обратить внимание и на некоторые недостатки.

Первый мы уже отмечали - это отсутствие объектного подхода. Функциональные требования не сгруппированы в осмысленные наборы (объектные интерфейсы), к которым могло бы применяться наследование. Подобное положение, как известно из технологии программирования, чревато появлением слишком большого числа комбинаций функциональных компонентов, несопоставимых между собой.

В современном программировании ключевым является вопрос накопления и многократного использования знаний. Стандарты - одна из форм накопления знаний. Следование в ОК "библиотечному", а не объектному подходу сужает круг фиксируемых знаний, усложняет их корректное использование.

К сожалению, в "Общих критериях" отсутствуют архитектурные требования, что является естественным следствием избранного старомодного программистского подхода "снизу вверх". На наш взгляд, это серьезное упущение. Технологичность средств безопасности, следование общепризнанным рекомендациям по протоколам и программным интерфейсам, а также апробированным архитектурным решениям, таким как менеджер/агент, - необходимые качества изделий информационных технологий, предназначенных для поддержки критически важных функций, к числу которых, безусловно, относятся функции безопасности. Без рассмотрения интерфейсных аспектов системы оказываются нерасширяемыми и изолированными. Очевидно, с практической точки зрения это недопустимо. В то же время, обеспечение безопасности интерфейсов - важная задача, которую желательно решать единообразно.

Требования доверия безопасности

Установление доверия безопасности, согласно "Общим критериям", основывается на активном исследовании объекта оценки.

Форма представления требований доверия, в принципе, та же, что и для функциональных требований. Специфика состоит в том, что каждый элемент требований доверия принадлежит одному из трех типов:

- действия **разработчиков**;
- представление и содержание **свидетельств**;
- действия **оценщиков**.

Всего в ОК 10 классов, 44 семейства, 93 компонента требований доверия безопасности. Перечислим классы:

- разработка (требования для поэтапной детализации функций безопасности от краткой спецификации до *реализации*);
- поддержка жизненного цикла (требования к модели жизненного цикла, включая порядок устранения недостатков и защиту среды разработки);
- *тестирование*;
- **оценка уязвимостей** (включая оценку стойкости функций безопасности);
- **поставка и эксплуатация**;
- управление конфигурацией;
- руководства (требования к эксплуатационной документации);
- **поддержка доверия** (для поддержки этапов жизненного цикла после сертификации);
- оценка профиля защиты;
- оценка задания по безопасности.

Применительно к требованиям доверия в "Общих критериях" сделана весьма полезная вещь, не реализованная, к сожалению, для функциональных требований. А именно, введены так называемые оценочные уровни доверия (их семь), содержащие осмысленные комбинации компонентов.

Оценочный уровень доверия 1 (начальный) предусматривает анализ **функциональной спецификации**, спецификации интерфейсов, эксплуатационной

документации, а также независимое *тестирование*. Уровень применим, когда угрозы не рассматриваются как серьезные.

Оценочный уровень доверия 2, в дополнение к первому уровню, предусматривает наличие **проекта верхнего уровня** объекта оценки, выборочное независимое *тестирование*, анализ стойкости функций безопасности, поиск разработчиком явных уязвимых мест.

На третьем уровне ведется контроль среды разработки и управление конфигурацией объекта оценки.

На уровне 4 добавляются полная спецификация интерфейсов, **проекты нижнего уровня**, анализ подмножества *реализации*, применение неформальной **модели** *политики безопасности*, независимый анализ уязвимых мест, автоматизация управления конфигурацией. Вероятно, это самый высокий уровень, которого можно достичь при существующей технологии программирования и приемлемых затратах.

Уровень 5, в дополнение к предыдущим, предусматривает применение формальной модели *политики безопасности*, полуформальных функциональной спецификации и проекта верхнего уровня с **демонстрацией соответствия** между ними. Необходимо проведение анализа скрытых каналов разработчиками и оценщиками.

На уровне 6 *реализация* должна быть представлена в структурированном виде. Анализ соответствия распространяется на проект нижнего уровня.

Оценочный уровень 7 (самый высокий) предусматривает формальную *верификацию* проекта объекта оценки. Он применим к ситуациям чрезвычайно высокого риска.

На этом мы заканчиваем краткий обзор "Общих критериев".

Гармонизированные критерии Европейских стран

Наше изложение "Гармонизированных критериев" основывается на версии 1.2, опубликованной в июне 1991 года от имени соответствующих органов четырех стран - Франции, Германии, Нидерландов и Великобритании.

Принципиально важной чертой Европейских Критериев является отсутствие требований к условиям, в которых должна работать информационная система. Так называемый **спонсор**, то есть организация, запрашивающая сертификационные услуги, формулирует цель оценки, то есть описывает условия, в которых должна работать система, возможные угрозы ее безопасности и предоставляемые ею защитные функции. Задача органа сертификации - оценить, насколько полно достигаются поставленные цели, то есть насколько корректны и эффективны архитектура и *реализация* **механизмов безопасности** в описанных спонсором условиях. Таким образом, в терминологии "Оранжевой книги", Европейские Критерии относятся к гарантированности безопасной работы системы. Требования к *политике безопасности* и наличию защитных механизмов не являются составной частью Критериев. Впрочем, чтобы облегчить формулировку цели оценки, Критерии содержат в качестве приложения описание десяти классов функциональности, типичных для правительственных и коммерческих систем.

Европейские Критерии рассматривают все основные составляющие информационной безопасности - **конфиденциальность**, **целостность**, **доступность**.

В Критериях проводится различие между системами и продуктами. **Система** - это конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении. **Продукт** - это аппаратно-программный "пакет", который можно купить и по своему усмотрению встроить в ту или

иную систему. Таким образом, с точки зрения информационной безопасности основное отличие между системой и продуктом состоит в том, что система имеет конкретное окружение, которое можно определить и изучить сколь угодно детально, а продукт должен быть рассчитан на использование в различных условиях.

Из практических соображений важно обеспечить единство критериев оценки продуктов и систем - например, чтобы облегчить оценку системы, составленной из ранее сертифицированных продуктов. По этой причине для систем и продуктов вводится единый термин - объект оценки.

Каждая система и/или продукт предъявляет свои требования к обеспечению конфиденциальности, целостности и доступности. Чтобы удовлетворить эти требования, необходимо предоставить соответствующий набор **функций (сервисов) безопасности**, таких как *идентификация* и *аутентификация*, управление доступом или *восстановление после сбоев*.

Сервисы безопасности реализуются посредством конкретных механизмов. Чтобы объекту оценки можно было доверять, необходима определенная степень уверенности в наборе функций и механизмов безопасности. Степень уверенности мы будем называть гарантированностью. Гарантированность может быть большей или меньшей в зависимости от тщательности проведения оценки.

Гарантированность затрагивает два аспекта - **эффективность** и **корректность** средств безопасности. При проверке эффективности анализируется соответствие между целями, сформулированными для объекта оценки, и имеющимся набором функций безопасности. Точнее говоря, рассматриваются вопросы адекватности функциональности, взаимной согласованности функций, простоты их использования, а также возможные последствия эксплуатации известных слабых мест защиты. Кроме того, в понятие эффективности входит способность механизмов защиты противостоять прямым атакам (**мощность механизма**). Определяются три градации мощности - базовая, средняя и высокая.

Под корректностью понимается правильность *реализации* функций и механизмов безопасности. В Критериях определяется семь возможных *уровней гарантированности* корректности - от E0 до E6 (в порядке возрастания). Уровень E0 означает отсутствие гарантированности. При проверке корректности анализируется весь жизненный цикл объекта оценки - от *проектирования* до эксплуатации и *сопровождения*.

Общая оценка системы складывается из минимальной мощности механизмов безопасности и *уровня гарантированности* корректности.

Гармонизированные критерии Европейских стран явились для своего времени весьма передовым стандартом, они создали предпосылки для появления "Общих критериев".

Интерпретация "Оранжевой книги" для сетевых конфигураций

В 1987 году Национальным центром компьютерной безопасности США была опубликована интерпретация "Оранжевой книги" для сетевых конфигураций. Данный документ состоит из двух частей. Первая содержит собственно интерпретацию, во второй рассматриваются сервисы безопасности, специфичные или особенно важные для сетевых конфигураций.

В первой части вводится минимум новых понятий. Важнейшее из них - **сетевая доверенная вычислительная база**, распределенный аналог *доверенной вычислительной*

базы изолированных систем. Сетевая доверенная вычислительная база формируется из всех частей всех компонентов сети, обеспечивающих информационную безопасность. Доверенная сетевая система должна обеспечивать такое распределение защитных механизмов, чтобы общая *политика безопасности* реализовывалась, несмотря на уязвимость коммуникационных путей и на параллельную, асинхронную работу компонентов.

Прямой зависимости между вычислительными базами компонентов, рассматриваемых как изолированные системы, и фрагментами сетевой вычислительной базы не существует. Более того, нет прямой зависимости и между уровнями безопасности отдельных компонентов и уровнем безопасности всей сетевой конфигурации. Например, в результате объединения двух систем класса B1, обладающих несовместимыми правилами кодирования *меток безопасности*, получается сеть, не удовлетворяющая требованию целостности меток. В качестве противоположного примера рассмотрим объединение двух компонентов, один из которых сам не обеспечивает протоколирование действий пользователя, но передает необходимую информацию другому компоненту, который и ведет протокол. В таком случае распределенная система в целом, несмотря на слабость компонента, удовлетворяет требованию *подотчетности*.

Чтобы понять суть положений, вошедших в первую часть, рассмотрим интерпретацию требований к *классу безопасности* C2. Первое требование к этому классу - поддержка *произвольного управления доступом*. Интерпретация предусматривает различные варианты распределения сетевой доверенной вычислительной базы по компонентам и, соответственно, различные варианты распределения механизмов управления доступом. В частности, некоторые компоненты, закрытые для прямого доступа пользователей, могут вообще не содержать подобных механизмов.

Интерпретация отличается от самих "Критериев" учетом динамичности сетевых конфигураций. Предусматривается наличие средств проверки подлинности и корректности функционирования компонентов перед их включением в сеть, наличие протокола взаимной проверки компонентами корректности функционирования друг друга, а также присутствие средств оповещения администратора о неполадках в сети. Сетевая конфигурация должна быть устойчива к отказам отдельных компонентов или коммуникационных путей.

Среди защитных механизмов в сетевых конфигурациях на первом месте стоит **криптография**, помогающая поддерживать как конфиденциальность, так и целостность. Следствием использования криптографических методов является необходимость *реализации* механизмов управления ключами.

Систематическое рассмотрение вопросов доступности является новшеством по сравнению не только с "Оранжевой книгой", но и с рекомендациями X.800. Сетевой сервис перестает быть доступным, когда пропускная способность коммуникационных каналов падает ниже минимально допустимого уровня или сервис не в состоянии обслуживать запросы. Удаленный ресурс может стать недоступным и вследствие нарушения равноправия в обслуживании пользователей. *Доверенная система* должна иметь возможность обнаруживать ситуации недоступности, уметь возвращаться к нормальной работе и противостоять атакам на доступность.

Для обеспечения непрерывности функционирования могут применяться следующие защитные меры:

• внесение в конфигурацию той или иной формы **избыточности** (резервное оборудование, запасные каналы связи и т.п.);

• наличие средств **реконфигурирования** для изоляции и/или замены узлов или коммуникационных каналов, отказавших или подвергшихся атаке на доступность;

• **рассредоточенность** сетевого **управления**, отсутствие **единой точки отказа**;

• наличие средств **нейтрализации отказов** (обнаружение отказавших компонентов, оценка последствий, восстановление после отказов);

• выделение **подсетей** и **изоляция** групп **пользователей** друг от друга.

Одним из важнейших в "Оранжевой книге" является понятие *монитора обращений*. Применительно к структурированию сетевой конфигурации можно сформулировать следующее утверждение, обеспечивающее достаточное условие корректности фрагментирования *монитора обращений*.

Пусть каждый субъект (то есть процесс, действующий от имени какого-либо пользователя) заключен внутри одного компонента и может осуществлять непосредственный доступ к объектам только в пределах этого компонента. Далее, пусть каждый компонент содержит свой *монитор обращений*, отслеживающий все локальные попытки доступа, и все мониторы реализуют согласованную *политику безопасности*. Пусть, наконец, коммуникационные каналы, связывающие компоненты, сохраняют конфиденциальность и целостность передаваемой информации. Тогда совокупность всех мониторов образует единый *монитор обращений* для всей сетевой конфигурации.

Данное утверждение является теоретической основой декомпозиции распределенной ИС в объектно-ориентированном стиле в сочетании с криптографической защитой коммуникаций.

Тема 6. Административный уровень информационной безопасности

Вводятся ключевые понятия - политика безопасности и программа безопасности. Описывается структура соответствующих документов, меры по их разработке и сопровождению. Меры безопасности увязываются с этапами жизненного цикла информационных систем.

6.1. Основные понятия

К ***административному уровню информационной безопасности*** относятся действия общего характера, предпринимаемые руководством организации.

Главная цель мер *административного уровня* - сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Основой программы является *политика безопасности*, отражающая подход организации к защите своих информационных активов. Руководство каждой организации должно осознать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов.

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. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

Термин *"политика безопасности"* является не совсем точным переводом английского словосочетания "security policy", однако в данном случае калька лучше отражает смысл этого понятия, чем лингвистически более верные "правила безопасности". Мы будем иметь в виду не отдельные правила или их наборы (такого рода решения выносятся на процедурный уровень, речь о котором впереди), а стратегию организации в области информационной безопасности. Для выработки стратегии и проведения ее в жизнь нужны, несомненно, политические решения, принимаемые на самом высоком уровне.

Под ***политикой безопасности*** мы будем понимать совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов.

Такая трактовка, конечно, гораздо шире, чем набор *правил разграничения доступа* (именно это означал термин "security policy" в "Оранжевой книге" и в построенных на ее основе нормативных документах других стран).

ИС организации и связанные с ней интересы субъектов - это сложная система, для рассмотрения которой необходимо применять объектно-ориентированный подход и понятие уровня детализации. Целесообразно выделить, по крайней мере, три таких уровня, что мы уже делали в примере и сделаем еще раз далее.

Чтобы рассматривать ИС предметно, с использованием актуальных данных, следует составить *карту информационной системы*. Эта *карта*, разумеется, должна быть изготовлена в объектно-ориентированном стиле, с возможностью варьировать не только *уровень детализации*, но и видимые грани объектов. Техническим средством составления, сопровождения и визуализации подобных *карт* может служить свободно распространяемый каркас какой-либо системы управления.

6.2. Политика безопасности

С практической точки зрения политику безопасности целесообразно рассматривать на трех уровнях детализации. К верхнему уровню можно отнести решения, затрагивающие организацию в целом. Они носят весьма общий характер и, как правило, исходят от руководства организации. Примерный список подобных решений может включать в себя следующие элементы:

- решение сформировать или пересмотреть комплексную программу обеспечения информационной безопасности, назначение ответственных за продвижение программы;
- формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;
- обеспечение базы для соблюдения законов и правил;
- формулировка административных решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

Для политики верхнего уровня цели организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане может стоять уменьшение числа потерь, повреждений или искажений данных. Для организации, занимающейся продажей компьютерной техники, вероятно, важна актуальность информации о предоставляемых услугах и ценах и ее доступность максимальному числу потенциальных покупателей. Руководство режимного

предприятия в первую очередь заботится о защите от несанкционированного доступа, то есть о конфиденциальности.

На верхний уровень выносится управление защитными ресурсами и *координация* использования этих ресурсов, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности.

Политика верхнего уровня должна четко очерчивать сферу своего влияния. Возможно, это будут все компьютерные системы организации (или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками своих домашних компьютеров). Возможна, однако, и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы.

В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и проведению ее в жизнь. В этом смысле *политика безопасности* является основой подотчетности персонала.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины. Во-первых, организация должна соблюдать существующие законы. Во-вторых, следует контролировать действия лиц, ответственных за выработку программы безопасности. Наконец, необходимо обеспечить определенную степень исполнительности персонала, а для этого нужно выработать систему поощрений и наказаний.

Вообще говоря, на верхний уровень следует выносить минимум вопросов. Подобное вынесение целесообразно, когда оно сулит значительную экономию средств или когда иначе поступить просто невозможно.

Британский стандарт BS 7799:1995 рекомендует включать в документ, характеризующий политику безопасности организации, следующие разделы:

- вводный, подтверждающий озабоченность высшего руководства проблемами информационной безопасности;
- организационный, содержащий описание подразделений, комиссий, групп и т.д., отвечающих за работы в области информационной безопасности;
- классификационный, описывающий имеющиеся в организации материальные и информационные ресурсы и необходимый уровень их защиты;
- штатный, характеризующий меры безопасности, применяемые к персоналу (описание должностей с точки зрения информационной безопасности, организация обучения и переподготовки персонала, порядок реагирования на нарушения режима безопасности и т.п.);
- раздел, освещающий вопросы *физической защиты*;
- управляющий раздел, описывающий подход к управлению компьютерами и компьютерными сетями;
- раздел, описывающий *правила разграничения* доступа к производственной информации;
- раздел, характеризующий *порядок разработки* и сопровождения систем;
- раздел, описывающий меры, направленные на обеспечение *непрерывной работы* организации;
- юридический раздел, подтверждающий соответствие политики безопасности действующему законодательству.

К среднему уровню можно отнести вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных эксплуатируемых организацией систем. Примеры таких вопросов - отношение к передовым (но, возможно, недостаточно проверенным) технологиям, доступ в Internet (как совместить свободу доступа к информации с защитой от внешних угроз?), использование домашних компьютеров, применение пользователями неофициального программного обеспечения и т.д.

Политика среднего уровня должна для каждого аспекта освещать следующие темы:

Описание аспекта. Например, если рассмотреть применение пользователями неофициального программного обеспечения, последнее можно определить как ПО, которое не было одобрено и/или закуплено на уровне организации.

Область применения. Следует определить, где, когда, как, по отношению к кому и чему применяется данная *политика безопасности*. Например, касается ли политика, связанная с использованием неофициального программного обеспечения, организаций-субподрядчиков? Затрагивает ли она сотрудников, пользующихся портативными и домашними компьютерами и вынужденных переносить информацию на производственные машины?

Позиция организации по данному аспекту. Продолжая пример с неофициальным программным обеспечением, можно представить себе позиции полного запрета, выработки процедуры приемки подобного ПО и т.п. Позиция может быть сформулирована и в гораздо более общем виде, как набор целей, которые преследует организация в данном аспекте. Вообще стиль документов, определяющих политику безопасности (как и их перечень), в разных организациях может сильно отличаться.

Роли и обязанности. В "политический" документ необходимо включить информацию о должностных лицах, ответственных за реализацию политики безопасности. Например, если для использования неофициального программного обеспечения сотрудникам требуется разрешение руководства, должно быть известно, у кого и как его можно получить. Если неофициальное программное обеспечение использовать нельзя, следует знать, кто следит за выполнением данного правила.

Законопослушность. Политика должна содержать общее описание запрещенных действий и наказаний за них.

Точки контакта. Должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией. Обычно "точкой контакта" служит определенное должностное лицо, а не конкретный человек, занимающий в данный момент данный пост.

Политика безопасности нижнего уровня относится к конкретным информационным сервисам. Она включает в себя два аспекта - цели и правила их достижения, поэтому ее порой трудно отделить от вопросов реализации. В отличие от двух верхних уровней, рассматриваемая *политика* должна быть определена более подробно. Есть много вещей, специфичных для отдельных видов услуг, которые нельзя единым образом регламентировать в рамках всей организации. В то же время, эти вещи настолько важны для обеспечения режима безопасности, что относящиеся к ним решения должны приниматься на управленческом, а не техническом уровне. Приведем несколько примеров вопросов, на которые следует дать ответ в политике безопасности нижнего уровня:

- кто имеет право доступа к объектам, поддерживаемым сервисом?
- при каких условиях можно читать и модифицировать данные?

• как организован удаленный доступ к сервису?

При формулировке целей политики нижнего уровня можно исходить из соображений целостности, доступности и конфиденциальности, но нельзя на этом останавливаться. Ее цели должны быть более конкретными. Например, если речь идет о системе расчета заработной платы, можно поставить цель, чтобы только сотрудникам отдела кадров и бухгалтерии позволялось вводить и модифицировать информацию. В более общем случае цели должны связывать между собой объекты сервиса и действия с ними.

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем подробнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими средствами. С другой стороны, слишком жесткие правила могут мешать работе пользователей, вероятно, их придется часто пересматривать. Руководству предстоит найти разумный компромисс, когда за приемлемую цену будет обеспечен приемлемый уровень безопасности, а сотрудники не окажутся чрезмерно связаны. Обычно наиболее формально задаются права доступа к объектам ввиду особой важности данного вопроса.

6.3. Программа безопасности

После того, как сформулирована *политика безопасности*, можно приступать к составлению программы ее реализации и собственно к реализации.

Чтобы понять и реализовать какую-либо программу, ее нужно структурировать по уровням, обычно в соответствии со структурой организации. В простейшем и самом распространенном случае достаточно двух уровней - верхнего, или центрального, который охватывает всю организацию, и нижнего, или служебного, который относится к отдельным услугам или группам однородных сервисов.

Программу верхнего уровня возглавляет лицо, отвечающее за информационную безопасность организации. У этой программы следующие главные цели:

• управление рисками (*оценка рисков*, выбор эффективных средств защиты);

• *координация* деятельности в области информационной безопасности, пополнение и распределение ресурсов;

• *стратегическое планирование*;

• *контроль* деятельности в области информационной безопасности.

В рамках программы верхнего уровня принимаются стратегические решения по обеспечению безопасности, оцениваются технологические новинки. Информационные технологии развиваются очень быстро, и необходимо иметь четкую политику отслеживания и внедрения новых средств.

Контроль деятельности в области безопасности имеет двустороннюю направленность. Во-первых, необходимо гарантировать, что действия организации не противоречат законам. При этом следует поддерживать контакты с внешними контролирующими организациями. Во-вторых, нужно постоянно отслеживать состояние безопасности внутри организации, реагировать на случаи нарушений и дорабатывать защитные меры с учетом изменения обстановки.

Следует подчеркнуть, что программа верхнего уровня должна занимать строго определенное место в деятельности организации, она должна официально приниматься и поддерживаться руководством, а также иметь определенный штат и бюджет.

Цель программы нижнего уровня - обеспечить надежную и экономичную защиту конкретного сервиса или группы однородных сервисов. На этом уровне решается, какие следует использовать механизмы защиты; закупаются и устанавливаются технические средства; выполняется повседневное администрирование; отслеживается состояние слабых мест и т.п. Обычно за программу нижнего уровня отвечают администраторы сервисов.

6.4. Синхронизация программы безопасности с жизненным циклом систем

Если синхронизировать программу безопасности нижнего уровня с *жизненным циклом* защищаемого сервиса, можно добиться большего эффекта с меньшими затратами. Программисты знают, что добавить новую возможность к уже готовой системе на порядок сложнее, чем изначально спроектировать и реализовать ее. То же справедливо и для информационной безопасности.

В *жизненном цикле* информационного сервиса можно выделить следующие этапы:

Инициация. На данном этапе выявляется необходимость в приобретении нового сервиса, документируется его предполагаемое назначение.

Закупка.На данном этапе составляются спецификации, прорабатываются варианты приобретения, выполняется собственно *закупка*.

Установка. Сервис устанавливается, конфигурируется, тестируется и вводится в *эксплуатацию*.

Эксплуатация. На данном этапе сервис не только работает и администрируется, но и подвергается модификациям.

Выведение из эксплуатации. Происходит переход на новый сервис.

Рассмотрим действия, выполняемые на каждом из этапов, более подробно.

На этапе *инициации* оформляется понимание того, что необходимо приобрести новый или значительно модернизировать существующий сервис; определяется, какими характеристиками и какой функциональностью он должен обладать; оцениваются финансовые и иные ограничения.

С точки зрения безопасности важнейшим действием здесь является оценка критичности как самого сервиса, так и информации, которая с его помощью будет обрабатываться. Требуется сформулировать ответы на следующие вопросы:

- какого рода информация предназначается для обслуживания новым сервисом?
- каковы возможные последствия нарушения конфиденциальности, целостности и доступности этой информации?
- каковы угрозы, по отношению к которым сервис и информация будут наиболее уязвимы?
- есть ли какие-либо особенности нового сервиса (например, территориальная распределенность компонентов), требующие принятия специальных процедурных мер?
- каковы характеристики персонала, имеющие отношение к безопасности (квалификация, благонадежность)?
- каковы законодательные положения и внутренние правила, которым должен соответствовать новый сервис?

Результаты оценки критичности являются отправной точкой в составлении спецификаций. Кроме того, они определяют ту меру внимания, которую служба безопасности организации должна уделять новому сервису на последующих этапах его *жизненного цикла*.

Этап *закупки* - один из самых сложных. Нужно окончательно сформулировать требования к защитным средствам нового сервиса, к компании, которая может претендовать на роль поставщика, и к квалификации, которой должен обладать персонал, использующий или обслуживающий закупаемый продукт. Все эти сведения оформляются в виде спецификации, куда входят не только аппаратура и программы, но и документация, обслуживание, обучение персонала. Разумеется, особое внимание должно уделяться вопросам совместимости нового сервиса с существующей конфигурацией. Подчеркнем также, что нередко средства безопасности являются необязательными компонентами коммерческих продуктов, и нужно проследить, чтобы соответствующие пункты не выпали из спецификации.

Когда продукт закуплен, его необходимо *установить*. Несмотря на кажущуюся простоту, *установка* является очень ответственным делом. Во-первых, новый продукт следует сконфигурировать. Как правило, коммерческие продукты поставляются с отключенными средствами безопасности; их необходимо включить и должным образом настроить. Для большой организации, где много пользователей и данных, начальная настройка может стать весьма трудоемким и ответственным делом.

Во-вторых, новый сервис нуждается в процедурных регуляторах. Следует позаботиться о чистоте и охране помещения, о документах, регламентирующих использование сервиса, о подготовке планов на случай экстренных ситуаций, об организации обучения пользователей и т.п.

После принятия перечисленных мер необходимо провести тестирование. Его полнота и комплексность могут служить гарантией безопасности *эксплуатации* в штатном режиме.

Период *эксплуатации* - самый длительный и сложный. С психологической точки зрения наибольшую опасность в это время представляют незначительные изменения в конфигурации сервиса, в поведении пользователей и администраторов. Если безопасность не поддерживать, она ослабевает. Пользователи не столь ревностно выполняют должностные инструкции, администраторы менее тщательно анализируют регистрационную информацию. То один, то другой пользователь получает дополнительные привилегии. Кажется, что в сущности ничего не изменилось; на самом же деле от былой безопасности не осталось и следа.

Для борьбы с эффектом медленных изменений приходится прибегать к периодическим проверкам безопасности сервиса. Разумеется, после значительных модификаций подобные проверки являются обязательными.

При *выведении из эксплуатации* затрагиваются аппаратно-программные компоненты сервиса и обрабатываемые им данные. Аппаратура продается, утилизируется или выбрасывается. Только в специфических случаях необходимо заботиться о физическом разрушении аппаратных компонентов, хранящих конфиденциальную информацию. Программы, вероятно, просто стираются, если иное не предусмотрено лицензионным соглашением.

При *выведении данных из эксплуатации* их обычно переносят на другую систему, архивируют, выбрасывают или уничтожают. Если архивирование производится с намерением впоследствии прочитать данные в другом месте, следует позаботиться об аппаратно-программной совместимости средств чтения и записи. Информационные технологии развиваются очень быстро, и через несколько лет устройств, способных

прочитать старый носитель, может просто не оказаться. Если данные архивируются в зашифрованном виде, необходимо сохранить ключ и средства расшифровки. При архивировании и хранении архивной информации нельзя забывать о поддержании конфиденциальности данных.

Тема 7. Основные программно-технические меры

Вводится понятие сервиса безопасности. Рассматриваются вопросы архитектурной безопасности, предлагается классификация сервисов.

7.1. Основные понятия программно-технического уровня информационной безопасности

Программно-технические меры, то есть меры, направленные на контроль компьютерных сущностей - оборудования, программ и/или данных, образуют последний и самый важный рубеж информационной безопасности. Напомним, что ущерб наносят в основном действия легальных пользователей, по отношению к которым процедурные регуляторы малоэффективны. Главные враги - некомпетентность и неаккуратность при выполнении служебных обязанностей, и только программно-технические меры способны им противостоять.

Компьютеры помогли автоматизировать многие области человеческой деятельности. Вполне естественным представляется желание возложить на них и обеспечение собственной безопасности. Даже физическую защиту все чаще поручают не охранникам, а интегрированным компьютерным системам, что позволяет одновременно отслеживать перемещения сотрудников и по организации, и по информационному пространству.

Это вторая причина, объясняющая важность программно-технических мер.

Следует, однако, учитывать, что быстрое развитие информационных технологий не только предоставляет обороняющимся новые возможности, но и объективно затрудняет обеспечение надежной защиты, если опираться исключительно на меры программно-технического уровня. Причин тому несколько:

- повышение быстродействия микросхем, развитие архитектур с высокой степенью параллелизма позволяет методом грубой силы преодолевать барьеры (прежде всего криптографические), ранее казавшиеся неприступными;
- развитие сетей и сетевых технологий, увеличение числа связей между информационными системами, рост пропускной способности каналов расширяют круг злоумышленников, имеющих техническую возможность организовывать атаки;
- появление новых *информационных сервисов* ведет и к образованию новых уязвимых мест как "внутри" сервисов, так и на их стыках;
- конкуренция среди производителей программного обеспечения заставляет сокращать сроки разработки, что приводит к снижению качества тестирования и выпуску продуктов с дефектами защиты;
- навязываемая потребителям парадигма постоянного наращивания мощности аппаратного и программного обеспечения не позволяет долго оставаться в рамках надежных, апробированных конфигураций и, кроме того, вступает в конфликт с бюджетными ограничениями, из-за чего снижается доля ассигнований на безопасность.

Перечисленные соображения лишний раз подчеркивают важность комплексного подхода к информационной безопасности, а также необходимость гибкой позиции при выборе и сопровождении программно-технических регуляторов.

Центральным для программно-технического уровня является понятие *сервиса безопасности*.

Следуя объектно-ориентированному подходу, при рассмотрении информационной системы с единичным уровнем детализации мы увидим совокупность предоставляемых ею *информационных сервисов*. Назовем их ***основными***. Чтобы они могли функционировать и обладали требуемыми свойствами, необходимо несколько уровней *дополнительных (вспомогательных) сервисов* - от СУБД и мониторов транзакций до ядра операционной системы и оборудования.

К ***вспомогательным*** относятся сервисы безопасности (мы уже сталкивались с ними при рассмотрении стандартов и спецификаций в области ИБ); среди них нас в первую очередь будут интересовать универсальные, высокоуровневые, допускающие использование различными *основными* и *вспомогательными сервисами*. Далее мы рассмотрим следующие сервисы:

- *идентификация* и *аутентификация*;
- *управление доступом*;
- *протоколирование* и *аудит*;
- *шифрование*;
- *контроль целостности*;
- *экранирование*;
- *анализ защищенности*;
- обеспечение *отказоустойчивости*;
- обеспечение *безопасного восстановления*;
- *туннелирование*;
- *управление*.

Будут описаны требования к *сервисам безопасности*, их функциональность, возможные методы реализации и место в общей архитектуре.

Если сопоставить приведенный перечень сервисов с классами функциональных требований "Общих критериев", то бросается в глаза их существенное несовпадение. Мы не будем рассматривать вопросы, связанные с *приватностью*, по следующей причине. На наш взгляд, *сервис безопасности*, хотя бы частично, должен находиться в распоряжении того, кого он защищает. В случае же с *приватностью* это не так: критически важные компоненты сосредоточены не на клиентской, а на серверной стороне, так что *приватность* по существу оказывается свойством предлагаемой информационной услуги (в простейшем случае *приватность* достигается путем сохранения конфиденциальности серверной регистрационной информации и защитой от перехвата данных, для чего достаточно перечисленных *сервисов безопасности*).

С другой стороны, наш перечень шире, чем в "Общих критериях", поскольку в него входят *экранирование*, *анализ защищенности* и *туннелирование*. Эти сервисы имеют важное значение сами по себе и, кроме того, могут комбинироваться с другими сервисами для получения таких необходимых *защитных средств*, как, например, виртуальные частные сети.

Совокупность перечисленных выше *сервисов безопасности* мы будем называть полным набором. Считается, что его, в принципе, достаточно для построения надежной защиты на программно-техническом уровне, правда, при соблюдении целого ряда

дополнительных условий (отсутствие уязвимых мест, безопасное администрирование и т.д.).

Для проведения классификации *сервисов безопасности* и определения их места в общей архитектуре меры безопасности можно разделить на следующие виды:

- *превентивные*, препятствующие нарушениям ИБ;
- меры *обнаружения нарушений*;
- *локализующие*, сужающие зону воздействия нарушений;
- меры по *выявлению нарушителя*;
- меры восстановления режима безопасности.

Большинство *сервисов безопасности* попадает в число *превентивных*, и это, безусловно, правильно. *Аудит* и *контроль целостности* способны помочь в *обнаружении нарушений*; активный *аудит*, кроме того, позволяет запрограммировать реакцию на нарушение с целью локализации и/или прослеживания. Направленность сервисов *отказоустойчивости* и *безопасного восстановления* очевидна. Наконец, *управление* играет инфраструктурную роль, обслуживая все аспекты ИС.

7.2. Особенности современных информационных систем, существенные с точки зрения безопасности

Информационная система типичной современной организации является весьма сложным образованием, построенным в многоуровневой архитектуре клиент/сервер, которое пользуется многочисленными внешними сервисами и, в свою очередь, предоставляет собственные сервисы вовне. Даже сравнительно небольшие магазины, обеспечивающие расчет с покупателями по пластиковым картам (и, конечно, имеющие внешний Web-**сервер**), зависят от своих информационных систем и, в частности, от защищенности всех компонентов систем и коммуникаций между ними.

С точки зрения безопасности наиболее существенными представляются следующие аспекты современных ИС:

- **корпоративная сеть** имеет несколько территориально разнесенных частей (поскольку организация располагается на нескольких производственных площадках), связи между которыми находятся в ведении внешнего поставщика сетевых услуг, выходя за пределы зоны, контролируемой организацией;
- корпоративная сеть имеет одно или несколько подключений к **Internet**;
- на каждой из производственных площадок могут находиться критически важные серверы, в доступе к которым нуждаются сотрудники, работающие на других площадках, мобильные пользователи и, возможно, сотрудники других организаций;
- для доступа пользователей могут применяться не только компьютеры, но и потребительские устройства, использующие, в частности, беспроводную связь;
- в течение одного сеанса работы пользователю приходится обращаться к нескольким *информационным сервисам*, опирающимся на разные аппаратно-программные платформы;
- к **доступности** *информационных сервисов* предъявляются жесткие требования, которые обычно выражаются в необходимости круглосуточного функционирования с максимальным временем простоя порядка нескольких минут;
- информационная система представляет собой сеть с **активными агентами**, то есть в процессе работы программные компоненты, такие как **апплеты** или **сервлеты**,

передаются с одной машины на другую и выполняются в целевой среде, поддерживая связь с удаленными компонентами;

- не все пользовательские системы контролируются сетевыми и/или системными администраторами организации;
- программное обеспечение, особенно полученное по сети, не может считаться надежным, в нем могут быть ошибки, создающие проблемы в защите;
- конфигурация информационной системы постоянно изменяется на уровнях административных данных, программ и аппаратуры (меняется состав пользователей, их привилегии и версии программ, появляются новые сервисы, новая аппаратура и т.п.).

Следует учитывать еще по крайней мере два момента. Во-первых, для каждого сервиса основные грани ИБ (доступность, целостность, конфиденциальность) трактуются по-своему. Целостность с точки зрения системы *управления* базами данных и с точки зрения почтового сервера - вещи принципиально разные. Бессмысленно говорить о безопасности локальной или иной сети вообще, если сеть включает в себя разнородные компоненты. Следует *анализировать защищенность* сервисов, функционирующих в сети. Для разных сервисов и защиту строят по-разному. Во-вторых, основная угроза информационной безопасности организаций по-прежнему исходит не от внешних злоумышленников, а от собственных сотрудников.

В силу изложенных причин далее будут рассматриваться распределенные, разнородные, многосервисные, эволюционирующие системы. Соответственно, нас будут интересовать решения, ориентированные на подобные конфигурации.

7.3. Архитектурная безопасность

Сервисы безопасности, какими бы мощными они ни были, сами по себе не могут гарантировать надежность программно-технического уровня защиты. Только проверенная архитектура способна сделать эффективным объединение сервисов, обеспечить управляемость информационной системы, ее способность развиваться и противостоять новым угрозам при сохранении таких свойств, как высокая производительность, простота и удобство использования.

Теоретической основой решения проблемы архитектурной безопасности является следующее фундаментальное утверждение, которое мы уже приводили, рассматривая интерпретацию "Оранжевой книги" для сетевых конфигураций.

"Пусть каждый субъект (то есть процесс, действующий от имени какого-либо пользователя) заключен внутри одного компонента и может осуществлять непосредственный доступ к объектам только в пределах этого компонента. Далее пусть каждый компонент содержит свой монитор обращений, отслеживающий все локальные попытки доступа, и все мониторы проводят в жизнь согласованную политику безопасности. Пусть, наконец, коммуникационные каналы, связывающие компоненты, сохраняют конфиденциальность и целостность передаваемой информации. Тогда совокупность всех мониторов образует единый монитор обращений для всей сетевой конфигурации."

Обратим внимание на три принципа, содержащиеся в приведенном утверждении:

- необходимость выработки и проведения в жизнь единой политики безопасности;
- необходимость обеспечения конфиденциальности и целостности при сетевых взаимодействиях;

• необходимость формирования составных сервисов по содержательному принципу, чтобы каждый полученный таким образом компонент обладал *полным набором защитных средств* и с внешней точки зрения представлял собой единое целое (не должно быть информационных потоков, идущих к незащищенным сервисам).

Если какой-либо (составной) сервис не обладает *полным набором защитных средств* (состав полного набора описан выше), необходимо привлечение дополнительных сервисов, которые мы будем называть экранирующими. Экранирующие сервисы устанавливаются на путях доступа к недостаточно защищенным элементам; в принципе, один такой сервис может *экранировать* (защищать) сколь угодно большое число элементов.

С практической точки зрения наиболее важными являются следующие принципы архитектурной безопасности:

• **непрерывность защиты** в пространстве и времени, невозможность миновать защитные средства;

• следование признанным стандартам, использование апробированных решений;

• иерархическая организация ИС с небольшим числом сущностей на каждом уровне;

• усиление самого **слабого звена**;

• невозможность перехода в **небезопасное состояние**;

• минимизация привилегий;

• разделение обязанностей;

• **эшелонированность обороны**;

• разнообразие защитных средств;

• простота и управляемость информационной системы.

Поясним смысл перечисленных принципов.

Если у злоумышленника или недовольного пользователя появится возможность миновать защитные средства, он, разумеется, так и сделает. Определенные выше экранирующие сервисы должны исключить подобную возможность.

Следование признанным стандартам и использование апробированных решений повышает надежность ИС и уменьшает вероятность попадания в тупиковую ситуацию, когда обеспечение безопасности потребует непомерно больших затрат и принципиальных модификаций.

Иерархическая организация ИС с небольшим числом сущностей на каждом уровне необходима по технологическим соображениям. При нарушении данного принципа система станет неуправляемой и, следовательно, обеспечить ее безопасность будет невозможно.

Надежность любой обороны определяется самым слабым звеном. Злоумышленник не будет бороться против силы, он предпочтет легкую победу над слабостью. (Часто самым слабым звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.)

Принцип невозможности перехода в небезопасное состояние означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ. Образно говоря, если в крепости механизм подъемного моста ломается, мост оставляют поднятым, препятствуя проходу неприятеля.

Применительно к программно-техническому уровню принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей. Этот принцип позволяет уменьшить ущерб от случайных или умышленных некорректных действий пользователей и администраторов.

Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, чтобы один человек не мог нарушить критически важный для организации процесс или создать брешь в защите по заказу злоумышленников. В частности, соблюдение данного принципа особенно важно, чтобы предотвратить злонамеренные или неквалифицированные действия системного администратора.

Принцип эшелонированности обороны предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать программно-технические средства, за *идентификацией* и *аутентификацией* - *управление доступом* и, как последний рубеж, - *протоколирование* и *аудит*. Эшелонированная оборона способна, по крайней мере, задержать злоумышленника, а благодаря наличию такого рубежа, как *протоколирование* и *аудит*, его действия не останутся незамеченными. Принцип разнообразия защитных средств предполагает создание различных по своему характеру оборонительных рубежей, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками.

Очень важен принцип простоты и управляемости информационной системы в целом и защитных средств в особенности. Только для простого защитного средства можно формально или неформально доказать его корректность. Только в простой и управляемой системе можно проверить согласованность конфигурации различных компонентов и осуществлять централизованное администрирование. В этой связи важно отметить интегрирующую роль Web-сервиса, скрывающего разнообразие обслуживаемых объектов и предоставляющего единый, наглядный интерфейс. Соответственно, если объекты некоторого вида (например, таблицы базы данных) доступны через Web, необходимо заблокировать прямой доступ к ним, поскольку в противном случае система будет сложной и плохо управляемой.

Для обеспечения высокой доступности (непрерывности функционирования) необходимо соблюдать следующие принципы архитектурной безопасности:

- внесение в конфигурацию той или иной формы **избыточности** (резервное оборудование, запасные каналы связи и т.п.);
- наличие средств обнаружения нештатных ситуаций;
- наличие средств **реконфигурирования** для восстановления, **изоляции** и/или замены компонентов, отказавших или подвергшихся атаке на доступность;
- рассредоточенность сетевого *управления*, отсутствие **единой точки отказа**;
- выделение подсетей и изоляция групп пользователей друг от друга. Данная мера, являющаяся обобщением разделения процессов на уровне операционной системы, ограничивает зону поражения при возможных нарушениях информационной безопасности.

Еще один важный архитектурный принцип - минимизация объема защитных средств, выносимых на клиентские системы. Причин тому несколько:

• для доступа в корпоративную сеть могут использоваться **потребительские устройства** с ограниченной функциональностью;

• конфигурацию клиентских систем трудно или невозможно контролировать.

К необходимому минимуму следует отнести реализацию *сервисов безопасности* на сетевом и транспортном уровнях и поддержку механизмов *аутентификации*, устойчивых к сетевым угрозам.

Тема 8. Информационные угрозы. Методы защиты информации. Предмет защиты. Средства защиты

Знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности.

8.1 Основные определения и критерии классификации угроз

Угроза - это потенциальная возможность определенным образом нарушить информационную безопасность.

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

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).

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 использования 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.

8.1 Способы неправомерного доступа к информации

Залогом успешной борьбы с несанкционированным доступом к информации и перехватом данных служит четкое представление о каналах утечки информации.

Интегральные схемы, на которых основана работа компьютеров, создают высокочастотные изменения уровня напряжения и токов. Колебания распространяются по проводам и могут не только трансформироваться в доступную для понимания форму, но и перехватываться специальными устройствами. В компьютер или монитор могут устанавливаться устройства для перехвата информации, которая выводится на монитор или вводится с клавиатуры. Перехват возможен и при передаче информации по внешним каналам связи, например, по телефонной линии.

8.2 Методы защиты

На практике используют несколько групп методов защиты, в том числе:

- **препятствие на пути предполагаемого похитителя**, которое создают физическими и программными средствами;
- **управление**, или оказание воздействия на элементы защищаемой системы;
- **маскировка**, или преобразование данных, обычно – криптографическими способами;
- **регламентация**, или разработка нормативно-правовых актов и набора мер, направленных на то, чтобы побудить пользователей, взаимодействующих с базами данных, к должному поведению;
- **принуждение**, или создание таких условий, при которых пользователь будет вынужден соблюдать правила обращения с данными;
- **побуждение**, или создание условий, которые мотивируют пользователей к должному поведению.

Каждый из методов защиты информации реализуется при помощи различных категорий средств. Основные средства – организационные и технические.

Регламент по обеспечению информационной безопасности – внутренний документ организации, который учитывает особенности бизнес-процессов и информационной инфраструктуры, а также архитектуру системы.

8.3 Организационные средства защиты информации

Разработка комплекса организационных средств защиты информации должна входить в компетенцию службы безопасности.

Чаще всего специалисты по безопасности:

- **разрабатывают внутреннюю документацию**, которая устанавливает правила работы с компьютерной техникой и конфиденциальной информацией;
- **проводят инструктаж** и периодические проверки персонала; инициируют подписание дополнительных соглашений к трудовым договорам, где указана ответственность за разглашение или неправомерное использование сведений, ставших известных по работе;
- **разграничивают зоны ответственности**, чтобы исключить ситуации, когда массивы наиболее важных данных находятся в распоряжении одного из сотрудников; организуют работу в общих программах документооборота и следят, чтобы критически важные файлы не хранились вне сетевых дисков;
- **внедряют программные продукты**, которые защищают данные от копирования или уничтожения любым пользователем, в том числе топ-менеджментом организации;
- **составляют планы восстановления системы** на случай выхода из строя по любым причинам.

Если в компании нет выделенной ИБ-службы, выходом станет приглашение специалиста по безопасности на аутсорсинг. Удаленный сотрудник сможет провести аудит ИТ-инфраструктуры компании и дать рекомендации по ее защите от внешних и внутренних угроз. Также аутсорсинг в ИБ предполагает использование специальных программ для защиты корпоративной информации.

Технические средства защиты информации

Группа технических средств защиты информации совмещает аппаратные и программные средства. Основные:

- резервное копирование и удаленное хранение наиболее важных массивов данных в компьютерной системе – на регулярной основе;
- дублирование и резервирование всех подсистем сетей, которые имеют значение для сохранности данных;
- создание возможности перераспределять ресурсы сети в случаях нарушения работоспособности отдельных элементов;
- обеспечение возможности использовать резервные системы электропитания;
- обеспечение безопасности от пожара или повреждения оборудования водой;
- установка программного обеспечения, которое обеспечивает защиту баз данных и другой информации от несанкционированного доступа.

В комплекс технических мер входят и меры по обеспечению физической недоступности объектов компьютерных сетей, например, такие практические способы, как оборудование помещения камерами и сигнализацией.

Аутентификация и идентификация

Чтобы исключить неправомерный доступ к информации применяют такие способы, как идентификация и аутентификация.

Идентификация – это механизм присвоения собственного уникального имени или образа пользователю, который взаимодействует с информацией. **Аутентификация** – это система способов проверки совпадения пользователя с тем образом, которому разрешен допуск.

Эти средства направлены на то, чтобы предоставить или, наоборот, запретить допуск к данным. Подлинность, как правила, определяется тремя способами: программой, аппаратом, человеком. При этом объектом аутентификации может быть не только человек, но и техническое средство (компьютер, монитор, носители) или данные. Простейший способ защиты – пароль.

Тема 9. Тема: Методы и средства обеспечения безопасности информации.

В современном обществе информация является очень ценным ресурсом в любой деятельности человека. Поэтому каждое предприятие заинтересованно в своей информационной безопасности. Информационной безопасностью называют меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Целью информационной безопасности является защита ценности системы, сохранить и гарантировать точность и целостность информации, а также минимизировать разрушения, если информация будет модифицирована или разрушена. Информационная безопасность требует учета всех событий, в ходе которых информация создается, модифицируется, распространяется или, когда к ней обеспечивается доступ. Обеспечения информационной безопасности организации осуществляются на практике

использованием различных механизмов защиты, для создания которых применяют следующие средства:

- физические;
- аппаратные;
- программные;
- аппаратно-программные (технические);
- криптографические;
- административные (организационные);
- законодательные (правовые);
- морально-этические.

Физические средства защиты - это разного рода механические, электронно-механические устройства, специально предназначенные для образования физических препятствий на возможных путях проникновения и доступа возможных нарушителей к компонентам автоматической системы и защищаемой информации, а также технические средства визуального наблюдения, связи и охранной сигнализации. Физическая безопасность связана с введением мер защиты, которые защищают от стихийных бедствий, например, таких как пожар, наводнение, ураган, землетрясение.

Аппаратные средства защиты — это различные электронные, электромеханические устройства, прямо встроенные в блоки автоматизированной информационной системы или оформленные в виде автономных устройств и сопрягающиеся с этими блоками. Их задача внутренняя защита структурных элементов средств и систем вычислительной техники, например, процессоров, терминалов, периферийного оборудования. Реализуются это с помощью метода управления доступом (идентификация, аутентификация и проверка полномочий субъектов системы, регистрация, реагирование).

Программные средства защиты используются для выполнения логических и интеллектуальных функций защиты. Включаются либо в состав программного обеспечения автоматизированной информационной системы, либо в состав средств, комплексов и систем аппаратуры контроля. Программные средства защиты являются наиболее распространенным видом защиты, так как они универсальны, просты в использовании, имеется возможностью изменения и развития. Данное обстоятельство делает их и самыми уязвимыми элементами защиты информационной системы организации. В настоящее время создано большое количество операционных систем, систем управления базами данных, сетевых пакетов и пакетов прикладных программ, включающих разнообразные средства защиты информации.

Аппаратно-программные средства защиты представляют собой различные электронные устройства и специальные программы, входящие в состав автоматической системы предприятия и исполняющие самостоятельно или в комплексе с другими средствами, функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации).

Криптографический метод защиты информации основанный на принципе ее шифрования. Криптографический метод может быть осуществлен как программными, так и аппаратными средствами. Средство криптографической защиты информации осуществляет криптографическое перестройку информации для обеспечения ее

безопасности. Криптографическая защита или криптографическое преобразование информации, шифрование является одним из важных способов защиты информации.

Административный метод защиты является методом организационного характера, регламентирующие процессы функционирования системы обработки данных, применением ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой так, чтобы в максимальной степени затруднить или исключить возможность реализации угроз безопасности или минимизировать размер потерь в случае их осуществления. Главная цель административных мер сформировать политику в области обеспечения безопасности информации и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые средства защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

К морально-этическим средствам относятся нормы поведения и правила обращения с информацией. Которые традиционно сложились или складываются по мере распространения электронно-вычислительных машин в обществе, стране. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты. Однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные, например, общепризнанные нормы честности, так и писаные, то есть оформленные в некоторый устав правил или предписаний. Морально-этические средства защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений.

Нужно сказать, что, на данном этапе общемирового развития, роль информационной среды очень велика. Информация является системообразующим фактором во всех этапах жизни общества, она все более активно влияет на состояние политической, экономической, оборонной, личной, имущественной и других составляющих безопасности. Поэтому несмотря на то, что построение эффективной системы информационной безопасности является сложным и непрерывным процессом, этому нужно уделять значительное внимания. А именно оперировать данными методами которые обеспечат информационную безопасность.

Тема 10. Программно-аппаратные средства информационной защиты.

Необходимость защиты информации очевидна для всех, даже для далеких от IT-сферы людей. Частые утечки конфиденциальных данных, например, сведений о клиентах банков с номерами их карт или персональных данных детей, угрожают личной безопасности пострадавших и несут проблемы виновникам инцидентов. Программно-аппаратная защита с использованием современных технических средств призвана снизить риск утечек, ограничив внутренний доступ к информационным системам.

Для чего нужна программно-аппаратная защита информации

Аппаратные средства защиты в большинстве случаев охраняют информацию, доступ к которой ограничен на основании требований закона, например, государственную или банковскую тайну, персональные данные. Поэтому правила их использования полностью или частично регламентируются на уровне государства. Статус охраняемой информации определяется законами, например, законом «О персональных данных», правила выбора аппаратно-программных средств – нормативными актами и рекомендациями ФСТЭК РФ.

Обеспечение безопасности информации на программно-аппаратном уровне предохраняет сведения от несанкционированного доступа и снижает риски хищения и дальнейшего неправомерного использования полученных сведений.

Комплекс аппаратно-программной защиты состоит из двух частей:

- аппаратное устройство;
- программный модуль.

Принцип работы системы состоит в том, что при попытке получения доступа к данным программа отправляет запрос к устройству, обеспечивающему работу ключа (токену, ридеру, электронному идентификатору, после подключения которого к компьютеру тот дает разрешение на работу), и функционирует только при его положительной реакции.

С точки зрения надежности эта методика выглядит предпочтительнее, чем просто программная защита, но стоимость аппаратной части делает ее доступной только для крупных и средних компаний или государственных организаций.

10.1 Защита от НСД

При выборе методов и средств защиты данных нужно учитывать, что существует несколько принципов защиты от несанкционированного доступа (НСД). На них основана работа средств программно-аппаратной защиты:

- доступ к данным предоставляется только тем пользователям, которые уполномочены его получить на уровне внутренних документов компании;
- каждый уполномоченный пользователь имеет доступ только к своему уровню информации, его прав недостаточно для работы с данными, находящимися в сфере ответственности других пользователей;
- перечень операций, которые допустимо выполнять с данными, строго регламентирован, и зависит от изначально заданных прав пользователей.

Для защиты от НСД в аппаратно-программных средствах должен быть механизм распознавания уполномоченного пользователя и его авторизации (идентификации и аутентификации).

Процесс авторизации состоит из трех этапов:

1. Идентификация. Пользователь должен передать системе свой идентифицирующий признак, например, логин и пароль. При использовании аппаратных средств становится возможной и более глубокая степень идентификации по отпечатку пальца, сетчатке глаза, иным биометрическим признакам или на основании владения определенным устройством (магнитная карточка, электронный ключ);

2. Аутентификация. Этот процесс в работе программно-аппаратных средств нацелен на сравнение заявленного пользователем идентифицирующего признака с теми, которые хранятся в памяти устройства. В ходе аутентификации устанавливается подлинность пользователя. Она может реализовываться на основе простой или

усложненной PIN-идентификации. В обоих случаях персональный идентификационный номер пользователя сравнивается с эталоном. При простом механизме идентификации система проводит обычное сравнение и в случае совпадения выдает разрешение на дальнейшую работу. При сложном, защищенном, система посылает запрос ключу, тот «отвечает» отправкой 64-разрядного ключа. Система складывает число с введенным пользователем PIN-кодом, направляя полученный результат ключу, тот проводит итоговую идентификацию, при положительном результате которой выдает разрешение на работу;

3. Авторизация. После того как подлинность пользователя установлена, аппаратно-программным средством определяется объем предоставленных ему прав.

Электронные ключи

Работа программно-аппаратных средств защиты информации становится невозможной, если их архитектурой не предусмотрено наличие электронных ключей. Они представляют собой явление предметного мира, физическое устройство, снабженное электронной начинкой и содержащее уникальную информацию, позволяющую идентифицировать пользователя.

Ключи бывают трех видов:

1. Специализированный электронный чип.
2. Микросхема перепрограммируемой памяти, имеющая собственные источники электропитания.
3. Ключ на базе микропроцессора.

Выбор технологии, на которой основан ключ, связан с типом аппаратного средства. Ранее ключи совмещались с рабочей станцией посредством обычных портов, через которые подключаются принтер или МФУ, что создавало неудобство для пользователей. Развитие USB-технологий упростило использование электронных ключей при работе с аппаратно-программными средствами защиты информации.

Как работает электронный ключ? Устройство, содержащее код легитимного пользователя, опознается программной частью системы, в результате осуществляется допуск к работе. Помимо данных, идентифицирующих пользователя, в ключе могут содержаться сведения о программе, используемой аппаратной частью: номер, данные о выпуске, дата оформления лицензии.

Данные, содержащиеся в памяти ключа, могут перепрограммироваться в дистанционном режиме, что усиливает безопасность. Электронные ключи применяются и для защиты авторских прав разработчика программы: считают число лицензий и не допускают их использование в большем количестве, чем оговорено в соглашении.

Как взламывается аппаратно-программная защита и как избежать взлома

Принимая решение о выборе аппаратно-программного средства, необходимо понимать, что современные технологии позволяют взламывать системы с недостаточным уровнем защиты. При этом стоимость аппаратной части высока. Современные версии ключей, токены, основаны на новейших технологиях, которые позволяют избежать ряда рисков, но не в полном объеме.

Для несанкционированного проникновения (взлома) в систему обычно используется один из двух методов:

- поиск и использование уязвимостей в программной части;
- эмулирование (подмена) данных, содержащихся в электронном ключе.

В первом случае из программы (приложения) удаляются части, в которых содержится код, обеспечивающий работу механизмов защиты. Это могут быть команды опроса электронного ключа (направление запроса в отдельном токе данных) или команды сравнения введенных данных с эталоном. Второй путь взлома, эмулирование электронного ключа, связан с использованием специальных программных средств – эмуляторов. Программа отправляет приложению обращения, содержащие, правильные ответы.

Если в первом случае методом защиты будет стандартное ограничение прав пользователей, исключающее вмешательство в программный код, во втором рекомендуется вкладывать в конструкцию устройства алгоритм хаотического обмена данными.

Следует учитывать, что реализация схемы эмуляции ключа крайне сложна и доступна немногим специалистам. Взаимодействие эмулятора ключа с программой осуществляется одним из двух способов:

- путем подмены драйвера;
- через точку входа API вызова ключа.

В первом случае решением станет регулярный аудит системных файлов, проверяющих их изменения. Во втором – шифрование той части программы, которая отвечает за взаимодействие с ключом, или реализация опции постоянного контроля его целостности. Дополнительным способом контроля целостности будет использование электронной подписи. Одним из решений станут микроконтроллеры. Это утилиты, которые отсылают сразу несколько запросов, позволяющих сверить точность введенного ключа. В некоторых программных продуктах реализуется до 18 алгоритмов, на основании которых производятся дополнительные вычисления, обеспечивающие точность аутентификации и контролирующие только легитимный доступ к информации.

Программно-аппаратные механизмы защиты информации находят все большее применение. Они используются не только для защиты локальных сетей, но и для работы с облачными хранилищами. Цена устройств по мере развития технологий снижается. Поэтому при разработке архитектуры собственной информационной системы, в целях обеспечения максимально достижимого уровня безопасности, следует рассмотреть возможность их применения.

Тема 11. Симметричное и несимметричное шифрование. Шифрование заменой. Монофоническая замена.

Шифрова́ние — обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. Главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации. Важной особенностью любого алгоритма шифрования является использование ключа, который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма.

Пользователи являются авторизованными, если они обладают определённым аутентичным ключом. Вся сложность и, собственно, задача шифрования состоит в том, как именно реализован этот процесс.

В целом, шифрование состоит из двух составляющих — зашифровывание и расшифровывание.

С помощью шифрования обеспечиваются три состояния безопасности информации:

• Конфиденциальность.

Шифрование используется для скрытия информации от неавторизованных пользователей при передаче или при хранении.

• Целостность.

Шифрование используется для предотвращения изменения информации при передаче или хранении.

• Идентифицируемость.

Шифрование используется для аутентификации источника информации и предотвращения отказа отправителя информации от того факта, что данные были отправлены именно им.

Для того, чтобы прочитать зашифрованную информацию, принимающей стороне необходимы ключ и дешифратор (устройство, реализующее алгоритм расшифровывания). Идея шифрования состоит в том, что злоумышленник, перехватив зашифрованные данные и не имея к ним ключа, не может ни прочитать, ни изменить передаваемую информацию. Кроме того, в современных криптосистемах (с открытым ключом) для шифрования, расшифрования данных могут использоваться разные ключи. Однако, с развитием криптоанализа, появились методики, позволяющие дешифровать закрытый текст без ключа. Они основаны на математическом анализе переданных данных.

11.1 Методы шифрования

Симметричное шифрование использует один и тот же ключ и для зашифровывания, и для расшифровывания.

• ***Асимметричное шифрование*** использует два разных ключа: один для зашифровывания (который также называется открытым), другой для расшифровывания (называется закрытым).

Эти методы решают определённые задачи и обладают как достоинствами, так и недостатками. Конкретный выбор применяемого метода зависит от целей, с которыми информация подвергается шифрованию.

Симметричное шифрование

Симметричное шифрование

В симметричных криптосистемах для шифрования и расшифровывания используется один и тот же ключ. Отсюда название — *симметричные*. Алгоритм и ключ выбирается заранее и известен обеим сторонам. Сохранение ключа в секретности является важной задачей для установления и поддержки защищённого канала связи. В связи с этим, возникает проблема начальной передачи ключа (синхронизации ключей). Кроме того существуют методы криптоатак, позволяющие так или иначе дешифровать информацию не имея ключа или же с помощью его перехвата на этапе согласования. В целом эти моменты являются проблемой криптостойкости конкретного алгоритма шифрования и являются аргументом при выборе конкретного алгоритма.

Симметричные, а конкретнее, алфавитные алгоритмы шифрования были одними из первых алгоритмов. Позднее было изобретено асимметричное шифрование, в котором ключи у собеседников разные.

Алгоритмы шифрования данных широко применяются в компьютерной технике в системах сокрытия конфиденциальной и коммерческой информации от злонамеренного использования сторонними лицами. Главным принципом в них является условие, что *передатчик и приемник заранее знают алгоритм шифрования*, а также ключ к сообщению, без которых информация представляет собой всего лишь набор символов, не имеющих смысла.

Классическими примерами таких алгоритмов являются **симметричные криптографические алгоритмы**, перечисленные ниже:

- Простая перестановка
- Одиночная перестановка по ключу
- Двойная перестановка
- Перестановка «Магический квадрат»

Простая перестановка

Простая перестановка без ключа — один из самых простых методов шифрования. Сообщение записывается в таблицу по столбцам. После того, как открытый текст записан колонками, для образования шифртекста он считывается по строкам. Для использования этого шифра отправителю и получателю нужно договориться об общем ключе в виде размера таблицы. Объединение букв в группы не входит в ключ шифра и используется лишь для удобства записи несмыслового текста.

Одиночная перестановка по ключу

Более практический метод шифрования, называемый одиночной перестановкой по ключу, очень похож на предыдущий. Он отличается лишь тем, что колонки таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы.

Двойная перестановка

Для дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Этот способ известен под названием двойная перестановка. Для этого размер второй таблицы подбирают так, чтобы длины её строк и столбцов отличались от длин в первой таблице. Лучше всего, если они будут взаимно простыми. Кроме того, в первой таблице можно переставлять столбцы, а во второй строки. Наконец, можно заполнять таблицу зигзагом, змейкой, по спирали или каким-то другим способом. Такие способы заполнения таблицы если и не усиливают стойкость шифра, то делают процесс дешифрования гораздо более занимательным.

Перестановка «Магический квадрат»

Магическими квадратами называются квадратные таблицы со вписанными в их клетки последовательными натуральными числами от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Подобные квадраты широко применялись для вписывания шифруемого текста по приведенной в них нумерации. Если потом выписать содержимое таблицы по строкам, то получалась шифровка перестановкой букв. На первый взгляд кажется, будто магических квадратов очень мало. Тем не менее, их число очень быстро возрастает с увеличением размера квадрата. Так, существует лишь один магический квадрат размером 3 x 3, если не принимать во внимание его повороты. Магических квадратов 4 x 4 насчитывается уже 880, а число магических квадратов размером 5 x 5 около 250000. Поэтому магические квадраты больших размеров могли быть хорошей основой для надежной системы

шифрования, потому что ручной перебор всех вариантов ключа для этого шифра немыслим.

Недостатками симметричного шифрования является проблема передачи ключа собеседнику и невозможность установить подлинность или авторство текста. Поэтому, например, в основе технологии цифровой подписи лежат асимметричные схемы.

Асимметричное шифрование (с открытым ключом)

Асимметричное шифрование

В системах с открытым ключом используются два ключа — открытый и закрытый, связанные определённым математическим образом друг с другом. Открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для шифрования сообщения и для проверки ЭЦП. Для расшифровки сообщения и для генерации ЭЦП используется секретный ключ.

Данная схема решает проблему симметричных схем, связанную с начальной передачей ключа другой стороне. Если в симметричных схемах злоумышленник перехватит ключ, то он сможет как «слушать», так и вносить правки в передаваемую информацию. В асимметричных системах другой стороне передается открытый ключ, который позволяет шифровать, но не расшифровывать информацию. Таким образом решается проблема симметричных систем, связанная с синхронизацией ключей.

Если необходимо наладить канал связи в обе стороны, то первые две операции необходимо проделать на обеих сторонах, таким образом, каждый будет знать свои закрытый, открытый ключи и открытый ключ собеседника. Закрытый ключ каждой стороны не передается по незащищенному каналу, тем самым оставаясь в секретности.

Асимметричное шифрование с открытым ключом базируется на следующих принципах:

- Можно сгенерировать пару очень больших чисел (открытый ключ и закрытый ключ) так, чтобы, зная открытый ключ, нельзя было вычислить закрытый ключ за разумный срок. При этом механизм генерации является общеизвестным.
- Имеются надёжные методы шифрования, позволяющие зашифровать сообщение открытым ключом так, чтобы расшифровать его можно было только закрытым ключом. Механизм шифрования является общеизвестным.
- Владелец двух ключей никому не сообщает закрытый ключ, но передает открытый ключ контрагентам или делает его общеизвестным.

Если необходимо передать зашифрованное сообщение владельцу ключей, то отправитель должен получить открытый ключ. Отправитель шифрует свое сообщение открытым ключом получателя и передает его получателю (владельцу ключей) по открытым каналам. При этом расшифровать сообщение не может никто, кроме владельца закрытого ключа.

В результате можно обеспечить надёжное шифрование сообщений, сохраняя ключ расшифровки секретным для всех - даже для отправителей сообщений.

Тема 12. Методы защиты информации: собственная, активная и пассивная защиты.

Цель: изучить средства собственной, активной и пассивной защиты информации.

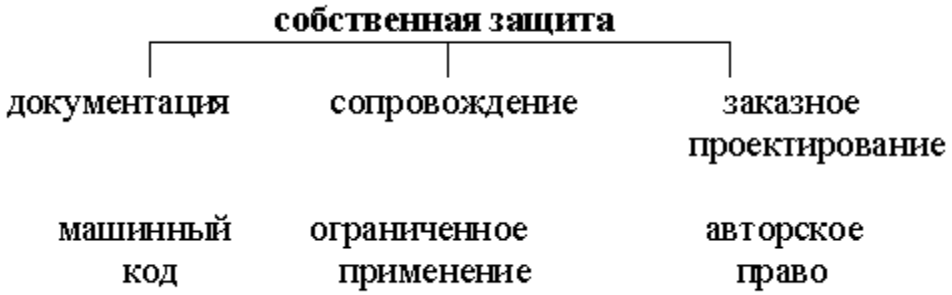
1. Собственная защита
2. Активная защита

3. Пассивная защита
4. Способы защиты информации

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

12.1. Собственная защита

Собственная защита программ - это термин, определяющий те элементы защиты, которые присущи самому программному обеспечению или сопровождают его продажу и препятствуют незаконным действиям пользователя. Средства собственной защиты можно представить следующим образом:



Документация, сопровождающая любое программное обеспечение, является субъектом авторского права и может выполнять функции защиты. Этому способствуют следующие факторы: её репродуцирование стоит достаточно дорого, особенно если оригинал выполнен в цвете и не может быть качественно воспроизведен одноцветным копировальным устройством; обычно программы распространяются, будучи представленными в машинном коде, что затрудняет анализ их структуры и обеспечивает определенную степень защиты. В последнем случае весьма важно, чтобы сохранялось сопровождение программы со стороны разработчика, особенно в тех случаях, когда программа не полностью отлажена.

Ограниченное применение как способ защиты реализуется в том случае, когда программное обеспечение используется небольшим числом пользователей, каждый из которых известен по имени. Эта ситуация относительно легко контролируется в окружении, пользующемся доверием, хотя могут возникать проблемы с отдельными работниками, нанятыми на ограниченный срок. В этих случаях следует оговорить условия работы с программными средствами в заключаемом контракте.

Заказное проектирование предполагает разработку программного обеспечения для специальных целей. Если программа используется редко, то её кража в коммерческих целях маловероятна; однако если кража произошла, то именно эти детали дают ключ к источнику несанкционированного копирования.

Рекомендуется также расставлять отличительные метки в стандартных программных модулях для того, чтобы идентифицировать программы, поставляемые добросовестным покупателям. Цена индивидуальной разметки каждой копии программы должна быть тщательно соразмерена с ожидаемой коммерческой прибылью.

12.2. Активная защита

Средства активной защиты делятся на две группы: внутренние и внешние, используемые в составе компьютера и вне его соответственно. Средства активной защиты

- совокупность средств защиты, которые инициируются при возникновении особых обстоятельств - вводе неправильного пароля, указании неправильной даты или времени при запуске программы на выполнение или других подобных условий. Попытки получить доступ к точной информации без разрешения на это могут также служить спусковым крючком для активизации защиты.

12.3. Внутренние средства активной защиты

Внутренние средства активной защиты характеризуются тем, что их обычно не рекламируют хакерам: они либо блокируют программу, либо уничтожают ее. Ключи защиты для блокирования выполнения программы могут быть настроены на любое недозволенное действие, которое будет обнаружено. Обычно это ключи, настроенные на дату, определенное время или на перечень разрешенных ресурсов; в наибольшей степени это относится к арендуемым лицензионным программам, для которых период использования и требуемые ресурсы бывают однозначно определены. Проверка уровня авторских полномочий необходима, чтобы блокировать доступ к точной информации или другим ресурсам, запрещенным для использования.

Инициализация наблюдения может начаться с регистрации в системном журнале использования терминала или реализовываться в виде подтверждения подлинности структуры программы; следует проверить, что средства защиты, включенные в программу, не подвергались изменению или

Искажение программы представляет собой интересный прием изменения функций, хотя возможны и более решительные действия, например, стирание памяти. Программы-вирусы вызывают постепенное разрушение программы.

12.4. Внешние средства активной защиты

В группе этих средств общепринятые сигналы тревоги, которые известны или неизвестны хакеру, приводят в состояние готовности средства защиты, что может быть вызвано различными ситуациями. Они могут быть активизированы при возникновении многих условий. Такие внешние факторы включают также использование ключевых слов, чтобы вызвать распечатку названия программы или имени ее владельца. Хотя описанное и не является защитой от пиратства, это тем не менее способствует увеличению объема продаж, если число случайных копий уменьшится. Общепринятые сигналы тревог более сродни созданию среды защиты компьютера, когда требуется подтверждение подлинности операции, особенно при копировании.

Запуск распечатки этикетки или других деталей из защищенных участков программы осуществляется только при наличии ключевых слов.

Пример реализации

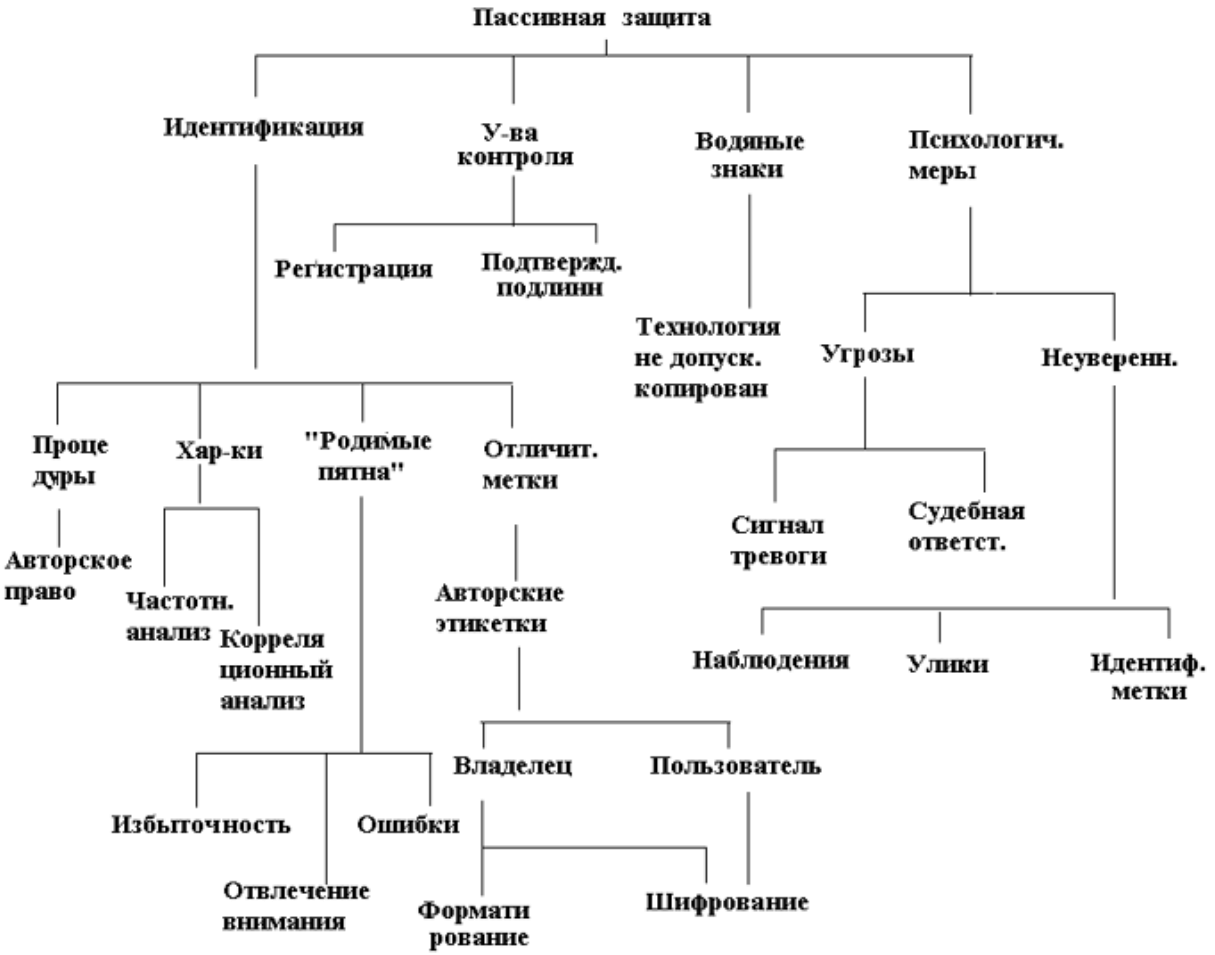
Ввод пароля;
IF пароль введен неверно THEN
BEGIN
печать сообщения об ошибке;
сигнал тревоги;
END
ELSE
печать сообщения о разрешении доступа;
END PROGRAM.

12.5. Пассивная защита

К средствам пассивной защиты относятся предостережения, контроль, а также методы, направленные на поиск улик и доказательство копирования, чтобы создать обстановку неотвратимости раскрытия.

12.6. Идентификация программ

Идентификация программы или отдельного модуля представляет интерес в том случае, когда другие методы защиты не приносят успеха. Эти вопросы слабо освещены в литературе. Широко обсуждаются проблемы авторского права для отдельной процедуры программы и взаимосвязь между идеей и способом ее реализации. Выделение объективных характеристик программы - довольно сложная процедура, тем не менее, признаки подобия двух программ или модулей, содержащихся в больших программах, указать можно. Проблема заключается в том, чтобы уметь идентифицировать программы, которые изменены хакером, погружены в другую программу или откомпилированы в машинный код. Оценка относительной частоты появления операторов или машинных команд - практический способ количественной оценки характеристики программы. Эта величина изменяется при внесении хакером изменений в программу, однако, в большой программе для существенного изменения характеристики требуется выполнить значительную работу; к этому следует добавить возможность появления дополни тельных ошибок или не согласующихся процедур, которые уменьшают надежность программы.



Для получения корреляционных характеристик, связанных с вставкой программного модуля в большую программу, требуются трудоемкие расчеты, хотя можно указать ряд важных признаков, которые указывали бы на целесообразность более детальных исследований.

Понятие "родимые пятна" используется для описания характеристик, появляющихся в результате естественного процесса разработки программы и относящихся к особенностям стиля программирования, ошибкам и избыточностям, которые не должны иметь места в независимо написанной программе. Каждое из них может служить убедительной уликой нарушения авторского права.

Отличительные метки относятся к таким признакам, которые не являются случайными, а вводятся специально, чтобы дать информацию об авторе или владельце авторского права. Другое использование идентификационных меток - выявление путей незаконного копирования или других злоумышленных действий. Термин "отличительная метка" относится к пассивным средствам защиты, которые при нормальном функционировании не проявляют себя по отношению к пользователю.

Одно из убедительных доказательств копирования- наличие скопированных ошибок. В каждой программе остаются избыточные части, которые были необходимы для отладки в процессе проектирования программного продукта, а затем не были удалены. Таким образом, в любой программе содержится встроенная улика, которая тем или иным способом сохраняет следы разработки.

Убедительность улики повышается, если отличительная метка, содержащая информацию о владельце авторского права, закодирована. Использование закодированных отличительных меток - довольно распространенная практика, т.к. при этом они остаются доступными и в машинном коде. Отличительные метки не являются в полной мере избыточными для того, кто организует контроль за данными и в состоянии отделить на их фоне действительно избыточные данные.

Можно разработать методы, которые позволят использовать закодированные в программе данные. Один из них связан с форматированием выходных данных в закодированной форме, что обусловлено необходимостью проверки кодирования при удаленной передаче, и это требует дополнительной работы.

Важная особенность отличительных меток заключается в том, что они не известны нарушителю.

12.7. Устройства контроля

Устройства регистрации событий, процедур или доступа к данным могут рассматриваться как часть общей системы защиты, причем как программ, так и данных. Подтверждение подлинности программы охватывает проблемы от установления идентичности функционирования текущей программы и ее оригинала до подтверждения адекватности средств защиты. Это важно, если используются устройства с низким уровнем защищенности, когда возможен обход проверок, связанных с защитой.

12.8. Водяные знаки

Использование водяных знаков как метода выявления подделки занимает особое место, поскольку препятствует созданию точной копии, которую пользователь не мог бы отличить от оригинала.

12.9. Психологические методы защиты

Эти методы основаны на том, чтобы создать у нарушителя чувство неуверенности и психологического напряжения, заставляя его все время помнить, что в похищенном программном продукте могут сохраняться средства защиты. Поэтому полезно было бы дать объявление, что в программное обеспечение встроены механизмы защиты (независимо от того, так ли это на самом деле). Существует огромное число хитроумных способов расстановки отличительных меток в программе и никакой хакер не может быть уверен, что ему удалось уничтожить все ключи и механизмы защиты.

12.10. Способы защиты информации

Задачей технических средств защиты информации является либо ликвидация каналов утечки информации, либо снижение качества получаемой злоумышленником информации. Основным показателем качества речевой информации считается разборчивость – слоговая, словесная, фразовая и др. Чаще всего используют слоговую разборчивость, измеряемую в процентах. Принято считать, что качество акустической информации достаточное, если обеспечивается около 40 % слоговой разборчивости. Если разобрать разговор практически невозможно (даже с использованием современных технических средств повышения разборчивости речи в шумах), то слоговая разборчивость соответствует около 1–2 %.

Предупреждение утечки информации по акустическим каналам сводится к пассивным и активным способам защиты. Соответственно, все приспособления защиты информации можно смело разделить на два больших класса – пассивные и активные. Пассивные – измеряют, определяют, локализуют каналы утечки, ничего не внося при этом во внешнюю среду. Активные – «зашумляют», «выжигают», «раскачивают» и уничтожают всевозможные спецсредства негласного получения информации.

Пассивное техническое средство защиты – устройство, обеспечивающее скрытие объекта защиты от технических способов разведки путем поглощения, отражения или рассеивания его излучений. К пассивным техническим средствам защиты относятся экранирующие устройства и сооружения, маски различного назначения, разделительные устройства в сетях электроснабжения, защитные фильтры и т. д. Цель пассивного способа – максимально ослабить акустический сигнал от источника звука, например, за счет отделки стен звукопоглощающими материалами.

По результатам анализа архитектурно-строительной документации формируется комплекс необходимых мер по пассивной защите тех или иных участков. Перегородки и стены по возможности должны быть слоистыми, материалы слоев – подобраны с резко отличающимися акустическими характеристиками (например, бетон—поролон). Для уменьшения мембранного переноса желательно, чтобы они были массивными. Кроме того, разумнее устанавливать двойные двери с воздушной прослойкой между ними и уплотняющими прокладками по периметру косяка. Для защиты окон от утечки информации их лучше делать с двойным остеклением, применяя звукопоглощающий материал и увеличивая расстояние между стеклами для повышения звукоизоляции, использовать шторы или жалюзи. Желательно оборудовать стекла излучающими вибродатчиками. Различные отверстия во время ведения конфиденциальных разговоров следует перекрывать звукоизолирующими заслонками.

Другим пассивным способом пресечения утечки информации является правильное устройство заземления технических средств передачи информации. Шина заземления и заземляющего контура не должна иметь петель, и ее рекомендуется выполнять в виде

ветвящегося дерева. Магистрали заземления вне здания следует прокладывать на глубине около 1,5 м, а внутри здания – по стенам или специальным каналам (для возможности регулярного осмотра). В случае подключения к магистрали заземления нескольких технических средств соединять их с магистралью нужно параллельно. При устройстве заземления нельзя применять естественные заземлители (металлические конструкции зданий, имеющие соединение с землей, проложенные в земле металлические трубы, металлические оболочки подземных кабелей и т. д.).

Так как обычно разнообразные технические приборы подключены к общей сети, то в ней возникают различные наводки. Для защиты техники от внешних сетевых помех и защиты от наводок, создаваемых самой аппаратурой, необходимо использовать сетевые фильтры. Конструкция фильтра должна обеспечивать существенное снижение вероятности возникновения внутри корпуса побочной связи между входом и выходом из-за магнитных, электрических либо электромагнитных полей. При этом однофазная система распределения электроэнергии должна оснащаться трансформатором с заземленной средней точкой, трехфазная – высоковольтным понижающим трансформатором.

Экранирование помещений позволяет устранить наводки от технических средств передачи информации (переговорных комнат, серверных и т. п.). Лучшими являются экраны из листовой стали. Но применение сетки значительно упрощает вопросы вентиляции, освещения и стоимости экрана. Чтобы ослабить уровни излучения технических средств передачи информации примерно в 20 раз, можно рекомендовать экран, изготовленный из одинарной медной сетки с ячейкой около 2,5 мм либо из тонколистовой оцинкованной стали толщиной 0,51 мм и более. Листы экранов должны быть между собой электрически прочно соединены по всему периметру. Двери помещений также необходимо экранировать, с обеспечением надежного электроконтакта с дверной рамой по всему периметру не реже, чем через 10–15 мм. При наличии в помещении окон их затягивают одним или двумя слоями медной сетки с ячейкой не более 2 мм. Слои должны иметь хороший электроконтакт со стенками помещения.

Активное техническое средство защиты – устройство, обеспечивающее создание маскирующих активных помех (или имитирующих их) для средств технической разведки или нарушающие нормальное функционирование средств негласного съема информации. Активные способы предупреждения утечки информации можно подразделить на обнаружение и нейтрализацию этих устройств.

К активным техническим средствам защиты относятся также различные имитаторы, средства постановки аэрозольных и дымовых завес, устройства электромагнитного и акустического зашумления и другие средства постановки активных помех. Активный способ предупреждения утечки информации по акустическим каналам сводится к созданию в «опасной» среде сильного помехового сигнала, который сложно отфильтровать от полезного.

Современная техника подслушивания дошла до такого уровня, что становится очень сложно обнаружить приборы считывания и прослушивания. Самыми распространенными методами выявления закладочных устройств являются: визуальный осмотр; метод нелинейной локации; металлодетектирование; рентгеновское просвечивание.

Проводить специальные меры по обнаружению каналов утечки информации и дорого, и долго. Поэтому в качестве средств защиты информации часто выгоднее

использовать устройства защиты телефонных переговоров, генераторы пространственного зашумления, генераторы акустического и виброакустического зашумления, сетевые фильтры. Для предотвращения несанкционированной записи переговоров используют устройства подавления диктофонов.

Подавители диктофонов (также эффективно воздействующие и на микрофоны) применяют для защиты информации с помощью акустических и электромагнитных помех. Они могут воздействовать на сам носитель информации, на микрофоны в акустическом диапазоне, на электронные цепи звукозаписывающего устройства. Существуют стационарные и носимые варианты исполнения различных подавителей.

В условиях шума и помех порог слышимости для приема слабого звука возрастает. Такое повышение порога слышимости называют акустической маскировкой. Для формирования виброакустических помех применяются специальные генераторы на основе электровакуумных, газоразрядных и полупроводниковых радиоэлементов.

На практике наиболее широкое применение нашли генераторы шумовых колебаний. Шумогенераторы первого типа применяются для подавления непосредственно микрофонов как у радиопередающих устройств, так и у диктофонов, т. е. такой прибор банально вырабатывает некий речеподобный сигнал, передаваемый в акустические колонки и вполне эффективно маскирующий человеческую речь. Кроме того, такие устройства применяются для борьбы с лазерными микрофонами и стетоскопическим прослушиванием. Надо отметить, что акустические шумогенераторы – едва ли не единственное средство для борьбы с проводными микрофонами. При организации акустической маскировки следует помнить, что акустический шум создает дополнительный дискомфорт для сотрудников, для участников переговоров (обычная мощность генератора шума составляет 75–90 дБ), однако в этом случае удобство должно быть принесено в жертву безопасности.

Известно, что «белый» или «розовый» шум, используемый в качестве акустической маскировки, по своей структуре имеет отличия от речевого сигнала. На знании и использовании этих отличий как раз и базируются алгоритмы шумоочистки речевых сигналов, широко используемые специалистами технической разведки. Поэтому наряду с такими шумовыми помехами в целях активной акустической маскировки сегодня применяют более эффективные генераторы «речеподобных» помех, хаотических последовательностей импульсов и т. д. Роль устройств, преобразующих электрические колебания в акустические колебания речевого диапазона частот, обычно выполняют малогабаритные широкополосные акустические колонки. Они обычно устанавливаются в помещении в местах наиболее вероятного размещения средств акустической разведки.

«Розовый» шум – сложный сигнал, уровень спектральной плотности которого убывает с повышением частоты с постоянной крутизной, равной 3–6 дБ на октаву во всем диапазоне частот. «Белым» называется шум, спектральный состав которого однороден по всему диапазону излучаемых частот. То есть такой сигнал является сложным, как и речь человека, и в нем нельзя выделить какие-то преобладающие спектральные составляющие. «Речеподобные» помехи формируются путем микширования в различных сочетаниях отрезков речевых сигналов и музыкальных фрагментов, а также шумовых помех, или из фрагментов самого скрываемого речевого сигнала при многократном наложении с различными уровнями (наиболее эффективный способ).

Системы ультразвукового подавления излучают мощные неслышимые человеческим ухом ультразвуковые колебания (около 20 кГц). Данное ультразвуковое воздействие приводит к перегрузке усилителя низкой частоты диктофона и к значительным искажениям записываемых (передаваемых) сигналов. Но опыт использования этих систем показал их несостоятельность. Интенсивность ультразвукового сигнала оказывалась выше всех допустимых медицинских норм воздействия на человека. При снижении интенсивности ультразвука невозможно надежно подавить подслушивающую аппаратуру.

Акустический и виброакустический генераторы вырабатывают шум (речеподобный, «белый» или «розовый») в полосе звуковых сигналов, регулируют уровень шумовой помехи и управляют акустическими излучателями для постановки сплошной шумовой акустической помехи. Вибрационный излучатель служит для постановки сплошной шумовой вибропомехи на ограждающие конструкции и строительные коммуникации помещения. Расширение границ частотного диапазона помеховых сигналов позволяет снизить требования к уровню помехи и снизить словесную разборчивость речи.

На практике одну и ту же поверхность приходится зашумлять несколькими виброизлучателями, работающими от разных, некоррелированных друг с другом источников помеховых сигналов, что явно не способствует снижению уровня шумов в помещении. Это связано с возможностью использования метода компенсации помех при подслушивании помещения. Данный способ заключается в установке нескольких микрофонов и двух– или трехканальном съеме смеси скрываемого сигнала с помехой в пространственно разнесенных точках с последующим вычитанием помех.

Электромагнитный генератор (генератор второго типа) наводит радиопомехи непосредственно на микрофонные усилители и входные цепи диктофона. Данная аппаратура одинаково эффективна против кинематических и цифровых диктофонов. Как правило, для этих целей применяют генераторы радиопомех с относительно узкой полосой излучения, чтобы снизить воздействие на обычную радиоэлектронную аппаратуру (они практически не оказывают воздействия на работу сотовых телефонов стандарта GSM, при условии, что связь по телефону была установлена до включения подавителя). Электромагнитную помеху генератор излучают направленно, обычно это конус 60–70°. А для расширения зоны подавления устанавливают вторую антенну генератора или даже четыре антенны.

Следует знать, что при неудачном расположении подавителей могут возникать ложные срабатывания охранной и пожарной сигнализации. Приборы с мощностью больше 5–6 Вт не проходят по медицинским нормам воздействия на человека.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Изучить теоретический материал.
2. Ответить на контрольные вопросы.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое защита?
2. Что такое собственная защита программ?
3. Средства собственной защиты программ.
4. Почему документация может выполнять функции защиты?
5. Ограниченное применение как способ защиты.
6. Заказное проектирование как способ защиты.
7. Отличительные метки как способ защиты.

8. Что такое активная защита?
9. Классификация средств активной защиты.
10. Активная внутренняя защита.
11. Виды активной внутренней защиты.
12. Активная внешняя защита.
13. Виды активной внешней защиты.
14. Что относится к средствам пассивной защиты?
15. Идентификация программ как метод пассивной защиты.
16. Выделение объективных характеристик программы.
17. Опишите понятие "Родимые пятна".
19. Устройства контроля как метод пассивной защиты.
20. Водяные знаки как метод пассивной защиты.
21. Психологические методы защиты.

Тема 13. Шифрование методом перестановки. Кодирование.

Элементы информационных объектов представляются элементами данных по определенному закону. Кодирование — процесс не случайный. Он происходит согласно избранному информационному методу, который исполняет роль метода кодирования.

Метод кодирования информации устанавливает соответствие между элементами записываемого информационного объекта и элементами данных, полученных в результате записи.

Выбор метода кодирования информации — важный вопрос технологического раздела информатики. Он должен быть согласован с выбором инструмента и материала записи. Он также должен удовлетворять критериям, о которых сказано выше.

Для удобства изучения методы кодирования информации принято рассматривать по категориям. Роль этих категорий выполняют так называемые схемы кодирования.

Существуют три основные схемы кодирования. Это аналоговое, табличное и цифровое кодирование.

Схемы аналогового кодирования распространены в живой природе. В ходе развития научно-технического прогресса общество постепенно адаптировало их под свои нужды. Именно аналоговое кодирование нашло наиболее раннее применение при записи изображений, звука, видео.

Схемы табличного кодирования не имеют и не могут иметь реализаций в живой природе — это изобретение общества. Люди пользуются табличным кодированием с того момента как научились на пальцах обозначать предметы, животных, людей. На табличном кодировании основаны все виды письменности. Табличное кодирование обеспечивает большинство потребностей неавтоматизированного общественного информационного обмена.

Среди табличных схем кодирования особо выделяют две самостоятельные категории:

схемы таблично-символьного кодирования;

схемы таблично-цифрового кодирования.

Таблично-символьное кодирование широко используют при непосредственном информационном обмене, а схемы табличного и цифрового кодирования применяют, когда информационный обмен между людьми осуществляется с помощью средств

вычислительной техники. Например, для обмена письменными сообщениями достаточно схем символьного кодирования. Но если сообщение должно быть отправлено по телеграфу или по электронной почте, то без цифрового кодирования не обойтись.

Цифровое кодирование не имеет реализаций ни в живой природе, ни в непосредственном информационном обмене между людьми. Это достижение современного общества. Применяется оно в системах автоматического информационного обмена и действует при сохранении информации или при её передаче между техническими устройствами.

Шифрование перестановкой заключается в том, что символы открытого текста переставляются по определенному правилу в пределах некоторого блока этого текста. Данные преобразования приводят к изменению только порядка следования символов исходного сообщения.

При достаточной длине блока, в пределах которого осуществляется перестановка, и сложном неповторяющемся порядке перестановки можно достигнуть приемлемой для простых практических приложений стойкости шифра.

Шифрование методами перестановки

Шифрование перестановкой заключается в том, что символы открытого текста переставляются по определенному правилу в пределах некоторого блока этого текста. Данные преобразования приводят к изменению только порядка следования символов исходного сообщения.

При достаточной длине блока, в пределах которого осуществляется перестановка, и сложном неповторяющемся порядке перестановки можно достигнуть приемлемой для простых практических приложений стойкости шифра.

Метод простой перестановки

При шифровании методом простой перестановки производят деление открытого текста на блоки одинаковой длины равной длине ключа. Ключ длины *n* представляет собой последовательность неповторяющихся чисел от 1 до *n*. Символы открытого текста внутри каждого из блоков переставляют в соответствие с символами ключа. Элемент ключа Ki в заданной позиции блока говорит о том, что на данное место будет помещен символ открытого текста с номером Ki из соответствующего блока.

Пример 4.

Зашифруем открытый текст «ПРИЕЗЖАЮДНЕМ» методом перестановки с ключом К=3142.

п	р	и	е	з	ж	а	ю	д	н	е	м
и	п	е	р	а	з	ю	ж	е	д	м	н

Для дешифрования шифротекста необходимо символы шифротекста перемещать в позицию, указанную соответствующим им символом ключа Ki.

Например, зашифруем текст

ГРУЗИТЕ_АПЕЛЬСИНЫ_БОЧКАХ блоком размером 8*3 и ключом 5- 8-1-3-7-4-6-2.

Таблица простой перестановки будет иметь вид:

Ключ							
5	8	1	3	7	4	6	2
Г	Р	У	З	И	Т	Е	_
А	П	Е	Л	Ь	С	И	Н
Ы	_	Б	О	Ч	К	А	Х

Зашифрованное сообщение:
УЕБ_НХЗЛОЕСЛГАЫЕИАИЬЧРП_

Перестановка, усложненная по таблице

При усложнении перестановки по таблицам для повышения стойкости шифра в таблицу перестановки вводятся неиспользуемые клетки таблицы. Количество и расположение неиспользуемых элементов является дополнительным ключом шифрования.

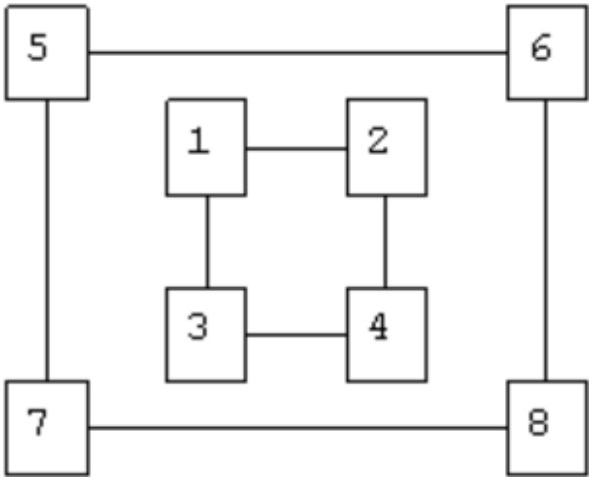
При шифровании текста в неиспользуемые элементы не заносятся символы текста и в зашифрованный текст из них не записываются никакие символы - они просто пропускаются. При расшифровке символы зашифрованного текста также не заносятся в неиспользуемые элементы.

Для дальнейшего увеличения криптостойкости шифра можно в процессе шифрования менять ключи, размеры таблицы перестановки, количество и расположение неиспользуемых элементов по некоторому алгоритму, причем этот алгоритм становится дополнительным ключом шифра.

Перестановка, усложненная по маршрутам

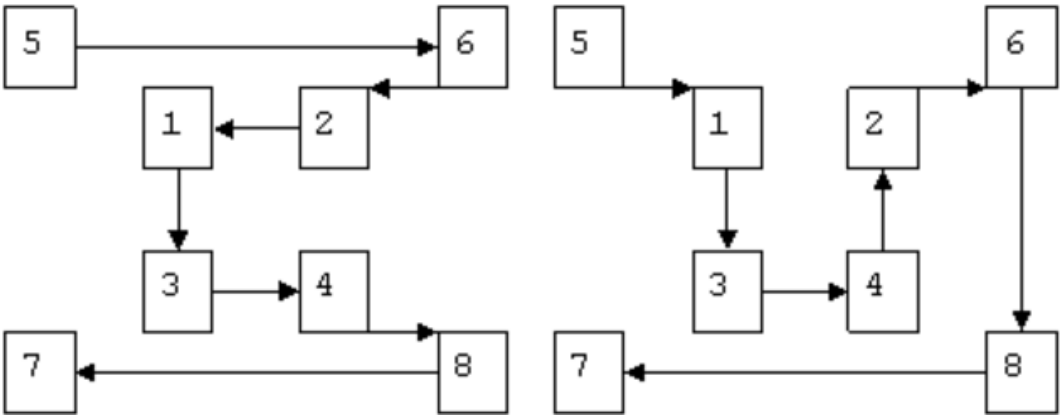
Высокую стойкость шифрования можно обеспечить усложнением перестановок по маршрутам типа гамильтоновских. При этом для записи символов шифруемого текста используются вершины некоторого гиперкуба, а знаки зашифрованного текста считываются по маршрутам Гамильтона, причем используются несколько различных маршрутов. Для примера рассмотрим шифрование по маршрутам Гамильтона при n=3.

Структура трехмерного гиперкуба:



Номера вершин куба определяют последовательность его заполнения символами шифруемого текста при формировании блока. В общем случае n- мерный гиперкуб имеет n^2 вершин.

Маршруты Гамильтона имеют вид:



Последовательность перестановок символов в шифруемом блоке для первой схемы 5-6-2-1-3-4-8-7, а для второй 5-1-3-4-2-6-8-7. Аналогично можно получить последовательность перестановок для других маршрутов: 5- 7-3-1-2-6-8-4, 5-6-8-7-3-1-2-4, 5-1-2-4-3-7-8-6 и т.д.

Размерность гиперкуба, количество вид выбираемых маршрутов Гамильтона составляют секретный ключ метода.

Стойкость простой перестановки однозначно определяется размерами используемой матрицы перестановки. Например, при использовании матрицы 16*16 число возможных перестановок достигает 1.4E26. Такое число вариантов невозможно перебрать даже с использованием ЭВМ. Стойкость усложненных перестановок еще выше. Однако следует иметь в виду, что при шифровании перестановкой полностью сохраняются вероятностные характеристики исходного текста, что облегчает криптоанализ.

Кодирование и шифрование информации.

В современном обществе успех любого вида деятельности сильно зависит от обладания определенными сведениями (информацией) и от отсутствия их (ее) у конкурентов. Чем сильней проявляется указанный эффект, тем больше потенциальные убытки от злоупотреблений в информационной сфере и тем больше потребность в защите информации. Одним словом, возникновение индустрии обработки информации привело к возникновению индустрии средств ее защиты и к актуализации самой проблемы защиты информации, проблемы информационной безопасности.

Одна из наиболее важных задач (всего общества) – задача кодирования сообщений и шифрования информации.

Вопросами защиты и скрытия информации занимается наука **криптология** (*криптос*– тайный,*логос*– наука).

Криптология имеет два основных направления – криптографию и криптоанализ. Цели этих направлений противоположны. Криптография занимается построением и исследованием математических методов преобразования информации, а криптоанализ – исследованием возможности расшифровки информации без ключа. Термин "криптография" происходит от двух греческих слов: *криптос* и *грофейн*– писать. Таким образом, это тайнопись, система перекодировки сообщения с целью сделать его непонятным для непосвященных лиц и дисциплина, изучающая общие свойства и принципы систем тайнописи.

Основные понятия кодирования и шифрования

Код – правило соответствия набора знаков одного множества X знакам другого множества Y. Если каждому символу X при кодировании соответствует отдельный знак Y, то это кодирование. Если для каждого символа из Y однозначно отыщется по некоторому правилу его прообраз в X, то это правило называется декодированием.

Кодирование – процесс преобразования букв (слов) алфавита X в буквы (слова) алфавита Y.

При представлении сообщений в ЭВМ все символы кодируются байтами.

Пример 1.

Если каждый цвет кодировать двумя битами, то можно закодировать не более $2^2 = 4$ цветов, тремя – $2^3 = 8$ цветов, восемью битами (байтом) – $2^8=256$ цветов. Для кодирования всех символов на клавиатуре компьютера достаточно 8 байтов.

Сообщение, которое мы хотим передать адресату, назовем **открытым сообщением.** Оно, естественно, определено над некоторым алфавитом.

Зашифрованное сообщение может быть построено над другим алфавитом. Назовем его **закрытым сообщением**. Процесс преобразования открытого сообщения в закрытое сообщение и есть **шифрование**.

Если **A**– открытое сообщение, **B**– закрытое сообщение (шифр) ,**f** – правило шифрования, то **f(A) = B**.

Правила шифрования должны быть выбраны так, чтобы зашифрованное сообщение можно было расшифровать. Однотипные правила (например, все шифры типа шифра Цезаря, по которому каждый символ алфавита кодируется отстоящим от него на n позиций символом) объединяются в классы, и внутри класса определяется некоторый параметр (числовой, символьный табличный и т.д.), позволяющий перебирать (варьировать) все правила. Такой параметр называется шифровальным ключом. Он, как правило, секретный и сообщается лишь тому, кто должен прочесть зашифрованное сообщение (обладателю ключа).

При кодировании нет такого секретного ключа, так как кодирование ставит целью лишь более сжатое, компактное представление сообщения.

Если **k**– ключ, то можно записать **f(k(A)) = B**. Для каждого ключа **k**, преобразование **f(k)** должно быть обратимым, то есть **f(k(B)) = A**. Совокупность преобразования **f(k)** и соответствия множества **k** называется **шифром**.

Тема 14. Методы разграничения доступа и методы защиты дисков.

Цель: освоение средств администратора защищенных версий ОС Windows, изучение методов защиты дисков.

1. Регистрация пользователей и групп в системе
2. Определение их привилегий
3. Определение параметров политики безопасности, относящихся к аутентификации и авторизации пользователей при интерактивном входе
4. Защита дисков

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Информационная безопасность - это комплекс мероприятий, обеспечивающий для охватываемой им информации следующие факторы:

- конфиденциальность - возможность ознакомиться с информацией имеют в своем распоряжении только те лица, кто владеет соответствующими полномочиями;

- целостность - возможность внести изменение в информацию должны иметь только те лица, кто на это уполномочен;
- доступность - возможность получения авторизованного доступа к информации со стороны уполномоченных лиц в соответствующий санкционированный для работы период времени.

Под защитой информации подразумевается комплекс мероприятий, проводимых с целью предотвращения от действий угроз безопасности информации, где угроза является потенциальной возможностью нарушения безопасности информации.

Возникновение проблемы обеспечения информационной безопасности при подключении организаций к мировым открытым сетям напрямую связано с их основными достоинствами - оперативностью, открытостью, глобальностью.

В общем виде основными угрозами информационной безопасности при подключении к Internet являются:

1. Несанкционированный (неавторизированный) доступ (НДС) внешних пользователей сети Internet к какому-либо виду сервисного обслуживания, предоставляемого легальным пользователям (подобная угроза возникнет, если пользователи некоторых банковских сетей попытаются воспользоваться сервисом telnet, позволяющим выполнять на удаленном компьютере команды, как если бы эти пользователи сидели за терминалом, непосредственно подключенном к данному компьютеру);

2. Доступ к информации и базам данных организаций без идентификации (установление тождественности неизвестного объекта известному, на основании совпадения признаков; опознание) и аутентификации (процедура проверки подлинности, например: проверка подлинности пользователя путём сравнения введённого им пароля с паролем, сохранённым в базе данных пользователей) внешнего пользователя в сети, включая проникновение к ресурсам абонентов в абонентских пунктах или на хосты с целью НСД к информации, ее разрушения или искажения.

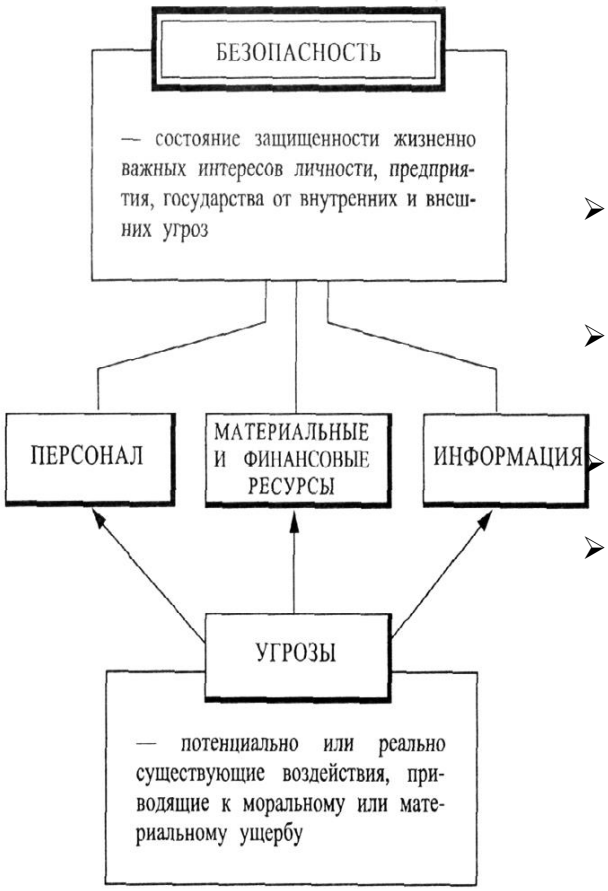
Несанкционированный доступ к информации (НСД) - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Новые терминологические определения видам информационных преступлений:

- «компьютерные преступления»,
- «коммуникационные преступления»,
- «кибербандитизм».

Безопасность - это состояние защищенности жизненно важных интересов личности, предприятия, государства от внутренних и внешних угроз.

Компоненты безопасности - персонал, материальные и финансовые средства и информация (рисунок 1).



Анализ состояния дел в сфере защиты информации показывает, что уже сложилась вполне сформировавшаяся концепция и структура защиты, основу которой составляют:

- весьма развитый арсенал технических средств защиты информации, производимых на промышленной основе;
- значительное число фирм, специализирующихся на решении вопросов ЗИ;
- достаточно четко очерченная система взглядов на эту проблему;
- наличие значительного практического опыта и другое.

И тем не менее, злоумышленные действия над информацией не только не уменьшаются, но и имеют достаточно устойчивую тенденцию к росту. Опыт показывает, что для борьбы с этой тенденцией необходима стройная и целенаправленная организация процесса защиты информационных ресурсов.

Таким образом, система защиты информации - это организованная совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз.

Удовлетворить современные требования по обеспечению безопасности предприятия и защиты его конфиденциальной информации может только система безопасности предприятия. Под системой безопасности понимается организованная совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз (рисунок 2).

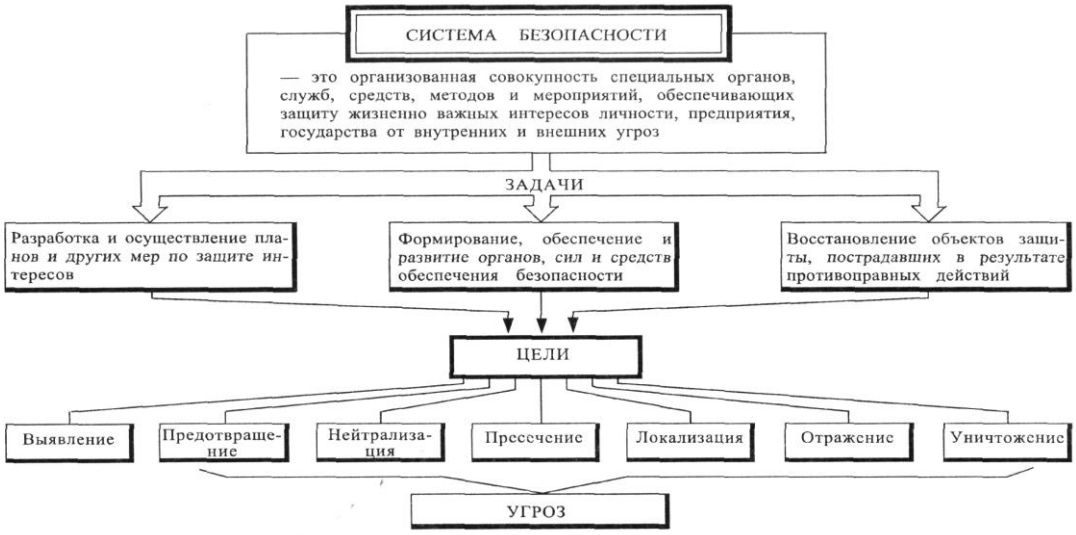


Рисунок 2 - Структура системы безопасности предприятия

Как и любая система, система информационной безопасности имеет свои цели, задачи, методы и средства деятельности, которые согласовываются по месту и времени в зависимости от условий.

Понимая информационную безопасность как «состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций», правомерно определить угрозы безопасности информации и их цели, а также иные условия и действия, нарушающие безопасность (рисунок 3).

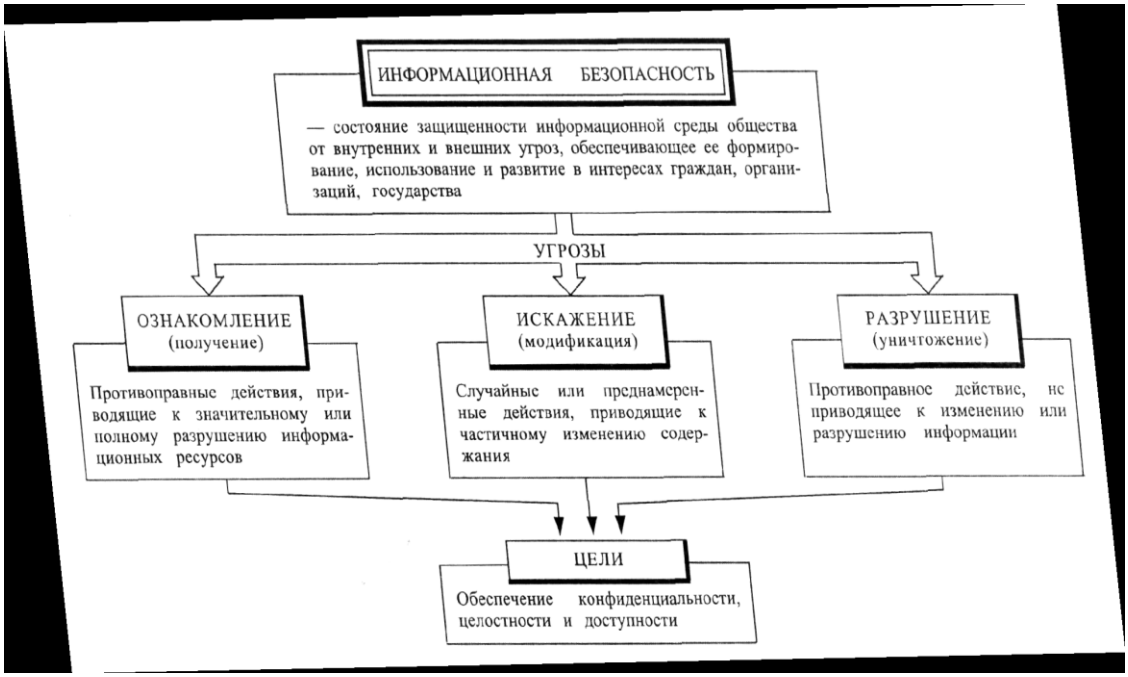


Рисунок 3 – Структура угроз информационной безопасности

Существуют следующие способы аутентификации пользователей:

К первой группе относятся способы аутентификации, основанные на том, что пользователь знает некоторую подтверждающую его подлинность информацию (парольная аутентификация и аутентификация на основе модели «рукопожатия»).

Ко второй группе относятся способы аутентификации, основанные на том, что пользователь имеет некоторый материальный объект, который может подтвердить его подлинность (например, пластиковую карту с идентифицирующей пользователя информацией).

К третьей группе относятся способы аутентификации, основанные на таких данных, которые позволяют однозначно считать, что пользователь и есть тот самый субъект, за которого себя выдает (биометрические данные, особенности клавиатурного почерка и росписи мышью и т.п.).

Слабость парольной аутентификации.

Чтобы пароль был запоминающимся, его зачастую делают простым (имя подруги, название спортивной команды и т.п.). 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, запрограммировав полный перебор (предполагается, что алгоритм шифрования известен)

Надежность аутентификации может быть повышена с помощью паролей следующим образом:

- 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");

Реакция системы на попытку подбора паролей может быть следующей:

- ограничение числа попыток входа в систему;
- скрытие логического имени последнего работавшего пользователя (знание логического имени может помочь нарушителю подобрать или угадать его пароль);
- учет всех попыток (успешных и неудачных) входа в систему в журнале аудита.

Защита дисков.

Вопрос о защите МД возник вместе с появлением в составе РС НМД, что произошло в 1978 г. (компьютер Apple).

Вопрос защиты МД решался схемно. Схема расстраивала работу утилиты копирования, поставляемой разработчиком, путем изменения формата записи.

Проанализировать и решить такую защиту может только квалифицированный инженер.

Методы защиты МД используют 2 принципа:

- препятствие копированию на другой диск (защита от копирования);
- препятствие просмотру или операции обратного ассемблирования (защита от просмотра).

Первый принцип защищает программу от несанкционированного воспроизведения. Второй от несанкционированной проверки. Эти принципы не являются взаимосвязанными. Коммерческие программы, как правило, используют оба вида защиты.

Простейший метод защиты диска от копирования сводится к защите от утилиты копирования.

Для этого можно изменить формат диска, чтобы утилита копирования не могла его распознать. Один из вариантов – сохранение на диске пустой неформатированной дорожки или сектора.

Утилита копирования сбивается на такой дорожке и копирование прекращается.

Для работы с такими дисками ДОС должна быть модифицирована с учетом формата дисков.

При нестандартном форматировании можно изменять (уменьшать) число секторов, дорожек, а также их размер.

Путем внесения изменений в подсчет контрольных сумм можно добиться защиты от копирования, так как при несовпадении КС записанной и полученной при считывании сектор считается неверно считанным. Таким образом, диск может использоваться только собственной, модифицированной ДОС.

Аналогично можно вносить изменения в коды пролога и эпилога.

Обойти рассмотренные методы защиты может программа побитового копирования, которая минимально использует идентифицирующую информацию диска. Она с произвольной точки выполняет побитовое считывание с диска. Правильность операции проверяется считыванием и сравнением.

Сложные механизмы защиты включают в себя использование сигнатур. Сигнатура – это вторичный признак диска, используемый в качестве идентификационной метки диска – оригинала.

Он не копируется программным способом. То есть программа – копировщик не в состоянии скопировать ее.

К сигнатурным методам защиты, относятся:

1. Сигнатура внутренней дорожки. Стандарт использования предусматривает использование 0-39 дорожки для IBM PC (0-34 для APPLE PC). Если в защищенной программе предусмотреть использование (форматирование) внутренних дорожек, то их можно использовать как сигнатуры, подтверждающие оригинальность диска. Там можно разместить каталог диска, который не прочтется при стандартном копировании.

2. Сигнатура промежуточных дорожек. Путем установления головок в промежуточное положение можно записать информацию в промежуточных дорожках (не используя стандартных). Стандартная копирующая программа не может прочитать информацию с промежуточных дорожек.

3. Синхронизация дорожек. Если при стандартном форматировании 0-сектор расположен в произвольном месте, то на диске с синхронизированными дорожками 0-сектора располагаются регулярно.

Синхронизация должна быть поддержана программой форматирования. При загрузке с диска программа самозагрузки проверяет относительное положение 0-сектора, путем регистрации времени задержки, если задержка не соответствует ожидаемой самозагрузка отменяется.

4. Проверка на блокировку Зп. Простейший способ защиты Зп – заклеить прорезь, которая выполняет роль сигнатуры.

Основная цель сигнатурных методов - создать дополнительные трудности при копировании дисков путем учета их особенностей. При копировании стандартными

средствами создается неработоспособная копия. Эти методы рассчитаны на использование стандартных носителей

Другой путь защиты – сделать носитель уникальным, то есть сопроводить его уникально идентифицирующей сигнатурой. На этом подходе строятся следующие методы защиты:

Подсчет битов.

1. Подсчет битов основан на разности скоростей вращения дисков. Полное число битов на дорожку зависит от скорости вращения диска. Эти биты подсчитываются и записываются в дескриптор диска. Программа - загрузчик подсчитывает число битов при загрузке и сравнивает с содержимым дескриптора, проверял оригинальность диска. У диска - копии данные загрузчика не совпадут с содержимым дескриптора. Можно отформатировать диск с различным числом битов на дорожку, создав, таким образом, уникальный диск.

Практически невозможно преодолеть защиту от сигнатуры, регистрирующей количество битов от индексного отверстия до заданного сектора.

2.Случайные сигнатуры. В качестве сигнатуры может быть выбрана любая область диска, которая дублируется в произвольной части диска. При загрузке области сравниваются на идентичность.

3.Нарушение синхронизации основано на введении дополнительных битов при записи на диск и использование их в качестве сигнатур. Сигнатурное копирование прерывается при обнаружении “лишних” битов.

4. Регистрационные номера. Если каждому диску присвоить свой регистрационный № и хранить его в нескольких местах на диске, его можно использовать в качестве уникального дескриптора диска. Программа – анализатор должна быть зашифрована и разнесена с дескриптором.

5. Коллизия имен. Система учета запрашивает при первом обращении к диску название фирмы – пользователя и распечатывает его при последующем использовании.

6. Зашифрованные дескрипторы. Дескриптор диска зашифровывается, но не засекречивается. Сигнатура состоит в выявлении участков с нарушением синхронизации участков диска. Программа загрузки выявляет нарушение синхронизации, составляет их список, формулирует дескриптор, проверяет его на соответствие с записанным на диске.

7. Маскировка дорожек использует принцип вложенного шифрования. Каждый новый уровень расшифровывает предшествующий.

Карты копирования.

Наиболее уязвимой является программа во время ее исполнения, так как она находится в ОЗУ. Защитное ПО должно препятствовать проникновению в программу при ее исполнении.

В 1982 г создана 1-я карта копирования для PC Apple II. Это программно-аппаратное средство. При попытке копирования программа переносится в ОЗУ и начинает выполнятся. Срабатывает переключатель, который вызывает прерывание МП. Карта копирования изменяет адрес прерывания, управление передается карте управления, где записывается состояние PC в момент прерывания, которое сохраняется на резервном диске.

Перспективные механизмы защиты.

1. Преднамеренное разрушение поверхности основано на частичном разрушении поверхности носителя и использовании этой информации в качестве сигнатуры.

2. Использование дисководов с переменной программно – управляемой скоростью.

3. Хранение программ на жестких дисках в зашифрованном виде и др.

Анализ методов защиты дисков.

Преимущества методов защиты дисков – учитываются интересы разработчиков, а не пользователей:

- они легко воспроизводятся;
- обеспечивают высокую степень защиты;
- не требуют заполнения информации по защите;
- позволяют использовать заказное ПО.

Недостатки:

- отказ от стандартных процедур дублирования;
- зависимость пользователя от изготовителя;
- трудности при замене дисков и переносе программ;
- нестандартные ОС;
- снижение надежности;
- меньшая доступность;
- высокая стоимость.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Задание 1. Освоить средства регистрации пользователей.

Войти в систему с правами администратора.

- открыть список зарегистрированных пользователей (Панель управления | Администрирование | Управление компьютером | Локальные пользователи и группы | Пользователи);
- с помощью команды контекстного меню (Новый пользователь) создать для себя учетную запись с произвольным логическим именем, введя в качестве строки описания текст «Студент группы --»);
  - копию экранной формы создания новой учетной записи,
  - копию экранной формы со списком зарегистрированных пользователей,
  - список команд контекстного меню (при отсутствии выделения имени пользователя в списке),
  - объяснения смысла четырех дополнительных параметров создаваемой учетной записи;
- выделить имя вновь зарегистрированного пользователя и с помощью команды контекстного меню (Свойства) просмотреть ее свойства;
- включить в отчет о лабораторной работе копию экранной формы со свойствами учетной записи на вкладке «Общие» и объяснение разницы между отключением и блокировкой учетной записи;
- включить в отчет о лабораторной работе копию экранной формы со свойствами учетной записи на вкладке «Членство в группах» и ответ на вопрос, в какую группу по умолчанию включается вновь созданный пользователь;
- с помощью кнопок «Добавить», «Дополнительно» и «Поиск» включить вновь созданного пользователя также в группу «Опытные пользователи»;
- включить в отчет о лабораторной работе копии экранных форм, используемых при

добавлении пользователя в другую группу, и ответ на вопрос, как можно удалить пользователя из группы;

- включить в отчет о лабораторной работе список команд контекстного меню при выбранном имени учетной записи вместе с пояснениями их смысла, а также ответы на вопросы
  - когда должна применяться команда «Задать пароль»,
  - в чем опасность ее применения,
  - как должна происходить смена пароля пользователем.

Задание 2. Освоить средства работы с группами:

- открыть список групп (Панель управления | Администрирование | Управление компьютером | Локальные пользователи и группы | Группы);
- включить в отчет сведения об автоматически создаваемых группах пользователей, их именах и характеристиках прав их членов;
- создать новую группу в системе с именем «Начинающие пользователи» и включить в отчет о лабораторной работе копию используемого при этом экрана и сведения о порядке создания в системе новых групп пользователей, а также ответ на вопрос, в чем целесообразность разбиения множества пользователей на группы.

Задание 3. Освоить порядок назначения прав пользователям:

- открыть окно настройки прав пользователей (Панель управления | Администрирование | Локальная политика безопасности | Локальные политики | Назначение прав пользователя);
- исключить группу пользователей «Все» из числа групп, обладающих правом «Доступ к компьютеру из сети»;
- исключить пользователя «Гость» из числа пользователей, обладающих правом «Локальный вход в систему»;
- добавить группу «Начинающие пользователи» к списку пользователей, обладающих правом «Локальный вход в систему»;
- включить в отчет о лабораторной работе копии экранов, используемых при назначении прав пользователям, и сведения о порядке выполнения этих действий;
- с помощью раздела справки Windows «Назначение прав пользователя» включить в отчет о лабораторной работе пояснения отдельных привилегий пользователей системы. Обязательно ответить на вопрос, почему использование данного права должно быть ограничено.

Задание 4. Освоить определение параметров политики безопасности, относящихся к аутентификации и авторизации пользователей при интерактивном входе:

- открыть окно определения параметров безопасности для паролей (Панель управления | Администрирование | Локальная политика безопасности | Политики учетных записей | Политика паролей);
- включить в отчет о лабораторной работе сведения о порядке назначения максимального и минимального сроков действия паролей и ответ на вопрос о смысле подобных ограничений;
- включить в отчет о лабораторной работе сведения о порядке назначения минимальной длины и ограничений на сложность паролей, а также ответы на вопросы, какие и почему требования по сложности предъявляются к паролям в операционной системе Windows (с помощью справочной подсистемы);
- включить в отчет о лабораторной работе сведения о назначении параметров «Требовать

неповторяемости паролей» и «Хранить пароли всех пользователей в домене, используя обратимое шифрование» (с помощью справки Windows);

- включить в отчет о лабораторной работе копии экранных форм, используемых при определении параметров политики безопасности, относящихся к паролям;
- открыть окно определения параметров безопасности для политики блокировки учетных записей (Панель управления | Администрирование | Локальная политика безопасности | Политики учетных записей | Политика блокировки учетных записей);
- включить в отчет о лабораторной работе копии экранных форм, используемых при определении параметров политики безопасности, и сведения о назначении этих параметров.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Каковы основные цели угроз безопасности информации в компьютерных системах?
2. Насколько средства, изученные при выполнении лабораторной работы, могут нейтрализовать эти угрозы?
3. Каковы другие признаки, в соответствии с которыми может быть проведена классификация угроз безопасности в компьютерных системах?
4. Каковы основные каналы утечки конфиденциальной информации в компьютерных системах?
5. Насколько средства, изученные при выполнении лабораторной работы, могут перекрыть эти каналы?
6. Какие существуют способы аутентификации пользователей
7. В чем слабость парольной аутентификации
8. Как может быть повышена надежность аутентификации с помощью паролей
9. Какой может быть реакция системы на попытку подбора паролей
10. Кому может быть разрешен доступ по чтению и по записи к базе учетных записей пользователей
11. Как должны храниться пароли в базе учетных записей пользователей
12. В чем смысл объединения пользователей в группы

Тема 15. Методы оценки степени защиты информации. Показатели оценки уровня защиты информации.

В настоящее время, использование информации способствует развитию всех сфер деятельности государства в целом и отдельно взятого предприятия в частности, и, в конечном счете, приводит к значительным успехам в экономике, бизнесе, финансах и т.д.

Обладание ценной информацией, предоставляет существенные преимущества, при этом возлагает на ее обладателей, высокую степень ответственности за ее сохранность и защиту от возможного внешнего воздействия различного рода факторов и событий, носящих как преднамеренный, так и случайный характер. Обеспечение информационной безопасности в органах власти и организациях (далее – организации) является неотъемлемой частью общей системы управления, необходимой для достижения уставных целей и задач. Значимость систематической целенаправленной деятельности по обеспечению информационной безопасности становится тем более высокой, чем выше степень автоматизации на предприятии бизнес-процессов. Обеспечение информационной безопасности, основные требования, организационные и технические меры и процедуры

непосредственно регламентируются федеральным законодательством, и надзор за выполнением требований осуществляется органами власти.

В информационной системе объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенноцифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации. Одним из основных этапов процесса управления информационной безопасностью (ИБ) является оценка состояния системы обеспечения информационной безопасности (СОИБ).

Оценка состояния СОИБ выполняется: при осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных, оценке эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных, при проведении контроля за принимаемыми мерами по обеспечению безопасности персональных данных на этапах предпроектного обследования и аттестации государственных и иных информационных систем, обрабатывающих ИОД, не содержащую сведений составляющих государственную тайну, а также общедоступную информацию;

при оценке эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных;

при контроле выполнения требований по обеспечению безопасности ПДн при их обработке в ИСПДн.

Оценка состояния ИБ выполняется по всем ИС, функционирующим в организации. В ходе оценки состояния проверке подвергаются:

разработанные в организации организационно-распорядительные документы;

наличие и квалификация специалистов;

выполнение технических мер по защите информации для каждого сегмента ИС, обрабатывающей защищаемую информацию.

Так, для защиты информации ограниченного доступа (служебная информация, коммерческая тайна) необходимо разработать и иметь в наличии 17 документов для защищаемого помещения и 27 документов на АС. Для обеспечения безопасности ПДн операторы должны разработать и иметь в наличии от 69 до 78 документов. В свою очередь оценка соответствия состава мер защиты ИОД, не содержащей сведений, составляющих 7 государственную тайну, должна осуществляться для ИС 4-го уровня защиты как минимум по 36 параметрам, входящим в базовый набор требований, а для ИС 1-го уровня защиты – по 83 параметрам. Для общедоступной информации оценка должна проводиться по 18 параметрам. Оценка соответствия состава мер защиты для ИСПДн 4-го уровня защищенности ПДн должна выполняться по 26 параметрам, входящим в базовый набор требований, а для ИСПДн 1-го уровня защищенности ПДН – по 68 параметрам. Таким образом, если принять, что в организации имеется только по одной ИС, обрабатывающей соответственно служебную информацию, персональные данные, коммерческую тайну и общедоступную информацию, т.е. имеется четыре сегмента, то в этом случае оценке подлежат 157 – 168 организационнораспорядительных документа и 116 параметров, если в организации функционируют ИС 4-го уровня защиты и ИСПДн 4-го уровня защищенности ПДн, если в организации функционируют ИС 1-го уровня

защиты и ИСПДн 1-го уровня защищенности ПДн, то оценка должна проводиться по 282 параметрам. Результаты оценки состояния (контроля эффективности) принятых мер защиты информации должны представляться как в качественном, так и количественном формате. Следовательно, задача оценки эффективности мер защиты информации, является достаточно сложной, емкой, рутинной и требует привлечения квалифицированных экспертов (специалистов). Очевидно, решение этой задачи обусловливает необходимость применения методик базирующихся на современном математическом аппарате с возможностью автоматизации этой процедуры.

Методика оценки состояния системы обеспечения информационной безопасности организации.

Разработка методики оценки состояния информационной безопасности организации.

Методика предназначена для организации и проведения оценки состояния системы информационной безопасности на предпроектной стадии создания систем защиты информации, при проведении внутреннего (внешнего) аудита информационной безопасности, аттестации информационных систем по требованиям безопасности информации, оценки эффективности реализованных в рамках систем защиты персональных данных ИСПДн.

Методика является завершающим этапом технологии оценки состояния СОИБ и реализуется путем выполнения следующих процедур:

1 этап - Подготовка и ввод исходных данных в БД ПОС СОИБ;

2 этап - Проведение контроля реализации требований;

3 этап - Расчет комплексных показателей оценки состояния СОИБ;

4 этап - Интерпретация результатов вычислений;

5 этап - Разработка рекомендаций по совершенствованию СОИБ. На первом этапе осуществляется:

1. Первичное заполнение базы данных (БД).

В базу данных вводится следующая информация:

- перечень видов, защищаемой информации $\{h^{и}\}$. основными видами, защищаемой информации являются: служебная информация; коммерческая тайна; персональные данные; общедоступная и другие сведения конфиденциального характера в соответствии с;

- перечни требований к составу ОРД, изложенных в нормативных правовых актах $\{p^{нп}\}$ и нормативных документах $\{p^{нд}\}$ в области обеспечения информационной безопасности. Таблицы требований формируются для каждого вида, защищаемой информации. В качестве примера, в приложении Г приведены требования к составу ОРД для обеспечения безопасности персональных данных;

- перечни требований к структурным подразделениям $\{p^{с}\}$ и квалификации сотрудников данных подразделений $\{p^{к}\}$. В приложении Д представлены требования к квалификации сотрудников подразделений по ТЗИ.

- перечень типов информационных систем $\{\delta\}$. В приложении Е представлен перечень возможных типов информационных систем;

- перечень требований, предъявляемых к СЗИ информационных систем и СЗИ информационных систем персональных данных, а также к уровню защищенности персональных данных $\{p^{фп}\}$. В приложении Ж приведен перечень требований к СЗИ в

соответствии с, в приложение И к уровню защищенности персональных данных.

- классы защищенности информационных систем $\{q^{ис}\}$. Устанавливаются четыре класса защищенности информационной системы, определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс – четвертый, самый высокий – первый. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных.

Эта информация, представляет собой класс нормативно-справочной информации, которая актуальна для любых организаций.

2. Определение и ввод в БД коэффициентов весомости a_i, b_1, b_2, b_3.

Расчет значений коэффициентов весомости осуществляется на основе мнения специалистов (экспертов). Для проведения экспертной оценки формируется группа из 5 – 7 экспертов. Экспертиза проводится с использованием процедуры непосредственной оценки. Один из методов определения весов состоит в следующем. Пусть x_{ij} – оценка фактора i, данная j-ым экспертом, i = 1÷n , j = 1÷m, n – число сравниваемых объектов, m – число экспертов.

Тогда вес i-го объекта, подсчитанный по оценкам всех экспертов (w_i), равен:

$$W_i = \frac{\sum_{j=1}^{m} w_{ij}}{m},$$

где где w_{ij} – вес i-го объекта, подсчитанный по оценкам j-го эксперта, равен:

$$w_{ij} = \frac{x_{ij}}{\sum_{i}^{n} x_{ij}}$$

Для анализа разброса и согласованности оценок применяются следующие статистические характеристики – меры разброса:

а) среднее квадратическое отклонение, вычисляемое по известной формуле:

$$\sigma = \sqrt{\frac{\sum_{j=1}^{m} \left(x_j - \overline{x}_э\right)^2}{m-1}},$$

где x_j - оценка, данная j-ым экспертом; m - количество экспертов; $x_э$ - обобщенная оценка группы экспертов

$$\overline{x}_э = \frac{\sum_{j=1}^{m} x_j}{m}.$$

где x_j - оценка j-го эксперта, j = 1 ÷ m, m – число экспертов;

б) коэффициент вариации (V), который обычно выражается в процентах:

$$V = \frac{\sigma}{\overline{x}_э} \cdot 100\%.$$

Результаты вычислений оформляются в виде таблицы 3.1.

3. Ввод в базу данных характеристик ИС:

типы информационных систем, функционирующих в организации; количество информационных систем каждого типа;

классы защищенности информационных систем каждого типа.

Ввод данных осуществляется с использованием диалогового окна представленного на рисунке 3.1.

Таблица 3.1 Значения коэффициентов весомости

Обозначение коэффициента весомости	Значение коэффициента весомости	Среднее квадратическое отклонение, **(σ)**	Коэффициент вариации, **(V)**
a_1			
a_2			
a_i			
b_1			
b_2			
b_3			

Этап 2. При проведении контроля реализации требований осуществляются следующие мероприятия:

Шаг 1. Формирование анкет для проведения контроля реализации требований;

Шаг 2. Непосредственное проведение контроля реализации требований; Шаг 3. Ввод результатов контроля в БД.

Шаг 1. Проведение контроля реализации требований осуществляется методом анкетирования. С учетом имеющейся в БД информации, введенных исходных данных автоматически формируются следующие анкеты:

анкета требований к составу ОРД, изложенных в нормативных правовых актах, представлена в таблице 3.2.;

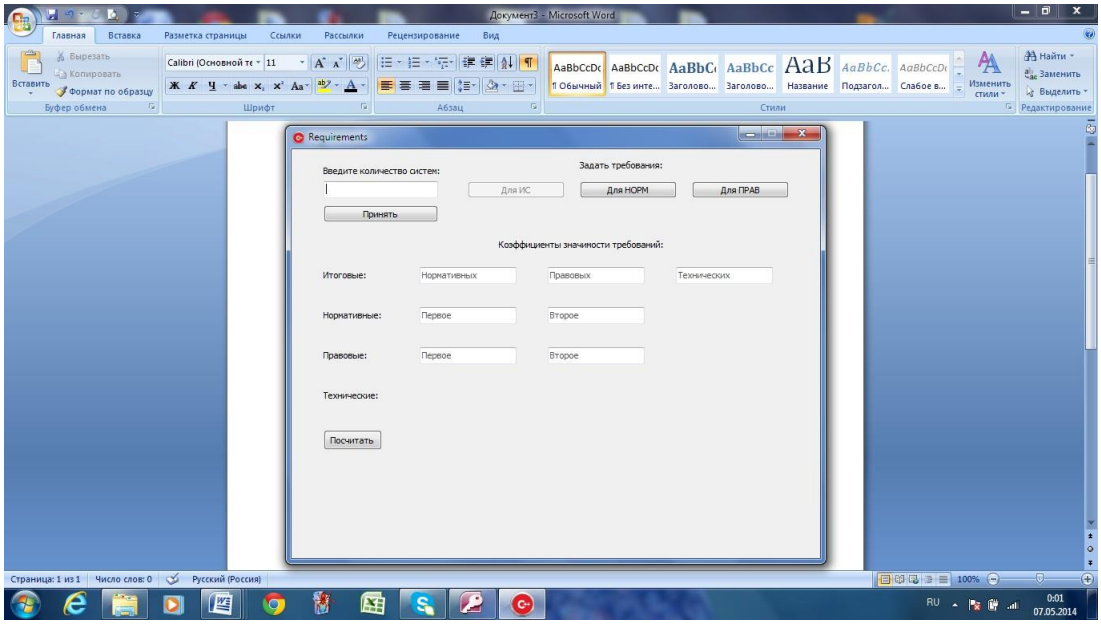


Рисунок 3.1 – Диалоговое окно ввода информации

Таблица 3.2 Анкета требований к составу ОРД, изложенных в нормативных правовых актах

Номер требования (s)	Наименование документа	Единичные показатели, фактическое выполнение требования ($р^{фнп}_{s}$)
1	Политика информационной безопасности	
2	Правила рассмотрения запросов субъектов персональных данных или их представителей	
21	Правила работы с обезличенными данными	
S = 21		

анкета требований к составу ОРД, изложенных в нормативных документах в области защиты информации. Содержание анкеты представлено в таблице 3.3;

Таблица 3.3 Анкета требований к составу ОРД, изложенных в нормативных документах

Номер требовани я (n)	Наименование документа	Единичн ые показатели, фактическое выполнение требования ($р^{фнд}_{s}$)
1		
2		
18		
N = 18		

анкета требований к уровню квалификации специалистов по ТЗИ, которая оформляется в виде таблицы 3.4;

анкета требований к составу подразделений, специалистов, обеспечивающих защиту информации в организации. Анкета оформляется в виде таблицы 3.5.

анкета требований к системе защиты информации информационной системы, в том числе ИСПДн. Данные требования определяются с учетом класса защищенности информационной системы и базового набора требований к системе защиты информации информационной системы, в том числе ИСПДн, изложенные в документах [9, 11, 12]. Содержание анкеты представлено в таблице 3.6. В приложении К приведена анкета требований к системе защиты информации информационной системы 4 класса защищенности, а в приложении Л анкета требований к системе защиты информации информационной системы персональных данных 2 класса защищенности персональных данных.

Таблица 3.4 Анкета требований к уровню квалификации специалистов по ТЗИ

N (l)	Наименова ни е должности	Номер требован ия (q^{l})	Наименование квалификационных требований к специалистам	Един ичные показатели, факти ческо е выполнени е ($р^{фl}$)
1	Главный специалист по ТЗИ	1	Высшее профессиональное образование по специальности "Информационная безопасность"	

		2	стаж работы по технической защите информации не менее 5 лет, в том числе на руководящих должностях не менее 3 лет.	
		q^1 = 2		
6	Администратор по обеспечению безопасности информации	1	Высшее профессиональное образование по специальности "Информационная безопасность"	
		2	стаж работы в должности специалиста по защите информации не менее 3 лет.	
		q^6 = 2		
I = 6				

Таблица 3.5 Анкета требований к составу подразделений, специалистов, обеспечивающих защиту информации в организации

№ п/п (m)	Наименование требования	Единичные показатели, фактическое выполнение ($p^{фс}_m$)
1	Наличие структурного подразделения	
8		
M = 8		

Количество анкет с требованиями к системам защиты информации информационных систем соответствует количеству информационных систем, функционирующих в организации.

Таблица 3.6 Анкета требований к системе защиты информации ИС (ИСПДн) класса защищенности

№ ФП r	Наименование ФП	Номер меры h_r	Наименование требуемой меры	Единичные показатели, фактическое выполнение $p^{ф}_{rh}$
1	Идентификация и аутентификация субъектов доступа и объектов доступа	1	Идентификация и аутентификация пользователей, являющихся работниками оператора	1
		2	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	0
		3		
		4		
		5	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	0
		h_1 = 5		
11	Защита информационной системы, ее средств, систем связи и передачи данных	1	Обеспечение ЗИ от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы КЗ, в том числе беспроводным каналам связи	1
		2	Запрет несанкционированной	1

			удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	
		h_{11} = 2		
R = 11				

Шаг 2. Контроль реализации требований выполняется членами комиссии, осуществляющими аудит информационной безопасности организации. В ходе контроля проверяется выполнение требований по каждой анкете и в графе

«Единичные показатели, фактическое выполнение» проставляется «1» в случае выполнения требования и «0» в противном случае.

Шаг 3. По завершении контроля реализации требований данные из анкет (графа «Единичные показатели, фактическое выполнение») вводятся в систему с использованием диалогового окна представленного на рисунке 3.1. После ввода фактических значений единичных показателей требований к СОИБ организации производится запуск на решение задачи оценки СОИБ предъявляемым требованиям.

Этап 3. После запуска задачи оценки состояния СОИБ программа по алгоритму (см. раздел 2.4 и рисунок 2.14) осуществляет расчет показателей состояния СОИБ в соответствии с выражениями (2.1 – 2.10).

Этап 4. Результаты вычислений могут выдаваться как в количественном виде с соответствующей цветовой подсветкой, так и графической форме.

На данном этапе осуществляется решение задач оценки и анализа состояния СОИБ.

При формировании значений показателей оценки в количественном виде соответствие оценки состояния, ее значения и цветовой гаммы определяется с учетом характеристик представленных в таблице 3.7.

Таблица 3.7 Характеристика состояния системы обеспечения информационной безопасности

Оценка состояния системы обеспечения информационной безопасности	Значение комплексного показателя, %	Цвет поля
«отлично»	W = 100	зелѐный
«хорошо»	70 ≤ W < 100	жѐлтый
«удовлетворительно»	40 ≤ W < 70	розовый
«неудовлетворительно»	0 ≤ W <40	красный

Вывод на экран значений комплексных показателей выполняется следующим образом.

После решения задачи на экране отображаются значения комплексных показателей соответствия, предъявляемым требованиям: СОИБ в целом; правовых, организационных и технических мер защиты информации. На экран информация выводится в виде, представленном на рисунке 3.2.

Рисунок 3.2 – Результаты оценки состояния системы обеспечения информационной безопасности организации

В случае, если полученные результаты имеют оценку «отлично», то работа на этом завершается. Если полученные результаты имеют оценку ниже «отлично», то специалист переходит в режим анализа состояния СОИБ с целью выявления слабых мест путем нажатия на соответствующую кнопку (стрелка на рисунке 3.2).

После нажатия кнопки на экран в диалоговом окне в виде, как показано на рисунке 3.3, высвечиваются подсистемы значения оценочных показателей у которых ниже «отлично»

Рисунок 3.3 – Результаты оценки состояния систем защиты информации информационных систем

Получив информацию по СЗИ ИС и нажав на кнопку (стрелка на рисунке 3.3), в диалоговом окне появится информация в виде, представленном на рисунке 3.4.

В диалоговом окне выводится информация по тем функциональным подсистемам СЗИ ИС, в которых не выполнены все требования по защите информации.

На данном шаге выявляются единичные показатели, по которым не выполнены требования по защите информации. Для этого должностное лицо нажимает на соответствующую кнопку (стрелка на рисунке 3.4). Форма представления информации показана на рисунках 3.5, 3.6.

Единичные показатели выводятся в табличной форме позволяющей делать прокрутку для просмотра всего перечня. На экран выводятся только не выполненные требования единичных показателей.

Рисунок 3.5 – Результаты оценки состояния функциональных подсистем системы защиты информации

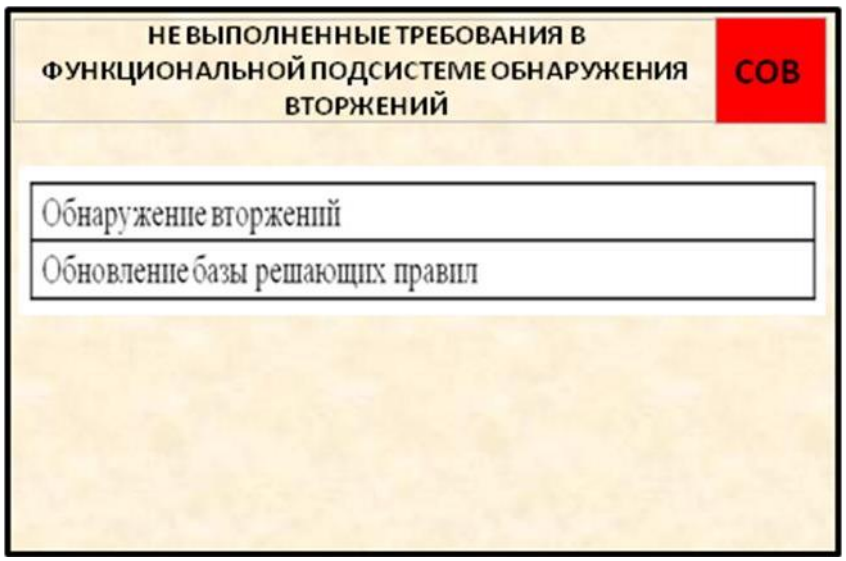


Рисунок 3.6 – Результаты оценки выполнения требований единичных показателей

В такой же последовательности выполняются шаги 1 – 4 и случаях, если правовые и организационные меры по защите информации имеют оценку ниже

«отлично».

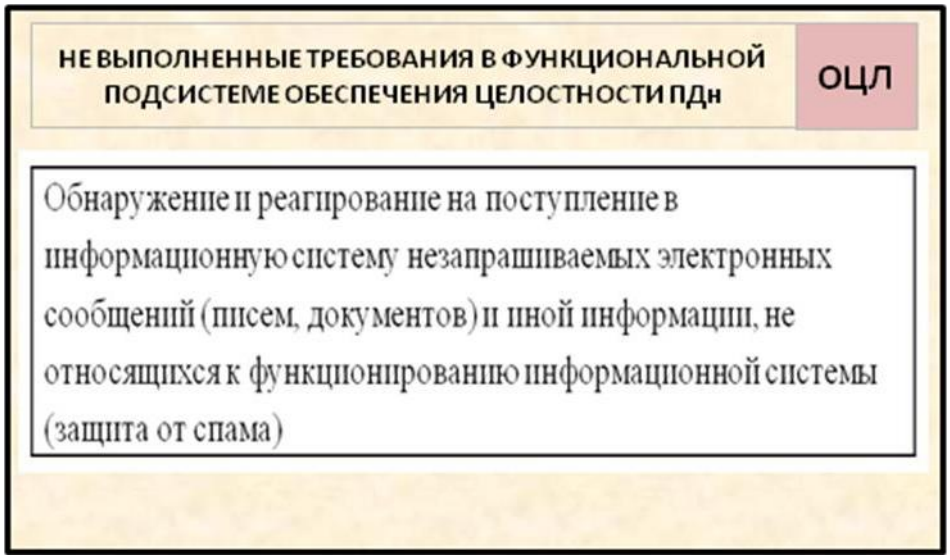


Рисунок 3.7 – Результаты оценки выполнения требований единичных показателей

Таким образом, суть работ четвертого этапа сводится к анализу и выявлению, в конечном счете, всех не выполненных требований по всем направлениям работ по обеспечению информационной безопасности в организации. Особенностью данного этапа является то, что должностному лицу последовательно на экран выводятся данные только по состоянию, имеющих оценку «хорошо», «удовлетворительно» и «неудовлетворительно». Тем самым концентрируется внимание только на не решенных задачах по обеспечению информационной безопасности в организации.

Вывод результатов оценки состояния СЗИ ИС в графическом виде осуществляется в диалоговом окне, показанном на рисунке 3.8.

На рисунке 3.8, в качестве примера, представлены результаты оценки состояния СЗИ ИС для организации, в которой функционируют две ИС, обрабатывающие коммерческую тайну (КТ) и персональные данные (ПДн).

Представление информации в таком виде позволяет должностному лицу в целом увидеть состояние СЗИ как по всем информационным системам, так и по отдельным функциональным подсистемам этих информационных систем.

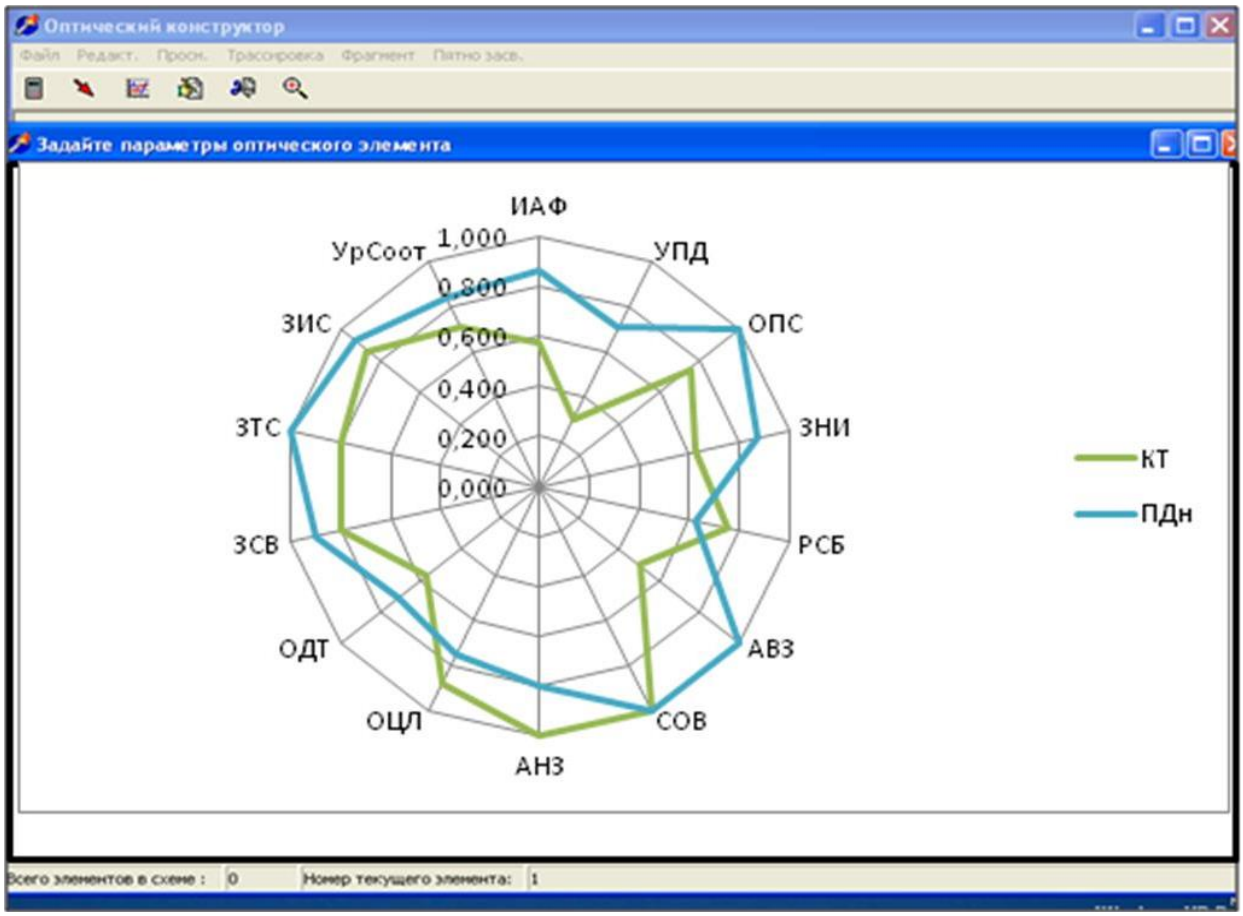


Рисунок 3.8 - Результаты оценки состояния СЗИ ИС

На этапе 5 выполняется формирование перечня рекомендаций по совершенствованию состояния информационной безопасности в организации.

Шаг 1. В формате текстового редактора Word автоматически формируется перечень не выполненных единичных показателей в виде таблицы. Наименования показателей соответствует тем, как они внесены в базу данных. Пример сформированного перечня представлен на рисунке 3.9.

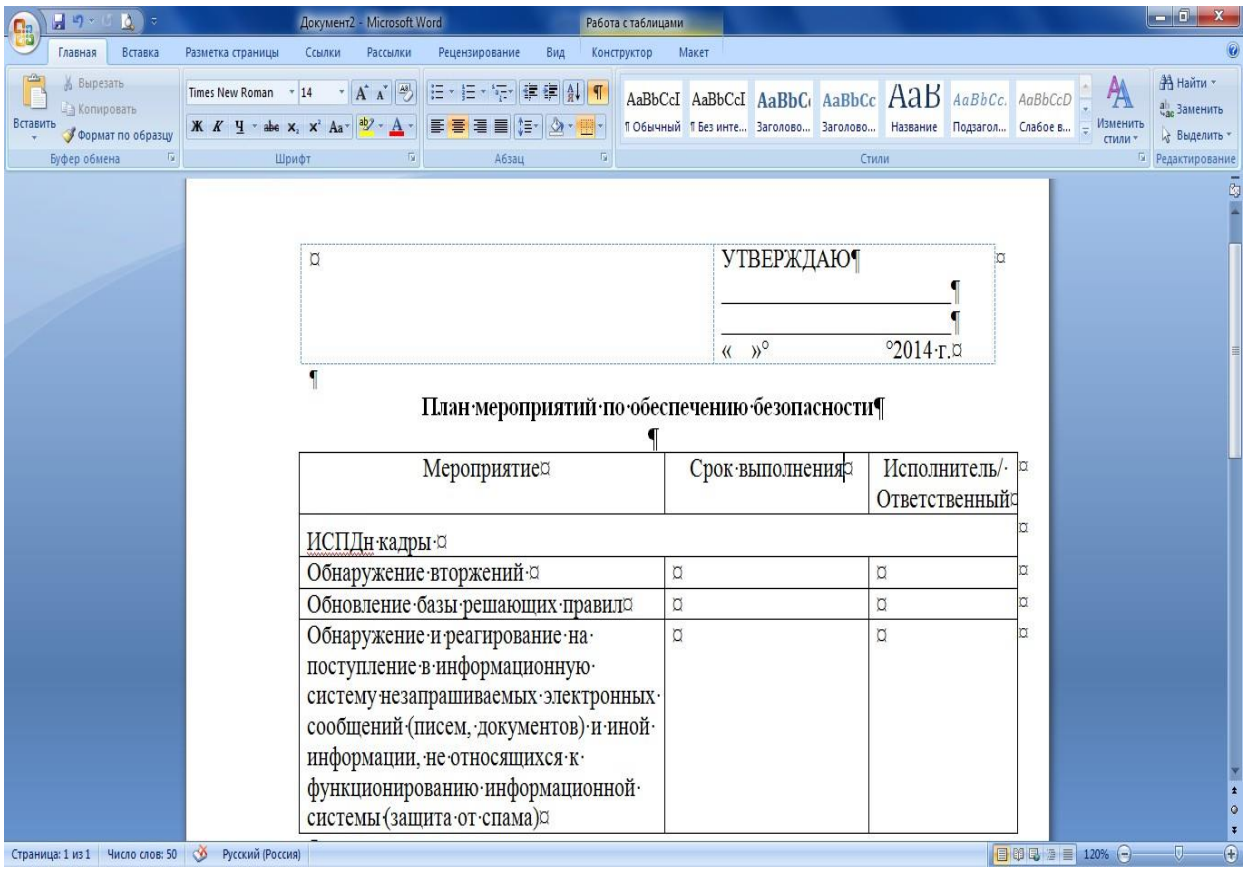


Рисунок 3.9 – Проект Плана мероприятий по обеспечению информационной безопасности

Шаг 2. Должностное лицо на экране корректирует содержание графы «Мероприятия», заполняет графы «Срок выполнения», «Исполнитель/Ответственный» и выводит План реализации на печать с последующим представлением его на утверждение руководителю организации. На рисунке 3.10 приведен пример скорректированного Плана реализации рекомендаций по совершенствованию СОИБ организации.

На рисунке 3.11 представлена последовательность реализации процедур методики оценки состояния системы обеспечения информационной безопасности организации.

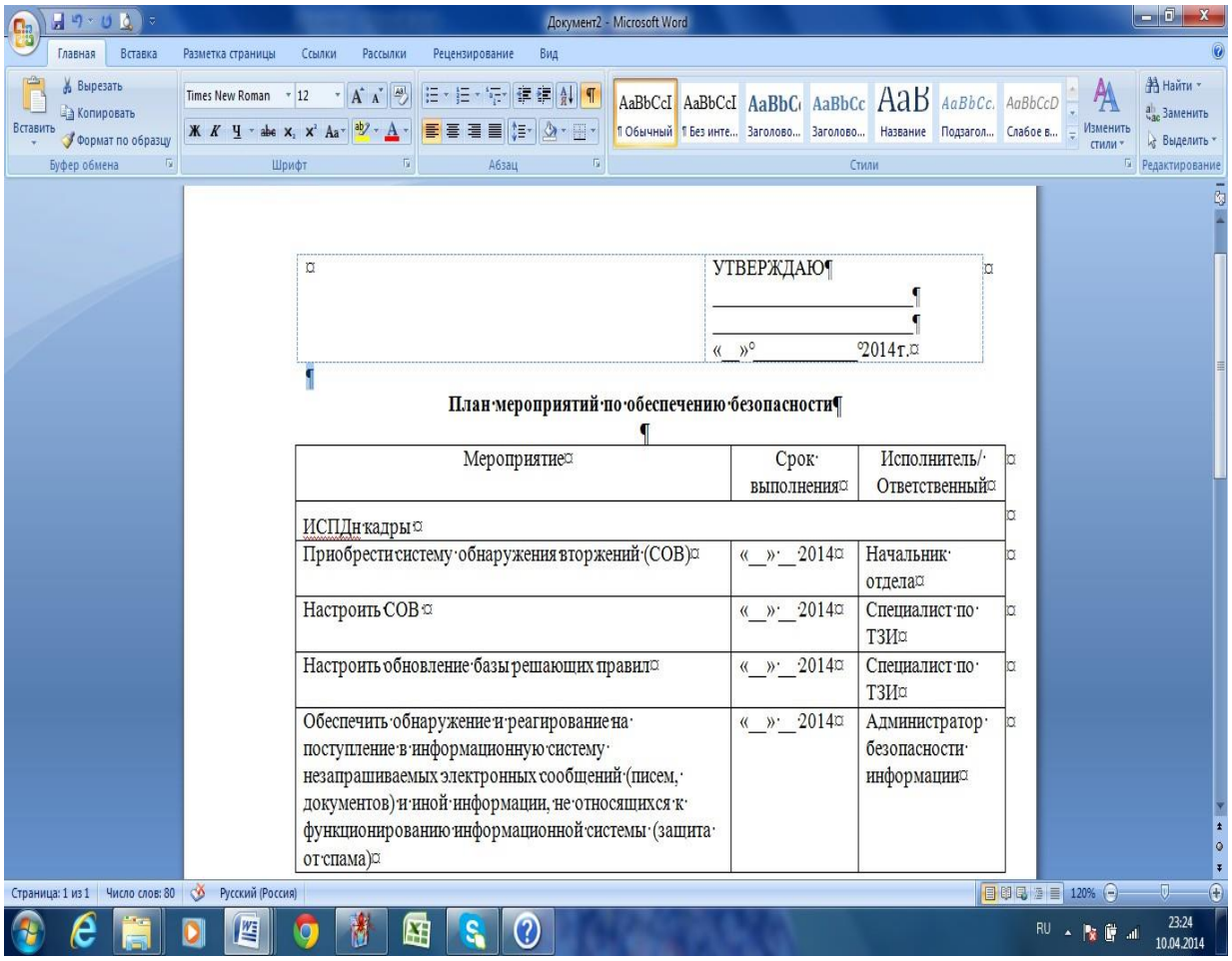


Рисунок 3.10 – Скорректированный проект Плана мероприятий по обеспечению информационной безопасности

При проведении в организации повторного аудита информационной безопасности, если характеристики СЗИ ИС не изменялись, то методика реализуется с блока формирования анкет контроля выполнения требований.

В случае изменения требований к защите информации, получения практики эксплуатации информационных систем, изменения структуры СОИБ, появления новых информационных систем реализация методики начинается с блока первичного заполнения БД. Это вызвано необходимостью корректировки исходных данных и приведения их в соответствии с нормативными правовыми актами и нормативными документами в области информационной безопасности.

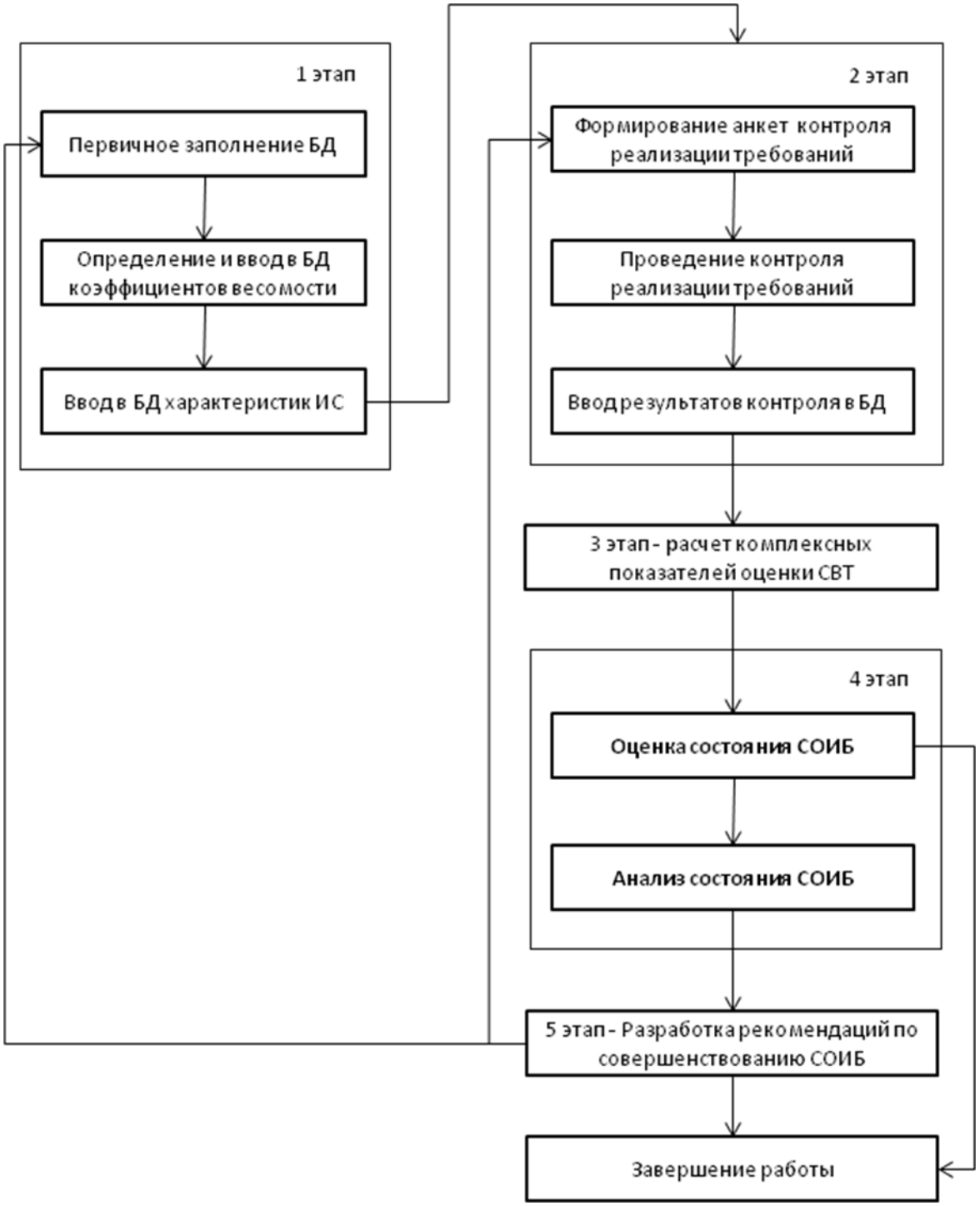


Рисунок 3.11 – Последовательность реализации процедур методики оценки состояния системы обеспечения информационной безопасности

Разработанная методика оценки состояния СОИБ в отличие от существующих, позволяет выполнять экспресс-оценку состояния информационной безопасности организации при проведении аудита информационной безопасности, периодического контроля эффективности обеспечения ЗИ, автоматизировать процесс выработки рекомендаций по совершенствованию информационной безопасности организации, а также обеспечивает решение задач оценки и анализа состояния СОИБ.

Тема 16. Модели и методы оптимального управления процессами обеспечения безопасности.

17.1 Модели защиты информации.

Основные модели защиты информации.

Существует множество моделей защиты информации. Но все они являются модификациями трёх основных: дискреционной, мандатной и ролевой.

Дискреционная модель обеспечивает произвольное управление доступом субъектов к объектам и контроль за распространением прав доступа. В рамках этой модели система обработки информации представляется в виде совокупности активных сущностей – субъектов, которые осуществляют доступ к информации, пассивных сущностей – объектов, содержащих защищаемую информацию и конечного множества прав доступа, означающих полномочия на выполнение соответствующих действий. Принято считать, что все субъекты одновременно являются и объектами (обратное неверно). Поведение системы характеризуется текущим состоянием, текущее состояние характеризуется тройкой множеств: субъектов, объектов и матрицы прав доступа, описывающей текущие права доступа субъектов к объектам.

Мандатная модель управления доступом основана на правилах секретного документооборота, принятых в государственных учреждениях многих стран. Всем участникам процесса обработки защищаемой информации и документам, в которых она содержится, назначается специальная метка, получившая название уровень безопасности. Все уровни безопасности упорядочиваются по доминированию. Контроль доступа основывается на двух правилах:

1. Субъект имеет право читать только те документы, уровень безопасности которых ниже или равен уровню субъекта.
2. Субъект имеет право заносить информацию только в документы, уровень которых выше или равен уровню субъекта.

Ролевая модель представляет собой существенно усовершенствованную дискреционную модель, однако её нельзя отнести ни к дискреционным, ни к мандатным моделям, потому что управление доступом в ней осуществляется как на основе матрицы прав доступа для ролей, так и с помощью правил, регламентирующих назначение ролей пользователям и их активацию во время сеансов. В ролевой модели классическое понятие субъект замещается понятиями пользователь и роль (см. рисунок 1.).

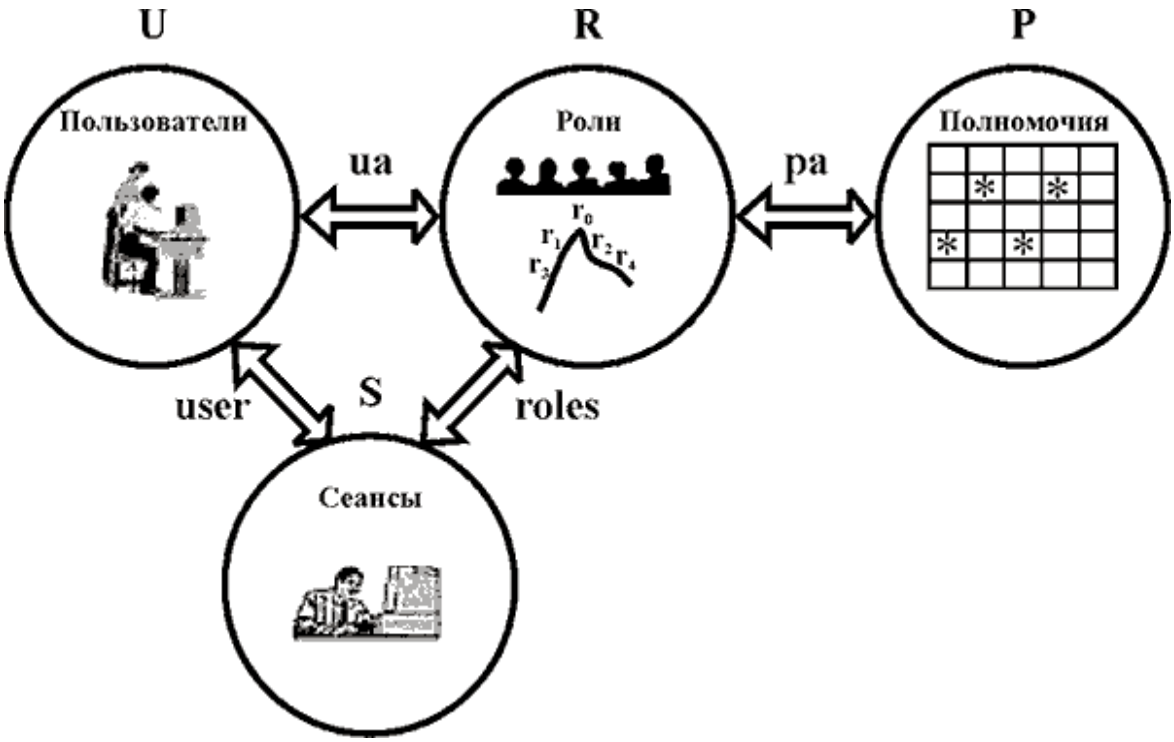


Рисунок 1 Ролевая модель управления доступом

1.2. Реализация ядра безопасности.

Основное назначение надежной вычислительной базы - выполнять функции монитора обращений, то есть контролировать допустимость выполнения субъектами определенных операций над объектами. Монитор проверяет каждое обращение пользователя к программам или данным на предмет согласованности со списком действий, допустимых для пользователя. От монитора обращений требуется выполнение трех свойств:

изолированность. Монитор должен быть защищен от отслеживания своей работы;

полнота. Монитор должен вызываться при каждом обращении, не должно быть способов его обхода;

верифицируемость. Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в полноте тестирования.

Реализация монитора обращений называется ядром безопасности. Ядро безопасности - это основа, на которой строятся все защитные механизмы. Помимо перечисленных выше свойств монитора обращений, ядро должно гарантировать собственную неизменность.

Перед дальнейшим описанием сделаны некоторые предположения относительно архитектуры информационной системы;

-вся информация в ней представлена в виде атрибутов (свойств, полей, членов-данных) объектов определенных в системе классов.

-доступ к информации осуществляется через свойства объектов, а изменение информации происходит посредством выполнения методов объектов.

-информация об объектах, свойствах и методах хранится в базе данных, которая может являться обычной реляционной СУБД.

В этом случае необходимо применение объектно-ориентированного расширения, например, в виде слоя хранимых процедур. Возможна также схема с выделением объектного расширения в виде специализированного сервера объектов. Ниже расширение

рассматривается и выделено на схеме, как виртуальная объектно-ориентированная машина.

Объектом системы будем называть любой экземпляр определенного в системе класса, а субъектом - объект, который в данный момент времени инициирует изменение состояния какого-либо другого объекта, в том числе и самого себя, а, следовательно, и всей системы в целом. Особыми субъектами в системе являются те из них, которые могут выступать в качестве изначальных инициаторов того или иного изменения состояния системы. Таковыми будут, например, объекты класса "Пользователь" или "Сервис", которые ассоциированы с внешними по отношению к системе объектами окружающего мира.

Рассмотрим схему взаимодействия системы с пользовательскими процессами посредством ядра безопасности:

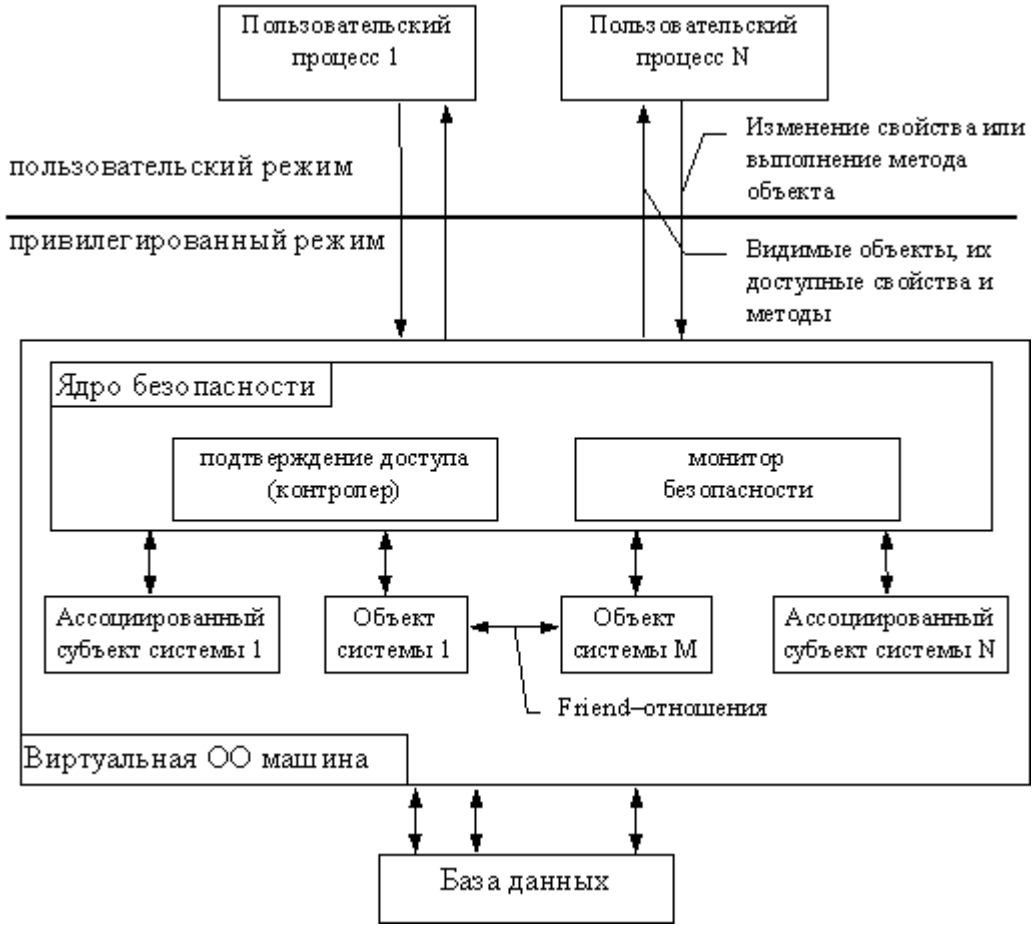


Рис.2. Схема взаимодействия субъектов и объектов системы

Очевидно, что реализация взаимодействия объектов информационной системы с ядром безопасности должна быть осуществлена на как можно более высоких уровнях абстракции классов. Реализация не должна допускать переопределения со стороны подклассов, в противном случае будут нарушены принципы изолированности и полноты монитора.

Рассмотрим обобщенные требования к безопасности для объекта абстрактного класса системы:

определение видимости данного объекта для субъекта;

разделение доступа к свойствам данного объекта со стороны субъекта (свойство инкапсулирует реализацию обращения к членам данным и/или эмулирует логический член данных, физически отсутствующий в классе);

разделение доступа к методам данного объекта со стороны субъекта;

регистрация изменений состояния данного объекта.

Очевидно также, что потребность в безопасности необходима для общедоступных (public) и публикуемых (published) свойств и методов. Различия между общедоступными и публикуемыми методами состоит в том, что публикуемый метод также является общедоступным, но может быть инициирован пользователем, когда тот запрашивает у объекта список возможных операций с ним. Таким образом, он является общедоступным методом для внешних по отношению к системе объектов через определенный в системе интерфейс опубликования, на уровне взаимодействия "пользователь-система". Например, класс имеет методы "Рассчитать значение по параметру" (public, используется другими объектами) и "Показать текущие значения параметров" (published, выдается в качестве возможного варианта действия пользователю).

Friend-отношения могут рассматриваться только как заранее оговоренный случай внутреннего взаимодействия объектов системы, например получение значений некоторых членов данных напрямую. Некорректное применение friend-отношений может привести к образованию "дыры" в ядре безопасности, через которую можно будет неконтролируемо извлекать или изменять информацию. По личному мнению автора, применение friend-отношений можно полностью исключить на этапе проектирования.

Состояние объекта в системе определяется вектором его свойств и, соответственно, текущими состояниями каждого из этих свойств, то есть: Obj(Property1, Property 2, ..., Property N). С другой стороны, объект предоставляет субъектам свои методы: Obj(Method1, Method 2, ..., Method M). С точки зрения обеспечения безопасности, нас интересуют только те свойства и методы, которые являются общедоступными и публикуемыми. Способы доступа к самому объекту со стороны субъекта могут быть описаны, как множество значений: [нет, есть]. Способы доступа к свойствам могут быть описаны, как множество значений: [нет, чтение, запись]. Способы доступа к методам могут быть описаны, как множество значений: [нет, выполнение].

Для математического описания подобной схемы доступа достаточно использования трех матриц:

M1: (объекты X субъекты) со множеством значений [нет, есть];

M2: (свойства X субъекты) со множеством значений [нет, чтение, запись]

M3: (методы X субъекты) со множеством значений [нет, выполнение].

Все три матрицы являются динамически изменяющими размерность и разреженными, поэтому возможно их хранение в виде массива кортежей <субъект, объект, значение>, то есть хранение матриц по столбцам для непустых значений.

Предположение о том, что объект может изменять доступ к своим свойствам и методам в процессе своего существования требует описания начального и конечных состояний жизни объекта и процедур создания и удаления объекта данного класса. Очевидно, чтобы определить права доступа субъекта к объекту, необходимо вначале создать этот объект. С другой стороны, чтобы создать объект, субъекту необходимо иметь на это право, то есть иметь право на выполнение конструктора объекта. Разрешение

подобной дилеммы состоит в рассмотрении понятия класса, как активного участника процесса, а не пассивного шаблона создания объекта.

Для этого необходимо определять права доступа субъекта к свойствам и методам класса, так же, как и к его объекту. Данные установки будут также использоваться, как "установки по умолчанию" для созданного объекта в системе. Таким образом, мы будем иметь "шаблон прав доступа" для субъекта по отношению к данному классу объектов. Это позволяет еще более разрядить матрицу схем доступа и хранить в ней только схемы тех объектов, доступ к которым для одного и более субъектов был изменен.

Удаление может быть инициировано субъектом, имеющим право выполнения деструктора объекта. При удалении объекта из системы, информация о правах доступа к нему со стороны других субъектов также должна быть удалена. Случай логического удаления объекта или архивации может рассматриваться как обычное исполнение одного из его методов.

17.2 Методы защиты информации

Информация играет главенствующую роль в обеспечении безопасности всех объектов жизнедеятельности общества. Этим объясняется тот факт, что защита от утечки информации является важнейшим направлением деятельности государства. Вся существующая информация предоставляется на разных физических носителях и в различной форме:

документальной форме;

речевой или акустической форме;

телекоммуникационной форме.

Документальная информация содержится в графическом и буквенно-цифровом виде на бумаге и на магнитных носителях. Ее главной особенностью является то, что она содержит данные, которые нуждаются в защите, в сжатом виде. Речевая информация формируется в процессе ведения переговоров, а также при работе системы звуковоспроизведения или звукоусиления. Носителями данного вида информации могут быть акустические механические колебания, что распространяются во внешнее пространство от источника. Телекоммуникационная информация рождается в технических средствах хранения и обработки данных в процессе передачи по каналам связи. В данном случае носителем информации является электрический ток. А если данные передаются по оптическому каналу и радиоканалу, то носитель – электромагнитные волны.

Основные методы защиты информации в зависимости от объекта.

Главными объектами информации могут быть:

1. Информационные ресурсы. Данные ресурсы могут содержать сведения, которые относятся к государственной тайне и к конфиденциальным данным.

2. Средства и системы информатизации (системы и сети, а также информационно-вычислительные комплексы), программные средства (операционные системы, СУБД, а также другие разновидности прикладного и общесистемного программного обеспечения), системы связи и АСУ. То есть сюда относятся те средства и системы, которые обрабатывают только «закрытую» информацию. Подобные системы и средства считаются техническими средствами обработки, приема, передачи и сохранения данных.

3. Технические средства и системы, которые не относятся к средствам информатизации, но размещаются в помещениях, где обрабатываются секретные данные. Данные технические средства и системы являются вспомогательными.

В зависимости от этого наиболее распространенными методами защиты информации являются:

1. Препятствие. Это метод защиты информации, который подразумевает физическое ограничение пути к носителям защищаемой информации.

2. Метод управления доступом. Он подразумевает защиту информационных ресурсов посредством контроля применения каждого из них. К данным методам можно отнести технические и программные средства, а также элементы баз данных.

3. Маскировка. Это метод защиты информации, который подразумевает ее криптографическое закрытие. При передаче данных по длинным каналам этот метод считается единственно надежным.

4. Регламентация. Данный метод подразумевает защиту информационных данных, при которой становится минимальной вероятность несанкционированного доступа.

5. Принуждение. Это метод защиты информации, при котором персонал и пользователи системы обязательно должны соблюдать правила обращения со всеми защищенными сведениями – передача, обработка и использование данных. Если они не выполняют данные условия, то могут подвергаться административной или материальной ответственности.

6. Побуждение. Сюда относятся такие методы защиты информации, при которых персонал и пользователя побуждают придерживаться установленного порядка, соблюдая этические и моральные нормы (написанные и регламентированные).

К методам защиты информации, которые ограничивают доступ, можно отнести:

1. Идентификация ресурсов компьютерной сети, их пользователей и персонала (присвоение объектам персонального идентификатора).

2. Метод опознания или подлинности объекта по тому идентификатору, который был указан при входе в систему.

3. Контроль полномочий, который подразумевает анализ соответствия времени суток, дня, ресурсов и запрашиваемых процедур согласно установленному регламенту.

4. Установление регламента для того, чтобы разрешить диапазон рабочего времени.

5. Регистрация каждого обращения к тем ресурсам, что защищаются.

6. Реакция ограничения в случае совершения попытки несанкционированного доступа (отказ в запросе или включение сигнализации).

Методы защиты информации очень разнообразны, но их однозначно необходимо использовать во всех сферах повседневной жизни.

Организационные методы защиты информации.

В компетенцию службы безопасности обязательно должна входить разработка комплекса организационных средств защиты информации. Чаще всего компетентные специалисты применяют такие методы информационной защиты:

1. Разрабатывают внутренние нормативные документы, в которых должны быть установлены правила работы с конфиденциальной информацией и компьютерной техникой.

2. Проводят периодические проверки персонала и инструктаж касаемо сохранение конфиденциальных данных. Кроме этого должны инициировать подписание дополнительных соглашений к трудовому договору, в которых четко прописана ответственность работника за неправомерное использование или разглашение сведений, которые стали ему известные в процессе осуществления его профессиональной деятельности.

3. Служба безопасности также должна разграничить зоны ответственности для исключения тех ситуаций, когда наиболее важная информация находится в доступе только одного сотрудника. Кроме вышеперечисленных методов защиты информации компетентные сотрудники должны организовать работу в общих программах документооборота и проследить, чтобы особо важные файлы не хранились вне сетевых дисков.

4. Внедряют программные комплексы, которые защищают информацию от уничтожения или копирования любым пользователем системы, в том числе топ-менеджером компании.

5. Составляют планы, которые могут восстановить систему в том случае, если она выйдет из строя.

Технические методы защиты информации.

Основные технические методы защиты информации включают программные и аппаратные средства. К ним можно отнести:

1. Обеспечение удаленного хранения и резервного копирования наиболее важных информационных данных на регулярной основе.

2. Резервирование и дублирование всех подсистем, которые содержат важную информацию.

3. Перераспределение ресурсов сети в том случае, если нарушена работоспособность ее отдельных элементов.

4. Обеспечение возможности применять резервные системы электрического питания.

5. Обеспечение безопасности информационных данных и надлежащей защиты в случае возникновения пожара или повреждения компьютерного оборудования водой.

6. Установка такого программного обеспечения, которое сможет обеспечить надлежащую защиту информационных баз данных в случае несанкционированного доступа.

Тема 17. Криптографические алгоритмы.

Цель: реализовать простейший алгоритм шифрования.

1. Регистрация пользователей и групп в системе

2. Определение их привилегий

3. Определение параметров политики безопасности, относящихся к аутентификации и авторизации пользователей при интерактивном входе

4. Защита дисков

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Криптография в переводе с греческого означает «тайнопись». Смысл этого термина подчеркивает основную задачу криптографии – защитить или сохранить в тайне

необходимую информацию. Развитие средств защиты создал три метода защиты информации:

- физический способ защиты;
- стеганографический способ защиты;
- криптографический способ защиты.

Физическая защита – физическая защита носителей информации, защита от перехвата, уничтожение носителей при угрозе захвата данных (американский самолет), обнаружение «утечки».

Стеганография – способы сделать носитель невидимый (Грибоедов, Ришелье, голова раба, невидимые чернила, микроточка).

Криптографический способ защиты. Этот способ защиты наиболее распространен в наши дни.

Итак, криптография есть способ защиты информации. Она обеспечивает:

- секретность данных, т.е. защиту от несанкционированного знакомства с содержанием;
- аутентификацию сообщений, т.е. подтверждение их подлинности, подлинности сторон, времени создания;
- невозможность отказа от авторства, т.е. электронную подпись;
- целостность данных, т.е. защиту от несанкционированного изменения содержания.

Это в свою очередь позволяет решать следующие прикладные задачи:

- электронная Цифровая Подпись (ЭЦП);
- электронные деньги;
- электронная жеребьевка;
- одновременное подписание контрактов;
- защита ценных бумаг и документов от подделок;
- электронное голосование.

Некоторые общие тезисы о защите информации:

- криптография – одно из многих средств защиты;
- надо защищать то, что дорого;
- нельзя создать систему защиты информации раз и навсегда, следует все время отслеживать последние разработки в этом направлении, совершенствовать систему и т.п.
- надо искать компромисс между стоимостью защиты (стоимостью шифрования) и требуемой степени безопасности (нельзя ловить рыбу на золотой крючок);
- проблемы надежно шифровать нет, важно, чтобы коммерческие масштабы шифрование отвечали некоторым оптимальным требованиям цены и скорости;
- 80% угроз для информационной безопасности являются сотрудники и/или сбой аппаратуры.

Условно развитие криптографии можно разбить на три периода:

- Донаучный. В этот период не было единого системного подхода к криптографии. Криптография не была объектом исследования определенной области науки.

- Научный. Этот период начинается с работ Шенона «Теория связи в секретных системах», которые он опубликовал в 1949г.
- Современный. Этот период начинается с работы двух математиков Диффи У. и Хеллмана М. «Новые направления в криптографии» (1976).

В 1978г. на основе концепции, которая была изложена работе «Новые направления в криптографии», три математика Ривест, Шамир, Адлеман предложили принципиально новый криптографический метод шифрования, который называется RSA. Имя метода составлено из первых букв фамилий этих ученых.

Так как в донаучный период криптография не была объектом исследования определенного направления, то ею занимались на уровне ремесла или увлечения специалисты разных профессий. Среди авторов криптографических методов были полководцы, руководители государств, священники, дипломаты, юристы и т.д. Среди авторов криптографических систем защиты были даже известные исторические деятели, такие как римский император Юлий Цезарь, кардинал Ришелье, американский президент Джефферсон. Начиная со средних веков, вопросы криптографии все более включаются в сферу исследования математиков.

Основное понятие в криптографии – шифр. Шифр – это преобразование исходного, секретного сообщения с целью его защиты. Выбор конкретного преобразования открытого текста определяется наиболее секретной частью криптографической защиты – так называемым ключом защиты. Здесь надо подчеркнуть разницу между шифрованием и кодированием информации.

Кодирование – это преобразование информации, в котором отсутствует ключ. Оно используется не для достижения защиты информации, а для представления данных в другом формате для выполнения каких-нибудь технических задач. Например, азбука Морзе, архиватор, представление информации для реализации графическое изображения. В кодировании секретом является выбранный формат представления данных, технические, теоретические и алгоритмические детали, которые используются для реализации выбранного представления. Архиватор на первых порах использовался для сокрытия информации.

В 1883г. Керкгоффс сформулировал шесть требований к системам шифрования:

1) система должна быть нераскрываемой, если не теоретически, то практически;

2) компрометация системы не должна причинять неудобства ее пользователям;

3) секретный ключ должен быть легко запоминаемым без каких-либо записей;

4) криптограмма должна быть представлена в такой форме, чтобы ее можно было передать по телеграфу;

5) аппаратура шифрования должна быть портативной и такой, чтобы ее мог обслуживать один человек;

6) система должна быть простой. Она не должна требовать ни запоминания длинного перечня правил, ни большого умственного напряжения.

Эти правила можно трактовать как некоторое условие сертификации криптосистем того времени. Если проанализировать эти старые требования шифрования, пожалуй, только пункты 3, 4 и 5 стали как бы несущественными

в современных криптографических системах. Можно сказать, они выполняются автоматически в современных информационных технологиях.

Пункт первый требований в современных условиях можно интерпретировать как стойкость шифров от атак. Шестое требование можно истолковать, как построение доступных по стоимости криптографических систем (современная интерпретация простоты есть стоимость). Однако фундаментальным и незыблемым требованием к криптографическим системам остается второе требование. Ввиду важности и незыблемости этого требования оно выделено в перечне жирным шрифтом. В настоящее время это требование называется правилом Керкгоффса. Суть его состоит в том, что при построении криптографической системы надо исходить из того что противнику известен алгоритм шифрования, а стойкость шифрование зависит только от ключа шифрования (Пример Энигма).

Классы шифров:

- Простые замены – поточные шифры простой замены, блочные шифры простой замены. К таким шифрам, например, относятся шифр Цезаря, квадрат Полибия, шифр Плейфера, двойной квадрат. Заметим, что шифры простой замены легко взломать, используя частотный анализ.
- Перестановки – сциталь Лесандра, табличные способы перестановки, таблица с усложненными элементами.
- Многоалфавитные шифры замены – квадрат Виженера, шифр Грансфельда.

В 1949 году Шенон сформулировал два основных принципа для разработки стойких шифров. Это принцип «перемешивания» и принцип «рассеивания».

Суть «перемешивания» состоит в том, чтобы при шифровании текстов, которые отличаются незначительно, перемешивание должно приводить к существенному изменению результата. Суть «рассеивания» состоит в том, чтобы влияние одного символа открытого текста распространялось бы на как можно большее количество символов. Шеннон предложил и общую структуру таких шифров как суперпозицию простых преобразований блочных символов.

Шифры перестановки.

Эти шифры, наверное, являются самыми древними из всех шифров. В таких шифрах символы исходного открытого текста переставляются по определенному правилу. В качестве примера рассмотрим шифр простой перестановки, который использует шифрующие таблицы. В шифрующую таблицу (табл. 1) по вертикали без пробелов записывается исходное сообщение:

Я ПРИДУ ЗА ТОБОЙ ВОСЕМЬ ВЕЧЕРА,

а считывание шифртекста происходит по горизонтали:

ЯУБСЕПЗОЕЧРАЙМЕИТВЬРДООВА.

Таблица 1

Я	У	Б	С	Е
П	З	О	Е	Ч
Р	А	Й	М	Е
И	Т	В	Ь	Р
Д	О	О	В	А

Ключом в данном методе шифрования является размер таблицы и правило считывания букв. Расшифровка сообщения происходит в обратном порядке: шифр текст разбивается на блоки длиной, равной длине строки, затем эти блоки записываются один под другим с последующим вертикальным считыванием:

Я ПРИДУ ЗА ТОБОЙ ВОСЕМЬ ВЕЧЕРА.

Шифры замены

В этих шифрах символы исходного открытого текста заменяются символами входного или другого алфавита по некоторому оговоренному правилу. В шифрах простой замены замена происходит на символы алфавита исходного текста (одноалфавитная подстановка).

Полибианский квадрат. За два века до нашей эры греческий писатель и историк Полибий изобрел для целей шифрования квадратную таблицу 5x5, заполненную случайным образом 24 буквами греческого алфавита и пробелом (табл. 2).

Таблица 2

λ	ε	υ	ω	γ
ρ	ζ	δ	σ	ο
μ	η	β	ξ	τ
ψ	π	θ	α	κ
χ	ν	<пробел>	φ	ι

При шифровании находилась буква в таблице и заменялась на букву ниже в том же столбце. Если буква находилась внизу столбца, то она заменялась на верхнюю букву этого же столбца. Очевидно, ключом здесь является сама таблица.

Система шифрования Цезаря. В качестве другого примера рассмотрим одну из древнейших систем шифрования - систему шифрования Гая Юлия Цезаря, известного римского императора-полководца (около 50 г. до нашей эры).

В этой системе каждая буква исходного текста заменяется на букву этого же алфавита, которая является циклически смещенной на *K* букв вправо по длине алфавита. В шифре Цезаря это смещение было равно 3 (табл. 3). Значение *K* есть ключ этого шифра. Интересно отметить, что Цезарь никогда не менял значения ключа. В период жизни Цезаря всеобщая неграмотность населения вселяла уверенность в невозможности постичь написанное в виде шиф-ртекста. В табл. 3 иллюстрируются одноалфавитные замены в шифре Цезаря.

Известное выражение Цезаря «VENI, VIDI, VICI» («Пришел, увидел, победил») в виде шифртекста будет выглядеть как «YHQL, YLGL, YLFL».

Таблица 3

A->D	J->M	S->V
B->E	K->N	T->W
C->F	L->O	U->X
D->G	M->P	V->Y
E->H	N->Q	W->Z
F->I	O->R	X->A
G->J	P->S	Y->B
H->K	Q->T	Z->C
I->L	R->U	-

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Задание 1 (без использования программирования)

1. Зашифровать с помощью шифрующей таблицы либо другого алгоритма какое либо стихотворение.

2. Расшифровать стихотворение (шифр, использующий шифрующую таблицу, ключом является размер таблицы 12x7):

а)УрелпелшлицшльлаьтьиПмаьуяётношфрддлкднаамерооооиоуыядИяовкйтмбйцуднвеодыозЗебаеарне;

3. Ответить на вопрос: что можно сделать для увеличения стойкости шифра перестановки, использующего шифрующие таблицы.

4. Оформить отчет.

Задание 2 (с использованием программирования)

1. Реализовать программу шифрования (зашифрование и расшифрование) по одному из алгоритмов (язык программирования выбирается самостоятельно):
   - шифр простой перестановки, который использует шифрующие таблицы (ключ - размер таблицы);
   - систему шифрования Гая Юлия Цезаря (ключом является буква алфавита).
2. Реализовать программу дешифрования (подбора ключа или нахождения исходного текста) на основе известного шифртекста.
3. Ответить на вопрос: что можно сделать для увеличения стойкости шифра перестановки, использующего шифрующие таблицы?
4. Сделать вывод о сложности подбора пароля.
5. Оформить отчет (краткий текст и программы).

Тема 18. Оценка надежности защитных механизмов. Принципы оценки надежности защиты.

Под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов и интересов субъектов, связанных с использованием информационных систем. Из этого довольно очевидного положения можно вывести два важных следствия:

1. Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно различаться. Для иллюстрации достаточно сопоставить режимные военные организации и коммерческие структуры. В данной работе информационная безопасность рассматривается с точки зрения наиболее массовой- коммерческой категории пользователей.
2. Информационная безопасность не сводится исключительно к защите информации. Субъект информационных отношений может пострадать (понести убытки) не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в обслуживании клиентов. Более того, для многих открытых организаций (например, учебных) собственно защита информации стоит по важности отнюдь не на первом месте.

На практике важнейшими являются три аспекта информационной безопасности:

• *доступность* (возможность за разумное время получить требуемую информационную услугу);

• *целостность* (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

• *конфиденциальность* (защита от несанкционированного прочтения).

Кроме того, использование информационных систем должно производиться в соответствии с существующим законодательством. Данное положение, разумеется, применимо к любому виду деятельности, однако информационные технологии специфичны в том отношении, что развиваются исключительно быстрыми темпами. Почти всегда законодательство отстает от потребностей практики, и это создает в обществе определенную напряженность. Для информационных технологий подобное отставание законов, нормативных актов, национальных и отраслевых стандартов оказывается особенно болезненным.

Формирование режима информационной безопасности - проблема комплексная. Меры по ее решению можно подразделить на четыре уровня:

• законодательный (законы, нормативные акты, стандарты и т.п.);

• административный (действия общего характера, предпринимаемые руководством организации);

• процедурный (конкретные меры безопасности, имеющие дело с людьми);

• программно-технический (конкретные технические меры).

При формировании режима информационной безопасности следует учитывать современное состояние информационных технологий. Почти все организации ждут от информационных систем, в первую очередь, полезной функциональности. Компьютерные системы покупаются не ради защиты данных, а, наоборот, защита данных строится ради экономически выгодного использования компьютерных систем. Для получения полезной функциональности естественно обратиться к наиболее современным решениям в области информационных технологий. Значит, говоря о защите, следует иметь в виду прежде всего современные аппаратные и программные платформы. Важно учитывать следующие характеристики подобных систем:

• глобальную связанность;

• разнородность корпоративных информационных систем;

• распространение технологии клиент/сервер.

Одним из следствий глобальной связанности является меньшая эффективность мер физической защиты, общее усложнение проблем, связанных с защитой от несанкционированного доступа, необходимость привлечения для их решения новых программно-технических средств, например межсетевых экранов (firewalls).

Разнородность аппаратных и программных платформ требует от изготовителей средств защиты соблюдения определенной технологической дисциплины. Важны не только чисто защитные характеристики, но и возможность встраивания в современные корпоративные информационные системы. Если, например, продукт, предназначенный для криптографической защиты, способен функционировать исключительно на платформе Intel/DOS, то его практическая применимость вызывает серьезные сомнения.

Следствия использования технологии клиент/сервер для информационной безопасности, коротко говоря, состоят в том, что:

- каждый сервис имеет свою трактовку главных аспектов информационной безопасности (доступности, целостности, конфиденциальности);
- каждый сервис имеет свою трактовку понятий субъекта и объекта;
- каждый сервис имеет специфические угрозы;
- каждый сервис нужно по-своему администрировать;
- средства безопасности в каждый сервис нужно встраивать по-особому;
- операционная система - просто группа сервисов, она перестает быть главной с точки зрения защиты.

Полезно мысленно применить сформулированные положения к двум употребительным сервисам - СУБД и электронной почте. Трактовка понятия целостности для СУБД будет подробно рассматриваться во второй части данной публикации; в общих чертах она общеизвестна. В то же время для электронной почты желательно обеспечить целостность как каждого из пересылаемых писем (неизменность содержимого, а также отправителя и списка получателей), так и всего потока сообщений (защиту от кражи, дублирования и переупорядочивания сообщений). Ясно, что такая трактовка целостности не применима к СУБД.

Далее, и для СУБД, и для электронной почты имеет место такая угроза конфиденциальности, как получение информации путем логического вывода. Но если в случае СУБД логические выводы строятся, в основном, на агрегировании информации, то для электронной почты важнейшим источником выводов служит анализ трафика.

Дальнейшее изложение будет строиться следующим образом. Сначала мы рассмотрим основы классического подхода к информационной безопасности. Имеются в виду "Критерии оценки надежных компьютерных систем" ("Оранжевая книга"), Интерпретация "Критериев" для сетевых конфигураций (документ, очень важный с методологической точки зрения, входящий в так называемую "Радужную серию") и Гармонизированные критерии Европейских стран (здесь мы также сосредоточимся на концептуально важных положениях). Затем мы перейдем к рассмотрению практических аспектов защиты современных информационных систем.

Вторая часть публикации будет посвящена исключительно вопросам обеспечения информационной безопасности систем управления базами данных.

18.1 Критерии оценки надежных компьютерных систем

В "Оранжевой книге" надежная система определяется как "система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа".

Степень доверия, или надежность систем, оценивается по двум основным критериям:

Политика безопасности -набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь имеет право оперировать с определенными наборами данных. Чем надежнее система, тем строже и многообразнее должна быть политика безопасности. В зависимости от сформулированной политики можно выбирать конкретные механизмы, обеспечивающие безопасность системы. Политика безопасности - это активный компонент защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.

Гарантированность - мера доверия, которая может быть оказана архитектуре и реализации системы. Гарантированность может проистекать как из тестирования, так и из проверки (формальной или нет) общего замысла и исполнения системы в целом и ее компонентов. Гарантированность показывает, насколько корректны механизмы, отвечающие за проведение в жизнь политики безопасности. Гарантированность можно считать пассивным компонентом защиты, надзирающим за самими защитниками.

Важным средством обеспечения безопасности является механизм *подотчетности* (протоколирования). Надежная система должна фиксировать все события, касающиеся безопасности. Ведение протоколов должно дополняться *аудитом*, то есть анализом регистрационной информации.

Концепция *надежной вычислительной базы* является центральной при оценке степени гарантированности, с которой систему можно считать надежной. Надежная вычислительная база - это совокупность защитных механизмов компьютерной системы (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности. Надежность вычислительной базы определяется исключительно ее реализацией и корректностью исходных данных, которые вводит административный персонал (например, это могут быть данные о степени благонадежности пользователей).

Вообще говоря, компоненты вне вычислительной базы могут не быть надежными, однако это не должно влиять на безопасность системы в целом. В результате, для оценки надежности компьютерной системы достаточно рассмотреть только ее вычислительную базу, которая, как можно надеяться, достаточно компактна.

Основное назначение надежной вычислительной базы - выполнять функции *монитора обращений*, то есть контролировать допустимость выполнения субъектами определенных операций над объектами. Монитор проверяет каждое обращение пользователя к программам или данным на предмет согласованности со списком действий, допустимых для пользователя.

От монитора обращений требуется выполнение трех свойств:

Изолированность. Монитор должен быть защищен от отслеживания своей работы;

Полнота. Монитор должен вызываться при каждом обращении, не должно быть способов его обхода;

Верифицируемость. Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в полноте тестирования.

Реализация монитора обращений называется *ядром безопасности*. Ядро безопасности - это основа, на которой строятся все защитные механизмы. Помимо перечисленных выше свойств монитора обращений, ядро должно гарантировать собственную неизменность.

Границу надежной вычислительной базы называют *периметром безопасности*. Как уже указывалось, от компонентов, лежащих вне периметра безопасности, вообще говоря, не требуется надежности. С развитием распределенных систем понятию "периметр безопасности" все чаще придают другой смысл, имея в виду границу владений определенной организации. То, что внутри владений, считается надежным, а то, что вне, - нет. Связь между внутренним и внешним мирами осуществляют посредством шлюзовой системы (межсетевого экрана, firewall), которая, по идее, способна противостоять потенциально ненадежному или даже враждебному окружению.

18.2 Европейские Критерии.

Европейские Критерии рассматривают следующие составляющие информационной безопасности:

- конфиденциальность, то есть защиту от несанкционированного получения информации;
- целостность, то есть защиту от несанкционированного изменения информации;
- доступность, то есть защиту от несанкционированного удержания информации и ресурсов.

В Критериях проводится различие между системами и продуктами. Система - это конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении. Продукт - это аппаратно-программный "пакет", который можно купить и по своему усмотрению встроить в ту или иную систему. Таким образом, с точки зрения информационной безопасности основное отличие между системой и продуктом состоит в том, что система имеет конкретное окружение, которое можно определить и изучить сколь угодно детально, а продукт должен быть рассчитан на использование в различных условиях. Угрозы безопасности системы носят вполне конкретный и реальный характер. Относительно угроз продукту можно лишь строить предположения. Разработчик может специфицировать условия, пригодные для функционирования продукта; дело покупателя обеспечить выполнение этих условий.

Из практических соображений важно обеспечить единство критериев оценки продуктов и систем - например, чтобы облегчить и удешевить оценку системы, составленной из ранее сертифицированных продуктов. В этой связи для систем и продуктов вводится единый термин - объект оценки. В соответствующих местах делаются оговорки, какие требования относятся исключительно к системам, а какие - только к продуктам.

Каждая система и/или продукт предъявляет свои требования к обеспечению конфиденциальности, целостности и доступности. Чтобы удовлетворить эти требования, необходимо предоставить соответствующий набор функций (сервисов) безопасности, таких как идентификация и аутентификация, управление доступом или восстановление после сбоев.

Сервисы безопасности реализуются посредством конкретных механизмов. Например, для реализации функции идентификации и аутентификации можно использовать такой механизм, как сервер аутентификации Kerberos.

Чтобы объект оценки можно было признать надежным, необходима определенная степень уверенности в наборе функций и механизмов безопасности. Степень уверенности мы будем называть гарантированностью. Гарантированность может быть большей или меньшей в зависимости от тщательности проведения оценки.

Гарантированность затрагивает два аспекта - эффективность и корректность средств безопасности. При проверке эффективности анализируется соответствие между целями, сформулированными для объекта оценки, и имеющимся набором функций безопасности. Точнее говоря, рассматриваются вопросы адекватности функциональности, взаимной согласованности функций, простоты их использования, а также возможные последствия эксплуатации известных слабых мест защиты. Кроме того, в понятие эффективности входит способность механизмов защиты противостоять прямым атакам (мощность механизма). Определяется три градации мощности - базовая, средняя и высокая.

Под корректностью понимается правильность реализации функций и механизмов безопасности. В Критериях определяется семь возможных уровней гарантированности корректности - от E0 до E6 (в порядке возрастания). Уровень E0 обозначает отсутствие гарантированности (аналог уровня D "Оранжевой книги"). При проверке корректности анализируется весь жизненный цикл объекта оценки - от проектирования до эксплуатации и сопровождения.

Общая оценка системы складывается из минимальной мощности механизмов безопасности и уровня гарантированности корректности. Теоретически эти два аспекта независимы, хотя на практике нет смысла проверять правильность реализации "по высшему разряду", если механизмы безопасности не обладают даже средней мощностью.

Функциональность

В Европейских Критериях средства, имеющие отношение к информационной безопасности, рассматриваются на трех уровнях детализации. Наиболее абстрактный взгляд касается лишь целей безопасности. На этом уровне мы получаем ответ на вопрос, зачем нужны функции безопасности. Второй уровень содержит спецификации функций безопасности. Мы узнаем, какая функциональность на самом деле обеспечивается. Наконец, на третьем уровне содержится информация о механизмах безопасности. Мы видим, как реализуется декларированная функциональность.

Спецификации функций безопасности - важнейшая часть описания объекта оценки. Критерии рекомендуют выделить в этих спецификациях разделы со следующими заголовками:

- идентификация и аутентификация;
- управление доступом;
- подотчетность;
- аудит;
- повторное использование объектов;
- точность информации;
- надежность обслуживания;
- обмен данными.

Большинство из перечисленных тем мы рассматривали при анализе "Оранжевой книги". Здесь мы остановимся лишь на моментах, специфичных для Европейских Критериев.

Под идентификацией и аутентификацией понимается не только проверка подлинности пользователей в узком смысле, но и функции для регистрации новых пользователей и удаления старых, а также функции для генерации, изменения и проверки аутентификационной информации, в том числе средства контроля целостности. Сюда же относятся функции для ограничения числа повторных попыток аутентификации.

Средства управления доступом также трактуются Европейскими Критериями достаточно широко. В этот раздел попадают, помимо прочих, функции, обеспечивающие временное ограничение доступа к совместно используемым объектам с целью поддержания целостности этих объектов - мера, типичная для систем управления базами данных. В этот же раздел попадают функции для управления распространением прав доступа и для контроля за получением информации путем логического вывода и агрегирования данных (что также типично для СУБД).

Под точностью в Критериях понимается поддержание определенного соответствия между различными частями данных (точность связей) и обеспечение неизменности данных при передаче между процессами (точность коммуникаций). Точность выступает как один из аспектов целостности информации.

Функции надежности обслуживания должны гарантировать, что действия, критичные по времени, будут выполнены ровно тогда, когда нужно, не раньше и не позже, и что некритичные действия нельзя перевести в разряд критичных. Далее, должна быть гарантия, что авторизованные пользователи за разумное время получат запрашиваемые ресурсы. Сюда же относятся функции для обнаружения и нейтрализации ошибок, необходимые для минимизации простоев, а также функции планирования, позволяющие гарантировать время реакции на внешние события.

К области обмена данными относятся функции, обеспечивающие коммуникационную безопасность, то есть безопасность данных, передаваемых по каналам связи. Здесь Европейские Критерии предлагают следующие подзаголовки:

- аутентификация;
- управление доступом;
- конфиденциальность данных;
- целостность данных;
- невозможность отказаться от совершенных действий.

Набор функций безопасности может специфицироваться с использованием ссылок на заранее определенные классы функциональности. В Европейских Критериях таких классов десять. Пять из них (F-C1, F-C2, F-B1, F-B2, F-B3) соответствуют классам безопасности "Оранжевой книги".

Класс F-IN предназначается для объектов оценки с высокими потребностями по обеспечению целостности данных и программ, что типично для систем управления базами данных. При описании класса F-IN вводится понятие роли, выдвигается требование по предоставлению доступа к определенным объектам только с помощью предопределенных процессов. Должны различаться следующие виды доступа: чтение, запись, добавление, удаление, переименование (для всех объектов), выполнение, удаление, переименование (для выполняемых объектов), создание и удаление объектов.

Класс F-AV характеризуется повышенными требованиями к доступности. Это существенно, например, для систем управления технологическими процессами. В разделе "Надежность обслуживания" описания этого класса специфицируется, что объект оценки должен восстанавливаться после отказа отдельного аппаратного компонента таким образом, чтобы все критически важные функции оставались постоянно доступными. То же должно быть верно для вставки отремонтированного компонента, причем после этого объект оценки возвращается в состояние, устойчивое к одиночным отказам. Независимо от уровня загрузки должно гарантироваться время реакции на определенные события и отсутствие тупиков.

Класс F-DI характеризуется повышенными требованиями к целостности передаваемых данных. Перед началом общения стороны должны быть в состоянии проверить подлинность друг друга. При получении данных должна предоставляться возможность проверки подлинности источника. При обмене данными должны предоставляться средства контроля ошибок и их исправления. В частности, должны обнаруживаться все повреждения или намеренные искажения адресной и

пользовательской информации. Знание алгоритма обнаружения искажений не должно давать возможность производить нелегальную модификацию. Должны обнаруживаться и трактоваться как ошибки попытки воспроизведения ранее переданных сообщений.

Класс F-DC характеризуется повышенными требованиями к конфиденциальности передаваемой информации. Перед поступлением данных в каналы связи должно автоматически выполняться шифрование с использованием сертифицированных средств. На приемном конце также автоматически производится расшифровка. Ключи шифрования должны быть защищены от несанкционированного доступа.

Класс F-DX характеризуется повышенными требованиями и к целостности, и к конфиденциальности информации. Его можно рассматривать как объединение классов F-DI и F-DC с дополнительными возможностями шифрования, действующими из конца в конец, и с защитой от анализа трафика по определенным каналам. Должен быть ограничен доступ к ранее переданной информации, которая в принципе может способствовать нелегальной расшифровке.

Тема 19: Криптографические методы защиты информации: симметричное шифрование

Цель: изучить виды симметричных криптосистем. Научится использовать их на практике.

1. Суть симметричного шифрования
2. Классификация симметричных криптосистем
3. Блочные и потоковые шифры
4. Алгоритм DEA
5. Алгоритм TDEA
6. Стандарт шифрования AES
7. Алгоритм IDEA
8. Другие симметричные криптоалгоритмы
9. Шифры Брюса Шнайера и шифры Ривеста

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

В настоящее время все существующие криптосистемы принято разделять на два класса: симметричные и асимметричные.

Соответственно, говорят о симметричной криптографии и асимметричной криптографии.

В симметричных криптосистемах одним и тем же секретным ключом осуществляется и шифрование, и расшифрование:

$E_k(P) = C$

$D_k(C) = P$,

где E – функция зашифрования, k – ключ, P – открытый текст, C – шифртекст, D – функция расшифрования.

При этом справедливо следующее равенство:

$$D_k(E_k(P)) = P$$

Потоковые и блочные шифры

Алгоритмы, которые обрабатывают открытый текст побитово (побайтово), называют ***потоковыми алгоритмами*** или потоковыми шифрами.

Алгоритмы, которые обрабатывают группы битов (блоки) открытого текста, называют ***блочными алгоритмами*** или блочными шифрами.

Долгое время в компьютерных алгоритмах типичный размер блока был равен 64 битам. Это достаточно большое значение, чтобы затруднить анализ, и в то же время достаточно малое, чтобы быть удобным для работы.

В настоящее время используются 128-разрядные блоки, так как длина блока в 64 бита не удовлетворяет современным требованиям эффективности и надежности алгоритмов.

Наиболее широко применяемыми на практике симметричными криптосистемами долгое время являлись системы DES (стандарт США), IDEA (европейский стандарт), ГОСТ (стандарт РФ) и их модификации.

Алгоритм DEA

Самым известным и широко распространенным компьютерным алгоритмом шифрования является **алгоритм DEA**, лежащий в основе DES (Data Encrypt Standard) - стандарта шифрования данных США.

Алгоритм DEA был опубликован в 1973 году и в течение почти 20 лет считался криптографически стойким.

В процессе шифрования с помощью алгоритма DEA последовательно производятся преобразования (раунды) над 64-битовыми блоками:

$$P, \Phi_1, \Phi_2, ..., \Phi_{16}, P^{-1}, \qquad (1.1)$$

где P – заданная подстановка; $\Phi_i = V_i T$ - преобразование (сеть) Файстеля (H. Feistel), являющееся основой многих симметричных алгоритмов:

$T(L, R) = (R, L)$ – перестановка левой и правой частей;

$V_i = V(L_i, R_i) = (L_i, R_i \oplus F(R_{i-1}, K_i))$;

$$L_0 R_0; \quad L_i = R_{i-1}, \quad R_i = L_{i-1} \oplus F(R_{i-1}, K_i), \quad (i = 1,...,16);$$

где K_i – ключи, получаемые на основе 56-битового секретного ключа K; F – функция раунда.

Схему формирования шифра DEA см. в презентации к лекции.

Расшифрование производится с помощью преобразований (1.1) на основе ключа K, причем ключи K_i генерируются в обратном порядке.

Обратим внимание, оригинальный алгоритм DEA был разработан для реализации в виде микросхемы, а не эффективного программного кода, поэтому на практике оказывается очень медленным.

Алгоритм TDEA

Одной из составляющих стандарта шифрования данных США 1999 г. является **алгоритм TDEA («тройной» DEA)**. В алгоритме TDEA для зашифрования используется три ключа и трижды применяется алгоритм DEA:

$C = E_{k3}(D_{k2}(E_{k1}(P)))$

Расшифрование представляет собой следующее преобразование:

$P = D_{k1}(E_{k2}(D_{k3}(C)))$

Длина ключа TDEA оказывается равной 168 бит.

В [Federal Information Processing Standard PUB 46-3] содержатся следующие рекомендации относительно TDEA.

- Использование оригинального алгоритма DEA с 56-битовым ключом допускается только в действующих системах. Новые разработки должны поддерживать TDEA.
- Правительственным организациям, применяющим системы на основе DEA, настоятельно рекомендуется перейти к использованию TDEA.

Однако существенным недостатком TDEA является то, что алгоритм оказывается очень медленным в условиях программной реализации. Оригинальный алгоритм DEA был разработан в середине 70-х годов XX в. для реализации в виде микросхемы, а не эффективного программного кода. Алгоритм TDEA, соответственно, оказывается еще более медленным. Кроме того, длина блока (64 бит), используемая в DEA и TDEA, не удовлетворяет современным требованиям эффективности и защищенности, предпочтительнее использование блоков большей длины.

Стандарт шифрования AES

Названные проблемы призван был решить новый усовершенствованный стандарт шифрования AES (Advanced Encryption Standard). С 1997 г. NIST (Национальный институт стандартов и технологий США) принимал предложения по созданию такого стандарта. Обратим внимание на требования, которые предъявлялись NIST: AES должен иметь стойкость не меньше TDEA, но быть существенно эффективным, кроме того, AES должен быть симметричным блочным шифром с длиной блока в 128 бит, поддерживающим использование 128-, 192- и 256-битовых ключей.

В течение нескольких лет криптографическое сообщество разрабатывало и обсуждало приемника для алгоритма DES. В результате был создан алгоритм **AES** (Advanced Encryption Standard), который был опубликован в 2001 году (FIPS 197).

Новый стандарт был принят на основе открытого конкурса, в котором участвовали алгоритмы, предложенные математиками из многих стран мира: США, Канады, Австралии, Бельгии, Германии, Норвегии, Франции, Японии, Южной Кореи, Коста-Рики. Победителем конкурса стал алгоритм Rijndael, разработанный бельгийскими криптографами Винсентом Рэменом и Йоном Даменом.
Название алгоритма образовано из первых букв фамилий его авторов, поэтому в транскрипции с фламандского оно произносится примерно так: «рэндал». [Голдовский, 85]

AES представляет собой блочный, симметричный алгоритм шифрования с длиной блока 128 бит. Длина ключа может принимать значения 128, 192 или 256 бит (AES-128, AES-192 и AES-256, соответственно). Таким образом, в обозримом будущем алгоритм защищен от атак методом полного перебора ключей. К достоинствам алгоритма относятся также высокое быстродействие и умеренные требования к памяти. И, следовательно, он может быть реализован в различных устройствах, включая SIM-карты мобильного телефона и смарт-карты.

Обратим особое внимание и на то, что алгоритм Rijndael не защищен патентами и доступен для свободного использования в любых программных продуктах. Поэтому, AES стал практически (де-факто, не де-юро) международным стандартом.

Алгоритм IDEA

Тщательному анализу со стороны криптоаналитиков подвергался широко известный **алгоритм IDEA**, представляющий собой симметричный блочный шифр с длиной ключа 128 бит.

В процессе преобразования IDEA данные подвергаются комбинированным операциям XOR, побитовому сложению и умножению в течение 8 раундов. В результате получаются сложные преобразования, вызывающие трудности криптоанализа.

Алгоритм IDEA был разработан сотрудниками Швейцарского федерального института технологий (г. Цюрих) Сюдзя Лай и Джеймсом Мэсси. Опубликован в 1990/1991 годах.

Он считается более стойким, чем традиционный DEA, и представляет основу программы шифрования PGP, применяемой пользователями Internet.

Разработчиком программы PGP, вначале известной как программы шифрования электронной почты, является Фил Циммерман. Создав PGP, он опубликовал программу в Internet. За это власти США возбудили против него уголовное дело. «За экспорт криптостойких шифров» его приравняли к торговцам оружием и наркотиками, признав тем самым, что алгоритмы, входящие в PGP - IDEA и RSA «оказались слишком крепким орешком для правительственных чиновников».

Благодаря действительно «хорошим» алгоритмам шифрования и такой рекламе программа PGP быстро завоевала популярность у пользователей всего мира. После закрытия уголовного дела Ф. Циммерман основал фирму PGP Inc. Сегодня он консультирует крупнейшие компании и организации по вопросам безопасности и является признанным специалистом в области криптографии.

Другие симметричные криптоалгоритмы

Таким образом, существует множество симметричных криптоалгоритмов. Отметим следующие из них:

алгоритм ГОСТ с 256-битовым ключом, основанный на концепции алгоритма DEA, но более оптимальный для программной реализации;

алгоритм Blowfish с переменной (до 448 бит) длиной ключа, разработанный Б. Шнайером (B. Schneier) в 1993 г.;

алгоритм RC5, разработанный Р. Райвестом (R. Rivest) в 1995 г. и представляющий собой блочный шифр с параметрами: размер блока, размер ключа, число раундов;

алгоритм CAST-128, разработанный в 1997 г. К. Адамсом (C. Adams) и С. Таваресом (S.Tavares), который подвержен криптоанализу только полным перебором ключей (допускается использование ключей длиной от 40 до 128 бит);

Особо отметим алгоритмы, разработанные двумя известными специалистами в области криптографии Брюсом Шнайером и Роном Райвестом.

Шифры Брюса Шнайера и шифры Ривеста

Брюс Шнаейр (B. Schneier) - независимый консультант и самый известный во всем мире специалист по криптографии

Алгоритм Blowfish (1993 г.) – 64 разрядный блочный шифр с переменной (от 32 до 448 бит) длиной ключа

Превосходит DES по скорости и стойкости. НЕПАТЕНТОВАННЫЙ, бесплатный и беспошлинный. Используется во многих коммерческих приложениях.

Алгоритм Twofish (кандидат на роль AES) – 128-разрядный блочный алгоритм, поддерживающий ключи длиной 128, 192, 256 разрядов.

Разработан компанией Б.Шнайера Counterpane Systems. НЕПАТЕНТОВАННЫЙ, бесплатный и беспошлинный.

Ronald (Ron) Rivest – ключевая фигура в современной криптографии. Он профессор Массачусетского технологического института, основатель компании RSA. Изобрел целую серию шифров, которые носят его имя – **Ron's code.**

Заметим, что в отличие от шифров Б. Шнаейреа, все шифры Ривеста

ПАТЕНТОВАННЫЕ

RC2 – 64-разрядный блочный шифр с ключом переменной длины (экспорт при ограничении ключа до 40 разрядов). Скорость больше, чем у DES.

RC4 (1994 г.) – усовершенствованный RC2.

RC5 (1995г.) – усовершенствованный RC4. Семейство алгоритмов, так как реализуется для различных параметров: длина блока, длина ключа, количество раундов.

RC6 (кандидат на роль AES) – 128-блочный шифр на базе RC5**.**

Несколько слов о безопасности симметричных криптосистем

Забегая вперед, обратим внимание, что для криптоанализа симметричных систем разработано множество методов:

- метод полного перебора ключей,
- методы криптоанализа с использованием теории статистических решений,
- разностный криптоанализ и его модификации,
- линейный криптоанализ.

С помощью данных методов осуществлены эффективные криптоатаки на большинство симметричных криптосистем.

Безопасность симметричных криптосистем определяется двумя факторами:

- стойкостью самого алгоритма,
- длиной ключей.

Критерием качественного шифрования служит следующий принцип:

стойкость шифра должна определяться только секретностью ключа (правило Кирхгоффса -Dutchman A. Kerckhoffs) .

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. **Задача:**

Криптоаналитик перехватил 2 сообщения: одно зашифровано алгоритмом DES ключом длиной 56 бит, а второе алгоритмом AES (Rijndael) ключом длиной 256 бит. Требуется оценить время необходимое криптоаналитику для перебора всех ключей по первому и второму сообщению, если компьютер криптоаналитика перебирает около 1 млрд. ключей в секунду.

Пример решения задачи:

Попробуем оценить время на перебор всех ключей к первому сообщению, зашифрованному алгоритмом DES. Найдем общее количество возможных ключей: $N=2^{56}=72057594037927936$. Оценим
время $t=72057594037927936/1000000000 \approx 72057594$ сек$\approx$834 дня$\approx$2,3 года.

Самостоятельно оцените время необходимое криптоаналитику для перебора всех ключей ко второму сообщению, зашифрованному алгоритмом AES (Rijndael) и сделайте аналитический вывод о сравнительной криптостойкости алгоритмов.

Пусть у криптоаналитика в распоряжении не один, а 100 идентичных компьютеров, способных работать одновременно над разными множествами ключей. Решите задачу о времени перебора ключей с учетом этого условия и сделайте вывод о падении

уровня криптостойкости алгоритмов DES и AES при количественном увеличении вычислительных мощностей.

Сколько криптоаналитику нужно компьютеров, чтобы перебрать все ключи к сообщению, зашифрованному алгоритмом AES, за 1 год. Сделайте вывод.

2. **Раскодируйте фразу AES (Rijndael) алгоритме шифрования 256 бит, ключ 123**

U2FsdGVkX1+iDeOqw0Hv5PKKMaDDZz8KqbEPZQhCHusVjM+3Rsi2s6+S47a2pCzk
PCJIvKtyguJt/OSGl0PL+gcPvJYN38g7masXJDQ5nJuapPSZr9zSCXoes72EME4H
IpLgLJreBppY7tI2Ej3VbcBrqKK8aSR927HNmmlCsafY9fxN4nUBhfMgVFVrQkPV
CQqUwr9HCIMDKx1vFeobFpaDAlDvvMH296skAqMWsTjjZ59b9+gWC6MgdT47NnsI
pKsiIlxOL8H5+/XaTe2LPPKglNQqGXKwgoHpC5Wr+efCE9tiykjMrqVHZDSLfmJ1
p+yt6JO5PFILoGDdzNPoWDVhJYvz3S3zjX2L5y0nnbuVhj2srgoU7H8MEIc0IKIX
MikxXJ5Q18jR7XYrWntcqNDxfVUv3a3We+bAU+Gp15S6bmLE+cy338cNcEndEEuY
cLE9iiu+0wFh66Av5qKa5ctZLHQTFn+LKDbUNmjtw1ISwl0UcNidbYRCpfxss7YT
UFQMywB70VFgdPvAtHrZ0KIZWbs1ZW6kv28l/liZdxg=

3. **Раскодируйте фразу в алгоритме шифрования RC4, ключ 2**

0b/TrdKw0JTQsdGXw4jRhCnTl9O80rXTssKn0q/RjNO80ZTSqNGA0J3CnsO50anChN
Gk0bPTjtKtwrnSldCP0oRn0LbRt9CT0ITRp9GT079N0LjCrdCP0oLQjtKg0qXSldCTG9C805n
RptK30YXSqdOc0aDCldKf0qTRrNO906DCptK50anTmdKf05rTp9O9MtGk05XTqtOV0ILQk
dKV0rnRvNGF0KXCj9GTwpbSp8KV053Su9GS0YXRltO20IPRj9C80Y7Dr9G406PRodGv0K
rRv9OhwoPRmtOV04zRqNOI07A=

4. **Решите задачу.**

Тридцати двум буквам русского алфавита А, Б, В, ..., Э, Ю, Я приписаны соответственно числа 1, 2, 3, ..., 30, 31, 0 (буквы Е и Ё отождествляются). Выбрано некоторое нечетное число k (секретный ключ). Шифрование текста осуществляется побуквенно следующим образом:
1) число a, соответствующее данной букве, умножается на k,
2) вычисляется остаток r от деления a*k на 32,
3) выписывается буква, соответствующая числу r.
Расшифруйте криптограмму:
МН ЩЩКФД ГШМОМЫД ЦЫДЩЩ.

5. **Реши задачу.**

Шифр Цезаря. Криптограмма ЩНТШНЬ получена из открытого текста циклическим сдвигом букв русского алфавита (А...ДЕЖ...ЩЬ...Я) на k знаков вправо. Найдите ключ k, восстановите исходное сообщение, а затем зашифруйте его циклическим сдвигом на k знаков влево.

Тема 20. Использование электронной цифровой подписи (ЭЦП).

20.1 Электронно-цифровая подпись (ЭЦП) - это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Электронно-цифровая подпись - это программно-криптографическое средство, которое обеспечивает:

• проверку целостности документов;

• конфиденциальность документов;

• установление лица, отправившего документ.

Преимущества использования электронно-цифровой подписи

Использование электронно-цифровой подписи позволяет:

• значительно сократить время, затрачиваемое на оформление сделки и обмен документацией;

• усовершенствовать и удешевить процедуру подготовки, доставки, учета и хранения документов;

• гарантировать достоверность документации;

• минимизировать риск финансовых потерь за счет повышения конфиденциальности информационного обмена;

• построить корпоративную систему обмена документами.

Виды электронно-цифровой подписи

Существует три вида электронной цифровой подписи:

• простая электронно-цифровая подпись;

• усиленная неквалифицированная электронно-цифровая подпись;

• усиленная квалифицированная электронно-цифровая подпись.

Простая электронно-цифровая подпись

Посредством использования кодов, паролей или иных средств, простая электронно-цифровая подпись подтверждает факт формирования электронной подписи определенным лицом.

Простая электронно-цифровая подпись имеет низкую степень защиты. Она позволяет лишь определить автора документа.

Простая электронно-цифровая подпись не защищает документ от подделки.

Усиленная неквалифицированная электронно-цифровая подпись

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронный документ;

3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) создается с использованием средств электронной подписи.

Усиленная неквалифицированная электронно-цифровая подпись имеет среднюю степень защиты.

Чтобы использовать неквалифицированную электронную подпись, необходим сертификат ключа ее проверки.

Усиленная квалифицированная электронно-цифровая подпись

Для квалифицированной электронной подписи характерны признаки неквалифицированной электронной подписи.

Усиленная квалифицированная электронно-цифровая подпись соответствует следующим дополнительным признакам подписи:

1) ключ проверки электронной подписи указан в квалифицированном сертификате;

2) для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям законодательства.

Усиленная квалифицированная электронно-цифровая подпись является наиболее универсальной и стандартизованной подписью с высокой степенью защиты.

Документ, визированный такой подписью, аналогичен бумажному варианту с собственноручной подписью.

Использовать такую подпись можно и без каких-либо дополнительных соглашений и регламентов между участниками электронного документооборота.

Если под документом стоит квалифицированная подпись, можно точно определить, какой именно сотрудник организации ее поставил.

А также установить, изменялся ли документ уже после того, как был подписан.

Где приобрести ЭЦП

Сегодня сделатьЭЦП можно быстро и легко. Для этого нужно отправить онлайн заявку в один из аккредитованных удостоверяющих центров и предоставить необходимые документы.

Простая электронно-цифровая подпись

Обращение заявителей - юридических лиц за получением государственных и муниципальных услуг осуществляется путем подписания обращения уполномоченным лицом с использованием простой электронной подписи.

Использование простой электронной подписи для получения государственной услуги допускается, если законами или иными нормативными актами не установлен запрет на обращение за получением государственной услуги в электронной форме, а также не установлено использование в этих целях иного вида электронной подписи

Усиленная неквалифицированная электронно-цифровая подпись

Случаи, в которых информация в электронной форме, подписанная неквалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в Налоговом кодексе не определены.

Для целей налогового учета документ, оформленный в электронном виде и подписанный неквалифицированной электронной подписью, не может являться документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

Поэтому, хотя хозяйствующие стороны при наличии юридически действительного соглашения могут организовать электронный документооборот, применяя усиленную неквалифицированную электронную подпись, если есть вероятность возникновения споров с контролирующим органом, смысл в таких документах утрачивается.

Усиленная квалифицированная электронно-цифровая подпись

Для некоторых видов отчетности использование квалифицированной подписи прямо определено нормативными документами.

Электронный счет-фактуру следует подписывать только усиленной квалифицированной электронной подписью руководителя либо иных лиц, уполномоченных на это приказом (иным распорядительным документом) или доверенностью от имени организации, индивидуального предпринимателя.

Заявление о постановке на учет (снятии с учета) в налоговом органе заверяется только усиленной квалифицированной подписью.

Заявления о возврате или зачете суммы налога также принимаются только в случае, если они визированы усиленной квалифицированной электронной подписью.

20.2 Использование электронной цифровой подписи в Казахстане

1. Электронная цифровая подпись равнозначна собственноручной подписи подписывающего лица и влечет одинаковые юридические последствия при выполнении следующих условий:

1) удостоверена подлинность электронной цифровой подписи при помощи открытого ключа, имеющего регистрационное свидетельство;

2) лицо, подписавшее электронный документ, правомерно владеет закрытым ключом электронной цифровой подписи;

3) электронная цифровая подпись используется в соответствии со сведениями, указанными в регистрационном свидетельстве;

Пункт дополнен подпунктом 4 в соответствии с Законом РК от 24.11.15 г. № 419-V

4) электронная цифровая подпись создана и регистрационное свидетельство выдано аккредитованным удостоверяющим центром Республики Казахстан или иностранным удостоверяющим центром, зарегистрированным в доверенной третьей стороне Республики Казахстан.

В пункт 2 внесены изменения в соответствии с Законом РК от 15.07.10 г. № 337-IV (см. стар. ред.); изложен в редакции Закона РК от 24.11.15 г. № 419-V (см. стар. ред.); внесены изменения в соответствии с Законом РК от 25.06.20 г. № 347-VI (см. стар. ред.)

2. Закрытые ключи электронной цифровой подписи являются собственностью лиц, владеющих ими на законных основаниях.

Лицо может иметь закрытые ключи электронной цифровой подписи для различных информационных систем. Закрытые ключи электронной цифровой подписи не могут быть переданы другим лицам.

Допускается хранение закрытых ключей электронной цифровой подписи в удостоверяющем центре в соответствии с правилами создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре.

Пункт 3 изложен в редакции Закона РК от 24.11.15 г. № 419-V (см. стар. ред.)

3. Владелец регистрационного свидетельства электронной цифровой подписи юридического лица - руководитель юридического лица или лицо, его замещающее, вправе передавать работнику данного юридического лица или назначенному им лицу полномочия на использование электронной цифровой подписи от имени данного юридического лица.

20.3 Пример использования ЭЦП в государственных закупках

Электронная цифровая подпись (далее - ЭЦП) в государственных закупках, как и в иных сферах является средством подтверждения достоверности электронного документа. Зачастую ЭЦП называют реквизитом электронного документа, позволяющим установить отсутствие искажения информации в электронном документе и проверить принадлежность подписи владельцу сертификата ключа ЭЦП.

Что такое ЭЦП?

Согласно подпункту 12) пункта 1 Правил проведения электронных государственных закупок электронная цифровая подпись - это набор электронных цифровых символов, который подтверждает принадлежность подписи владельцу и достоверность электронного документа.

Аналогичное определение ЭЦП предусмотрено подпунктом 13) статьи 1 Закона Республики Казахстан "Об электронном документе и электронной цифровой подписи".

Что такое электронный документ?

Электронным документом является тот документ, в котором информация предоставлена в электронно-цифровой форме и удостоверена посредством ЭЦП (подпункт 37) статьи 1 Закона Республики Казахстан "О государственных закупках", подпункт 8) пункта 1 Правил проведения электронных государственных закупок, подпункт 10) статьи 1 Закона "Об электронном документе и электронной цифровой подписи").

При проведении электронных государственных закупок электронными документами являются документы, размещенные на веб-портале государственных закупок, а именно: объявление о проведении электронных государственных закупок, протоколы о допуске, итогах, проект договора о государственных закупках и т.д..

Использование ЭЦП в гос.закупках.

Согласно пункту 1 статьи 10 Закона "Об электронном документе и электронной цифровой подписи" электронная цифровая подпись, как и собственноручная подпись подписывающего лица, имеет равнозначную силу и влечет одинаковые юридические последствия, если:

- удостоверена подлинность ЭЦП при помощи открытого ключа, имеющего регистрационное свидетельство;
- лицо, подписавшее электронный документ, правомерно владеет закрытым ключом ЭЦП;
- ЭЦП используется в соответствии со сведениями, указанными в регистрационном свидетельстве.

ЭЦП при осуществлении государственных закупок используется должностными лицами государственных органов при удостоверении электронных документов, издаваемых ими в пределах своих полномочий и размещаемых на веб-портале государственных закупок (пункт 1 статьи 12 Закона "Об электронном документе и электронной цифровой подписи").

Кто является участников веб-портала гос.закупок?

В соответствии с подпунктом 4) статьи 1 Правил проведения электронных государственных закупок участниками веб-портала государственных закупок могут быть только заказчик, организатор госзакупок и потенциальный поставщик, зарегистрировавшийся на веб-портале.

Кто является уполномоченым представителем на веб-портале гос.закупок?

Подпунктом 11) пункта 1 Правил проведения электронных государственных закупок предусмотрено , что уполномоченным представителем на веб-портале может быть пользователь участника веб-портала, которому решением первого руководителя делегированы права на выполнение всех действий на веб-портале, в том числе и заверение электронных копий бумажных документов.

Подписывающее лицо вправе передавать полномочия на использование ЭЦП своему представителю в соответствии с нормами действующего законодательства (пункт 3 статьи 10 Закона "Об электронном документе и электронной цифровой подписи")

Уполномоченным представителем на веб-портале может быть лицо, кому только первым руководителем делегированы полномочия для для выполнение всех действий на веб-портале, в том числе и заверение электронных копий бумажных документов посредством ЭЦП, принадлежащей первому руководителю. Следовательно, подписывать

электронный документ на веб-портале государственных закупок вправе только первый руководитель или лицо, имеющее соответствующие полномочия. Делегирование полномочий в обратном порядке законом не предусмотрено.

Возможно ли подписание документа лицом, не имеющим ЭЦП?

Лицом, подписывающим электронный документ, может быть физическое или юридическое лицо, которое правомерно владеет закрытым ключом ЭЦП и обладает соответствующими правами на ее использование. (подпункт 6) статьи 1 Закона "Об электронном документе и электронной цифровой подписи")

Статьей 22 Закона Республики Казахстан "Об информатизации" предусмотрено, что согласно требованиям делопроизводства, документирование электронных информационных ресурсов и сведений об информационных системах осуществляют только их собственники и (или) владельцы.

Для получения доступа к электронным информационным ресурсам необходимо направить запрос собственнику или владельцу информационной системы одним из следующих способов:

- путем передачи запроса с использованием электронной почты или в форме электронного документа, заверенного ЭЦП;
- путем непосредственного обращения пользователя к общедоступным электронным информационным ресурсам.

Запрос, направленный в форме электронного документа, заверенного ЭЦП, приравнивается к запросу, направленному на бумажном носителе и подписанному собственноручно лицом, направившего запрос (статья 35 Закона "Об информатизации")

ЭЦП предназначена для идентификации лица, подписавшего электронный документ и является полноценной заменой (аналогом) собственноручной подписи в случаях, предусмотренных законом. Использование ЭЦП позволяет осуществить контроль целостности передаваемого документа. В государственных закупках предусмотрено, что все документы, предусмотренные для размещения на веб-портале утверждаются и подписываются председателем комиссии (первым руководителем). Таким образом, подписывать документ при проведении государственных закупок вправе только первый руководитель с помощью своей ЭЦП или лицо, кому делегированы им права на выполнение всех действий на веб-портале, в том числе и заверение электронных копий бумажных документов. Первый руководитель не вправе подписывать документы не принадлежащей ему ЭЦП.

Тема 21. Вирусы и антивирусная защита.

Цель работы: ознакомиться с теоретическими аспектами защиты информации от вредоносных программ: разновидностями вирусов, способами заражения и методы борьбы. Ознакомиться с различными видами программных средств защиты от вирусов. Проверка настроек антивирусов, сканирование файлов, папок и дисков, обновления антивирусной базы Получить навыки работы с антивирусным пакетом **Антивирус Касперского**.

Теоретические сведения

Компьютерный вирус - это специально написанная небольшая по размерам программа, которая может "приписывать" себя к другим программам (т.е. "заражать" их), а также выполнять различные нежелательные действия на компьютере. Программа,

внутри которой находится вирус, называется "зараженной". Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и "заражает" другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы или FAT-таблицу, "засоряет" оперативную память и т.д.). Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться не всегда, а при выполнении определенных условий. После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и она работает также, как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной.

Компьютерный вирус может испортить, т.е. изменить ненадлежащим образом, любой файл на имеющихся в компьютере дисках. Но некоторые виды файлов вирус может "заразить". Это означает, что вирус может "внедриться" в эти файлы, т.е. изменить их так, что они будут содержать вирус, который при некоторых обстоятельствах может начать свою работу.

Методы защиты от компьютерных вирусов

Каким бы не был вирус, пользователю необходимо знать основные методы защиты откомпьютерных вирусов.

Для защиты от вирусов можно использовать:

- общие средства защиты информации, которые полезны также и как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действийпользователя;
- профилактические меры, позволяющие уменьшить вероятность заражениявирусом;
- специализированные программы для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов. Имеютсядве основные разновидности этих средств:

- копирование информации - создание копий файлов и системных областей дисков;
- разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их недостаточно. Необходимо и применение специализированных программ для защиты от вирусов. Эти программы можно разделить на несколько видов:детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины (иммунизаторы).

Задание 1.

Подготовить доклад на тему: «Общие сведения и особенности работы антивируснойпрограммы [***Название антивирусной программы***]» (**Название антивирусной программы выбрать согласно своему варианту из *Вариантов заданий к работе***).

Задание 2.

Изучить антивирусный пакет ***Антивирус Касперского***. Подготовить отчет по лабораторной работе.

Порядок выполнения

1). Сканирование папок на наличие вирусов:

– Двойным щелчком на значке антивируса на панели индикации открыть главноеокно программы;

– Изучить содержимое окна: обратить внимание на дату последнего обновления антивирусной базы и дату последней полной проверки компьютера;

– В своей личной папке создать папку **Подозрительные файлы** и создать там 2 файла:***Текстовый файл*** и ***Документ Microsoft Word***. Имена файлов ввестисогласно своему варианту по **Вариантам задания к работе**;
– Выбрав пункт в главном окне программы пункт **Проверка – Быстрая проверка** идобавить в окно заданий папку **Подозрительные файлы**.
– Выполнить проверку папки. По завершению сканирования, используя кнопку «**Отчеты**» - «**Сохранить как…**», сохранить отчет с результатами проверки впапке **Подозрительные файлы**. Имя файла-отчета – **Scan_Log**.

2). Обновление антивирусной базы:

– Нажмите на пункт **Обновление** и, используя кнопку **Обновить**, осуществитеобновление базы известных вирусов.
– По завершению обновления, используя кнопку «**Отчеты**» - «**Сохранить как…**»,, сохранить отчет об обновлении в папке **Подозрительные файлы**. Имя файла- отчета – **Upd_Log.**
– Закройте окно **Антивируса Касперского**.

Задание 3.

Изучить антивирусный пакет **Avast!**

Порядок выполнения;

1. Найдите иконку антивируса Avast! В системном трее, правой кнопкой мышки вызовите меню и выберите «Открыть интерфейс пользователя Avast!»
2. Перейдите на вкладку «Сканировать компьютер». Вам будет представлены 4 вида сканирования: Экспресс, Полное, Сканирование носителей и возможность выбратьпапку для сканирования вручную.
3. Выберите «Сканирование съемных носителей» и нажмите кнопку «Пуск» в окне антивируса – будут автоматически проверены все подключенные к компьютерусъемные носители (диски, флэшки, дискеты).
4. По завершении сканирования выберите четвертый вид сканирования и вручнуюукажите любую папку на вашем съемном носителе и проверьте её.
5. Во вкладке «Экраны в реальном времени», в подменю «Экран файловой системы» нажав кнопку «Расширенные настройки» вы можете разрешить/запретить антивирусу следующие действия:

- Сканировать программы при выполнении (например, программа excel.exe будет сканироваться при каждом выполнении Microsoft Excel)
- Сканировать сценарии при выполнении (например, файл JS (JavaScript) будет сканироваться при каждом его выполнении)
- Сканировать библиотеки (DLL) при загрузке (при выполнении программы будут сканироваться её вспомогательные файлы – библиотеки DLL и т.д.)

6. Во вкладке «Экраны в реальном времени», в подменю «Веб-экран» нажав кнопку «Расширенные настройки» вы можете разрешить/запретить антивирусу следующие действия:

- Включить веб-сканирование
- Использовать интеллектуальное сканирование потока

7. Во вкладке «Обслуживание» в подменю «Обновить» есть возможность ручного запуска обновлений для «Модуля сканирования и определения вирусов» и непосредственно для программы. (По умолчанию модуль обновляется автоматически, а обновление программы запрашивает разрешения

пользователя).

8. По завершению сканирования, используя кнопку «**Отчеты**» - «**Сохранить как…**», сохранить отчет с результатами проверки

Задание 4.

Изучить антивирусный пакет **Dr. Web CureIt**

1. При запуске этого портативного антивируса вам будет предложено запустить его в режиме усиленной защиты – он необходим в случае, если вредоносные программы блокируют работу операционной системы. Нажмите «Отмена».
2. Далее появится предупреждение, т.к. использование антивируса бесплатно доступно только для лечения домашних компьютеров. Нажмите «Нет».
3. Нажмите «Пуск» и будет автоматически запущены быстрая проверка компьютера.В этом режиме проверяются:
   - Оперативная память
   - Загрузочные секторы всех дисков
   - Объекты автозапуска
   - Корневой каталог загрузочного диска
   - Корневой каталог диска установки Windows
   - Системный каталог Windows
   - Папка Мои Документы
   - Временный каталог системы
   - Временный каталог пользователя
4. По окончании быстрой проверки выбрать в меню пункт «Выборочно» и указатьпуть к съемному носителю – выполнить его проверку.
5. По завершению сканирования, используя кнопку «**Отчеты**» - «**Сохранить как…**», сохранить отчет с результатами проверки

Содержание отчета

1). Название и цель лабораторной работы;
2). Доклад на выбранную по варианту тему;
3). Содержимое файла **Scan_Log.txt** по пункту 1 **Порядка выполнения работы**
4). Содержание файла **Upd_Log.txt** по П.2 **Порядка выполнения работы.**
5). Выводы.

Контрольные вопросы

1). Что называется компьютерным вирусом?
2). Какая программа называется "зараженной"?
3). Что происходит, когда зараженная программа начинает работу?
4). Как может маскироваться вирус?
5). Каковы признаки заражения вирусом?
6). Каковы последствия заражения компьютерным вирусом?
7). По каким признакам классифицируются компьютерные вирусы?
8). Как классифицируются вирусы по среде обитания?
9). Какие типы компьютерных вирусов выделяются по способу воздействия?
10). Что могут заразить вирусы?
11). Как маскируются "невидимые" вирусы?
12). Каковы особенности самомодифицирующихся вирусов?
13). Какие методы защиты от компьютерных вирусов можно использовать?
14). В каких случаях применяют специализированные программы защиты откомпьютерных вирусов?
15). На какие виды можно подразделить программы защиты от компьютерных вирусов?
16). Как действуют программы-детекторы?

17). Что называется сигнатурой?
18). Всегда ли детектор распознает зараженную программу?
19). Каков принцип действия программ-ревизоров, программ-фильтров, программ-вакцин?
20). Как выглядит многоуровневая защита от компьютерных вирусов с помощьюантивирусных программ?
21). Перечислите меры защиты информации от компьютерных вирусов.
22). Каковы современные технологии антивирусной защиты?
23). Каковы возможности антивируса Касперского для защиты файловых серверов?почтовых серверов?
24). Какие модули входят в состав антивируса Касперского для защиты файловыхсистем?
25). Каково назначение этих модулей?
26). Какие элементы электронного письма подвергаются проверке на наличие вирусов?
27). Как обезвреживаются антивирусом Касперского обнаруженные подозрительныеили инфицированные объекты?
28). Как обновляется база вирусных сигнатур?

Варианты заданий к работе

Вариант	**Нзвание антивирусной программы**
1	Dr.Web
2	McAfee VirusScan
3	Антивирус Касперского
4	Panda Anti-Virus
5	Avast!
6	AVS
7	AVG
8	Avira
9	Clam AntiVirus
10	ClamWin
11	NOD32
12	Trojan Hunter
13	VirusBuster
14	Norton AntiVirus
15	Windows Live OneCare
16	PC-cillin
17	F-Prot
18	F-Secure Anti-Virus
19	Comodo AntiVirus
20	Windows Live OneCare
21	NOD32
22	Avast!
23	Dr.Web
24	Антивирус Касперского
25	Trojan Hunter

Тема 22. Законодательные акты Республики Казахстан в области защиты информации.

Обзор законодательства Республики Казахстан в сфере информационной безопасности.

22.1 Общий обзор

Информационная безопасность рассматривается в Казахстане как неотъемлемая часть национальной безопасности и трактуется как **состояние защищенности информационного пространства Республики Казахстан, а также прав и интересов человека и гражданина, общества и государства в информационной сфере от реальных и потенциальных угроз, при котором обеспечивается устойчивое развитие и информационная независимость страны**.

В соответствии с **Законом «О национальной безопасности**» информационная безопасность обеспечивается решениями и действиями государственных органов, организаций, должностных лиц, направленными на:

1) недопущение информационной зависимости Казахстана;

2) предотвращение информационной экспансии и блокады со стороны других государств, организаций и отдельных лиц;

3) недопущение информационной изоляции Президента, Парламента, Правительства и сил обеспечения национальной безопасности Республики Казахстан;

4) обеспечение бесперебойной и устойчивой эксплуатации сетей связи в целях сохранения безопасности Республики Казахстан, в том числе в особый период и при возникновении чрезвычайных ситуаций природного, техногенного характера, карантинов, иных чрезвычайных ситуаций;

5) выявление, предупреждение и пресечение утечки и утраты сведений, составляющих государственные секреты и иную защищаемую законом тайну;

6) недопущение информационного воздействия на общественное и индивидуальное сознание, связанного с преднамеренным искажением и распространением недостоверной информации в ущерб национальной безопасности;

7) обнаружение и дезорганизацию механизмов скрытого информационного влияния на процесс выработки и принятия государственных решений в ущерб национальной безопасности;

8) поддержание и развитие эффективной системы защиты информационных ресурсов, информационных систем и инфраструктуры связи, в которых циркулируют сведения, составляющие государственную, коммерческую и иную защищаемую законом тайну. Особое внимание придается системе обеспечения информационной безопасности, в том числе государственных электронных информационных ресурсов, информационных систем, информационно-коммуникационной инфраструктуры и критически важных объектов информационно-коммуникационной инфраструктуры.

Перечень условий, препятствующих информационной безопасности.

Запрещено:

1) распространение на территории Республики Казахстан печатной продукции и продукции иностранного средства массовой информации, содержание которых подрывает национальную безопасность;

2) разглашение государственных секретов и иной защищаемой законом тайны;

3) иностранным физическим и юридическим лицам, а также лицам без гражданства прямо и (или) косвенно владеть, пользоваться, распоряжаться и (или) управлять более 20 процентами акций (долей, паев) юридического лица – собственника средства массовой информации в Республике Казахстан или осуществляющего деятельность в этой сфере;

4) управление или эксплуатация магистральными линиями связи иностранцами, лицами без гражданства и иностранными юридическими лицами без создания юридического лица на территории Республики Казахстан;

5) создание и эксплуатация на территории Республики Казахстан сетей связи, центр управления которыми расположен за ее пределами;

6) приобретение или иное получение в собственность физическими и юридическими лицами самостоятельно или в составе группы лиц более 10 процентов голосующих акций, а также долей, паев организации, владеющей и (или) осуществляющей деятельность по управлению или эксплуатации линии связи в качестве оператора междугородной и (или) международной связи, без согласия уполномоченного органа в области связи и информации, а также органов национальной безопасности;

7) иностранцам, лицам без гражданства и иностранным юридическим лицам прямо и (или) косвенно владеть, пользоваться, распоряжаться и (или) управлять в совокупности более чем 49 процентами голосующих акций, а также долей, паев юридического лица, осуществляющего деятельность в области телекоммуникаций в качестве оператора междугородной и (или) международной связи, владеющего наземными (кабельными, в том числе волоконно-оптическими, радиорелейными) линиями связи без положительного решения Правительства Республики Казахстан, основанного на заключении уполномоченного органа в области связи и информации, согласованного с органами национальной безопасности;

8) ввод в эксплуатацию сетей связи, не отвечающих требованиям нормативных правовых актов по обеспечению оперативно-розыскных мероприятий.

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ КАЗАХСТАН ДО 2016 ГОДА И ЕЕ РЕАЛИЗАЦИЯ

В Казахстане действует **Концепция информационной безопасности (далее — концепция) .** Концепция содержит:

- основные положения государственной стратегии по обеспечению информационной безопасности, основные определения и термины;
- анализ текущей ситуации, цели и задачи, которые стоят перед государством по обеспечению информационной безопасности, ожидаемые результаты;
- основные принципы и общие подходы обеспечения информационной безопасности в РК.

Концепция информационной безопасности выражает совокупность официальных взглядов на сущность и содержание деятельности Республики Казахстан по обеспечению информационной безопасности государства и общества, их защите от внутренних и внешних угроз. Концепция определяет задачи, приоритеты, направления и ожидаемые результаты в области обеспечения информационной безопасности личности, общества и государства. Она является основой для конструктивного взаимодействия органов государственной власти, бизнеса и общественных объединений для защиты национальных интересов Республики Казахстан в информационной сфере. Концепция призвана обеспечить единство подходов к формированию и реализации государственной политики обеспечения информационной безопасности, а также методологическую основу для совершенствования нормативных правовых актов, регулирующих данную сферу.

В соответствии с концепцией, текущее состояние обеспечения информационной безопасности характеризуется следующими угрозами:

1) несовершенства системы обеспечения информационной безопасности и нарушения функционирования критически важных объектов информатизации;

2) низкого уровня производства, внедрения и использования современных информационно-коммуникационных технологий, не отвечающего объективным потребностям общества;

3) зависимости Республики Казахстан от импорта информационных технологий, средств информатизации и защиты информации, использование которых может причинить ущерб национальным интересам страны;

4) нарастания информационного противоборства между ведущими мировыми центрами силы, подготовки и ведения зарубежными государствами борьбы в информационном пространстве;

5) неконструктивной политики иностранных государств в области глобального информационного мониторинга, распространения информации и новых информационных технологий;

6) развития технологий манипулирования информацией;

7) возможности деструктивного информационного воздействия на общественное сознание и государственные институты, наносящего ущерб национальным интересам страны;

8) распространения недостоверной или умышленно искаженной информации, способной причинить ущерб национальным интересам Республики Казахстан;

9) открытости и уязвимости национального информационного пространства от внешнего воздействия;

10) недостаточной эффективности информационного обеспечения государственной политики;

11) слабой защищенности и низкой конкурентоспособности национального информационного пространства;

12) несоответствия качества национального контента объективным потребностям казахстанского общества и мировому уровню;

13) роста преступности, в том числе транснациональной, а также экстремистской и террористической деятельности с использованием информационно-коммуникационных технологий;

14) попыток несанкционированного доступа извне к информационным ресурсам Республики Казахстан, приводящих к причинению ущерба ее национальным интересам;

15) деятельности иностранных разведывательных и специальных служб, а также иностранных политических и экономических структур, направленные против интересов Республики Казахстан;

16) нарушений режима секретности при работе со сведениями, составляющими государственные секреты Республики Казахстан, а также преднамеренных неправомерных действий и непреднамеренных ошибок и нарушений при работе с информацией ограниченного доступа;

17) недостаточного развития системы правового регулирования информационной сферы;

18) стихийных бедствий и катастроф;

19) неправомерных действий государственных структур, приводящих к нарушению законных прав и интересов физических и юридических лиц, государства в информационной сфере.

22.2 Персональные данные и их защита

Законодательство Республики Казахстан о персональных данных и гарантии их защиты.

Вопросы правового регулирования персональных данных, включая биометрические данные, их сбор, хранение, передачу, распространение и другие действия, методы защиты персональных данных регулируются в Казахстане законом Республики Казахстан «О персональных данных и их защите». Закон регулирует общественные отношения в сфере персональных данных, а также определяет цель, принципы и правовые основы деятельности, связанные со сбором, обработкой и защитой персональных данных.

Закон определяет персональные данные – сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе; а биометрические данные как персональные данные, которые характеризуют физиологические и биологические особенности субъекта персональных данных, на основе которых можно установить его личность.

Закон разграничивает персональные данные по категории доступа к ним. Персональные данные по доступности подразделяются на общедоступные и ограниченного доступа.

Общедоступные персональные данные – персональные данные, доступ к которым является свободным с согласия субъекта или на которые в соответствии с законодательством Республики Казахстан не распространяются требования соблюдения конфиденциальности, в том числе биографические справочники, телефонные, адресные книги, общедоступные электронные информационные ресурсы, средства массовой информации и т.д. Персональные данные ограниченного доступа – персональные данные, доступ к которым ограничен законодательством Республики Казахстан.

По общему правилу, сбор персональных данных осуществляется с согласия субъекта, которому принадлежат эти персональные данные, или его законного представителя. Однако закон устанавливает перечень случаев, когда сбор персональных данных осуществляется без согласия субъекта или его законного представителя:

1) осуществления деятельности правоохранительных органов и судов, исполнительного производства;

2) осуществления государственной статистической деятельности;

3) использования государственными органами персональных данных для статистических целей с обязательным условием их обезличивания;

4) реализации международных договоров, ратифицированных Республикой Казахстан;

5) защиты конституционных прав и свобод человека и гражданина, если получение согласия субъекта или его законного представителя невозможно;

6) осуществления законной профессиональной деятельности журналиста и (или) деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии соблюдения требований законодательства Республики Казахстан по обеспечению прав и свобод человека и гражданина;

7) опубликования персональных данных в соответствии с законами Республики Казахстан, в том числе персональных данных кандидатов на выборные государственные должности;

8) неисполнения субъектом своих обязанностей по представлению персональных данных в соответствии с законами Республики Казахстан;

9) получения государственным органом, осуществляющим регулирование, контроль и надзор финансового рынка и финансовых организаций, информации от физических и юридических лиц в соответствии с законодательством Республики Казахстан;

10) в иных случаях, установленных законами Республики Казахстан.

Субъект, которому принадлежат персональные данные или его законный представитель дает (или отзывает) согласие на сбор, обработку персональных данных письменно или в форме электронного документа либо иным способом с применением элементов защитных действий.

Лицо, которое осуществляет сбор, хранение, передачу, распространение или другие действия с персональными данными, в соответствии с Законом называется оператор персональных данных. В качестве оператора баз персональных данных может выступать государственный орган, физическое и (или) любое другое юридическое лицо, которые осуществляют сбор, обработку и защиту персональных данных.

Законом предусматриваются следующие действия (операции) по обработке персональных данных:

Действия (операции) по обработке персональных данных	*Описание действий (операций) по обработке персональных данных*
Обработка персональных данных	Действия, направленные на накопление, хранение, изменение, дополнение, использование, распространение, обезличивание, блокирование и уничтожение персональных данных
Сбор персональных данных	Действия, направленные на получение персональных данных
Блокирование персональных данных	Действия по временному прекращению сбора, накопления, изменения, дополнения, использования, распространения, обезличивания и уничтожения персональных данных
Накопление персональных данных	Действия по систематизации персональных данных путем их внесения в базу, содержащую персональные данные
Уничтожение персональных данных	Действия, в результате совершения которых невозможно восстановить персональные данные
Обезличивание персональных данных	Действия, в результате совершения которых определение принадлежности персональных данных субъекту персональных данных невозможно
Использование	Действия с персональными данными, направленные

персональных данных	на реализацию целей деятельности собственника, оператора и третьего лица
Хранение персональных данных	Действия по обеспечению целостности, конфиденциальности и доступности персональных данных
Распространение персональных данных	Действия, в результате совершения которых происходит передача персональных данных, в том числе через средства массовой информации или предоставление доступа к персональным данным каким-либо иным способом
Трансграничная передача персональных данных	Передача персональных данных на территорию иностранных государств.

Субъект, которому принадлежат персональные данные, наделен следующими правами:

1) вправе знать о наличии у собственника и (или) оператора, а также третьего лица своих персональных данных, а также получать информацию, содержащую: подтверждение факта, цели, источников, способов сбора и обработки персональных данных; перечень персональных данных; сроки обработки персональных данных, в том числе сроки их хранения;

2) требовать от собственника и (или) оператора изменения и дополнения своих персональных данных при наличии оснований, подтвержденных соответствующими документами;

3) требовать от собственника и (или) оператора, а также третьего лица блокирования своих персональных данных в случае наличия информации о нарушении условий сбора, обработки персональных данных;

4) требовать от собственника и (или) оператора, а также третьего лица уничтожения своих персональных данных, сбор и обработка которых произведены с нарушением законодательства Республики Казахстан, а также в иных случаях, установленных настоящим Законом и иными нормативными правовыми актами Республики Казахстан;

5) отозвать согласие на сбор, обработку персональных данных, кроме случаев законом;

6) дать согласие (отказать) собственнику и (или) оператору на распространение своих персональных данных в общедоступных источниках персональных данных;

7) на защиту своих прав и законных интересов, в том числе возмещение морального и материального вреда;

8) на осуществление иных прав, предусмотренных настоящим Законом и иными законами Республики Казахстан.

Собственник и (или) оператор баз персональных данных является обязанными лицами, и в соответствии с законом на них возлагаются следующие обязательства:

1) утверждать перечень персональных данных, необходимый и достаточный для выполнения осуществляемых ими задач, если иное не предусмотрено законами Республики Казахстан;

2) принимать и соблюдать необходимые меры, в том числе правовые, организационные и технические, для защиты персональных данных в соответствии с законодательством Республики Казахстан;

3) соблюдать законодательство Республики Казахстан о персональных данных и их защите;

4) принимать меры по уничтожению персональных данных в случае достижения цели их сбора и обработки, а также в иных случаях, установленных настоящим Законом и иными нормативными правовыми актами Республики Казахстан;

5) представлять доказательство о получении согласия субъекта на сбор и обработку его персональных данных в случаях, предусмотренных законодательством Республики Казахстан;

6) сообщать информацию, относящуюся к субъекту, в течение трех рабочих дней со дня получения обращения субъекта или его законного представителя, если иные сроки не предусмотрены законами Республики Казахстан;

7) в случае отказа предоставить информацию субъекту или его законному представителю в срок, не превышающий трех рабочих дней со дня получения обращения, представлять мотивированный ответ, если иные сроки не предусмотрены законами Республики Казахстан;

8) в течение одного рабочего дня:
изменить и (или) дополнить персональные данные на основании соответствующих документов, подтверждающих их достоверность, или уничтожить персональные данные при невозможности их изменения и (или) дополнения;
блокировать персональные данные, относящиеся к субъекту, в случае наличия информации о нарушении условий их сбора, обработки;
уничтожить персональные данные в случае подтверждения факта их сбора, обработки с нарушением законодательства Республики Казахстан, а также в иных случаях, установленных настоящим Законом и иными нормативными правовыми актами Республики Казахстан;
снять блокирование персональных данных в случае не подтверждения факта нарушения условий сбора, обработки персональных данных.

Гарантии защиты персональных данных— защита персональных данных осуществляется путем применения комплекса мер, в том числе правовых, организационных и технических, в целях:
1) реализации прав на неприкосновенность частной жизни, личную и семейную тайну;
2) обеспечения их целостности и сохранности;
3) соблюдения их конфиденциальности;
4) реализации права на доступ к ним;
5) предотвращения незаконного их сбора и обработки.

По закону уполномоченный орган в сфере персональных данных является Правительство Республики Казахстан, которое наделено следующей компетенцией:

1) разрабатывает основные направления государственной политики в сфере персональных данных и их защиты;

2) осуществляет руководство деятельностью центральных исполнительных органов, входящих в структуру Правительства Республики Казахстан, местных исполнительных органов, в сфере персональных данных и их защиты;

3) утверждает порядок определения собственником и (или) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач;

4) утверждает порядок осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных;

5) выполняет иные функции, возложенные на него Конституцией, законами Республики Казахстан и актами Президента Республики Казахстан.

Государственные органы в пределах своей компетенции:

1) разрабатывают и (или) утверждают нормативные правовые акты в сфере персональных данных и их защиты;

2) рассматривают обращения физических и (или) юридических лиц по вопросам персональных данных и их защиты;

3) принимают меры по привлечению лиц, допустивших нарушения законодательства Республики Казахстан о персональных данных и их защите, к ответственности, установленной законами Республики Казахстан;

4) осуществляют иные полномочия, предусмотренные законами Республики Казахстан, актами Президента Республики Казахстан и Правительства Республики Казахстан.

Общий надзор за соблюдение законодательства о персональных данных и их защите осуществляют органы прокуратуры. За нарушение требований законодательства предусмотрена ответственность:

Виды правовой ответственности	*Описание норм ответственности за нарушение требований законодательства о персональных данных и их защите*
Уголовная ответственность	Статья 147 Уголовного Кодекса Республики Казахстан. Нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите 1. Несоблюдение мер по защите персональных данных лицом, на которое возложена обязанность принятия таких мер, если это деяние причинило существенный вред правам и законным интересам лиц, — наказывается штрафом в размере до трех тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового. 2. Незаконное собирание сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо причинение существенного вреда правам и законным интересам лица в результате незаконных сбора и (или) обработки иных персональных данных – наказывается штрафом в размере до пяти тысяч месячных расчетных показателей либо исправительными работами в том же

	размере, либо ограничением свободы на срок до трех лет, либо лишением свободы на тот же срок. 3. Деяния, предусмотренные частью второй настоящей статьи, совершенные лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации, либо путем незаконного доступа к электронным информационным ресурсам, информационной системе или незаконного перехвата информации, передаваемой по сети телекоммуникаций, либо в целях извлечения выгод и преимуществ для себя или для других лиц, или организаций – наказываются лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет или без такового. 4. Распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо причинение существенного вреда правам и законным интересам лица в результате незаконного сбора и (или) обработки иных персональных данных – наказывается лишением свободы на срок до пяти лет. 5. Распространение сведений, указанных в части четвертой настоящей статьи, в публичном выступлении, публично демонстрирующемся произведении, в средствах массовой информации или с использованием сетей телекоммуникаций – наказывается лишением свободы на срок до семи лет.
Административная ответственность	Статья 79 Кодекса Республики Казахстан «Об административных правонарушениях». Нарушение законодательства Республики Казахстан о персональных данных и их защите 1. Незаконный сбор и (или) обработка персональных данных – влекут штраф на физических лиц в размере двадцати, на должностных лиц, субъектов малого предпринимательства или некоммерческие организации – в размере тридцати, на субъектов среднего предпринимательства – в размере пятидесяти, на субъектов крупного предпринимательства – в размере ста месячных расчетных показателей, с конфискацией предметов и (или) орудия административного правонарушения или без таковой. 2. Те же деяния, совершенные собственником, оператором или третьим лицом с использованием своего служебного положения, если эти действия не влекут установленную законом уголовную ответственность – влекут штраф на физических лиц в размере пятидесяти, на должностных лиц, субъектов малого предпринимательства или некоммерческие организации – в размере

	семидесяти пяти, на субъектов среднего предпринимательства – в размере ста, на субъектов крупного предпринимательства – в размере двухсот месячных расчетных показателей, с конфискацией предметов и (или) орудия административного правонарушения или без таковой. 3. Несоблюдение собственником, оператором или третьим лицом мер по защите персональных данных – влечет штраф на физических лиц в размере ста, на должностных лиц, субъектов малого предпринимательства или некоммерческие организации – в размере ста пятидесяти, на субъектов среднего предпринимательства – в размере двухсот, на субъектов крупного предпринимательства – в размере трехсот месячных расчетных показателей. 4. Деяние, предусмотренное частью третьей настоящей статьи, повлекшее утерю, незаконный сбор и (или) обработку персональных данных, если эти деяния не влекут установленную законом уголовную ответственность, – влечет штраф на физических лиц в размере двухсот, на должностных лиц, субъектов малого предпринимательства или некоммерческие организации – в размере пятисот, на субъектов среднего предпринимательства – в размере семисот, на субъектов крупного предпринимательства – в размере тысячи месячных расчетных показателей.
Гражданско-правовая ответственность	1.Оспаривание действия (бездействия) субъекта, собственника и (или) оператора, а также третьего лица при сборе, обработке и защите персональных данных могут быть обжалованы в порядке, установленной главой 29 Гражданского процессуального Кодекса Республики Казахстан. 2. Споры, возникающие при сборе, обработке и защите персональных данных, подлежат рассмотрению в порядке, установленном Гражданским процессуальным Кодексом Республики Казахстан.

22.3 Борьба с киберпреступностью

В 2014 году в Казахстане был принят новый Уголовный кодекс. Одной особенностью нового уголовного закона было включение целого ряда составов уголовных правонарушений в сфере информатизации и связи. Предыдущая редакция Уголовного кодекса не содержала аналогичных составов. Поскольку эти составы включены в кодекс совсем недавно, мы не располагаем сведениями о возбужденных, расследованных уголовных делах по данным статьям. Нам также не известна судебная практика и избранные меры наказания для лиц, признанных виновными в совершении данных деяний.

Ниже в таблице представлены составы уголовных правонарушений и меры ответственности за их совершение, предусмотренные Уголовным кодексом Республики Казахстан в действующей редакции.

Статья 205.	1. Умышленный неправомерный доступ к охраняемой

Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций	законом информации, содержащейся на электронном носителе, в информационную систему или сеть телекоммуникаций, повлекший существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, – **наказывается штрафом в размере до трехсот месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до двухсот сорока часов, либо арестом на срок до семидесяти пяти суток, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового**. 2. То же деяние, совершенное в отношении государственных электронных информационных ресурсов или информационных систем государственных органов, – **наказывается штрафом в размере до пятисот месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до трехсот часов, либо арестом на срок до девяноста суток, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового.** 3. Деяния, предусмотренные частями первой или второй настоящей статьи, повлекшие по неосторожности тяжкие последствия, – **наказываются штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.**
Статья 206. Неправомерные уничтожение или модификация информации	1. Умышленные неправомерные уничтожение или модификация охраняемой законом информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, а равно ввод в информационную систему заведомо ложной информации, если это повлекло существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, – **наказываются штрафом в размере до пятисот**

	месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до трехсот часов, либо арестом на срок до девяноста суток, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового. 2. Те же деяния, совершенные: 1) в отношении государственных электронных информационных ресурсов или информационных систем государственных органов; 2) группой лиц по предварительному сговору, – **наказываются штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.** 3. Деяния, предусмотренные частями первой или второй настоящей статьи: 1) совершенные преступной группой; 2) повлекшие тяжкие последствия, – **наказываются лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.**
Статья 207. Нарушение работы информационной системы или сетей телекоммуникаций	1. Умышленные действия (бездействие), направленные на нарушение работы информационной системы или сетей телекоммуникаций, – **наказываются штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового.** 2. Те же деяния, совершенные: 1) в отношении государственных электронных информационных ресурсов или информационных систем государственных органов; 2) группой лиц по предварительному сговору, –

	наказываются штрафом в размере до четырех тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо ограничением свободы на срок до четырех лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового. 3. Деяния, предусмотренные частями первой или второй настоящей статьи: 1) совершенные преступной группой; 2) повлекшие тяжкие последствия, – **наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.**
Статья 208. Неправомерное завладение информацией	1. Умышленное неправомерное копирование или иное неправомерное завладение охраняемой законом информацией, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, если это повлекло существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, – **наказывается штрафом в размере до двухсот месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до ста восьмидесяти часов, либо арестом на срок до шестидесяти суток, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового.** 2. То же деяние, совершенное: 1) в отношении государственных электронных информационных ресурсов или информационных систем государственных органов; 2) группой лиц по предварительному сговору, – **наказывается штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без**

	такового. 3. Деяния, предусмотренные частями первой или второй настоящей статьи: 1) совершенные преступной группой; 2) повлекшие тяжкие последствия, – **наказываются лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.**
Статья 209. Принуждение к передаче информации	1. Принуждение к передаче охраняемой законом информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, под угрозой применения насилия либо уничтожения или повреждения имущества, а равно под угрозой распространения сведений, позорящих потерпевшего или его близких, либо иных сведений, оглашение которых может причинить существенный вред интересам потерпевшего или его близких, – **наказывается штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет или без такового.** 2. То же деяние: 1) сопряженное с применением физического насилия над лицом или его близкими; 2) совершенное группой лиц по предварительному сговору; 3) совершенное с целью получения информации из государственных электронных информационных ресурсов или информационных систем государственных органов, – **наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.** 3. Деяния, предусмотренные частями первой или второй настоящей статьи: 1) совершенные преступной группой; 2) повлекшие тяжкие последствия, – **наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью**

	на срок до пяти лет или без такового.
Статья 210. Создание, использование или распространение вредоносных компьютерных программ и программных продуктов	1. Создание компьютерной программы, программного продукта или внесение изменений в существующую программу или программный продукт с целью неправомерного уничтожения, блокирования, модификации, копирования, использования информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по сетям телекоммуникаций, нарушения работы компьютера, абонентского устройства, компьютерной программы, информационной системы или сетей телекоммуникаций, а равно умышленные использование и (или) распространение такой программы или программного продукта – **наказываются штрафом в размере до трех тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо ограничением свободы на срок до трех лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.** 2. Те же деяния, совершенные: 1) группой лиц по предварительному сговору; 2) лицом с использованием своего служебного положения; 3) в отношении государственных электронных информационных ресурсов или информационных систем государственных органов, – **наказываются ограничением свободы на срок от трех до семи лет либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.** 3. Деяния, предусмотренные частями первой или второй настоящей статьи: 1) совершенные преступной группой; 2) повлекшие тяжкие последствия, – **наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.**
Статья 211. Неправомерное распространение электронных информационных ресурсов ограниченного	1. Неправомерное распространение электронных информационных ресурсов, содержащих персональные данные граждан или иные сведения, доступ к которым ограничен законами Республики Казахстан или их собственником или владельцем, – **наказывается штрафом в размере до двухсот месячных**

доступа	**расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до ста восьмидесяти часов, либо арестом на срок до шестидесяти суток, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.** 2. То же деяние, совершенное: 1) группой лиц по предварительному сговору; 2) из корыстных побуждений; 3) лицом с использованием своего служебного положения, – **наказывается ограничением свободы на срок до пяти лет либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.** 3. Деяния, предусмотренные частями первой или второй настоящей статьи: 1) совершенные преступной группой; 2) повлекшие тяжкие последствия, – **наказываются лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового**.
Статья 212. Предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели	1. Заведомо противоправное оказание услуг по предоставлению аппаратно-программных комплексов, функционирующих в открытой информационно-коммуникационной сети, для размещения интернет-ресурсов, преследующих противоправные цели, – **наказывается штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до двух лет.** 2. То же деяние, совершенное группой лиц по предварительному сговору или преступной группой, – **наказывается лишением свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.**
Статья 213. Неправомерные	1. Изменение идентификационного кода абонентского устройства сотовой связи, создание дубликата карты

изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства	идентификации абонента сотовой связи, если эти действия совершены без согласия производителя или законного владельца, – **наказываются штрафом в размере до трехсот месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до двухсот сорока часов, либо арестом на срок до семидесяти пяти суток.** 2. Неправомерные создание, использование, распространение программ, позволяющих изменять идентификационный код абонентского устройства сотовой связи или создавать дубликат карты идентификации абонента сотовой связи, – **наказываются штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок.** 3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные преступной группой, – **наказываются лишением свободы на срок до пяти лет.**

ЗАКЛЮЧЕНИЕ

Изучение основ защиты информации, методов защиты и их классификацию позволит получить представление о теории и практических методах и средствах защиты информации, сформировать навыки их применения при реализации информационных процессов ввода, вывода, передачи, обработки и хранении информации.

Умение ставить и решать конкретные задачи по применению средств защиты информации позволит оптимизировать функционирование информационных систем (ИС) и оценивать уровень безопасности в ИС;

Знания и навыки в области информационной безопасности могут быть использованы обучающимися при выполнении выпускных работ, а так же в практике системного администрирования ЛВС.