МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

М. И. Шубинский

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЛЯ РАБОТНИКОВ БЮДЖЕТНОЙ СФЕРЫ

Учебное пособие

Санкт-Петербург

2012

Шубинский М.И. **Информационная безопасность для работников бюджетной сферы:** Учебное пособие. – СПб.: НИУ ИТМО, 2012. – 102 с.

В пособии изложены базовые положения информационной безопасности, используемые при построении информационных систем бюджетных учреждений и их последующего функционирования. Рассматриваются вопросы законодательства, авторизации и идентификации, криптографии и антивирусной защиты.

Издание адресовано студентам магистерской программы «Управление государственными информационными системами» по направлению 220100 «Системный анализ и управление» и слушателям дополнительной образовательной программы повышения квалификации «Электронное правительство и инновационные технологии управления», реализуемой Центром технологий электронного правительства НИУ ИТМО.

Рекомендовано к печати Ученым советом Магистерского корпоративного факультета (прот. № 1 от 06.04.2012).

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена Программа развития *государственного образовательного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет информационных технологий, механики и оптики» на 2009–2018 годы*.

Оглавление

Введение 5

Глава 1. Что такое информационная безопасность 7

1.1. Определение информационной безопасности 7
1.2. Основные угрозы информационной безопасности 9
1.3. Преднамеренные воздействия 10

Глава 2. Законодательство по вопросам информационной безопасности 13

2.1. Конституция Российской Федерации 13
2.2. Уголовный кодекс Российской Федерации 14
2.3. Закон «О государственной тайне» от 21 июля 1993 года N 5486-1 . 15
2.4. Закон «О коммерческой тайне» № 98-ФЗ от 2004 года 16
2.5. Закон «О персональных данных» №152-ФЗ от 2006 года 18
2.6. Закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года N 149-ФЗ 21
2.7. Закон «О лицензировании отдельных видов деятельности» 23
2.8. Гражданский кодекс Российской Федерации 25
2.9. Кодекс об административных правонарушениях Российской Федерации 28

Глава 3. Идентификация и аутентификация 31

3.1. Основные понятия 31
3.2. Парольная аутентификация 33
3.3. Идентификация/аутентификация с помощью биометрических данных 34

Глава 4. Введение в криптографию 37

4.1. Общее понятие о криптографии 37
4.2. Основные требования к криптографическому закрытию информации в АС 38
4.3. Организационные проблемы криптозащиты 44
4.4. Сертификация и стандартизация криптосистем 45

Глава 5. Вредоносное программное обеспечение и защита от него 46

5.1. Компьютерные вирусы 46
5.2. Метаморфные, загрузочные и макро-вирусы 49
5.3. Сетевые, почтовые, пиринговые и файловые вирусы 50
5.4. Анализ алгоритма вируса 52

5.5. Программные закладки 54
5.6. Модели воздействия программных закладок на компьютеры 56
5.7. Утилиты скрытого администрирования, Fishing, Spyware, Adware, Клавиатурные шпионы 58
5.8. Антивирусное программное обеспечение 60

Глава 6. Стандарты в области информационной безопасности .. 62

6.1. «Оранжевая книга» США 62
6.2. Классы безопасности 67
6.3. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» 75
6.4. Руководящие документы Гостехкомиссии России (ФСТЭК) 81

Заключение 87

Глоссарий 88

Рекомендуемая литература 98

Введение

Развитие современных информационных технологий сопровождается ростом числа компьютерных преступлений и связанных с ними хищений информации, а также материальных потерь.

По результатам одного из исследований были получены следующие результаты:

- около 60% опрошенных руководителей крупных и средних предприятий пострадали от компьютерных взломов за последний год;
- примерно 20% опрошенных из этого числа заявляют, что потеряли более миллиона долларов в ходе нападений;
- более 70% потерпели убытки в размере 50 тыс. долларов;
- свыше 20% атак были нацелены на промышленные секреты или документы, представляющие интерес прежде всего для конкурентов.

Федеральным законом "Об информации, информатизации и защите информации" определено, что информационные ресурсы, т.е. отдельные документы или массивы документов, в том числе и в информационных системах, являясь объектом отношений физических, юридических лиц и государства, подлежат обязательному учету и защите, как всякое материальное имущество собственника.

Закон также устанавливает, что «конфиденциальной информацией считается такая документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации», а меры по обеспечению ее конфиденциальности принимает собственник информации.

В настоящее время отсутствует какая-либо универсальная методика, позволяющая четко относить ту или иную информацию к категории коммерческой тайны.

Исходить можно только из принципа экономической выгоды и безопасности предприятия - чрезмерная "засекреченность" приводит к необоснованному удорожанию необходимых мер по защите информации и не способствует развитию бизнеса, тогда как широкая открытость может привести к большим финансовым потерям при разглашении коммерчески значимой информации.

Законом «О коммерческой тайне» права по отнесению информации к категории коммерческой тайны представлены руководителю юридического лица.

Стандарты и рекомендации образуют базис понятий, на котором строятся все работы по обеспечению информационной безопасности.

В то же время эти документы ориентированы в первую очередь на производителей и «оценщиков» систем и в гораздо меньшей степени - на пользователей.

Стандарты и рекомендации статичны, причем статичны, по крайней мере, в двух аспектах.

Во-первых, они не учитывают постоянной перестройки защищаемых систем и их окружения.

Во-вторых, они не содержат практических рекомендаций по формированию режима безопасности

Информационную безопасность нельзя купить, ее приходится каждодневно поддерживать, взаимодействуя при этом не только и не столько с компьютерами, сколько с людьми.

Иными словами, стандарты и рекомендации являются лишь отправной точкой на длинном и сложном пути защиты информационных систем организаций.

Для поддержания режима информационной безопасности особенно важны аппаратно-программные меры, поскольку основная угроза компьютерным системам исходит от самих этих систем (сбои оборудования, ошибки программного обеспечения, промахи пользователей и администраторов и т.п.).

Учебное пособие «Информационная безопасность для работников бюджетной сферы» предназначено для использования в рамках магистерской программы «Управление государственными информационными системами» по направлению «Системный анализ и управление».

Пособие предназначено также для использования в рамках системы дистанционного обучения Магистерского корпоративного факультета НИУ ИТМО и ориентировано на реализацию дополнительной образовательной программы повышения квалификации «Электронное правительство и инновационные технологии управления». Программа реализуется Центром технологий электронного правительства НИУ ИТМО и ориентирована на повышение квалификации государственных и муниципальных служащих по вопросам развития электронного правительства, информационного общества, применения инновационных технологий управления, построения единого информационного пространства органов государственной власти и местного самоуправления, а также оптимизации управления на основе перевода государственных и муниципальных услуг в электронный вид.

Глава 1.
Что такое информационная безопасность

От степени безопасности информационных технологий в настоящее время зависит материальное и моральное благополучие многих людей, а порой и их жизнь. Такова цена, которую приходится платить за повсеместное распространение сложных информационных систем, автоматически обрабатывающих большие массивы информации.

1.1. Определение информационной безопасности

Российский рынок средств защиты информации сегодня развивается довольно динамично. Но при этом в нашей стране отмечается значительное ежегодное увеличение количества зарегистрированных преступлений в сфере компьютерной информации. Следует отметить, что свыше 99% правонарушений совершается умышленно. Несмотря на то, что проблема информационной безопасности с каждым годом становится все острее, некоторые результаты исследования «Средства защиты информации от несанкционированного доступа», проводимого журналом «Информационная безопасность/Information Security» носят парадоксальный характер.

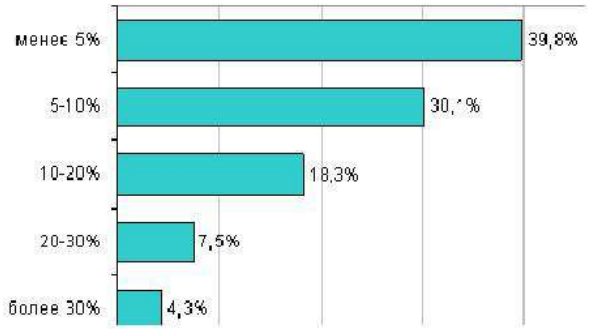

Рис. 1. **Процент расходов на защиту информации от общей суммы расходов на ИТ**

Большая часть опрошенных (39,8%) считают, что отечественные компании и организации весьма неохотно идут на увеличение расходов на информационную безопасность (см. диаграмму, **рис. 1**). Для сравнения: в большинстве зарубежных компаний, затраты на информационную безопасность составляют в среднем около 15% от бюджета информационных технологий компаний.

Таким образом, можно сделать вывод, что, несмотря на потери, которые зачастую несут предприятия, они не готовы вкладывать средства в работы, связанные с информационной безопасностью.

Для ответа на вопрос: что, от кого и как следует защищать в современных условиях, обратимся к исследованию, проведенному компанией Perimetrix, один из результатов которого приведен на рисунке (рис. 2) Оно весьма показательно в части иллюстрации мнения на этот счет потребителей средств защиты.

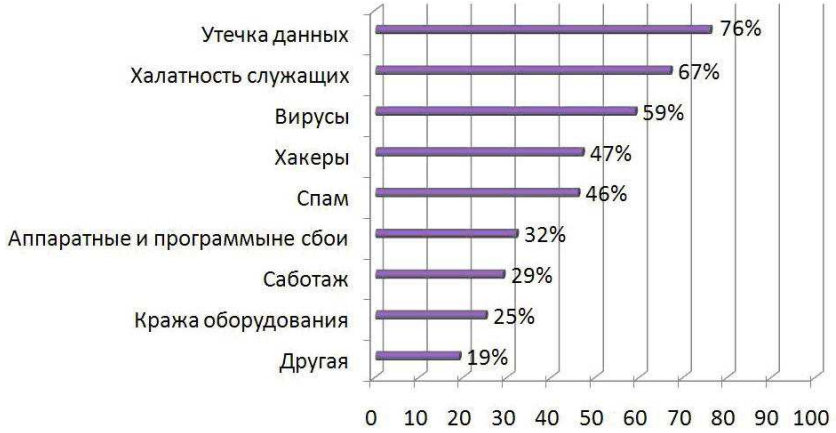

Рис. 2. **Данные аналитического центра Perimetrix за 2008 год**

Посмотрев внимательно на рис. 2, можно сделать вывод о том, что практически в равной мере для потребителей сегодня актуально решение задач защиты, как от внешних, так и от внутренних ИТ-угроз, обеспечение эффективного противодействия атакам и со стороны хакеров, и со стороны инсайдеров (санкционированных пользователей, допущенных к обработке информации на защищаемом вычислительном средстве), решение задач эффективного противодействия вирусным атакам, эксплойтам, вредоносным, шпионским и любым иным деструктивным программам, атакам на ошибки программирования в системном и прикладном ПО.

Под **информационной безопасностью** мы будем понимать защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации.

Наиболее существенными 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).

Нарушения доступности, целостности и конфиденциальности информации могут быть вызваны самыми разными воздействиями на информационные компьютерные системы.

1.2. Основные угрозы информационной безопасности

Современная автоматизированная информационная система (АИС) представляет собой сложную систему, состоящую из большого числа взаимосвязанных компонентов (модулей) различной степени автономности, обменивающихся между собой данными.

Каждый из модулей может подвергнуться внешнему воздействию или выйти из строя. Компоненты автоматизированной информационной системы можно разбить на следующие группы:

- **аппаратные средства** - компьютеры и их периферия (процессоры, мониторы, терминалы, дисководы, принтеры, контроллеры, кабели, линии связи и т.д.);
- **программное обеспечение** – специализированные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т.д.;
- **данные** - хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т.д.;
- **персонал** - обслуживающий персонал и пользователи.

Опасные воздействия на компьютерную информационную систему делятся на:

- случайные
- преднамеренные.

Как показывает опыта проектирования, изготовления и эксплуатации информационных систем, информация подвергается случайным воздействиям на всех этапах цикла жизни системы.

Причинами **случайных воздействий** при эксплуатации могут быть:

- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе персонала;
- аварийные ситуации из-за стихийных бедствий и отключений электропитания;
- помехи в линиях связи из-за воздействий внешней среды.

1.3. Преднамеренные воздействия

Рассмотрим более подробно категорию «преднамеренные действия», т.к. именно такие действия могут нанести максимальный ущерб организации.

Преднамеренные воздействия - это целенаправленные действия нарушителя.

В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами:

- взяткой;
- недовольством служащего своей карьерой;
- любопытством;
- конкурентной борьбой и т.п.

Можно составить гипотетическую модель потенциального нарушителя:

- нарушителем может быть как постороннее лицо, так и законный пользователь системы;
- нарушителю известна информация о принципах работы системы;
- квалификация нарушителя соответствует уровню квалификации разработчиков данной системы;
- нарушитель выбирает наиболее слабое звено в защите.

Наиболее распространенным и многообразным видом компьютерных нарушений является несанкционированный доступ (НСД).

НСД использует любую ошибку в системе защиты и возможен при неправильном или нерациональном выборе средств защиты, их некорректной установке и настройке.

Рассмотрим классификацию каналов НСД, по которым можно осуществить хищение, изменение или уничтожение информации:

1) Через человека:

- хищение носителей информации;
- чтение информации с экрана или клавиатуры (только хищение информации);

- чтение информации из распечатки (только хищение информации).

2) Через программу:

- перехват паролей;
- дешифровка зашифрованной информации;
- копирование информации с носителя (только хищение информации).

3) Через аппаратуру:

- подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации (только хищение информации);
- перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и т.д. (только хищение информации)

Особо остановимся на угрозах, которым подвергаются компьютерные сети.

Главная особенность компьютерной сети состоит в том, что ее компоненты физически распределены в пространстве. Связь между узлами сети осуществляется с помощью линий коммуникации и программно с помощью специфики механизма сообщений. При этом данные и управляющие сообщения, пересылаемые между узлами сети, передаются в виде пакетов обмена.

Атаки на компьютерные сети характерны тем, что они являются так называемыми удаленными атаками. Нарушитель может находиться за много километров от атакуемого объекта, при этом нападению может подвергаться не только конкретный компьютер, но и информация, передающаяся по сетевым каналам связи.

Формирование режима информационной безопасности - проблема комплексная. Меры по ее решению можно подразделить на пять уровней:

- законодательный (законы, нормативные акты, стандарты и т.п.);
- морально-этический (всевозможные нормы поведения, несоблюдение которых ведет к падению престижа конкретного человека или целой организации);
- административный (действия общего характера, предпринимаемые руководством организации);
- физический (механические, электромеханические и электронно-механические препятствия на возможных путях проникновения потенциальных нарушителей);
- аппаратно-программный (электронные устройства и специальные программы защиты информации).

Единая совокупность всех этих мер, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба, образуют систему защиты.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Перечислите, какие аспекты информационной безопасности являются наиболее существенными.
2. Что может являться причинами случайных воздействий при эксплуатации?
3. Что такое преднамеренное воздействие при эксплуатации, и какими мотивами оно может быть вызвано?
4. Через какие каналы, и каким образом может быть осуществлено НСД?
5. Какие бывают меры по формированию режима информационной безопасности?

Глава 2.
Законодательство по вопросам информационной безопасности

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.

Ниже на рисунке представлена примерная схема нормативных актов Российской Федерации, относящихся к вопросам информационной безопасности.

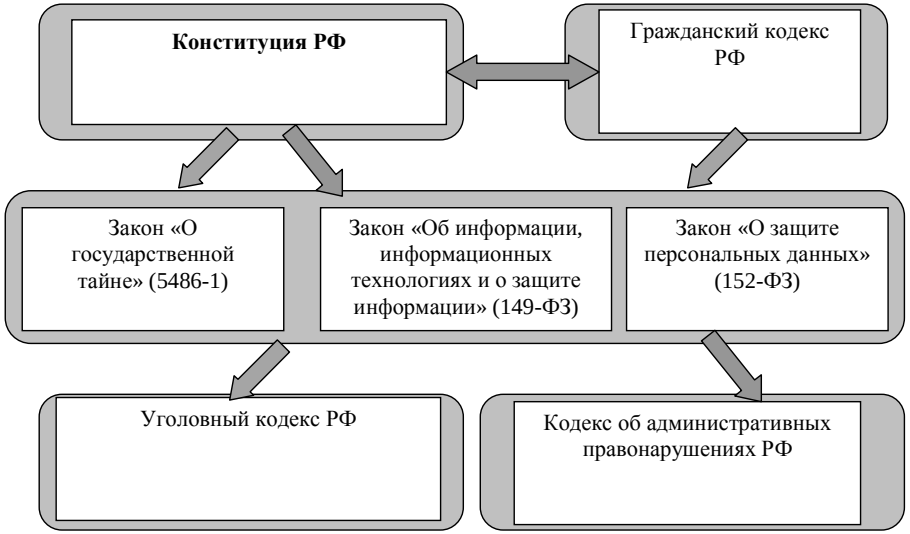

Рис. 3. **Схема взаимодействия законодательных актов, имеющих отношение к информационной безопасности**

2.1. Конституция Российской Федерации

Основным законом Российской Федерации является Конституция, принятая 12 декабря 1993 года. В соответствии **со статьей 24 Конституции**, органы государственной власти и органы местного

самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Право на информацию может реализовываться как средствами бумажных технологий, так и с помощью государственных информационных систем.

Статья 23 Конституции гарантирует право на личную и семейную тайну, право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, **статья 29** - право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Современная интерпретация этих положений включает обеспечение конфиденциальности данных, в том числе в процессе их передачи по компьютерным сетям, а также доступ к средствам защиты информации.

2.2. Уголовный кодекс Российской Федерации

Весьма продвинутым в плане информационной безопасности является **Уголовный кодекс** Российской Федерации. **Глава 28** - «Преступления в сфере компьютерной информации2 - содержит три статьи:

- статья 272. Неправомерный доступ к компьютерной информации;
- статья 273. Создание, использование и распространение вредоносных программ для ЭВМ;
- статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев, либо исправительными работами на срок от 6 месяцев до 1 года, либо лишением свободы на срок **до 2 лет**.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, - наказывается штрафом в размере от 100 000 до 300 000 рублей или в размере заработной платы или иного дохода осужденного за

период от 1 года до 2 лет, либо исправительными работами на срок от 1 года до 2 лет, либо арестом на срок от 3 до 6 месяцев, либо лишением свободы на срок **до 5 лет**.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок **до 3 лет** со штрафом в размере до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок **от 3 до 7 лет**.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, -

наказывается лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет, либо обязательными работами на срок от 180 до 240 часов, либо ограничением свободы на срок **до 2 лет**.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок **до 4 лет**.

2.3. Закон «О государственной тайне» от 21 июля 1993 года N 5486-1

Интересы государства в плане обеспечения конфиденциальности информации нашли наиболее полное выражение в **Законе «О государственной тайне»**. В нем **государственная тайна** определена как защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Там же дается определение **средств защиты информации**.

Согласно данному Закону, это технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих *государственную тайну*; средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Закон устанавливает **три степени секретности сведений**, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: «особой важности», «совершенно секретно» и «секретно».

В УК РФ есть статья **(Статья 283 УК РФ)**, определяющая наказание за разглашение государственной тайны**.**

1. Разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц, при отсутствии признаков государственной измены - наказывается арестом на срок от четырех до шести месяцев либо лишением свободы на срок **до 4 лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, - наказывается лишением свободы на срок **от 3 до 7 лет** с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

2.4. Закон «О коммерческой тайне» № 98-ФЗ от 2004 года

Коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Информация, составляющая коммерческую тайну (секрет производства) - сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой

информации принадлежит обладателю такой информации с учетом положений настоящего Федерального закона.

В законе говорится, что режим коммерческой тайны считается установленным после принятия обладателем информации следующих мер по охране конфиденциальности информации:

1) определение перечня информации, составляющей коммерческую тайну;

2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5) нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

В статье 11 говорится, что в целях охраны конфиденциальности информации работодатель обязан:

1) ознакомить под расписку работника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения им своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну, обладателями которой является работодатель и его контрагенты;

2) ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение.

В этой связи следует учитывать, что в УК РФ есть Статья 183 определяющая наказание за незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом - наказывается штрафом в размере до 80 000 рублей или в размере заработной платы или иного дохода осужденного за период от одного до шести месяцев либо лишением свободы на срок до 2 лет.

2. Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, - наказываются штрафом в размере до 120 000 рублей или в размере заработной платы или иного дохода осужденного за период до одного года с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на срок до 3 лет.

3. Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, - наказываются штрафом в размере до 200 000 рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на срок до 5 лет.

4. Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия, - наказываются лишением свободы на срок до 10 лет.

2.5. Закон «О персональных данных» №152-ФЗ от 2006 года

Целью закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну (статья 2).

В законе дается определение **персональных данных** - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация (статья 3).

В статье 5 говорится о принципах обработки персональных данных. Это:

1) законность целей и способов обработки персональных данных и добросовестность;

2) соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;

3) соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

4) достоверность персональных данных, их достаточность для целей обработки, недопустимость обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

5) недопустимость объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Статья 6 посвящена условиям обработки персональных данных:

1. Обработка персональных данных может осуществляться оператором с согласия субъектов персональных данных.

2. Согласия субъекта персональных данных не требуется в следующих случаях:

1) обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

2) обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

3) обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

4) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

5) обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

6) обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

7) осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

В статье 8 говорится об общедоступных источниках персональных данных:

1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

2. Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

Статья 10 обозначает, что обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается. Исключение составляют угрозы здоровью субъекту персональных данных, обработка персональных данных в медико-профилактических целях и в правоохранительных целях и др. при соблюдении определенных условий.

Статья 14 посвящена праву субъекта персональных данных на доступ к своим персональным данным (на основании 24 статьи Конституции РФ).

В статье 19 говорится о мерах по обеспечению безопасности персональных данных при их обработке. В частности, что оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Статья 22 вводит понятие «Уведомление об обработке персональных данных», которое означает, что оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных.

Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

1) относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения;

2) полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам

без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

4) являющихся общедоступными персональными данными;

5) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

6) необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;

7) включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

2.6. Закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года N 149-ФЗ

Закон на первое место ставит сохранение конфиденциальности информации.

Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.

В **статье 3** закона говорится о принципах правового регулирования отношений, возникающих в сфере информации, информационных технологий и защиты информации. Это:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

5) достоверность информации и своевременность ее предоставления;

6) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия.

В **статье 5** информация, в зависимости от категории доступа к ней, подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа). Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

В **статье 9** по вопросам ограничения доступа к информации говорится:

1. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

2. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

3. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

4. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

В **статье 16** говорится о защите информации:

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа,

3) реализацию права на доступ к информации.

Закон вводит понятие информационной системы и их подразделение на государственные, муниципальные и иные.

2.7. Закон «О лицензировании отдельных видов деятельности»

Федеральный Закон номер 128-ФЗ принят Государственной Думой 13 июля 2001 года и действует с 8 августа 2001 года.

Статья 17 Закона устанавливает перечень видов деятельности, на осуществление которых требуются лицензии. В области информационной безопасности лицензии требуются на следующие виды деятельности:

- распространение шифровальных (криптографических) средств;
- техническое обслуживание шифровальных (криптографических) средств;
- предоставление услуг в области шифрования информации;
- разработка и производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;
- выявление электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);
- разработка и (или) производство средств защиты конфиденциальной информации;
- техническая защита конфиденциальной информации;
- разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность;

– изготовление экземпляров аудиовизуальных произведений, программ для ЭВМ, баз данных и фонограмм на любых видах носителей (за исключением случаев, если указанная деятельность самостоятельно осуществляется лицами, обладающими правами на использование указанных объектов авторских и смежных прав в силу федерального закона или договора).

Необходимо учитывать, что, согласно статье 1, лицензирование:

– деятельности, связанной с защитой государственной тайны;
– деятельности в области связи;
– образовательной деятельности
– определяется другими законами.

Основные лицензирующие органы и их функции

Основными лицензирующими органами в области защиты информации являются Федеральная служба безопасности – ФСБ (ранее выдавало Федеральное агентство правительственной связи и информации – ФАПСИ, включенное в ФСБ) и Федеральная служба по техническому и экспортному контролю – ФСТЭК (ранее Гостехкомиссия при Президенте РФ). ФАПСИ ведает всем, что связано с криптографией, ФСТЭК лицензирует деятельность по защите конфиденциальной информации (Положение о сертификации средств защиты информации по требованиям безопасности информации). Все эти вопросы регламентированы соответствующими указами Президента и постановлениями Правительства РФ.

ФСТЭК России - это федеральный орган исполнительной власти, обладающий следующими полномочиями:

– обеспечение безопасности информации в ключевых системах информационной и телекоммуникационной инфраструктуры;
– организация деятельности государственной системы противодействия техническим разведкам и технической защиты информации и руководство ею;
– обеспечение технической защиты информации некриптографическими методами;
– создание средств защиты информации, содержащей сведения, составляющие государственную тайну;
– организация и проведение лицензирования деятельности по осуществлению мероприятий и/или оказанию услуг в области защиты государственной тайны (в части, касающейся противодействия техническим разведкам и/или технической защиты информации);

– разработка и/или производство средств защиты конфиденциальной информации, а также лицензирование иных видов деятельности в соответствии с законодательством Российской Федерации;
– организация разработки программ стандартизации, технических регламентов и национальных стандартов в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, обеспечения безопасности применяемых информационных технологий, а также в области противодействия техническим разведкам и технической защиты информации.
– осуществление экспортного контроля.

В подчинении ФСТЭК России находятся территориальные органы (управления ФСТЭК России по федеральным округам), Государственный научно-исследовательский испытательный институт проблем технической защиты информации и другие подведомственные организации.

2.8. Гражданский кодекс Российской Федерации

За обеспечение защиты авторских и смежных прав отвечает 4 глава Гражданского кодекса РФ, вступившая в действие с 1 января 2008 года.

Статья 1225. Охраняемые результаты интеллектуальной деятельности и средства индивидуализации

1. Результатами интеллектуальной деятельности и приравненными к ним средствами индивидуализации юридических лиц, товаров, работ, услуг и предприятий, которым предоставляется правовая охрана (интеллектуальной собственностью), являются:

2) программы для ЭВМ;

3) базы данных.

Статья 1236. Виды лицензионных договоров

1. Лицензионный договор может предусматривать:

1) предоставление лицензиату права использования результата интеллектуальной деятельности или средства индивидуализации с сохранением за лицензиаром права выдачи лицензий другим лицам (**простая (неисключительная) лицензия**);

2) предоставление лицензиату права использования результата интеллектуальной деятельности или средства индивидуализации без сохранения за лицензиаром права выдачи лицензий другим лицам (**исключительная лицензия**).

Статья 1259. Объекты авторских прав

К объектам авторских прав также относятся программы для ЭВМ, которые охраняются как литературные произведения.

Статья 1261. Программы для ЭВМ

Авторские права на все виды программ для ЭВМ (в том числе на операционные системы и программные комплексы), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код, охраняются так же, как авторские права на произведения литературы. **Программой для ЭВМ** является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.

Статья 1273. Свободное воспроизведение произведения в личных целях

Допускается без согласия автора или иного правообладателя и без выплаты вознаграждения воспроизведение гражданином исключительно в личных целях правомерно обнародованного произведения, за исключением:

3) воспроизведения программ для ЭВМ, кроме случаев, предусмотренных статьей 1280 настоящего Кодекса.

Статья 1280. Свободное воспроизведение программ для ЭВМ и баз данных. Декомпилирование программ для ЭВМ

1. Лицо, правомерно владеющее экземпляром программы для ЭВМ или экземпляром базы данных (пользователь), вправе без разрешения автора или иного правообладателя и без выплаты дополнительного вознаграждения:

1) внести в программу для ЭВМ или базу данных изменения исключительно в целях их функционирования на технических средствах пользователя и осуществлять действия, необходимые для функционирования таких программы или базы данных в соответствии с их назначением, в том числе запись и хранение в памяти ЭВМ (одной ЭВМ или одного пользователя сети), а также осуществить исправление явных ошибок, если иное не предусмотрено договором с правообладателем;

2) изготовить копию программы для ЭВМ или базы данных при условии, что эта копия предназначена только для архивных целей или для замены правомерно приобретенного экземпляра в случаях, когда такой экземпляр утерян, уничтожен или стал непригоден для использования. При этом копия программы для ЭВМ или базы данных не может быть использована в иных целях, чем цели, указанные в подпункте 1 настоящего

пункта, и должна быть уничтожена, если владение экземпляром таких программы или базы данных перестало быть правомерным.

2. Лицо, правомерно владеющее экземпляром программы для ЭВМ, вправе без согласия правообладателя и без выплаты дополнительного вознаграждения изучать, исследовать или испытывать функционирование такой программы в целях определения идей и принципов, лежащих в основе любого элемента программы для ЭВМ, путем осуществления действий, предусмотренных подпунктом 1 пункта 1 настоящей статьи.

3. Лицо, правомерно владеющее экземпляром программы для ЭВМ, вправе без согласия правообладателя и без выплаты дополнительного вознаграждения воспроизвести и преобразовать объектный код в исходный текст (декомпилировать программу для ЭВМ) или поручить иным лицам осуществить эти действия, если они необходимы для достижения способности к взаимодействию независимо разработанной этим лицом программы для ЭВМ с другими программами, которые могут взаимодействовать с декомпилируемой программой, при соблюдении следующих условий:

1) информация, необходимая для достижения способности к взаимодействию, ранее не была доступна этому лицу из других источников;

2) указанные действия осуществляются в отношении только тех частей декомпилируемой программы для ЭВМ, которые необходимы для достижения способности к взаимодействию;

3) информация, полученная в результате декомпилирования, может использоваться лишь для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, не может передаваться иным лицам, за исключением случаев, когда это необходимо для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, а также не может использоваться для разработки программы для ЭВМ, по своему виду существенно схожей с декомпилируемой программой для ЭВМ, или для осуществления другого действия, нарушающего исключительное право на программу для ЭВМ.

4. Применение положений, предусмотренных настоящей статьей, не должно наносить неоправданный ущерб нормальному использованию программы для ЭВМ или базы данных и не должно ущемлять необоснованным образом законные интересы автора или иного правообладателя.

Статья 1286. Лицензионный договор о предоставлении права использования произведения

3. Заключение лицензионных договоров о предоставлении права использования программы для ЭВМ или базы данных допускается путем

заключения каждым пользователем с соответствующим правообладателем договора присоединения, условия которого изложены на приобретаемом экземпляре таких программы или базы данных либо на упаковке этого экземпляра. Начало использования таких программы или базы данных пользователем, как оно определяется этими условиями, означает его согласие на заключение договора.

2.9. Кодекс об административных правонарушениях Российской Федерации

Статья 5.39. Отказ в предоставлении гражданину информации

Неправомерный отказ в предоставлении гражданину собранных в установленном порядке документов, материалов, непосредственно затрагивающих права и свободы гражданина, либо несвоевременное предоставление таких документов и материалов, непредставление иной информации в случаях, предусмотренных законом, либо предоставление гражданину неполной или заведомо недостоверной информации - влечет наложение административного штрафа на должностных лиц в размере от 500 до 1 000 рублей.

Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) - влечет предупреждение или наложение административного штрафа на граждан в размере от 300 до 500 рублей; на должностных лиц - от 500 до 1 000 рублей; на юридических лиц - от 5 000 до 10 000 рублей.

Статья 13.12. Нарушение правил защиты информации

1. Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), - влечет наложение административного штрафа на граждан в размере от 300 до 500 рублей; на должностных лиц - от 500 до 1 000 рублей; на юридических лиц - от 5 000 до 10 000 рублей.

2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), - влечет наложение административного штрафа

на граждан в размере от 500 до 1 000 рублей с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от 1 000 до 2 000 рублей; на юридических лиц - от 10 000 до 20 000 рублей с конфискацией несертифицированных средств защиты информации или без таковой.

3. Нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, - влечет наложение административного штрафа на должностных лиц в размере от 2 000 до 3 000 рублей; на юридических лиц - от 15 000 до 20 000 рублей.

4. Использование несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, - влечет наложение административного штрафа на должностных лиц в размере от 3 000 до 4 000 рублей; на юридических лиц - от 20 000 до 30 000 рублей с конфискацией несертифицированных средств, предназначенных для защиты информации, составляющей государственную тайну, или без таковой.

5. Грубое нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), - влечет наложение административного штрафа на лиц, осуществляющих предпринимательскую деятельность без образования юридического лица, в размере от 1 000 до 1 500 рублей или административное приостановление деятельности на срок до девяноста суток; на должностных лиц - от 1 000 до 1 500 рублей; на юридических лиц - от 10 000 до 15 000 рублей или административное приостановление деятельности на срок до девяноста суток.

Примечание. Понятие грубого нарушения устанавливается Правительством Российской Федерации в отношении конкретного лицензируемого вида деятельности.

Статья 13.13. Незаконная деятельность в области защиты информации

1. Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна), - влечет наложение административного штрафа на граждан в размере от 500 до 1 000 рублей с конфискацией средств защиты информации или без таковой; на должностных лиц - от

2 000 до 3 000 рублей с конфискацией средств защиты информации или без таковой; на юридических лиц - от 10 000 до 20 000 рублей с конфискацией средств защиты информации или без таковой.

2. Занятие видами деятельности, связанной с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, без лицензии, - влечет наложение административного штрафа на должностных лиц в размере от 4 000 до 5 000 рублей; на юридических лиц - от 30 000 до 40 000 рублей с конфискацией созданных без лицензии средств защиты информации, составляющей государственную тайну, или без таковой.

Статья 13.14. Разглашение информации с ограниченным доступом

Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью 1 статьи 14.33 настоящего Кодекса, - влечет наложение административного штрафа на граждан в размере от 500 до одной 1 000 рублей; на должностных лиц - от 4 000 до 5 000 рублей.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Какой закон устанавливает три степени секретности сведений?
2. Какие согласно 152 ФЗ существуют правила обработки персональных данных оператором?
3. Какие наказания согласно Уголовному кодексу РФ предполагаются за создание, использование и распространение вредоносных программ для ЭВМ?
4. Что говорится в статье 3 закона "Об информации, информационных технологиях и о защите информации" о принципах правового регулирования отношений?
5. На основании, какого закона налагается штраф за незаконную деятельность в области защиты информации?

Глава 3.
Идентификация и аутентификация

3.1. Основные понятия

Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов. **Идентификация и аутентификация** - это первая линия обороны, «проходная» информационного пространства организации**.**

На рис. 4 представлена обобщенная схема идентификации и аутентификации пользователя при его доступе в АС.

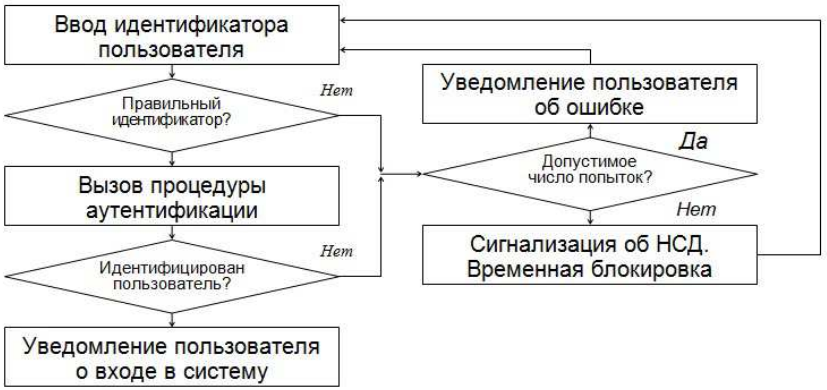

Рис. 4. **Обобщенная схема идентификации и аутентификации**

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя).

Посредством **аутентификации** вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает**.** В качестве синонима слова **«аутентификация»** иногда используют словосочетание «проверка подлинности».

Аутентификация бывает **односторонней** (обычно клиент доказывает свою подлинность серверу) и **двусторонней** (**взаимной**). Пример **односторонней аутентификации** - процедура входа пользователя в систему.

В сетевой среде, когда стороны **идентификации/аутентификации** территориально разнесены, у рассматриваемого сервиса есть два основных аспекта:

- что служит **аутентификатором** (то есть используется для подтверждения подлинности субъекта);
- как организован (и защищен) обмен данными **идентификации/аутентификации.**

Субъект может подтвердить свою подлинность, предъявив по крайней мере одну из следующих сущностей:

- нечто, что он знает (пароль, личный *идентификационный* номер, криптографический ключ и т.п.);
- нечто, чем он владеет (личную карточку или иное устройство аналогичного назначения);
- нечто, что есть часть его самого (голос, отпечатки пальцев и т.п., то есть свои биометрические характеристики).

В открытой сетевой среде между сторонами **идентификации/аутентификации** не существует доверенного маршрута; это значит, что в общем случае данные, переданные субъектом, могут не совпадать с данными, полученными и использованными для проверки подлинности.

Необходимо обеспечить защиту от пассивного и активного прослушивания сети, то есть от:

- перехвата,
- изменения
- и/или воспроизведения данных.

Передача паролей в открытом виде, очевидно, неудовлетворительна; не спасает положение и шифрование паролей, так как оно не защищает от **воспроизведения**. Нужны более сложные протоколы **аутентификации**.

Надежная **идентификация** и затруднена не только из-за сетевых угроз, но и по целому ряду причин:

- во-первых, почти все **аутентификационные** сущности можно узнать, украсть или подделать;
- во-вторых, имеется противоречие между надежностью **аутентификации**, с одной стороны, и удобствами пользователя и системного администратора с другой (так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить **аутентификационную** информацию - ведь на его место на время мог сесть другой человек, а это не только хлопотно, но и повышает вероятность того, что кто-то может подсмотреть за вводом данных;
- в-третьих, чем надежнее средство защиты, тем оно дороже.

Современные средства **идентификации/аутентификации** должны поддерживать концепцию **единого входа в сеть.**

Единый вход в сеть - это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная **идентификация/аутентификация** становится слишком обременительной.

К сожалению, пока нельзя сказать, что **единый вход в сеть** стал нормой, доминирующие решения пока не сформировались.

Таким образом, необходимо искать компромисс между надежностью, доступностью по цене и удобством использования и администрирования средств **идентификации и аутентификации**.

3.2. Парольная аутентификация

Главное достоинство **парольной аутентификации** - простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности.

Чтобы пароль был запоминающимся, его зачастую делают простым (имя подруги, название спортивной команды и т.п.). Однако простой пароль нетрудно угадать, особенно если знать пристрастия данного пользователя.

Недостатки парольной идентификации:

- иногда пароли с самого начала не хранятся в тайне, так как имеют стандартные значения, указанные в документации, и далеко не всегда после установки системы производится их смена;
- ввод пароля можно подсмотреть - иногда для подглядывания используются даже оптические приборы;
- пароли нередко сообщают коллегам, чтобы те могли, например, подменить на некоторое время владельца пароля, теоретически в подобных случаях более правильно задействовать средства управления доступом, но на практике так никто не поступает; а тайна, которую знают двое, это уже не тайна;
- пароль можно угадать «методом грубой силы», используя, скажем, словарь, если файл паролей зашифрован, но доступен для чтения, его можно скачать к себе на компьютер и попытаться подобрать пароль, запрограммировав полный перебор (предполагается, что алгоритм шифрования известен).

Тем не менее, следующие меры позволяют значительно повысить надежность парольной защиты:

– наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.);
– управление сроком действия паролей, их периодическая смена;
– ограничение доступа к файлу паролей;
– ограничение числа неудачных попыток входа в систему (это затруднит применение «метода грубой силы»);
– обучение пользователей;
– использование программных ***генераторов паролей*** (такая программа, основываясь на несложных правилах, может порождать только благозвучные и, следовательно, запоминающиеся пароли).

Перечисленные меры целесообразно применять всегда, даже если наряду с паролями используются другие методы аутентификации.

3.3. Идентификация/аутентификация с помощью биометрических данных

Биометрия представляет собой совокупность автоматизированных методов **идентификации и/или аутентификации** людей на основе их физиологических и поведенческих характеристик.

К числу физиологических характеристик принадлежат особенности:
– отпечатков пальцев;
– сетчатки и роговицы глаз;
– геометрия руки и лица и т.п.

К поведенческим характеристикам относятся:
– динамика подписи (ручной);
– стиль работы с клавиатурой.

На стыке физиологии и поведения находятся:
– анализ особенностей голоса;
– распознавание речи.

Системы идентификации по узору радужной оболочки и сетчатки глаз могут быть разделены на два класса:
– использующие рисунок радужной оболочки глаза;
– использующие рисунок кровеносных сосудов сетчатки глаза.

Поскольку вероятность повторения данных параметров равна 10-78, эти системы являются наиболее надежными среди всех биометрических систем. Такие средства применяются, например, в США в зонах военных и оборонных объектов.

Системы идентификации по отпечаткам пальцев являются самыми распространенными. Одна из основных причин широкого распространения

таких систем заключается в наличии больших банков данных по отпечаткам пальцев. Основными пользователями таких систем во всем мире являются полиция, различные государственные организации и некоторые банки.

Системы идентификации по геометрической форме руки используют сканеры формы руки, обычно устанавливаемые на стенах. Следует отметить, что подавляющее большинство пользователей предпочитают системы именно этого типа.

В общем виде работа с биометрическими данными организована следующим образом.

Сначала создается и поддерживается база данных характеристик потенциальных пользователей. Для этого биометрические характеристики пользователя снимаются, обрабатываются, и результат обработки (называемый биометрическим шаблоном) заносится в базу данных (исходные данные, такие как результат сканирования пальца или роговицы, обычно не хранятся).

В дальнейшем для идентификации (и одновременно аутентификации) пользователя процесс снятия и обработки повторяется, после чего производится поиск в базе данных шаблонов.

В случае успешного поиска личность пользователя и ее подлинность считаются установленными. Для аутентификации достаточно произвести сравнение с одним биометрическим шаблоном, выбранным на основе предварительно введенных данных.

К биометрии следует относиться весьма осторожно. Необходимо учитывать, что она подвержена тем же угрозам, что и другие методы аутентификации.

Во-первых, биометрический шаблон сравнивается не с результатом первоначальной обработки характеристик пользователя, а с тем, что пришло к месту сравнения. А, как известно, за время пути... много чего может произойти.

Во-вторых, биометрические методы не более надежны, чем база данных шаблонов.

В-третьих, следует учитывать разницу между применением биометрии на контролируемой территории, под бдительным оком охраны, и в «полевых» условиях, когда, например к устройству сканирования роговицы могут поднести муляж и т.п.

В-четвертых, биометрические данные человека меняются, поэтому база шаблонов нуждается в сопровождении, что создает определенные проблемы и для пользователей, и для администраторов

Но главная опасность состоит в том, что любая "пробоина" для биометрии оказывается фатальной. Пароли, при всей их ненадежности, в крайнем случае, можно сменить. Утерянную аутентификационную карту можно аннулировать и завести новую. Палец же, глаз или голос сменить

нельзя. Если биометрические данные окажутся скомпрометированы, придется, как минимум, производить существенную модернизацию всей системы.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Назовите причины возможного снижения надежности идентификации.
2. Приведите пример двухсторонней аутентификации.
3. Какие имеются проблемы при парольной аутентификации?
4. На каких характеристиках основана идентификация/аутентификация с помощью биометрических данных?
5. Каким угрозам подвержена биометрическая аутентификация?

Глава 4.
Введение в криптографию

4.1. Общее понятие о криптографии

Криптография - это дисциплина, изучающая способы защиты процессов информационного взаимодействия от целенаправленных попыток отклонить их от условий нормального протекания, основанные на криптографических преобразованиях, то есть преобразованиях данных по секретным алгоритмам. Важнейшей задачей криптографии является защита передаваемых по каналам связи или хранящихся в системах обработки информации данных от несанкционированного ознакомления с ними и от преднамеренного их искажения.

Криптография решает указанную задачу посредством шифрования защищаемых данных, что предполагает использование двух следующих взаимно обратных преобразований - шифрования и расшифровывания.
На рисунке 5 приведена схема преобразования данных при шифровании:

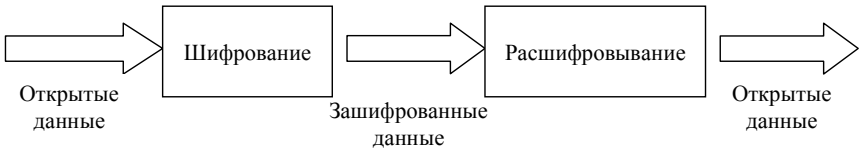

Рис. 5. **Схема преобразования данных при шифровании**

Шифром называется пара алгоритмов, реализующих каждое из указанных преобразований. Секретность второго из них делает данные недоступными для несанкционированного ознакомления, а секретность первого делает невозможным навязывание ложных данных.

Получение открытых данных из зашифрованных без знания алгоритма расшифрования называется **дешифрованием**.
Так как эти условия выполняются далеко не всегда, то в общем случае шифрование не является средством защиты от навязывания ложных данных.

Процедура расшифрования должна всегда восстанавливать открытое сообщение в его исходном виде, т.е. для каждого допустимого сообщения **T** преобразования шифрования и расшифрования должны удовлетворять следующему свойству: **T = D(E(T))**

Второе условие, которому должен удовлетворять шифр, следующее: он должен **шифровать** данные, то есть делать их непонятными для непосвященного.

Криптографические методы являются наиболее эффективными средствами защиты информации в автоматизированных системах (АС). А при передаче информации по протяженным линиям связи они являются единственным реальным средством предотвращения несанкционированного доступа. Любой криптографический метод характеризуется такими показателями, как **стойкость** и **трудоемкость**:

Стойкость метода - это тот минимальный объем зашифрованного текста, статистическим анализом которого можно вскрыть исходный текст. Таким образом, стойкость шифра определяет допустимый объем информации, зашифровываемый при использовании одного ключа.

Трудоемкость метода - определяется числом элементарных операций, необходимых для шифрования одного символа исходного текста.

4.2. Основные требования к криптографическому закрытию информации в АС

Сложность и стойкость криптографического закрытия данных должны выбираться в зависимости от объема и степени секретности данных.

Надежность закрытия должна быть такой, чтобы секретность не нарушалась даже в том случае, когда злоумышленнику становится известен метод шифрования.

Метод закрытия, набор используемых ключей и механизм их распределения не должны быть слишком сложными.

Выполнение процедур прямого и обратного преобразований должно быть формальным. Эти процедуры не должны зависеть от длины сообщений.

Ошибки, возникающие в процессе преобразования не должны распространяться по системе.

Вносимая процедурами защиты избыточность должна быть минимальной.

Начиная разговор о шифровании, определимся с терминологией на примере работы разведок: Разведчик – зашифровывает сообщение и отправляет его в «Центр», Центр (получатель сообщения) – расшифровывает его, а вражеская контрразведка – перехватив сообщение, пытается его прочесть – дешифрует сообщение.

Наиболее простой метод шифрования – подстановка. Символы шифруемого текста заменяются другими символами, взятыми из одного

алфавита (одноалфавитная замена) или нескольких алфавитов (многоалфавитная подстановка).

Одноалфавитная подстановка

Простейшая подстановка - прямая замена символов шифруемого сообщения другими буквами того же самого или другого алфавита.

Примеры таблиц замены приведены на рисунках 6 и 7.

Стойкость метода простой замены низкая.

Зашифрованный текст имеет те же самые статистические характеристики, что и исходный, поэтому зная стандартные частоты появления символов в том языке, на котором написано сообщение, и подбирая по частотам появления символы в зашифрованном сообщении, можно восстановить таблицу замены. Для этого требуется лишь достаточно длинный зашифрованный текст, для того, чтобы получить достоверные оценки частот появления символов. Поэтому простую замену используют лишь в том случае, когда шифруемое сообщение достаточно коротко.

а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
м	л	д	о	ы	в	а	ч	к	ю	ж	х	щ	з	ц	э
р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я
г	б	я	ъ	ш	т	ф	и	ь	н	е	у	п	с	р	й

Рис. 6. **Пример одноалфавитной замены**

а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
q	b	e	n	z	@	u	i	o	p	m	]	a	<	d	f
р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я
g	>	h	%	w	[	t	r	c	y	j	l	v	s	k	x

Рис. 7. **Пример многоалфавитной замены**

Стойкость метода равна 20 - 30, трудоемкость определяется поиском символа в таблице замены. Для снижения трудоемкости при шифровании таблица замены сортируется по шифруемым символам, а для расшифровки формируется таблица дешифрования, которая получается из таблицы замены сортировкой по заменяющим символам.

Многоалфавитная одноконтурная обыкновенная подстановка

Для замены символов используются несколько алфавитов, причем смена алфавитов проводится последовательно и циклически: первый символ заменяется на соответствующий символ из первого алфавита, второй - из второго алфавита, и т.д. пока не будут исчерпаны все алфавиты. После этого использование алфавитов повторяется.

Шифрование методом перестановки

При шифровании перестановкой символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока этого текста.

Простая перестановка

Выбирается размер блока шифрования в n столбцов и m строк и ключевая последовательность, которая формируется из натурального ряда чисел 1,2,...,n случайной перестановкой.

Шифрование проводится в следующем порядке:

- шифруемый текст записывается последовательными строками под числами ключевой последовательности, образуя блок шифрования размером n*m;
- зашифрованный текст выписывается колонками в порядке возрастания номеров колонок, задаваемых ключевой последовательностью;
- заполняется новый блок и т.д.;
- из зашифрованного текста выделяется блок символов размером n*m;
- этот блок разбивается на n групп по m символов;
- символы записываются в те столбцы таблицы перестановки, номера которых совпадают с номерами групп в блоке, расшифрованный текст читается по строкам таблицы перестановки;
- Выделяется новый блок символов и т.д.

По принципу действия все криптоалгоритмы делятся на три большие группы.

Тайнопись.

Ее принцип очень прост. Отправитель преобразовывает информацию по определенному алгоритму. После этого она представляет собой набор беспорядочных данных. О том, какие преобразования нужно совершить, чтобы получить информацию в первозданном виде, знает только ее получатель. То есть сам алгоритм хранится в тайне. Если же злоумышленник сможет его получить, он будет иметь свободный доступ ко всем данным, зашифрованным с его помощью. Тайнопись - самая старая группа криптографических алгоритмов.

Шифры с секретным ключом

Этот тип шифров подразумевает наличие некой информации (ключа), обладание которой позволяет как зашифровать, так и расшифровать сообщение.

С одной стороны, такая схема имеет те недостатки, что необходимо кроме открытого канала для передачи шифрограммы наличие также секретного канала для передачи ключа, а кроме того, при утечке информации о ключе, невозможно доказать, от кого из двух корреспондентов произошла утечка.

С другой стороны, среди шифров именно этой группы есть единственная в мире схема шифровки, обладающая абсолютной теоретической стойкостью. Все прочие можно расшифровать хотя бы в принципе. Такой схемой является обычная шифровка (например, операцией XOR) с ключом, длина которого равна длине сообщения. При этом ключ должен использоваться только раз. Любые попытки расшифровать такое сообщение бесполезны, даже если имеется априорная информация о тексте сообщения. Осуществляя подбор ключа, можно получить в результате любое сообщение.

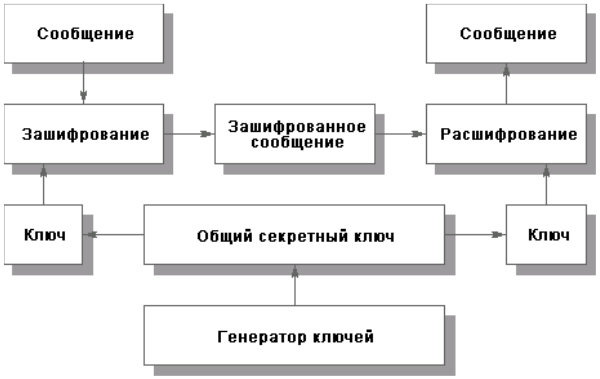

Рис. 8. **Схема шифрования сообщения методом «закрытого ключа»**

Шифры с открытым ключом

Шифры с открытым ключом подразумевают наличие двух ключей - открытого и закрытого; один используется для шифровки, другой для расшифровки сообщений. Открытый ключ публикуется - доводится до сведения всех желающих, секретный же ключ хранится у его владельца и является залогом секретности сообщений.

Суть метода в том, что зашифрованное при помощи секретного ключа может быть расшифровано лишь при помощи открытого и наоборот.

Ключи эти генерируются парами и имеют однозначное соответствие друг другу. Причём из одного ключа невозможно вычислить другой.

Характерной особенностью шифров этого типа, выгодно отличающих их от шифров с секретным ключом, является то, что секретный ключ здесь известен лишь одному человеку, в то время как в первой схеме он должен быть известен, по крайней мере, двоим.

Это даёт такие преимущества:

- не требуется защищённый канал для пересылки секретного ключа, вся связь осуществляется по открытому каналу;
- «что знают двое, знают все» - наличие *единственной* копии ключа уменьшает возможности его утраты и позволяет установить чёткую персональную ответственность за сохранение тайны;
- наличие двух ключей позволяет использовать данную шифровальную систему в двух режимах - секретная связь и цифровая подпись

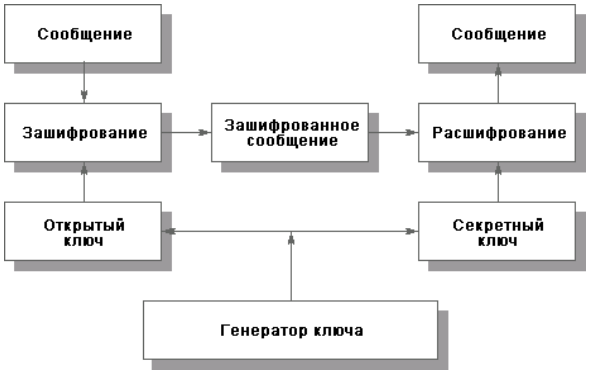

Рис. 9. **Схема шифрования сообщения методом «открытого ключа»**

Сообщение, зашифрованное при помощи открытого ключа какого-либо абонента, может быть расшифровано только им самим, поскольку только он обладает секретным ключом. Таким образом, чтобы послать закрытое сообщение, вы должны взять открытый ключ получателя и зашифровать сообщение на нём. После этого даже вы сами не сможете его расшифровать.

Когда мы действуем наоборот, то есть шифруем сообщение при помощи секретного ключа, то расшифровать его может любой желающий (взяв ваш открытый ключ). Но сам факт того, что сообщение было зашифровано вашим секретным ключом, служит подтверждением, что исходило оно именно от вас - единственного в мире обладателя секретного

ключа. Этот режим использования алгоритма называется цифровой подписью.

Хэш-функция

Как было показано выше, шифр с открытым ключом может использоваться в двух режимах: шифровки и цифровой подписи. Во втором случае не имеет смысла шифровать весь текст (данные) при помощи секретного ключа. Текст оставляют открытым, а шифруют некую «контрольную сумму» этого текста, в результате чего образуется блок данных, представляющий собой цифровую подпись, которая добавляется в конец текста или прилагается к нему в отдельном файле.

Упомянутая «контрольная сумма» данных, которая и "подписывается" вместо всего текста, должна вычисляться из всего текста, чтобы изменение любой буквы отражалось на ней. Во-вторых, указанная функция должна быть односторонняя, то есть вычислимая лишь «в одну сторону». Это необходимо для того, чтобы противник не смог целенаправленно изменять текст, подгоняя его под имеющуюся цифровую подпись.

Такая функция зовётся хэш-функцией. К её выбору следует отнестись тщательно. Неудачная хэш-функция позволит противнику подделать подписанное сообщение. Хэш-функция, так же, как и криптоалгоритмы, подлежит стандартизации и сертификации. В нашей стране она регламентируется ГОСТ Р-3411.

Кроме цифровой подписи хэш-функции используются и в других приложениях.

Например, при обмене сообщениями удалённых компьютеров, когда требуется аутентификация пользователя, может применяться метод, основанный на хэш-функции. Предположим, что один из компьютеров - клиент - должен несколько раз обратиться с запросами с компьютеру-серверу. Каждый раз проводить аутентификацию пользователя было бы неудобно. В то же время нельзя ограничиться проверкой лишь при первом контакте, поскольку злоумышленник может воспользоваться этим, подменив клиента после успешной проверки. Используется следующий метод. Компьютер-клиент генерирует случайное число и вычисляет от него одностороннюю функцию (хэш-функцию), затем эту же функцию от результата и так далее.

```
X0=Rnd();
X1=Hash(X0);
X2=Hash(X1);
X3=Hash(X2);
...
```

Эта последовательность X0...XN хранится в памяти клиента во время сеанса связи. При первом соединении и аутентификации на сервере клиент пересылает серверу последнее число последовательности XN. При

следующем контакте в качестве подтверждения, что запрос исходит от уже прошедшего проверку клиента, пересылается предыдущее число - XN-1. Поскольку хэш-функция односторонняя, легко проверить, что XN=Hash(XN-1). При следующем обращении к серверу пересылается XN-2 и так далее. Но для злоумышленника, даже если он перехватит соединение, станет непосильной задачей из XN-1 вычислить XN, то есть, взять обратную функцию от Hash().

4.3. Организационные проблемы криптозащиты

Значения стойкости шифров являются потенциальными величинами. Они могут быть реализованы при строгом соблюдении правил использования криптографических средств защиты.

Основные правила криптозащиты:

- Сохранение в тайне ключей.
- Исключение дублирования.
- Достаточно частая смена ключей.
- Нельзя допускать злоумышленнику возможности направить в систему ряд специально подобранных сообщений и получать их в зашифрованном виде. Такого взлома не может выдержать ни одна криптосистема!
- Важными аспектами организации криптозащиты являются выбор способа закрытия, распределение ключей и доставка их в места пользования (механизм распределения ключей).
- Выбор способа защиты тесно связан с трудоемкостью метода шифрования, степенью секретности закрываемых данных, стойкостью метода и объемом шифруемой информации.

Один из принципов криптографии является предположение о несекретности метода закрытия информации. Предполагается, что необходимая надежность закрытия обеспечивается только за счет сохранения в тайне ключей. Отсюда вытекает принципиальная важность формирования ключей, распределения их и доставка в пункты назначения.
\

Основными правилами механизма распределения ключей являются:

- ключи должны выбираться случайно;
- выбранные ключи должны распределяться таким образом, чтобы не было закономерностей в изменении ключей от пользователя к пользователю;
- должна быть обеспечена тайна ключей на всех этапах функционирования системы (ключи должны передаваться по линиям связи, почте или курьерами в зашифрованном виде с помощью другого ключа).

4.4. Сертификация и стандартизация криптосистем

Как уже было сказано, криптосистема не может считаться надёжной, если не известен полностью алгоритм её работы. Только зная алгоритм, можно проверить, устойчива ли защита. Однако проверить это может лишь специалист, да и то зачастую такая проверка настолько сложна, что бывает экономически нецелесообразна. Как же обычному пользователю, не владеющему математикой, убедиться в надёжности криптосистемы, которой ему предлагают воспользоваться?

Для неспециалиста доказательством надёжности может служить мнение компетентных независимых экспертов. Отсюда возникла система сертификации. Ей подлежат все системы защиты информации, чтобы ими могли официально пользоваться предприятия и учреждения. Использовать несертифицированные системы не запрещено, но в таком случае вы принимаете на себя весь риск, что она окажется недостаточно надёжной или будет иметь «чёрные ходы». Но чтобы продавать средства информационной защиты, сертификация необходима. Такие положения действуют в России и в большинстве стран.

У нас единственным органом, уполномоченным проводить сертификацию, является Федеральная служба безопасности (ФСБ).

Кроме того ФСБ лицензирует деятельность предприятий, связанную с разработкой, производством, реализацией и эксплуатацией шифровальных средств, а также защищенных технических средств хранения, обработки и передачи информации, предоставлением услуг в области шифрования информации

Для сертификации необходимым условием является соблюдение стандартов при разработке систем защиты информации. Стандарты выполняют сходную функцию. Они позволяют, не проводя сложных, дорогостоящих и даже не всегда возможных исследований, получить уверенность, что данный алгоритм обеспечивает защиту достаточной степени надёжности.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Чем отличается шифрование, расшифровывание и дешифрование?
2. На какие группы делятся криптоалгоритмы по принципу действия?
3. В чем ключевые различия между шифрованием с закрытым и открытым ключом?
4. Что такое хэш-функция?
5. Какие существуют организационные проблемы у криптозащиты?

Глава 5.
Вредоносное программное обеспечение и защита от него

5.1. Компьютерные вирусы

Считается, что термин «компьютерный вирус» впервые употребил сотрудник Лехайского университета (США) Ф.Коэн в 1984 г. на 7-й конференции по безопасности информации, проходившей в США. Однако строгого определения, что же такое компьютерный вирус, так и не дано.

Основная трудность, возникающая при попытках дать это определение, заключается в том, что практически все отличительные черты вируса (внедрение в другие объекты, скрытность, потенциальная опасность и проч.) либо присущи другим программам, которые никак вирусами не являются, либо существуют вирусы, которые не содержат указанных выше отличительных черт (за исключением возможности распространения).

Поэтому представляется возможным сформулировать только обязательное условие для того, чтобы некоторая последовательность выполняемого кода являлась вирусом.

Обязательным (необходимым) свойством компьютерного вируса является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

Однако данное условие не является достаточным. Следовательно, нет точно определенного закона, по которому «хорошие» файлы можно отличить от «вирусов». Более того, иногда даже для конкретного файла довольно сложно определить, является он вирусом или нет.

Вирус обычно имеет те же права доступа к сетевым ресурсам, что и пользователь, на компьютере которого находится этот вирус.

Вирусы можно разделить на классы по следующим основным признакам:

- среда обитания;
- заражаемая операционная система;
- особенности алгоритма работы;
- деструктивные возможности.

По **среде обитания** вирусы бывают:

- файловые;

- загрузочные;
- макро;
- сетевые.

Существует большое количество сочетаний - например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков. Другой пример такого сочетания - сетевой макро-вирус, который не только заражает редактируемые документы, но и рассылает свои копии по электронной почте.

По **деструктивным возможностям** вирусы можно разделить:

- безвредные, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
- неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и пр. эффектами;
- опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;
- очень опасные, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, вывести из строя оборудование.

Но даже если в алгоритме вируса не найдено ветвей, наносящих ущерб системе, этот вирус нельзя с полной уверенностью назвать безвредным, так как вирус, как и всякая программа может иметь ошибки.

Среди **особенностей алгоритма работы** вирусов выделяются следующие пункты:

- резидентность;
- использование стелс-алгоритмов;
- самошифрование и полиморфичность;
- метаморфичность.

Под термином «резидентность» (DOS'овский термин TSR - Terminate and Stay Resident) понимается способность вирусов оставлять свои копии в системной памяти, перехватывать некоторые события (например, обращения к файлам или дискам) и вызывать при этом процедуры заражения обнаруженных объектов (файлов и секторов). Резидентные копии вирусов остаются жизнеспособными вплоть до очередной перезагрузки, даже если на диске уничтожены все зараженные файлы.

Нерезидентные вирусы активны непродолжительное время — только в момент запуска зараженной программы. Для своего распространения они ищут на диске незараженные файлы и записываются в них. После того, как код вируса передает управление программе-носителю, влияние вируса на работу операционной системы сводится к нулю вплоть до очередного запуска какой-либо зараженной программы.

Резидентными можно считать макро-вирусы, поскольку они постоянно присутствуют в памяти компьютера во время работы зараженного редактора. При этом роль операционной системы берет на себя редактор, а понятие «перезагрузка операционной системы» трактуется как выход из редактора.

Использование Стелс-алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространенным стелс-алгоритмом является перехват запросов ОС на чтение/запись зараженных объектов.

Стелс-вирусы при этом либо временно лечат их, либо «подставляют» вместо себя незараженные участки информации. В случае макро-вирусов наиболее популярный способ — запрет вызовов меню просмотра макросов. Одним из первых файловых стелс-вирусов был вирус «Frodo», а загрузочным стелс-вирусом — «Brain». Следует отметить, что были разработаны и ответные меры. Используя специальные методики и программное обеспечение, можно организовать защиту и от стелс-вирусов.

Самошифрование и полиморфичность используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования вируса. Полиморфик-вирусы (polymorphic) - это достаточно трудно обнаруживаемые вирусы, не имеющие сигнатур, т.е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфик-вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

Первые антивирусные программы искали вирусы, сравнивая содержимое файлов и секторов диска с характерными фрагментами вирусов (с сигнатурами вирусов). Именно эти фрагменты хранились в вирусных базах данных антивирусных программ.

Чтобы исключить обнаружение свих изделий, разработчики компьютерных вирусов стали применять шифрование вирусного кода.

Шифрующийся вирус — это вирус, который при заражении новых файлов и системных областей диска шифрует собственный код, пользуясь для этого случайными паролями (ключами). Когда вирус получает управление, он расшифровывает свой собственный код и передает ему управление.

Современные антивирусы умеют расшифровывать код вируса, поэтому шифрующиеся вирусы могут быть эффективно обнаружены и уничтожены. С этой целью были разработаны так называемые полиморфные вирусы.

К полиморфик-вирусам относятся те из них, детектирование которых невозможно (или крайне затруднительно) осуществить при помощи так называемых вирусных масок - участков постоянного кода, специфичных для конкретного вируса. Достигается это двумя основными способами -

шифрованием основного кода вируса с непостоянным ключом и случайным набором команд расшифровщика или изменением самого выполняемого кода вируса.

Полиморфик-генераторы, как и конструкторы вирусов, не являются вирусами в прямом смысле этого слова, поскольку в их алгоритм не закладываются функции размножения, т.е. открытия, закрытия и записи в файлы, чтения и записи секторов и т.д. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика.

5.2. Метаморфные, загрузочные и макро-вирусы

Метаморфные вирусы

Метаморфные вирусы, так же изменяют свой код, но не используют алгоритмы шифрования. Различие проявляется в виде изменений внутри кода вируса.

Существует несколько технологий, позволяющих с успехом реализовывать данную методику.

Одна из этих технологий трансформации, используемая метамофными программами основана на вставке и удалении «мусора» внутри кода. Эти инструкции не влияют на работу вируса, но занимают некоторое количество места и усложняют анализ больших участков кода.

Другая технология – изменение базовых инструкций на уровне кода. Это означает переключение между несколькими отличающимися кодами, которые выполняют одну и ту же функцию.

Самой сложной трансформацией метаморфного вируса является замена целых блоков кода на функционально-эквивалентные. Например, умножение числа x на 3. Это можно выразить как «x*3». Однако в качестве альтернативы его можно заменить на сумму трех x: «x+x+x».

Загрузочные вирусы

Принцип действия загрузочных вирусов основан на алгоритмах запуска операционной системы при включении или перезагрузке компьютера - после необходимых тестов установленного оборудования (памяти, дисков и т.д.) программа системной загрузки считывает первый физический сектор загрузочного диска и передает на него управление.

При заражении дисков загрузочные вирусы «подставляют» свой код вместо какой-либо программы, получающей управление при загрузке системы. Принцип заражения, таким образом, одинаков: вирус «заставляет» систему при ее перезапуске считать в память и отдать управление не оригинальному коду загрузчика, а коду вируса.

Существует несколько вариантов размещения на диске первоначального загрузочного сектора и продолжения вируса: в сектора свободных кластеров логического диска, в неиспользуемые или редко используемые системные сектора, в сектора, расположенные за пределами диска.

Если продолжение вируса размещается в секторах, которые принадлежат свободным кластерам диска, то, как правило, вирус помечает эти кластеры как сбойные (так называемые псевдосбойные кластеры).

Макро-вирусы

Макро-вирусы являются программами на языках, встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.). Для своего размножения такие вирусы используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие. Для существования вирусов в конкретной системе (редакторе) необходимо наличие встроенного в систему макро-языка с возможностями:

- привязки программы на макро-языке к конкретному файлу;
- копирования макро-программ из одного файла в другой;
- возможность получения управления макро-программой без вмешательства пользователя (автоматические или стандартные макросы).

Данные особенности макро-языков предназначены для автоматической обработки данных в больших организациях или в глобальных сетях и позволяют организовать автоматизированный документооборот. С другой стороны, возможности макро-языков таких систем позволяют вирусу переносить свой код в другие файлы и заражать их.

5.3. Сетевые, почтовые, пиринговые и файловые вирусы

Сетевые вирусы (сетевые черви)

К ним относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию и захватить управление. Для внедрения в заражаемую систему червь может использовать различные механизмы: дыры, слабые пароли, уязвимости базовых и прикладных протоколов, открытые системы и человеческий фактор.

Существует несколько независимых стратегий распространения, среди которых в первую очередь следует выделить импорт данных из

адресной книги Outlook Express или аналогичного почтового клиента, просмотр локальных файлов жертвы на предмет поиска сетевых адресов, сканирование IP-адресов текущей подсети и генерация случайного IP-адреса. Чтобы не парализовать сеть чрезмерной активностью и не отрезать себе пути к распространению, вирус должен использовать пропускные способности захваченных им информационных каналов максимум наполовину, а лучше на десятую или даже сотую часть. Чем меньший вред вирус наносит сетевому сообществу, тем позже он оказывается обнаруженным и тем с меньшей поспешностью администраторы устанавливают соответствующие обновления.

Почтовые вирусы

Почтовый вирус использует для своего распространения каналы электронной почты. Заражение почтовым вирусом происходит в результате действий пользователей, просматривающих почту, а также из-за ошибок в почтовых программах и операционных системах.

Вредоносные объекты могут внедряться в почтовые сообщения следующими способами:

- в виде присоединенных файлов (файлов вложений);
- в виде ссылок на вредоносные объекты ActiveX или аплеты Java, расположенные на троянских Web-сайтах или на Web-сайтах злоумышленников;
- в виде конструкций, встраиваемых непосредственно в тело сообщения электронной почты, имеющего формат HTML.

Вместе с электронным сообщением можно передать любые файлы. Такие файлы называются присоединенными или файлами вложений (attachment file).Файлы вложений таят в себе угрозу для компьютера — через них на компьютер может проникнуть вирус, червь, троянская или другая вредоносная программа.

Вирусы для пиринговых сетей

В современном Интернете имеется большое количество сетей, предназначенных для обмена файлами без применения централизованного сервера. Эти сети позволяют пользователям Интернета свободно обмениваться музыкальными файлами, программами и другой информацией. Эти сети часто называются файлообменными или пиринговыми. Последнее из этих названий происходит от названия применяемого в таких сетях способа обмена данными узел-узел (Peer-To-Peer). Для пиринговых сетей разработчиками вредоносных программ были созданы специальные вирусы, называемые вирусами для пиринговых сетей:

Вирус пиринговых сетей — это вредоносная программа, специально предназначенная для систем обмена файлами между компьютерами

пользователей Интернета, такими как Windows Messenger, ICQ и т.д. Чтобы такой вирус попал на компьютер пользователя пиринговой сети, пользователю требуется выполнить какое либо действие, например, загрузить и запустить на выполнение файл.

Файловые вирусы

К данной группе относятся вирусы, которые при своем размножении тем или иным способом используют файловую систему какой-либо ОС. Внедрение файлового вируса возможно практически во все исполняемые файлы всех популярных ОС. По способу заражения файлов вирусы делятся на «overwriting», паразитические («parasitic»), компаньон-вирусы («companion»), вирусы-черви.

При инфицировании файла вирус может производить ряд действий, маскирующих и ускоряющих его распространение. К подобным действиям можно отнести обработку атрибута read-only, снятие его перед заражением и восстановление после. Многие файловые вирусы считывают дату последней модификации файла и восстанавливают ее после заражения. Для маскировки своего распространения некоторые вирусы перехватывают прерывание DOS, возникающее при обращении к защищенному от записи диску (INT 24h), и самостоятельно обрабатывают его.

5.4. Анализ алгоритма вируса

Наиболее удобным для хранения и анализа вируса объектом является файл, содержащий тело вируса. Для анализа файлового вируса желательно иметь зараженные файлы всех типов, поражаемых вирусом. Если необходимо проанализировать часть оперативной памяти, то при помощи некоторых утилит (например, AVPUTIL.COM) довольно просто выделить участок, где расположен вирус, и скопировать его на диск. Если же требуется анализ сектора MBR или boot-сектора, то скопировать их в файлы можно при помощи популярных «Нортоновских утилит» или AVPUTIL. Для хранения загрузочного вируса наиболее удобным является файл-образ зараженного диска. Для его получения необходимо отформатировать дискету, заразить ее вирусом, скопировать образ дискеты в файл и при необходимости компрессировать его (эту процедуру можно проделать при помощи «Нортоновских утилит», программ TELEDISK или DISKDUPE).

При анализе алгоритма вируса предстоит выяснить:

- способ размножения вируса;
- характер возможных повреждений, которые вирус нанес информации, хранящейся на дисках;
- метод лечения оперативной памяти и зараженных файлов (секторов).

При решении этих задач не обойтись без дизассемблера или отладчика (например, AVPUTIL, SoftICE, TurboDebugger, дизассемблеров Sourcer или IDA).

Несложные короткие вирусы быстро «вскрываются» стандартным отладчиком DEBUG, при анализе объемных и сложных полиморфик-стелс-вирусов не обойтись без дизассемблера.

Если необходимо быстро обнаружить метод восстановления пораженных файлов, достаточно пройтись отладчиком по началу вируса до того места, где он восстанавливает загруженную программу перед тем, как передать ей управление (фактически именно этот алгоритм чаще всего используется при лечении вируса). Если же требуется получить детальную картину работы вируса или хорошо документированный листинг, то здесь необходимы дизассемблеры с их возможностями восстанавливать перекрестные ссылки. Следует учитывать, во-первых, что некоторые вирусы достаточно успешно блокируют попытки трассировать их коды, а, во-вторых, при работе с отладчиком существует вероятность, что вирус вырвется из-под контроля.

При анализе файлового вируса необходимо выяснить, какие типы файлов поражаются вирусом, в какое место в файле записывается код вируса — в начало, конец или середину файла, в каком объеме возможно восстановление файла (полностью или частично), в каком месте вирус хранит восстанавливаемую информацию.

При анализе загрузочного вируса основной задачей является выяснение адреса (адресов) сектора, в котором вирус сохраняет первоначальный загрузочный сектор (если, конечно, вирус сохраняет его).

Для резидентного вируса требуется также выделить участок кода, создающий резидентную копию вируса и вычислить возможные адреса точек входа в перехватываемые вирусом прерывания. Необходимо также определить, каким образом и где в оперативной памяти вирус выделяет место для своей резидентной копии.

Существуют особые случаи, когда анализ вируса может оказаться очень сложной для пользователя задачей, например при анализе полиморфик-вируса.

Для анализа макро-вирусов необходимо получить текст их макросов. Если вирус шифрует свои макросы или использует стелс-приемы, то необходимо воспользоваться специальными утилитами просмотра макросов.

5.5. Программные закладки

Имеются вредоносные программы еще одного класса. Это так называемые ***программные закладки (трояны)***, которые могут выполнять хотя бы одно из перечисленных ниже действий:

- вносить произвольные искажения в коды программ, находящихся и оперативной памяти компьютера (например, внесение изменений в программу разграничения доступа может привести к тому, что она разрешит вход в систему всем без исключения пользователям вне зависимости от правильности введенного пароля) -программная закладка первого типа;
- копировать фрагменты информации (пароли, криптографические ключи, коды доступа, конфиденциальные электронные документы и др.), из одних областей оперативной или внешней памяти компьютера в другие - программная закладка второго типа;
- искажать выводимую на внешние компьютерные устройства или в канал связи информацию, полученную в результате работы других программ - программная закладка третьего типа.

Троянской программой (троянцем, или троянским конем) называется:

- программа, которая, являясь частью другой программы с известными пользователю функциями, способна втайне от него выполнять некоторые дополнительные действия с целью причинения ему определенного ущерба;
- программа с известными ее пользователю функциями, в которую были внесены изменения, чтобы, помимо этих функций, она могла втайне от него выполнять некоторые другие (разрушительные) действия.

Таким образом, троянской можно считать любую программу, которая втайне от пользователя выполняет какие-то нежелательные(неожидаемые) для него действия. Эти действия могут быть любыми — от определения регистрационных номеров программного обеспечения, установленного на компьютере, до составления списка каталогов на его жестком диске. А сама троянская программа может маскироваться под текстовый редактор, под сетевую утилиту или любую программу, которую пользователь пожелает установить на свой компьютер.

На сегодня известны троянские объекты следующих типов:

- троянские программы;
- троянские Web-сайты;
- троянские сообщения электронной почты.

Троянским называется такой Web-сайт, при посещении которого на компьютер пользователя незаметно устанавливаются вредоносные программные компоненты.

Сообщения электронной почты могут использоваться для переноса вредоносных программных объектов. Такие объекты присоединяются к телу сообщения в виде файлов, или встраиваются непосредственно в текст сообщения, имеющего формат HTML. Внешне сообщение электронной почты, содержащее в том или ином виде вредоносный программный код, может выглядеть как обычное, информационное. Однако стоит открыть такое сообщение для просмотра, и вредоносный код получит управление.

Большинство троянских программ предназначено для сбора конфиденциальной информации. Остальные троянцы создаются для причинения прямого ущерба компьютерной системе, приводя ее в неработоспособное состояние.

Чтобы программная закладка могла произвести какие-либо действия по отношению к другим программам или по отношению к данным, процессор должен приступить к исполнению команд, входящих в состав кода программной закладки. Это возможно только при одновременном соблюдении следующих условий:

- программная закладка должна попасть в оперативную память компьютера (если закладка относится к первому типу, то она должна быть загружена до начала работы другой программы, которая является целью воздействия закладки, или во время работы этой программы);
- работа закладки, находящейся в оперативной памяти, начинается при выполнении ряда условий, которые называются активизирующими.

Иногда сам пользователь провоцируется на запуск исполняемого файла, содержащего код программной закладки. С учетом замечания о том, что программная закладка должна быть обязательно загружена в оперативную память компьютера, можно выделить ***резидентные*** **закладки** (они находятся в оперативной памяти постоянно, начиная с некоторого момента и до окончания сеанса работы компьютера) и ***нерезидентные*** (такие закладки попадают в оперативную память компьютера аналогично резидентным, однако, в отличие от последних, выгружаются по истечении некоторого времени или при выполнении особых условий).

У всех программных закладок (независимо от метода их внедрения в компьютерную систему, срока их пребывания в оперативной памяти и назначения) имеется одна важная общая черта: они обязательно выполняют операцию записи в оперативную или внешнюю память системы. При отсутствии данной операции никакого негативного влияния программная закладка оказать не может.

5.6. Модели воздействия программных закладок на компьютеры

Перехват

В модели перехват программная закладка внедряется в ПЗУ, системное или прикладное программное обеспечение и сохраняет всю или выбранную информацию, вводимую с внешних устройств компьютерной системы или выводимую на эти устройства, в скрытой области памяти локальной или удаленной компьютерной системы. Объектом сохранения, например, могут служить символы, введенные с клавиатуры, или электронные документы, распечатываемые на принтере.

Данная модель может быть двухступенчатой. На первом этапе сохраняются только, например, имена или начала файлов. На втором накопленные данные анализируются злоумышленником с целью принятия решения о конкретных объектах дальнейшей атаки.

Искажение

В модели искажение программная закладка изменяет информацию, которая записывается в память компьютерной системы в результате работы программ, либо подавляет/инициирует возникновение ошибочных ситуаций в компьютерной системе.

Можно выделить статическое и динамическое искажение. Статическое искажение происходит всего один раз. При этом модифицируются параметры программной среды компьютерной системы, чтобы впоследствии в ней выполнялись нужные злоумышленнику действия.

Динамическое искажение заключается в изменении каким-либо параметром системных или прикладных процессов при помощи заранее активизированных закладок. Динамическое искажение можно условно разделить так: искажение на входе (когда на обработку попадает уже искаженный документ) и искажение на выходе (когда искажается информация, отображаемая для восприятия человеком, или предназначенная для работы других программ).

Существуют 4 основных способа воздействия программных закладок на цифровую подпись:

- искажение входной информации (изменяется поступающий на подпись электронный документ);
- искажение результата проверки истинности цифровой подписи (вне зависимости от результатов работы программы цифровая подпись объявляется подлинной);
- навязывание длины электронного документа (программе цифровой подписи предъявляется документ меньшей длины, чем на самом деле, и в результате цифровая подпись ставится только под частью исходного документа);

- искажение программы цифровой подписи (вносятся изменения в исполняемый код программы с целью модификации реализованного алгоритма).

В рамках модели «искажение» также реализуются программные закладки, действие которых основывается на инициировании или подавлении сигнала о возникновении ошибочных ситуаций в компьютерной системе.

Удаление информации

Работа с конфиденциальными электронными документами обычно сводится к последовательности следующих манипуляций с файлами:

- создание;
- хранение;
- коррекция;
- уничтожение.

Для защиты конфиденциальной информации обычно используется шифрование. Основная угроза исходит отнюдь не от использования нестойких алгоритмов шифрования и «плохих» криптографических ключей, а от обыкновенных текстовых редакторов и баз данных, применяемых для создания и коррекции конфиденциальных документов.

В процессе функционирования программные средства создают в оперативной или внешней памяти системы временные копии документов. Естественно, все эти временные файлы выпадают из поля зрения любых программ шифрования и могут быть использованы злоумышленником для того, чтобы составить представление о содержании хранимых в зашифрованном виде конфиденциальных документов.

Защита от программных закладок

Задача защиты от программных закладок может рассматриваться в трех принципиально различных вариантах:

- не допустить внедрения программной закладки в компьютерную систему;
- выявить внедренную программную закладку;
- удалить внедренную программную закладку.

Как и в случае борьбы с вирусами, задача решается с помощью средств контроля за целостностью запускаемых системных и прикладных программ, а также за целостностью информации, хранимой в компьютерной системе и за критическими для функционирования системы событиями. Однако данные средства действенны только тогда, когда сами они не подвержены влиянию программных закладок.

5.7. Утилиты скрытого администрирования, Fishing, Spyware, Adware, Клавиатурные шпионы

Утилиты скрытого администрирования (backdoor)

Троянские программы этого класса по своей сути является достаточно мощными утилитами удаленного администрирования компьютеров в сети. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые и распространяемые различными фирмами-производителями программных продуктов.

Единственная особенность этих программ заставляет классифицировать их как вредные троянские программы: отсутствие предупреждения об инсталляции и запуске. При запуске троянец устанавливает себя в системе и затем следит за ней, при этом пользователю не выдается никаких сообщений о действиях троянца в системе. Более того, ссылка на троянца может отсутствовать в списке активных приложений. В результате "пользователь" этой троянской программы может и не знать о ее присутствии в системе, в то время как его компьютер открыт для удаленного управления.

Функции Backdoor могут быть заложены в программу ее разработчиком, например, с целью получения в дальнейшем несанкционированного доступа к функциям программы или ко всей компьютерной системе пользователя программы.

Техника Fishing

Техника с названием fishing используется с целью выманить у пользователя Интернета персональную информацию (пароли, пин-коды и т.д.). При этом злоумышленники могут направлять ему поддельные сообщения электронной почты. В этих сообщениях, отправленных, например, от имени популярного Web-сайта или банка, может говориться о том, что по той или иной причине пользователь должен выслать банку пароль или пин-код.

Для ввода пароля пользователь заманивается на поддельный сайт, повторяющий по своему дизайну сайт банка, другой компании или организации. Пользователю могут демонстрироваться всплывающие окна, копирующие сайт.

Программы Spyware

Вредоносные программы Spyware устанавливаются на компьютер пользователя и собирают различную информацию о действиях пользователя. Обычно это информация, ценная для маркетологов, которая после сбора отсылается разработчику программы через Интернет.

Программы Spyware могут собирать и другую информацию:

- данные о качестве связи, способе подключения, скорости модема и т.д.;
- информацию о содержании жесткого диска с целью составления списка ПО, установленного на компьютере у пользователя;
- информацию о нажатых клавишах (клавиатурные шпионы);
- приложения, с которыми работает пользователь;
- сведения о посещении Web-сайтов и другой активности в Интернете;
- содержимое сообщений электронной почты

Программы Adware

Программы adware отображают рекламную информацию на компьютере. Эти программы могут отображать на экране всплывающие окна с рекламными баннерами и текстом, даже при отсутствии подключения к Интернету.

Клавиатурные шпионы

Одна из наиболее распространенных разновидностей программных закладок — клавиатурные шпионы (кейлоггеры). Такие программные закладки нацелены на перехват паролей пользователей операционной системы, а также на определение их легальных полномочий и прав доступа к компьютерным ресурсам.

Поведение клавиатурных шпионов в общем случае является довольно традиционным: типовой клавиатурный шпион обманным путем завладевает пользовательскими паролями, а затем переписывает эти пароли туда, откуда их может без особого труда извлечь злоумышленник. Различия между клавиатурными шпионами касаются только способа, который применяется ими для перехвата пользовательских паролей. Соответственно все клавиатурные шпионы делятся на три типа — имитаторы, фильтры и заместители.

5.8. Антивирусное программное обеспечение

Антивирусное ПО может использовать следующие методы обнаружения вирусов и других вредоносных программ:

- сканирование;
- эвристический анализ (блокирование подозрительных действий)
- CRC-сканирование (обнаружение изменений);
- анализ сетевого трафика;
- анализ баз данных почтовых программ;
- обнаружение вирусов в системе автоматизации документооборота.
- информацию о содержании жесткого диска с целью составления списка ПО, установленного на компьютере у пользователя;
- информацию о нажатых клавишах (клавиатурные шпионы);
- приложения, с которыми работает пользователь;
- сведения о посещении Web-сайтов и другой активности в Интернете;
- содержимое сообщений электронной почты

Качество антивирусной программы можно определить по следующим позициям:

- надежность и удобство работы — отсутствие «зависаний» антивируса и прочих технических проблем, требующих от пользователя специальной подготовки;
- качество обнаружения вирусов всех распространенных типов, сканирование внутри файлов-документов/таблиц (Word, Excel), упакованных и архивированных файлов;
- отсутствие «ложных срабатываний»;
- многоплатформенность антивирусного программного обеспечения;
- возможность лечения зараженных объектов;
- периодичность обновления;
- существование серверных версий с возможностью проверки сетевых дисков;
- скорость работы и другие полезные функции.

В настоящий момент имеется много как платных, так и бесплатных антивирусных программ и существует много разнообразных методик, определяющих их качество. Одна из них разработана в немецком исследовательском центре AV-Test.org, который постоянно сравнивает самые популярные антивирусные программы по разным показателям.

Часть результатов исследования за июль/август 2011 года вы можете увидеть гистограмме (на рис. 100, составленной согласно итогам проверки антивирусов для домашнего использования. Соревновались известные бренды по трем характеристикам — защита, восстановление и юзабилити

(удобство использования), за каждую из которых максимально возможный балл — 6.

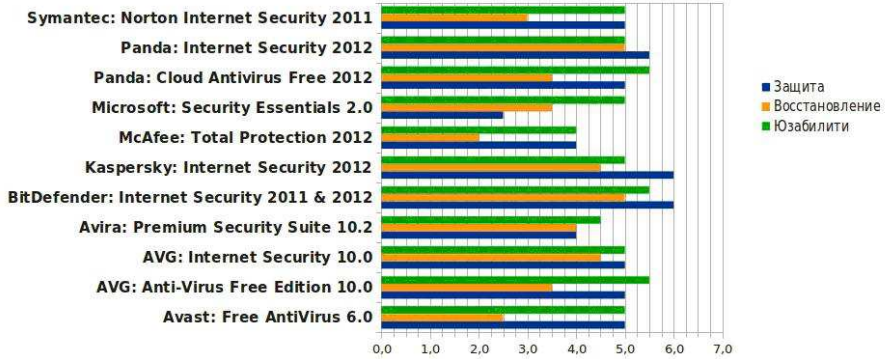

Рис. 10. **Результаты сравнения антивирусных программ**

Kaspersky Internet Security 2012 получил самую высокую оценку в защите от угроз, как и BitDefender Internet Security 2011-2012 – по 6 баллов, что и ожидаемо от платного ПО.

В вопросах восстановления компьютера от вирусов отлично себя показали также BitDefender и Panda Internet Security 2012 – по 5 баллов, а похвастаться отличным юзабилити могут бесплатные антивирусы Panda Cloud Antivirus Free Edition 1.5.1, AVG Anti-Virus Free Edition 10.0 и все тот же BitDefender Internet Security 2011 2012.

Microsoft Security Essentials 2.0 также принимал участие в тестировании антивирусов и набрал в общем 11 баллов. Неплохой показатель для бесплатного решения, хотя та же Panda Cloud набрала 14, как и бесплатный антивирус AVG Anti-Virus Free, который не так давно представил свою новую версию — AVG Anti-Virus Free 2012.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. На какие классы можно разделить вирусы?
2. В чем особенность метаморфных вирусов?
3. Что необходимо выяснить при анализе алгоритма вируса?
4. Какие проблемы при работе с конфиденциальными электронными документами могут возникнуть от создания компьютером временных копий документов?
5. По каким позициям можно определить качество антивирусной программы?

Глава 6.
Стандарты в области информационной безопасности

6.1. «Оранжевая книга» США

С 1983 по 1988 год Министерство обороны США и Национальный комитет компьютерной безопасности разработали систему стандартов в области компьютерной безопасности, которая включает более десяти документов. Этот список возглавляют «Критерии оценки безопасности компьютерных систем», которые по цвету обложки чаще называют «Оранжевой книгой». В 1995 году Национальный центр компьютерной безопасности США опубликовал «Пояснения к критериям безопасности компьютерных систем», объединившие все имеющиеся на тот момент дополнения и разъяснения к «Оранжевой книге».

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».

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 можно определить тестированием 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.

При оценке степени гарантированности, с которой систему можно считать надежной, центральной является концепция надежной вычислительной базы. **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).

Основное назначение надежной вычислительной базы - выполнять функции **монитора обращений**, то есть контролировать допустимость выполнения субъектами определенных операций над объектами. Каждое обращение пользователя к программам или данным проверяется 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.

Основные элементы политики безопасности

Согласно «Оранжевой книге», политика безопасности должна включать в себя по крайней мере следующие элементы:

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

Рассмотрим перечисленные элементы подробнее.

Произвольное управление доступом

Произвольное управление доступом - это метод ограничения 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 давать другим субъектам или отбирать у них права доступа к объекту.

Текущее состояние прав доступа при произвольном управлении описывается матрицей, в строках которой перечислены субъекты, а в столбцах - объекты. В клетках, расположенных на пересечении строк и столбцов, записываются способы доступа, допустимые для субъекта по

отношению к объекту, например: чтение, запись, выполнение, возможность передачи прав другим субъектам и т.п.

Очевидно, прямолинейное представление подобной матрицы невозможно (поскольку она очень велика), да и не нужно (поскольку она разрежена, то есть большинство клеток в ней пусты). В операционных системах более компактное представление матрицы доступа основывается или на структурировании совокупности субъектов (владелец/группа/прочие в ОС UNIX), или на механизме списков управления доступом, то есть на представлении матрицы по столбцам, когда для каждого объекта перечисляются субъекты вместе с их правами доступа. За счет использования метасимволов можно компактно описывать группы субъектов, удерживая тем самым размеры списков управления доступом в разумных рамках.

Большинство операционных систем и систем управления базами данных реализуют именно произвольное управление доступом. Главное его достоинство - гибкость, главные недостатки - рассредоточенность управления и сложность централизованного контроля, а также оторванность прав доступа от данных, что позволяет копировать секретную информацию в общедоступные файлы.

Безопасность повторного использования объектов

Безопасность повторного использования объектов - важное на практике дополнение средств управления доступом, предохраняющее от случайного или преднамеренного извлечения секретной 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.

Важно обратить внимание на следующий момент. Поскольку информация о субъектах также представляет собой объект, необходимо позаботиться о безопасности «повторного использования субъектов». Когда пользователь покидает организацию, следует не только лишить его возможности входа в систему, но и запретить доступ ко всем объектам. В противном случае новый сотрудник может получить ранее использовавшийся идентификатор, а с ним и все права своего предшественника.

Современные интеллектуальные периферийные устройства усложняют обеспечение безопасности повторного использования объектов. Действительно, принтер может буферизовать несколько страниц документа, которые останутся в памяти даже после окончания печати. Необходимо предпринять специальные меры, чтобы «вытолкнуть» их оттуда.

Впрочем, иногда организации защищаются от повторного использования слишком ревностно - путем уничтожения магнитных носителей. На практике заведомо достаточно троекратной записи случайных последовательностей бит.

Метки безопасности

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

Согласно «Оранжевой книге», метки безопасности состоят из двух частей: уровня секретности и списка категорий. Уровни секретности, поддерживаемые системой, образуют упорядоченное множество, которое может выглядеть, например, так:

- совершенно секретно;
- секретно;
- конфиденциально;
- несекретно.

Категории образуют неупорядоченный набор. Их назначение - описать предметную область, к которой относятся данные. В военной области каждая категория может соответствовать, например, определенному виду вооружений. Механизм категорий позволяет разделить информацию «по отсекам», что способствует лучшей защищенности. Субъект не может получить доступ к «чужим» категориям, даже если его уровень благонадежности - «совершенно секретно». Специалист по танкам не узнает тактико-технические данные самолетов.

Главная проблема, которую необходимо решать в связи с метками, - это обеспечение их **целостности**. Во-первых, не должно быть непомеченных субъектов и объектов, иначе в меточной безопасности появятся легко используемые бреши. Во-вторых, при любых операциях с данными метки должны оставаться правильными. В особенности это относится к экспорту и импорту данных. Например, печатный документ должен открываться заголовком, содержащим текстовое и/или графическое представление метки безопасности. Аналогично, при передаче файла по каналу связи должна передаваться и ассоциированная с ним метка, причем в таком виде, чтобы удаленная система могла ее трактовать, несмотря на возможные различия в уровнях секретности и наборе категорий.

Метки безопасности субъектов более подвижны, чем метки объектов. Субъект может в течение сеанса работы с системой изменять свою метку, естественно, не выходя за предопределенные для него рамки. Иными словами, он может сознательно занижать свой уровень благонадежности,

чтобы уменьшить вероятность непреднамеренной ошибки. Вообще, принцип минимизации привилегий - весьма разумное средство защиты.

Принудительное управление доступом

Принудительное 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 писать в секретные файлы, но не может - в несекретные (разумеется, должны также выполняться ограничения на набор категорий). На первый взгляд, подобное ограничение может показаться странным, однако оно вполне разумно. Ни при каких операциях уровень секретности информации не должен понижаться, хотя обратный процесс вполне возможен. Посторонний человек может случайно узнать секретные сведения и сообщить их куда следует, однако лицо, допущенное к работе с секретными документами, не имеет права раскрывать их содержание простому смертному.

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. В терминах принудительного управления нельзя выразить предложение «разрешить доступ к объекту X еще и для пользователя Y». Конечно, можно изменить метку безопасности пользователя Y, но тогда он, скорее всего, получит доступ ко многим дополнительным объектам, а не только к X.

Принудительное управление доступом реализовано во многих вариантах операционных систем и СУБД, отличающихся повышенными мерами безопасности. В частности, такие варианты существуют для SunOS и СУБД Ingres. Независимо от практического использования принципы принудительного управления являются удобным методологическим базисом для начальной классификации информации и распределения прав доступа. Удобнее мыслить в терминах уровней секретности и категорий, чем заполнять неструктурированную матрицу доступа.

6.2. Классы безопасности

Документ «Критерии оценки безопасности компьютерных систем» Министерства обороны США открыл путь к ранжированию информационных систем по степени надежности. В «Оранжевой книге» определяется четыре уровня надежности (безопасности) - D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. В настоящее время он пуст, и ситуация едва ли когда-нибудь изменится. По мере перехода от уровня C к A к надежности систем предъявляются все более жесткие требования. Уровни C и B подразделяются на классы (C1, C2, B1, B2, B3) с постепенным возрастанием надежности. Таким образом, всего имеется шесть классов безопасности - C1, C2, B1, B2, B3, A1. Чтобы система в результате процедуры сертификации могла быть отнесена к некоторому классу, ее политика безопасности и гарантированность должны удовлетворять приводимым ниже требованиям. Поскольку при переходе к каждому следующему классу требования только добавляются, будем говорить лишь о том новом, что присуще данному классу, группируя требования в согласии с предшествующим изложением.

Ниже представлены критерии оценки надежных компьютерных систем.

1). Требования к политике безопасности

Требования к политике безопасности, проводимой системой, подразделяются в соответствии с основными направлениями политики, предусматриваемыми «Оранжевой книгой».

Произвольное управление доступом:

Класс C1 - вычислительная база должна управлять доступом именованных пользователей к именованным объектам. Механизм управления (права для владельца/группы/прочих, списки управления доступом) должен позволять специфицировать разделение файлов между индивидами и/или группами.

Класс C2 - в дополнение к C1, права доступа должны определяться с точностью до пользователя. Механизм управления должен ограничивать распространение прав доступа - только авторизованный пользователь, например владелец объекта, может предоставлять права доступа другим пользователям. Все объекты должны подвергаться контролю доступа.

Класс B3 - в дополнение к C2, обязательно должны использоваться списки управления доступом с указанием разрешенных режимов. Должна быть возможность явного указания пользователей или их групп, доступ которых к объекту запрещен.

*(**Примечание.** Поскольку классы B1 и B2 не упоминаются, требования к ним в плане добровольного управления доступом те же, что и для C2. Аналогично, требования к классу A1 те же, что и для B3.)*

Повторное использование объектов:

Класс C2 - при выделении хранимого объекта из пула ресурсов вычислительной базы необходимо ликвидировать все следы предыдущих использований.

Метки безопасности:

Класс B1 - вычислительная база должна управлять метками безопасности, связанными с каждым субъектом и хранимым объектом. Метки являются основой функционирования механизма принудительного управления доступом. При импорте непомеченной информации соответствующий уровень секретности должен запрашиваться у авторизованного пользователя и все такие действия следует протоколировать.

Класс B2 - в дополнение к B1, помечаться должны все ресурсы системы, например ПЗУ, прямо или косвенно доступные субъектам.

Целостность меток безопасности:

Класс B1 - метки должны адекватно отражать уровни секретности субъектов и объектов. При экспорте информации метки должны преобразовываться в точное и однозначно трактуемое внешнее представление, сопровождающее данные. Каждое устройство ввода/вывода (в том числе коммуникационный канал) должно трактоваться как одноуровневое или многоуровневое. Все изменения трактовки и ассоциированных уровней секретности должны протоколироваться.

Класс B2 - в дополнение к B1, вычислительная база должна немедленно извещать терминального пользователя об изменении его метки безопасности. Пользователь может запросить информацию о своей метке. База должна поддерживать присваивание всем подключенным физическим устройствам минимального и максимального уровня секретности. Эти уровни должны использоваться при проведении в жизнь ограничений, налагаемых физической конфигурацией системы, например расположением устройств.

Принудительное управление доступом:

Класс B1 - вычислительная база должна обеспечить проведение в жизнь принудительного управления доступом всех субъектов ко всем хранимым объектам. Субъектам и объектам должны быть присвоены метки безопасности, являющиеся комбинацией упорядоченных уровней секретности, а также категорий. Метки являются основой принудительного

управления доступом. Надежная вычислительная база должна поддерживать по крайней мере два уровня секретности.

Вычислительная база должна контролировать идентификационную и аутентификационную информацию. При создании новых субъектов, например процессов, их метки безопасности не должны доминировать над меткой породившего их пользователя.

Класс B2 - в дополнение к B1, все ресурсы системы (в том числе ПЗУ, устройства ввода/вывода) должны иметь метки безопасности и служить объектами принудительного управления доступом.

2). Требования к подотчетности

Идентификация и аутентификация:

Класс C1 - пользователи должны идентифицировать себя, прежде чем выполнять какие-либо иные действия, контролируемые вычислительной базой. Для аутентификации должен использоваться какой-либо защитный механизм, например пароли. Аутентификационная информация должна быть защищена от несанкционированного доступа.

Класс C2 - в дополнение к C1, каждый пользователь системы должен уникальным образом идентифицироваться. Каждое регистрируемое действие должно связываться с конкретным пользователем.

Класс B1 - в дополнение к C2, вычислительная база должна поддерживать метки безопасности пользователей.

Предоставление надежного пути:

Класс B2 - вычислительная база должна поддерживать надежный коммуникационный путь к себе для пользователя, выполняющего операции начальной идентификации и аутентификации. Инициатива в общении по этому пути должна исходить исключительно от пользователя.

Класс B3 - в дополнение к B2, коммуникационный путь может формироваться по запросу, исходящему как от пользователя, так и от самой базы. Надежный путь может использоваться для начальной идентификации и аутентификации, для изменения текущей метки безопасности пользователя и т.п. Общение по надежному пути должно быть логически отделено и изолировано от других информационных потоков.

Аудит:

Класс C2 - вычислительная база должна создавать, поддерживать и защищать журнал регистрационной информации, относящейся к доступу к объектам, контролируемым базой. Должна быть возможность регистрации следующих событий:

- использование механизма идентификации и аутентификации;

– внесение объектов в адресное пространство пользователя, например открытие файла, запуск программы;
– удаление объектов;
– действия системных операторов, системных администраторов, администраторов безопасности;
– другие события, затрагивающие информационную безопасность.

Каждая регистрационная запись должна включать следующие поля:
– дата и время события;
– идентификатор пользователя;
– тип события;
– результат действия (успех или неудача).

Для событий идентификации/аутентификации регистрируется также идентификатор устройства, например терминала. Для действий с объектами регистрируются имена объектов.

Системный администратор может выбирать набор регистрируемых событий для каждого пользователя.

Класс B1 - в дополнение к C2, должны регистрироваться операции выдачи на печать и ассоциированные внешние представления меток безопасности. При операциях с объектами, помимо имен, регистрируются их метки безопасности. Набор регистрируемых событий может различаться в зависимости от уровня секретности объектов.

Класс B2 - в дополнение к B1, должна быть возможность регистрировать события, связанные с организацией тайных каналов с памятью.

Класс B3 - в дополнение к B2, должна быть 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.

3). Требования к гарантированности

Архитектура системы:

Класс C1 - 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. Ресурсы, контролируемые базой, могут составлять определенное подмножество всех субъектов и объектов системы.

Класс C2 - в дополнение к C1, вычислительная база должна изолировать защищаемые ресурсы в той мере, как это диктуется требованиями контроля доступа и подотчетности.

Класс B1 - в дополнение к C2, вычислительная база должна обеспечивать взаимную изоляцию процессов путем разделения их адресных пространств.

Класс B2 - в дополнение к B1, вычислительная база должна быть внутренне структурирована на хорошо определенные, относительно независимые модули. Вычислительная база должна эффективно использовать имеющееся оборудование для отделения элементов, критически важных с точки зрения защиты, от прочих компонентов системы. Модули базы должны проектироваться с учетом принципа минимизации привилегий. Для защиты логически раздельных хранимых объектов должны использоваться аппаратные средства, например сегментация. Должен быть полностью определен пользовательский интерфейс с вычислительной базой.

Класс B3 - в дополнение к B2, вычислительная база должна быть спроектирована и структурирована таким образом, чтобы использовать полный и концептуально простой защитный механизм. Этот механизм должен играть центральную роль во внутренней структуризации вычислительной базы и всей системы. База должна активно использовать разделение данных по уровням. Значительные инженерные усилия должны быть направлены на уменьшение сложности вычислительной базы и на вынесение из нее модулей, не являющихся критически важными с точки зрения защиты.

Целостность системы:

Класс C1 - должны быть в наличии аппаратные и/или программные средства, позволяющие периодически проверять корректность функционирования аппаратных и микропрограммных компонентов вычислительной базы.

Анализ тайных каналов передачи информации:

Класс B2 - системный архитектор должен тщательно проанализировать возможности по организации тайных каналов с памятью и оценить максимальную пропускную способность каждого выявленного канала.

Класс B3 - в дополнение к B2, аналогичная процедура должна быть проделана для временных каналов.

Класс A1 - в дополнение к B3, для анализа должны использоваться формальные методы.

Надежное администрирование:

Класс B2 - система должна поддерживать разделение функций оператора и администратора.

Класс B3 - в дополнение к B2, должна быть специфицирована роль администратора безопасности. Получить права администратора безопасности можно только после выполнения явных, протоколируемых действий. Не относящиеся к защите действия администратора безопасности должны быть по возможности ограничены.

Надежное восстановление:

Класс B3 - должны существовать процедуры и/или механизмы, позволяющие произвести восстановление после сбоя или иного нарушения работы без ослабления защиты.

Тестирование:

Класс C1 - 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 вычислительной базы.

Класс C2 - в дополнение к C1, тестирование должно подтвердить отсутствие очевидных недостатков в механизмах изоляции ресурсов и защиты регистрационной информации.

Класс B1 - в дополнение к C2, группа специалистов, полностью понимающих конкретную реализацию вычислительной базы, должна подвергнуть описание архитектуры, исходные и объектные коды тщательному анализу и тестированию. Цель должна состоять в выявлении всех дефектов архитектуры и реализации, позволяющих субъекту без должной авторизации читать, изменять, удалять информацию или приводить базу в состояние, когда она перестает обслуживать запросы других субъектов. Все выявленные недостатки должны быть исправлены или нейтрализованы, после чего база подвергается повторному тестированию, чтобы убедиться в отсутствии прежних или приобретении новых недостатков.

Класс B2 - в дополнение к B1, должна быть продемонстрирована относительная устойчивость вычислительной базы к попыткам проникновения.

Класс B3 - в дополнение к B2, должна быть продемонстрирована устойчивость вычислительной базы к попыткам проникновения.

Класс A1 - в дополнение к B3, тестирование должно продемонстрировать, что реализация вычислительной базы соответствует формальным спецификациям верхнего уровня.

Основу тестирования средств защиты от проникновения в систему должно составлять наличие спецификаций на исходные тексты.

Верификация спецификаций архитектуры:

Класс B1 - должна существовать неформальная или формальная модель политики безопасности, поддерживаемой вычислительной базой. Модель должна соответствовать основным посылкам политики безопасности на протяжении всего жизненного цикла системы.

Класс B2 - в дополнение к B1, модель политики безопасности должна быть формальной. Для вычислительной базы должны существовать описательные спецификации верхнего уровня, точно и полно определяющие ее интерфейс.

Класс B3 - в дополнение к B2, должны быть приведены убедительные аргументы соответствия между спецификациями и моделью.

Класс A1 - в дополнение к B3, помимо описательных должны быть представлены формальные спецификации верхнего уровня, относящиеся к аппаратным и/или микропрограммным элементам, составляющим интерфейс вычислительной базы. Комбинация формальных и неформальных методов должна подтвердить соответствие между спецификациями и моделью. Должны использоваться современные методы формальной спецификации и верификации систем, доступные Национальному центру компьютерной безопасности США.

Конфигурационное управление:

Класс B2 - в процессе разработки и сопровождения вычислительной базы должна использоваться система конфигурационного управления, обеспечивающая контроль за изменениями в описательных спецификациях верхнего уровня, иных архитектурных данных, реализационной документации, исходных текстах, работающей версии объектного кода, тестовых данных и документации. Конфигурационное управление должно обеспечивать соответствие друг другу всех аспектов текущей версии вычислительной базы. Должны предоставляться средства генерации новых версий базы по исходным текстам и средства для сравнения версий, чтобы убедиться в том, что произведены только запланированные изменения.

Класс A1 - в дополнение к B2, механизм конфигурационного управления должен распространяться на весь жизненный цикл и все компоненты системы, имеющие отношение к обеспечению безопасности, включая спецификации и документацию. Для защиты эталонной копии материалов, использующихся для генерации надежной вычислительной базы, должна использоваться комбинация физических, административных и технических мер.

Надежное распространение:

Класс A1 - должна поддерживаться целостность соответствия между эталонными данными, описывающими текущую версию вычислительной базы, и эталонной копией текстов этой версии. Должны существовать

процедуры, подтверждающие соответствие между поставляемыми клиентам аппаратными и программными компонентами и эталонной копией.

4). Требования к документации

Руководство пользователя по средствам безопасности:

Класс C1 - отдельный фрагмент документации (глава, том) должен описывать защитные механизмы, предоставляемые вычислительной базой, и их взаимодействие между собой, содержать рекомендации по их использованию.

Руководство администратора по средствам безопасности:

Класс C1 - руководство должно содержать сведения о функциях и привилегиях, которыми управляет системный администратор посредством механизмов безопасности.

Класс C2 - в дополнение к C1, должны описываться процедуры обработки регистрационной информации и управления файлами с такой информацией, а также структура записей для каждого типа регистрируемых событий.

Класс B1 - в дополнение к C2, руководство должно описывать функции оператора и администратора, затрагивающие безопасность, в том числе действия по изменению характеристик пользователей. Должны быть представлены рекомендации по согласованному и эффективному использованию средств безопасности, их взаимодействию друг с другом, по безопасной генерации новых версий вычислительной базы.

Класс B2 - в дополнение к B1, должны быть указаны модули вычислительной базы, содержащие механизмы проверки обращений. Должна быть описана процедура безопасной генерации новой версии базы после внесения изменений в исходные тексты.

Класс B3 - в дополнение к B2, должна быть описана процедура, обеспечивающая безопасность начального запуска системы и возобновления ее работы после сбоя.

Тестовая документация:

Класс C1 - разработчик системы должен представить экспертному совету документ, содержащий план тестов, процедуры прогона тестов и результаты тестов.

Класс B2 - в дополнение к C1, тесты должны подтверждать действенность мер по уменьшению пропускной способности тайных каналов передачи информации.

Класс A1 - в дополнение к B2, должно быть описано соответствие между формальными спецификациями верхнего уровня и исходными текстами.

Описание архитектуры:

Класс C1 - должны быть описаны подход к безопасности, используемый производителем, и применение этого подхода при реализации вычислительной базы. Если база состоит из нескольких модулей, должен быть описан интерфейс между ними.

Класс B1 - в дополнение к C1, должно быть представлено неформальное или формальное описание модели политики безопасности, проводимой в жизнь вычислительной базой. Необходимо наличие аргументов в пользу достаточности избранной модели для реализации политики безопасности. Должны быть описаны защитные механизмы базы и их место в модели.

Класс B2 - в дополнение к B1, модель политики безопасности должна быть формальной и доказательной. Должно быть показано, что описательные спецификации верхнего уровня точно отражают интерфейс вычислительной базы. Должно быть показано, как база реализует концепцию монитора обращений, почему она устойчива к попыткам отслеживания ее работы, почему ее нельзя обойти и почему она реализована корректно. Должна быть описана структура базы, чтобы облегчить ее тестирование и проверку соблюдения принципа минимизации привилегий. Документация должна содержать результаты анализа тайных каналов передачи информации и описание мер протоколирования, помогающих выявлять каналы с памятью.

Класс B3 - в дополнение к B2, должно быть неформально продемонстрировано соответствие между описательными спецификациями верхнего уровня и реализацией вычислительной базы.

Класс A1 - в дополнение к B3, должно быть неформально продемонстрировано соответствие между формальными спецификациями верхнего уровня и реализацией вычислительной базы.

6.3. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»

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).

«Общие критерии» на самом деле являются мета-стандартом, 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. 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 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. 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.

В ОК нет готовых классов защиты. Сформировать классификацию в терминах «Общих критериев» - значит определить несколько иерархически упорядоченных 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 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.

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. 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).

Например, 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.

Класс «Использование ресурсов», содержащий требования доступности, 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.

«Общие критерии» - продуманный и полный документ с точки зрения функциональных требований, однако в нем есть и некоторые недостатки, главный из которых - отсутствие объектного подхода. Функциональные требования не сгруппированы в осмысленные наборы (объектные интерфейсы), к которым могло бы применяться наследование. В «Общих критериях» отсутствуют архитектурные требования, что является естественным следствием избранного подхода «снизу вверх».

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» введены так называемые оценочные уровни доверия (семь), содержащие осмысленные комбинации компонентов:

Предусматривает анализ функциональной спецификации, спецификации интерфейсов, эксплуатационной документации, а также независимое тестирование. Уровень применим, когда угрозы не рассматриваются как серьезные.

В дополнение к первому уровню, предусматривает наличие проекта верхнего уровня объекта оценки, выборочное независимое тестирование, анализ стойкости функций безопасности, поиск разработчиком явных уязвимых мест.

Ведется контроль среды разработки и управление конфигурацией объекта оценки.

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.

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.

Реализация должна быть представлена в структурированном виде. Анализ соответствия распространяется на проект нижнего уровня.

Предусматривает формальную верификацию проекта объекта оценки. Он применим к ситуациям чрезвычайно высокого риска.

6.4. Руководящие документы Гостехкомиссии России (ФСТЭК)

Гостехкомиссия России (в настоящее время эти функции выполняет Федеральная служба технического и экспортного контроля - ФСТЭК) ведет активную нормотворческую деятельность, выпуская Руководящие документы (РД), играющие роль национальных оценочных стандартов в области информационной безопасности. В качестве стратегического направления была выбрана ориентация на «Общие критерии».

Список нормативных документов Гостехкомиссия и ФСТЭК:

– РД. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.
– РД. Защита от несанкционированного доступа к информации. Термины и определения.
– РД. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.
– РД. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
– РД. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники.
– РД. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации.
– РД. Защита информации. Специальные защитные знаки. Классификация и общие требования
– РД. Средства защиты информации. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин, автоматизированных кассовых систем и требования по защите информации. Сборник руководящих документов по защите информации от несанкционированного доступа.
– РД. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации.

Классификация по уровню контроля отсутствия не декларированных возможностей

- РД. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (часть 1, часть 2, часть3).
- РД. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности
- РД. Безопасность информационных технологий. Руководство по регистрации профилей защиты
- РД. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты.
- Руководство по разработке профилей защиты и заданий по безопасности.
- Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.
- Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных.
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка).
- ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.
- ГОСТ Р 50922-96. Защита информации. Основные термины и определения.
- ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.
- ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
- ГОСТ Р ИСО 7498-1-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель.
- ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.

- ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Ведение и общая модель.
- ГОСТ Р ИСО/МЭК 15408-2-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
- ГОСТ Р ИСО/МЭК 15408-3-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
- ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.
- ГОСТ Р ИСО/МЭК ТО 18044 «Информационная технология. Методы обеспечения безопасности. Руководство по менеджменту безопасностью информации».
- ГОСТ Р ИСО ТО 13569 «Финансовые услуги. Рекомендации по информационной безопасности».
- ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» Части 1, 2, 3.
- ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий».
- ГОСТ Р ИСО/МЭК ТО 19791 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем».
- ГОСТ Р ИСО/МЭК ТО 15446 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности».
- ГОСТ Р ИСО/МЭК 27006 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности».
- ГОСТ Р ИСО/МЭК 18028-1 «Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность информационных технологий. Часть 1. Менеджмент сетевой безопасности».
- ГОСТ Р ИСО/МЭК ТО 24762 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения».

– ГОСТ Р ИСО/МЭК ТО 18044 «Информационная технология. Методы обеспечения безопасности. Руководство по менеджменту безопасностью информации».

Для примера более подробно рассмотрим Руководящий документ - Классификация **автоматизированных систем (АС) по уровню защищенности от несанкционированного доступа (НСД)**.

Согласно ему, устанавливается девять классов защищенности АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Третья группа классифицирует АС, в которых работает один пользователь, имеющий доступ ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранящейся на носителях различного уровня конфиденциальности.

Группа содержит два класса - 2Б и 2А.

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

На таблице 1 представлена сводная номенклатура требований ко всем девяти классам защищенности АС.

Таблица 1. **Требования к защищенности автоматизированных систем**

Подсистемы и требования	Классы								
	3Б	**3А**	**2Б**	**2А**	**1Д**	**1Г**	**1В**	**1Б**	**1А**
1. Подсистема управления доступом									
1.1. Идентификация, проверка подлинности и контроль доступа субъектов: в систему;	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ;	-	-	-	+	-	+	+	+	+
к программам;	-	-	-	+	-	+	+	+	+
к томам, каталогам, файлам, записям, полям записей.	-	-	-	+	-	+	+	+	+
1.2. Управление потоками информации	-	-	-	+	-	-	+	+	+
2. Подсистема регистрации и учета									
2.1. Регистрация и учет: входа/выхода субъектов доступа в/из системы (узла сети);	+	+	+	+	+	+	+	+	+
выдачи печатных (графических) выходных документов;	-	+	-	+	-	+	+	+	+
запуска/завершения программ и процессов (заданий, задач);	-	-	-	+	-	+	+	+	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;	-	-	-	+	-	+	+	+	+
изменения полномочий субъектов доступа;	-	-	-	-	-	-	+	+	+
создаваемых защищаемых объектов доступа.	-	-	-	+	-	-	+	+	+
2.2. Учет носителей информации.	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей.	-	+	-	+	-	+	+	+	+
2.4. Сигнализация попыток нарушения защиты.	-	-	-	-	-	-	+	+	+
3. Криптографическая подсистема									
3.1. Шифрование конфиденциальной информации.	-	-	-	+	-	-	-	+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах.	-	-	-	-	-	-	-	-	+

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
3.3. Использование аттестованных (сертифицированных) криптографических средств.	-	-	-	+	-	-	-	+	+
4. Подсистема обеспечения целостности									
4.1. Обеспечение целостности программных средств и обрабатываемой информации.	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации.	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы защиты) информации в АС.	-	-	-	+	-	-	+	+	+
4.4. Периодическое тестирование СЗИ НСД.	+	+	+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД.	+	+	+	+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты.	-	+	-	+	-	-	+	+	+

Таблица 1

Представленная таблица позволяет специалистам по информационной безопасности провести анализ соответствия имеющейся АС тому или иному классу защищенности от НСД.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Какие элементы согласно «Оранжевой книге», должна включать в себя политика безопасности?
2. На чем основано принудительное управление доступом?
3. Как согласно «Оранжевой книге» определяются классы безопасности?
4. В чем состоит отличие «Оранжевой книги» от стандарта ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»?
5. Какие согласно РД Гостехкомиссии есть особенности у классов защищенности АС от НСД к информации?

Заключение

В заключение хочется отметить несколько особенностей данного учебного пособия.

Во-первых, оно написано не для специалистов по информационной безопасности, а как видно из названия - для работников бюджетных организаций. Конечно, прежде всего, оно рассчитано на тех, кто в государственных и муниципальных учреждениях назначен заниматься информационной безопасностью, и при этом не имеет профильного образования, а зачастую (в школах, поликлиниках, библиотеках и т.п.) имеет высшее образование, но не технической направленности.

Во-вторых, это пособие является первым из серии брошюр, написанных для данной аудитории и посвященных проблематике информационной безопасности. В связи с этим, в данной работе, прежде всего, освещены базовые вопросы ИБ, что позволит желающим «врасти» в проблематику и перестать бояться незнакомых терминов и определений. Эту же задачу решает приведенный ниже глоссарий по тематике информационной безопасности, собранный на основе руководящих документов (РД) Гостехкомиссии (ФСТЭК).

В-третьих, задачей данной работы было объяснить сложные вещи без описания серьезных технических и юридических особенностей, что, конечно, возможно далеко не всегда.

Все вышеперечисленное позволяет надеяться, что данное методическое пособие будет полезно не только магистрантам направления «Управление государственными информационными системами», но и многочисленной категории «бюджетников», обязанных по долгу службы заниматься вопросами информационной безопасности.

Глоссарий

Автоматизированная система (АС) - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций. *Автоматизированная система в защищенном исполнении (АСЗИ)* - автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и/или нормативных документов по защите информации.

Автоматизированное рабочее место (АРМ) - программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида.

Алгоритм - конечный набор предписаний для получения решения задачи посредством конечного количества операций.

Анализ защищенности - процесс обнаружения уязвимостей ресурсов автоматизированной системы, а также выработка рекомендаций по их устранению.

Анализ риска - систематический процесс определения величины рисков.

Антивирусное средство (АВС) - комплекс программно-технических и организационных мер и средств, предназначенных для выявления и предотвращения вирусного воздействия Атака действия, направленные на реализацию угроз несанкционированного доступа к информации, воздействия на нее или на ресурсы АИС с применением программных и (или) технических средств.

Аттестация объекта - информатизации деятельность по установлению соответствия комплекса организационно-технических мероприятий по защите объекта информатизации требованиям по безопасности информации.

Аудит, аудиторская проверка — процедура независимой оценки деятельности организации, системы, процесса, проекта или продукта.

Аудит безопасности (информации) - совокупность действий по независимой проверке и изучению документации автоматизированной информационной системы (АИС), а также по испытаниям средств защиты информации, направленная на обеспечение выполнения установленной политики безопасности информации и правил эксплуатации АИС, на выявление уязвимостей АИС и на выработку рекомендаций по устранению выявленных недостатков.

Аутентификация - предоставление гарантии заявленной идентичности объекта.

Аутентичность - свойство, гарантирующее, что субъект или ресурс идентичны заявленным.

Безопасность - качество или состояние защищенности от несанкционированного доступа или неконтролируемых потерь или воздействий.

Безопасность АИС - состояние защищенности автоматизированной информационной системы, при котором обеспечиваются конфиденциальность, доступность, целостность, подотчетность и подлинность ее ресурсов.

Безопасность информации - состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

Биометрические данные - измеримая биологическая или поведенческая характеристика, с достоверностью отличающая одного человека от другого, используемая для установления либо подтверждения личности человека.

Биометрия - идентификация человека по уникальным, присущим только ему биологическим признакам автоматические методы, используемые для распознавания личности или подтверждения заявленной личности человека на основе физиологических или поведенческих характеристик.

Блокирование информации - утрата информацией при ее обработке техническими средствами свойства доступности, выражающаяся в затруднении или прекращении санкционированного доступа к ней для проведения санкционированных операций по ознакомлению, документированию, модификации или уничтожению создание условий, препятствующих доступу к информации субъекту, имеющему право на него.

Верификация - процесс сравнения двух уровней спецификации средств вычислительной техники или автоматизированных систем на надлежащее соответствие.

Вирус (компьютерный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения.

Владелец информации - субъект, осуществляющий владение и пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации.

Владелец сертификата ключа подписи - физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Вредоносная программа - программа, используемая для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы автоматизированной информационной системы.

Вторжение (в АИС) - выявленный факт попытки НСД к ресурсам АИС.
Государственная тайна (ГТ) - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.
Гриф секретности - реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него.
Данные - информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека.
Дешифрование - процесс, обратный соответствующему обратимому процессу шифрования.
Достоверность - свойства соответствия предусмотренному поведению и результатам.
Доступ к информации - возможность получения информации и ее использование.
Доступность - свойство объекта находиться в состоянии готовности и возможности использования по запросу авторизованного логического объекта.
Доступность информации - состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.
Доступ к сведениям, составляющим ГТ - санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну.
Закладочное устройство - элемент средства съема информации или воздействия на нее, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации.
Закрытый ключ ЭП - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.
Зашифрование - процесс преобразования открытых данных в зашифрованные при помощи ключа.
Защита информация - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
Защита информации от несанкционированного воздействия - защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации,

приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.
Защищаемая автоматизированная информационная система - АИС, предназначенная для сбора, хранения, обработки, передачи и использования защищаемой информации с требуемым уровнем ее защищенности.
Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.
Защищаемый объект информатизации - объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.
Злоумышленник - нарушитель, намеренно (умышленно, со злым умыслом) идущий на нарушение.
Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.
Идентификатор - представление уполномоченного пользователя (например, строка символов), однозначно его идентифицирующее. Таким представление может быть либо полное или сокращенное имя этого пользователя, либо его псевдоним.
Информационная безопасность - свойство информации сохранять конфиденциальность, целостность и доступность.
Информационная безопасность объекта информатизации - состояние защищенности объекта информатизации, при котором обеспечивается безопасность информации и автоматизированных средств ее обработки.
Информационная инфраструктура - совокупность объектов информатизации, обеспечивающая доступ потребителей к информационным ресурсам.
Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.
Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.
Информация, составляющая коммерческую тайну (секрет производства) - сведения любого характера (производственные, технические,

экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Искусственные угрозы - угрозы АС, вызванные деятельностью человека.

Источник угрозы безопасности информации - субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

Канал утечки информации - совокупность источника информации, средства и способа, используемого для реализации угрозы.

Класс защищенности АС - определенная совокупность требований по защите информации, предъявляемых к автоматизированной системе.

Коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Комплексное обеспечение информационной безопасности - взаимосвязанный комплекс организационно-правовых, морально-этических, инженерно-технических методов, мероприятий, средств, направленных на обеспечение состояния информационной системы, характеризуемого способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, целостность, доступность информации в процессе ее обработки.

Компрометация - оглашение сведений, порочащих кого-либо, подрывающих доверие к кому-либо в коллективе, обществе.

Компьютерное преступление - осуществление несанкционированного доступа к информационному ресурсу, его модификация (подделка) или уничтожение с целью получения имущественных выгод для себя или для третьего лица, а также для нанесения, имущественного ущерба своему конкуренту.

Контроль доступа - проверка выполнения субъектами доступа установленных правил разграничения доступа в информационной системе.

Конфиденциальная информация - информация, требующая защиты.

Копия - точное воспроизведение текста какого-либо документа.

Криптографическая защита информации - защита информации с помощью ее криптографического преобразования.

Критичная информация - информация, требующая защиты из-за вероятности нанесения ущерба или возникновения риска нанесения

ущерба Критичность требования к тому, чтобы конкретная информация или средства обработки информации были доступны для ведения бизнеса.

Лицензирование в области защиты информации - деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ.

Меры обеспечения информационной безопасности - совокупность действий, направленных на разработку и/или практическое применение способов и средств обеспечения информационной безопасности.

Модель защиты - абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа.

Модель угроз (безопасности информации) - физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Мониторинг безопасности информации - постоянное наблюдение за процессом обеспечения безопасности информации в информационной системе с целью установить его соответствие требованиям безопасности информации.

Нарушитель безопасности информации - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах.

Непреднамеренные угрозы - неумышленные, случайные угрозы, вызванные ошибками в проектировании АС и ее элементов, ошибками в ПО, ошибками в действиях персонала (без злого умысла, в результате безответственности, некомпетентности, халатности).

Несанкционированное воздействие на информацию - воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

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

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким – либо признакам.

Объект защиты информации - информация, носитель информации или информационный процесс, в отношении которых необходимо

обеспечивать защиту в соответствии с поставленной целью защиты информации.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Организационно-технические мероприятия по обеспечению защиты информации - совокупность действий, направленных на применение организационных мер и программно-технических способов защиты информации на объекте информатизации.

Организационные меры защиты информации - меры, направленные на регламентацию производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.

Открытый ключ ЭП - уникальная последовательность символов, соответствующая закрытому ключу электронной подписи (ЭП), доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной подписи подлинности электронной подписи в электронном документе.

Пароль - идентификатор субъекта доступа, являющийся его (субъекта) секретом.

Перехват информации - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Политика информационной безопасности - совокупность требований и правил обеспечения информационной безопасности, разработанных в целях противодействия нарушителю по реализации угроз с учетом ценности защищаемой информации и стоимости системы обеспечения информационной безопасности.

Политика информационной безопасности организации - общее положение о намерениях и целях разработки программы обеспечения информационной безопасности организации.

Пользователь - любая сущность (человек-пользователь или внешний объект ИТ) вне объекта оценки, которая взаимодействует с объектом оценки.

Пользователь информации - субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Правовая защита информации - защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль над их исполнением.

Программная закладка - внесенные в программное обеспечение функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение не описанных в документации функций программного обеспечения, позволяющих осуществлять несанкционированные воздействия на информацию.

Пропускной режим - порядок прохода лиц, проезда транспортных средств, проноса и провоза вещей на охраняемые объекты, устанавливаемый соответствующими лицами, замещающими государственные должности в федеральных и региональных органах государственной власти, совместно с федеральными органами государственной охраны (ФСО), органами министерства внутренних дел (МВД) или Федеральной службы безопасности (ФСБ).

Распространение информации - действие, направленное на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Расшифрование - процесс преобразования зашифрованных данных в открытые при помощи шифра.

Риск - сочетание вероятности нанесения ущерба и тяжести этого ущерба.

Санкционированный доступ - доступ к информации, не нарушающий правила разграничения доступа.

Секретная информация - информация, содержащая сведения, отнесенные к государственной тайне.

Сертификация - это процедура, необходимая для подтверждения соответствия товаров, услуг и других объектов требованиям качества и безопасности форма осуществляемого органом по сертификации подтверждения соответствия объектов требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров.

Сеть - совокупность систем связи и систем обработки информации, которая может использоваться несколькими пользователями.

Система защиты информации - совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по

правилам и нормам, установленным соответствующими документами в области защиты информации.

Система защиты информации от НСД (СЗИ НСД) - комплекс организационных мер и программно-технических (при необходимости криптографических) средств защиты от несанкционированного доступа к информации (несанкционированных действий с ней) в автоматизированной системе.

Система разграничения доступа - совокупность реализуемых ПРД в СВТ или АС РД.

Собственник информации - субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами.

Средства шифрования - аппаратные, программные и программно-аппаратные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от НСД при ее обработке и хранении.

Субъект доступа (в ИС) - лицо или единица ресурса информационной системы, действия которого по доступу к ресурсам информационной системы регламентируются правилами разграничения доступа.

Техническая защита информации - защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Технический канал утечки информации - совокупность объекта технической разведки, физической среды и средства технической разведки, которыми добываются разведывательные данные.

Требование по защите информации - установленное правило или норма, которая должна быть выполнена при организации и осуществлении защиты информации, или допустимое значение показателя эффективности защиты информации.

Троянский конь - программа, содержащая дополнительные скрытые функции, с помощью которых используются законные полномочия субъекта для осуществления несанкционированного доступа к информации.

Угроза - совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба изделию ИТ или его владельцу.

Угроза безопасности информации - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Уничтожение информации - случайное или умышленное стирание информации на ее носителях при обработке техническими средствами, а также - хищение носителей и технических средств.

Управление доступом - функции, ограничивающие доступ к информации или средствам обработки информации только авторизованным лицам или приложениям, включая физическое управление доступом, основанное на размещении физических барьеров между неавторизованными лицами и защищаемыми информационными ресурсами, и логические средства управления доступом, использующие другие способы.

Управление рисками - процесс выявления, контроля и минимизации или устранения рисков безопасности, оказывающих влияние на информационные системы, в рамках допустимых.

Утечка информации - неконтролируемое распространение защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.

Уязвимость - недостаток или слабое место в автоматизированной информационной системе, которые могут быть условием реализации угрозы безопасности обрабатываемой в ней информации.

Физическая защита информации - защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Целостность информации - состояние защищенности информации, характеризуемое способностью автоматизируемой системы обеспечивать неизменность конфиденциальной информации при попытках НСД или случайных воздействий на неё в процессе обработки или хранения способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

Цифровая подпись - криптографическое преобразование, которое, будучи связано с элементом данных, обеспечивает услуги по аутентификации источника, целостности данных и неотказуемости подписавшей стороны.

Шифр - совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с применением ключей.

Шифрование - процесс зашифрования или расшифрования.

Электронная подпись (ЭП) - 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.

Рекомендуемая литература

1. *Галатенко В.А.* Основы информационной безопасности. - М.: Интернет-университет информационных технологий - ИНТУИТ.ру , 2008. - 208 с.
2. *Гордон Я.* Компьютерные вирусы без секретов.- М., 2004.
3. *Закупень Т.* Понятие и сущность информационной безопасности, и ее место в системе обеспечения национальной безопасности РФ // Информационные Ресурсы России. 2009. №4.
4. *Пюкке С.* Информация без опасности // Компьютерра. 2002. № 19.
5. *Форд Д.Л.* Персональная защита от хакеров. Руководство для начинающих. - М.: КУДИЦ-ОБРАЗ, 2002. - 272 с.

В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена Программа развития *государственного образовательного учреждения высшего профессионального образования «Санкт-Петербургский государственный университет информационных технологий, механики и оптики» на 2009–2018 годы*.

КАФЕДРА УПРАВЛЕНИЯ ГОСУДАРСТВЕННЫМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

Кафедра УГИС создана в 2011 году на Магистерском корпоративном факультете НИУ ИТМО.

Обучение на магистерской программе «Управление государственными информационными системами» направлено на приобретение теоретических знаний и практических навыков в сфере создания и развития ИТ-систем для нужд государственной власти и местного самоуправления.

Практическая часть обучения проходит на базе Центра технологий электронного правительства НИУ ИТМО, Санкт-Петербургского информационно-аналитического центра и других партнерских структур под руководством опытных экспертов и представителей органов власти.

Максим Игоревич Шубинский

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЛЯ РАБОТНИКОВ БЮДЖЕТНОЙ СФЕРЫ

Учебное пособие

В авторской редакции
Дизайн обложки С.Н. Ушаков
Верстка Ю.В. Байкеева
Редакционно-издательский отдел Санкт-Петербургского государственного университета информационных технологий, механики и оптики
Зав. РИО Н.Ф. Гусарова
Лицензия ИД № 00408 от 05.11.99
Подписано к печати
Заказ №
Тираж 100 экз.
Отпечатано на ризографе