**Федеральное государственное казенное образовательное
учреждение высшего образования
«Уральский юридический институт
Министерства внутренних дел Российской Федерации»**

Кафедра информационного обеспечения органов внутренних дел

М. Г. Гизатуллин

И. Ф. Файсханов

Основы информационной безопасности в органах внутренних дел

Учебное пособие

**Екатеринбург
2020**

ББК 67.401.114
Г467

Гизатуллин М. Г.

Г467 ***Основы информационной безопасности в органах внутренних дел:*** *учебное пособие* / М. Г. Гизатуллин, И. Ф. Файсханов. – Екатеринбург: Уральский юридический институт МВД России, 2020. – 51 с.

ISBN 978-5-88437-724-0

Рецензенты: ***Р. А. Усманов,*** начальник кафедры организации информационно-аналитического и документационного обеспечения деятельности органов внутренних дел Тюменского института повышения квалификации сотрудников органов внутренних дел МВД России, кандидат юридических наук;

А. А. Симаков, доцент кафедры информационных технологий в деятельности органов внутренних дел Омской академии МВД России, кандидат технических наук, доцент

В учебном пособии рассматриваются общие вопросы, затрагивающие сферу информационной безопасности, в том числе защиты информации, в целях формирования у сотрудников органов внутренних дел профессиональных компетенций в области обеспечения информационной безопасности.

Предназначено для курсантов и слушателей образовательных организаций МВД России, обучающиеся по специальностям 40.05.01 Правовое обеспечение национальной безопасности, 40.05.02 Правоохранительная деятельность, 38.05.01 Экономическая безопасность.

Обсуждено на заседании кафедры информационного обеспечения органов внутренних дел УрЮИ МВД России (протокол № 1 от 15 января 2020 г.).

Рекомендовано к использованию в образовательном процессе методическим советом УрЮИ МВД России (протокол № 7 от 17 февраля 2020 г.).

ISBN 978-5-88437-724-0 ББК 67.401.114

Перечень сокращений и обозначений

В настоящем учебном пособии применяют следующие сокращения и обозначения:

АС	– автоматизированная система;
АРМ	– автоматизированное рабочее место;
ВП	– выделенное помещение;
ВТ	– объект вычислительной техники;
ВТСС	– вспомогательные технические средства и системы;
ИВЦ	– информационно-вычислительный центр;
ИС	– информационная система;
КС	– компьютерная система;
Минобороны России	– Министерство обороны России;
МЭ	– межсетевой экран;
НСД	– несанкционированный доступ;
РФ	– Российская Федерация;
УрЮИ МВД России	– Уральский юридический институт МВД России;
ОС	– операционная система;
ОТСС	– основные технические средства и системы;
ПО	– программное обеспечение;
СЗИ	– средства защиты информации;
ТСОИ	– техническое средство обработки информации;
ФСБ России	– Федеральная служба безопасности России;
ФСТЭК России	– Федеральная служба по техническому и экспортному контролю России;
ЭВМ	– электронно-вычислительная машина

Введение

Решение проблем обеспечения информационной безопасности в наши дни имеет первостепенное значение. Причем это актуально на всех уровнях: личности, общества, государства. Информационная безопасность (наряду с геополитической, оборонной, экономической, научно-технической, социальной, духовной, культурологической, экологической и др.) – неотъемлемая составная часть национальной безопасности Российской Федерации, играющая важнейшую роль в системе ее обеспечения. В информационной безопасности множество самых разнообразных направлений и аспектов (политические, правовые, профессиональные, технические и т. д.). Знание этих разнообразных направлений и аспектов позволит лучше разбираться в проблемах безопасности, экономике, политике и др.

Любой современный «профессионал-юрист» («профессионал-экономист») должен обязательно иметь представление о способах и средствах обеспечения информационной безопасности, мерах защиты информации, системе защиты государственной тайны, защите персональных данных, а также о таких «феноменах», как угроза информационным ресурсам, информационное оружие, информационная война и др. Правоохранительные органы являются одним из основных элементов государства. Поэтому формирование у сотрудников органов внутренних дел основ культуры обеспечения информационной безопасности, приобретение ими теоретических знаний, практических умений, навыков и опыта деятельности в данной сфере – своего рода цель учебной дисциплины «Основы информационной безопасности в органах внутренних дел».

Обучающиеся УрЮИ МВД России по специальностям 40.05.01 Правовое обеспечение национальной безопасности, 40.05.02 Правоохранительная деятельность, 38.05.01 Экономическая безопасность в соответствии с учебными планами по указанным специальностям изучают учебную дисциплину «Основы информационной безопасности в органах внутренних дел».

Учебное пособие «Основы информационной безопасности в органах внутренних дел» предназначено для изучения обучающимися УрЮИ МВД России по специальностям 40.05.01 Правовое обеспечение национальной безопасности, 40.05.02 Правоохранительная деятельность, 38.05.01 Экономическая безопасность учебной дисциплины «Основы информационной безопасности в органах внутренних дел».

Учебное пособие «Основы информационной безопасности в органах внутренних дел» направлено на формирование у обучающихся УрЮИ МВД России следующих компетенций:

– общекультурная компетенция (для обучающихся по специальностям 40.05.01 Правовое обеспечение национальной безопасности, 40.05.02 Правоохранительная деятельность, 38.05.01 Экономическая безопасность): способность работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации;

– профессиональная компетенция (для обучающихся по специальностям 40.05.01 Правовое обеспечение национальной безопасности, 40.05.02 Правоохранительная деятельность): способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности;

– профессиональная компетенция (для обучающихся по специальности 38.05.01 Экономическая безопасность): способность соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности.

1. Основные понятия информационной безопасности органов внутренних дел

Основные вопросы, о которых далее пойдет речь, присущи как информационной безопасности в целом, так и информационной безопасности органов внутренних дел.

Принцип обеспечения безопасности (собственной безопасности) лежит в основе жизнедеятельности всех социальных систем. Он связан с потребностями системы (ее элементов) в выживании и прогрессивном развитии. Безопасность при этом определяют как неотъемлемое свойство (атрибут) системы, состоящее в способности на основе осознанной, целенаправленной деятельности обеспечивать такой порядок взаимосвязей, при котором дезорганизующее воздействие внешней среды и внутренних противоречий на жизненно важные интересы ограничивается пределами, отвечающими за потребности данной системы и ее элементов в устойчивом развитии.

В государственно-организованном обществе основными объектами безопасности являются человек, общество и государство, а основным субъектом обеспечения безопасности – государство, осуществляющее функции в этой области через органы законодательной, исполнительной и судебной властей.

Под безопасностью в общем смысле понимают состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Рассмотрим ряд общих понятий в области информационной безопасности согласно Доктрине информационной безопасности Российской Федерации (указ Президента Российской Федерации от 5 декабря 2016 г. № 646).

Информационная сфера – совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

Национальные интересы Российской Федерации в информационной сфере – объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы.

Угроза информационной безопасности Российской Федерации – совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере.

Информационная безопасность Российской Федерации – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Обеспечение информационной безопасности – осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления.

Силы обеспечения информационной безопасности – государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности.

Средства обеспечения информационной безопасности – правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности.

Система обеспечения информационной безопасности – совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности.

Информационная инфраструктура Российской Федерации – совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации.

Необходимо отметить, что информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества.

Информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации.

Национальными интересами в информационной сфере являются:

– обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации;

– обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации (далее – критическая информационная инфраструктура) и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время;

– развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности;

– доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения национальной безопасности Российской Федерации в области культуры;

– содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве.

Стоит отметить негативное воздействие на население средств массовой информации, которые представляют информацию в виде, дискредитирующем руководителей ведомств, органы исполнительной власти, государственные организации или Российскую Федерацию в целом. Наращивается информационное воздействие на население России.

В настоящее время отмечается высокая активность хакерских атак на объекты критической информационной инфраструктуры, в связи с чем ФСТЭК разработана нормативно-

правовая база для обеспечения информационной безопасности данных объектов, в которых реализация угроз конфиденциальности, целостности или доступности может привести к фатальным последствиям.

Рассмотрим также ряд общих понятий в области информационной безопасности согласно иным нормативным правовым актам.

Для удобства представим их в алфавитном порядке.

Актив – все, что имеет ценность для организации.

Различают следующие виды активов:

– информация;

– программное обеспечение;

– технические средства (например, компьютер);

– услуги и сервисы;

– люди и их квалификация, навыки и опыт;

– нематериальные активы (например, репутация и имидж).

Безопасность информации (данных) – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

Блокирование доступа к информации – прекращение или затруднение доступа законных пользователей к информации.

Вредоносная программа (программное обеспечение) – программа (программное обеспечение), предназначенная для осуществления несанкционированного доступа к информации и/или деструктивного воздействия на информацию или ресурсы информационной системы, нарушение их целостности и/или доступности.

Доступ к информации – возможность получения информации и ее использования.

Доступность информации (ресурсов информационной системы) – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Защита информации от несанкционированного доступа – защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Защита информации от преднамеренного воздействия – защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного, и/или воздействия другой физической природы, осуществляемого в террористических или криминальных целях.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информация – сведения, сообщения, данные независимо от формы их представления.

Инцидент информационной безопасности – одно или несколько нежелательных или не ожидаемых событий информационной безопасности, которые со значительной вероятностью приводят к компрометации бизнес-операций и создают угрозы для информационной безопасности.

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

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Модель угроз безопасности информации – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Модификация информации – целенаправленное изменение формы представления и содержания информации.

Нарушитель безопасности информации – физическое лицо (субъект), случайно или преднамеренно совершившее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах.

Различают внешнего и внутреннего нарушителей. Внутренний нарушитель – это злоумышленник, который на момент начала реализации угрозы находится внутри информационной системы (далее – ИС). Внешний нарушитель – это злоумышленник, который на момент начала реализации угрозы находится вне ИС.

Для реализации угроз в ИС внешний нарушитель должен тем или иным способом получить доступ к процессам, проходящим в ИС. При этом дальнейшие свои действия внешний нарушитель выполняет от имени созданного им нового или существующего в системе субъекта.

К внутренним нарушителям относят инсайдеров, несмотря на то, что они могут выполнять инструкции лиц, находящихся вне информационной системы.

Несанкционированный доступ к информации – доступ к информации ресурсам информационной системы, осуществляемый с нарушением установленных прав и/или правил доступа к информации ресурсам информационной системы с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному предназначению и техническим характеристикам.

Потенциал нарушителя – мера усилий, затрачиваемых нарушителем при реализации угроз безопасности информации в информационной системе.

Различают высокий, средний и низкий потенциалы нарушителя.

Высокий потенциал подразумевает наличие возможностей уровня предприятия / группы предприятий / государства по разработке и использованию специальных средств эксплуатации уязвимостей.

Средний потенциал подразумевает наличие возможностей уровня группы лиц / организации по разработке и использованию специальных средств эксплуатации уязвимостей.

Низкий потенциал подразумевает наличие возможностей уровня одного человека по приобретению (в свободном доступе на бесплатной или платной основе) и использованию специальных средств эксплуатации уязвимостей.

Потенциальная уязвимость – предполагаемая, но не подтвержденная уязвимость.

Предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Событие информационной безопасности – выявленное наступление состояния системы, сервисов или вычислительной сети, указывающее на возможное нарушение политики информационной безопасности, на сбой или отсутствие необходимых мер защиты или на прежде неизвестную ситуацию, относящейся к обеспечению безопасности.

Способ защиты информации – порядок и правила применения определенных принципов и средств защиты информации.

Угроза – возможная причина нежелательного инцидента, которая может нанести ущерб (информационной) системе или всей организации.

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

Уязвимость – слабость актива или управления, эксплуатация которой приведет к реализации одной или нескольких угроз.

Уязвимость – недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации.

Целостность информации – состояние информации, при котором обеспечивается ее неизменность в условиях преднамеренного и/или непреднамеренного воздействия на нее.

Информационное оружие – это специально подобранная информация, под воздействием которой происходят изменения в информационных системах и процессах (физических, биологических, социальных) в соответствии с замыслом субъекта его применения.

Применение информационного оружия – информационная война.

Информационная война – форма борьбы сторон с использованием специальных способов и средств для воздействия на информационную среду противника и защиты собственной в интересах достижения поставленных целей.

Вопросы и задания для самоконтроля

1. Как вы понимаете термин «Угроза информационной безопасности Российской Федерации»?
2. Дайте определение термину «Информационная безопасность Российской Федерации».
3. Дайте определение термину «Информация».
4. Дайте определение термину «Безопасность информации».
5. Дайте определение термину «Информационная система».
6. Дайте определение термину «Информационные технологии».
7. Дайте определение термину «Информационно-телекоммуникационная сеть».
8. Дайте определение термину «Доступность информации».
9. Дайте определение термину «Конфиденциальность информации».
10. Дайте определение термину «Целостность информации».

2. Обеспечение информационной безопасности в органах внутренних дел

Основные вопросы, о которых далее пойдет речь, присущи как информационной безопасности в целом, так и информационной безопасности органов внутренних дел.

Рассмотрим ряд общих вопросов в области обеспечения информационной безопасности согласно Доктрине информационной безопасности Российской Федерации (указ Президента Российской Федерации от 5 декабря 2016 г. № 646).

Стратегической целью обеспечения информационной безопасности в области обороны страны является защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.

Стратегическими целями обеспечения информационной безопасности в экономической сфере являются: сведение к минимально возможному уровню влияния негативных факторов, обусловленных недостаточным развитием отечественной отрасли информационных технологий и электронной промышленности, разработка и производство конкурентоспособ-

ных средств обеспечения информационной безопасности, а также повышение объемов и качества оказания услуг в области обеспечения информационной безопасности.

Стратегической целью обеспечения информационной безопасности в области науки, технологий и образования является поддержка инновационного и ускоренного развития системы обеспечения информационной безопасности, отрасли информационных технологий и электронной промышленности.

Стратегической целью обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства является формирование устойчивой системы неконфликтных межгосударственных отношений в информационном пространстве.

Основным направлением обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства является формирование устойчивой системы неконфликтных межгосударственных отношений в информационном пространстве.

Система обеспечения информационной безопасности является частью системы обеспечения национальной безопасности Российской Федерации.

Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

Система обеспечения информационной безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере с учетом предметов ведения федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, а также органов местного самоуправления, определяемых законодательством Российской Федерации в области обеспечения безопасности.

Состав системы обеспечения информационной безопасности определяется Президентом Российской Федерации.

Организационную основу системы обеспечения информационной безопасности составляют: Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, Центральный банк Российской Федерации, Военно-промышленная комиссия Российской Федерации, межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности.

Участниками системы обеспечения информационной безопасности являются: собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации и массовых коммуникаций, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы связи, операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационной безопасности.

Таким образом, для обеспечения безопасности информации в органах внутренних дел необходима четкая и слаженная система, построенная на принципах, изложенных в Доктрине информационной безопасности Российской Федерации (указ Президента Российской Федерации от 5 декабря 2016 г. № 646). Необходимо: обучение сотрудников органов внутренних дел правилам и принципам обеспечения безопасности информации, оснащение необходимой материально-технической базой подразделений органов внутренних дел, основательная проработка организационно-распорядительной документации, регламентирующей обязанности каждого сотрудника, регулярный полный и грамотный аудит системы информационной безопасности, преследующий цель предотвратить утечку информации.

Вопросы и задания для самоконтроля

1. Дайте характеристику стратегической цели обеспечения информационной безопасности в области обороны страны.
2. Дайте характеристику стратегических целей обеспечения информационной безопасности в экономической сфере.
3. Дайте характеристику стратегической цели обеспечения информационной безопасности в области науки, технологий и образования.
4. Дайте характеристику стратегической цели обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства.
5. Перечислите основные направления обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства.
6. Каким образом осуществляется обеспечение информационной безопасности?
7. На базе чего строится система обеспечения информационной безопасности?
8. Кем определяется состав системы обеспечения информационной безопасности?
9. Что составляет организационную основу системы обеспечения информационной безопасности?
10. Перечислите участников системы обеспечения информационной безопасности.

3. Защита информации от утечки на объектах информатизации органов внутренних дел

Решение задач информационной безопасности является одной из ключевых задач при управлении организацией, в первую очередь ввиду ценности информационных ресурсов в настоящее время.

Грамотное решение задач в области информационной безопасности напрямую зависит от политик безопасности, которые применяются в организации: они должны учитывать все аспекты технологического процесса обработки информации для того, чтобы наиболее уязвимые объекты были максимально защищены при появлении нарушителя.

Основные угрозы безопасности информации

Для начала необходимо сформулировать определение. Угроза безопасности информации представляет собой негативное явление преднамеренного или непреднамеренного характера, направленное на хищение, уничтожение или искажение информации. Каждый из данных факторов может являться критичным, если речь идет об информации ограниченного доступа.

Хищение информации представляет собой процесс, направленный на получение информации, распространение которой может нанести ущерб, например, репутации человека, финансовому благополучию организации или обороноспособности государства. Хищение возможно предотвратить путем введения комплекса мер для ограничения информации, например таких, как установка систем защиты информации на персональные компьютеры сотрудников, организационные меры, направленные на недопущение посторонних лиц на ра-

бочих местах, установку технических устройств, препятствующих допуску неавторизированных лиц: например, системы контроля и управления доступом, различных шлагбаумов и т. д.

Уничтожение представляет собой процесс преднамеренной или непреднамеренной ликвидации информации. Данный процесс возможно нейтрализовать путем введения обязательного резервирования информации критического характера, например, после каждого рабочего дня персональные компьютеры автоматически копируют информацию на сервер.

Искажение информации представляет собой преднамеренную или непреднамеренную подмену информации. Возможно предотвратить путем дублирования, введения избыточности передаваемой информации. Например, при передаче информации, искажение которой будет являться критичным, осуществлять передачу посредством технических средств и почты.

Информационные угрозы можно классифицировать по типу воздействия (рис. 1).

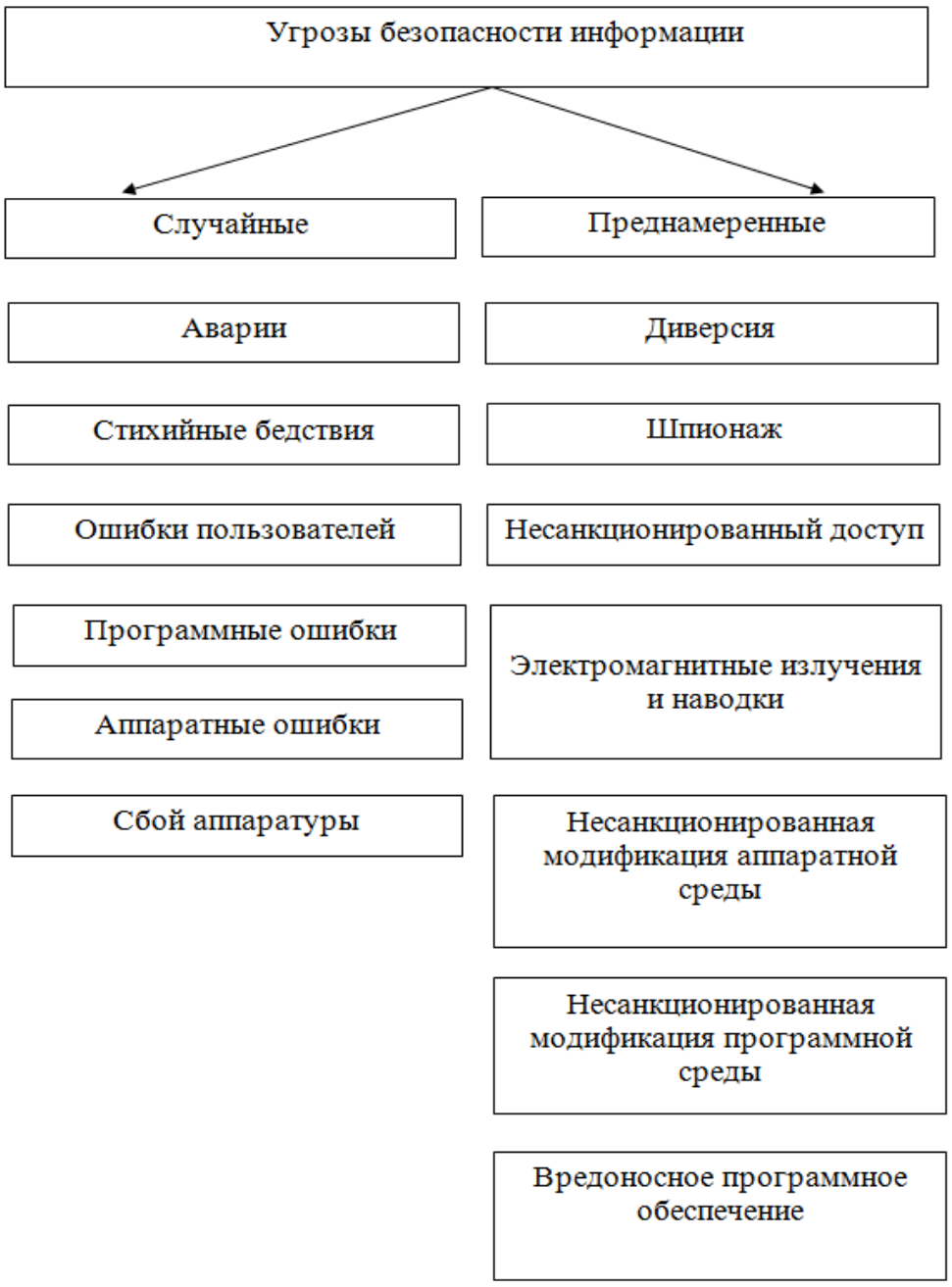

Рис. 1. Угрозы безопасности информации

Системная классификация угроз безопасности информации представлена в табл. 1.

Таблица 1

Системная классификация угроз безопасности информации

Параметры классификации	Значения параметров	Содержание значения параметра
1. Виды угроз	Физическая целостность Логическая структура Содержание Конфиденциальность Право собственности	Уничтожение (искажение) Искажение структуры Несанкционированная модификация Несанкционированное получение Присвоение чужого права
2. Природа происхождения	Случайная Преднамеренная	Отказы, сбои, ошибки, стихийные бедствия, побочные влияния Злоумышленные действия людей
3. Предпосылки появления	Объективные Субъективные	Количественная недостаточность элементов системы, качественная недостаточность элементов системы Разведка иностранных государств, промышленный шпионаж, уголовные элементы, недобросовестные сотрудники
4. Источники угроз	Люди Технические устройства Модели, алгоритмы, программы	Посторонние лица, пользователи, персонал Регистрации, передачи, хранения, переработки, выдачи Общего назначения, прикладные, вспомогательные
	Технологические схемы обработки Внешняя среда	Ручные, интерактивные, сетевые, внутримашинные Состояние атмосферы, побочные шумы, побочные сигналы

Краткий комментарий к параметрам классификации

1. Виды угроз.

Данный параметр является основополагающим, определяющим целевую направленность защиты информации.

2. Природа происхождения угроз.

Под случайным понимается такое происхождение угроз, которое обуславливается спонтанными и не зависящими от воли людей обстоятельствами, возникающими в системе в процессе ее функционирования. Наиболее известными событиями данного плана являются отказы, сбои, ошибки, стихийные бедствия и побочные влияния.

Сущность перечисленных событий (кроме стихийных бедствий) определяется следующим образом:

– отказ – нарушение работоспособности какого-либо элемента системы, приводящее к невозможности выполнения им своих функций;

– сбой – временное нарушение работоспособности какого-либо элемента системы, следствием чего может быть неправильное выполнение им в этот момент своей функции;

– ошибка – неправильное (разовое или систематическое) выполнение элементом одной или нескольких функций, происходящее вследствие специфического (постоянного или временного) его состояния;

– побочное влияние – негативное воздействие на систему в целом или отдельные ее элементы, оказываемое какими-либо явлениями, происходящими внутри системы или во внешней среде.

Преднамеренное происхождение угрозы обуславливается злоумышленными действиями людей.

3. Предпосылки появления угроз: объективные (количественная или качественная недостаточность элементов системы) и субъективные (деятельность разведорганов иностранных государств, промышленный шпионаж, деятельность уголовных элементов, действия недобросовестных сотрудников системы). Они интерпретируются следующим образом:

– количественная недостаточность – физическая нехватка одного или нескольких элементов системы, вызывающая нарушения технологического процесса обработки данных и/или перегрузку имеющихся элементов;

– качественная недостаточность – несовершенство конструкции (организации) элементов системы, в силу чего могут появляться возможности случайного или преднамеренного негативного воздействия на обрабатываемую или хранимую информацию;

– деятельность разведки иностранных государств – специально организуемая деятельность государственных органов, профессионально ориентированных на добывание необходимой информации всеми доступными способами и средствами. К основным видам разведки относятся агентурная (несанкционированная деятельность профессиональных разведчиков, завербованных агентов и так называемых «доброжелателей») и техническая, включающая радиоразведку (перехват радиоэлектронными средствами информации, циркулирующей в телекоммуникационных каналах), радиотехническую разведку (регистрацию спецсредствами электромагнитных излучений технических систем) и космическую разведку (использование космических кораблей и искусственных спутников Земли для наблюдения за территорией, ее фотографирования, регистрации радиосигналов и получения полезной информации любыми способами);

– промышленный шпионаж – негласная деятельность организации (ее представителей) по добыванию информации, специально охраняемой от несанкционированной утечки или хищения, с целью создания для себя благоприятных условий и получения максимальных выгод (недобросовестная конкуренция);

– злоумышленные действия уголовных элементов – хищение информации или компьютерных программ в целях наживы;

– действия недобросовестных сотрудников – хищение (копирование) или уничтожение информационных массивов и/или программ по эгоистическим или корыстным мотивам, а также в результате несоблюдения установленного порядка работы с информацией.

4. Источники угроз. Под источником угроз понимается непосредственный ее генератор или носитель: люди, технические средства, модели (алгоритмы), программы, внешняя среда.

Понятие и виды каналов утечки информации ограниченного доступа

Утечка информации представляет собой неконтролируемый процесс ухода информации ограниченного доступа за рамки перечня лиц, допущенных к данной информации. Иначе говоря, информация, непредназначенная для огласки, становится доступной перечню лиц, не допущенных к этой информации.

Различают следующие каналы утечки информации:

– агентурные;

– технические;

Агентурный канал утечки информации подразумевает вербовку лиц, представляющих интерес в плане добывания различной информации. Для этой цели применяются самые различные механизмы:

– манипуляция;

– угроза;

– шантаж;

– подкуп;

– манипуляция интересами человека;

– навязывание интересов.

Для установления контакта с лицом, которое интересно стороне разведки используются различные психологические приемы. После того, как контакт установлен, принимаются дальнейшие шаги по сближению с объектом и формированию у объекта иллюзии дружеской атмосферы при общении с разведчиком. Далее могут разыгрываться самые различные сценарии, которые направлены лишь на одну цель – добывание интересующей информации. Например, может быть смоделирована ситуация, что у мнимого друга объекта разведки срочно возникла необходимость передать какой-либо предмет, оставив его в конференц-зале. Ничего не подозревающий объект пронесет предмет с вмонтированным передатчиком и оставит его в конференц-зале, не вызвав подозрений у своих коллег. Сценарии возможны самого различного плана, вплоть до того, что разведчики могут пойти на жертвы ради добывания информации. Более того, они могут быть сами раскрыты и осуждены.

В систему связи в общем виде входит: источник информации, передатчик, канал передачи информации, приемник и получатель информации. Такая система используется в повседневной практике в соответствии со своим предназначением и является официальным средством передачи информации. Однако существуют определенные условия (помехи, изменения параметров и т. п.), при которых возможно образование системы передачи информации из одной точки в другую независимо от желания объекта и источника. При этом такой канал в явном виде не должен себя проявлять. По аналогии с каналом передачи информации такой канал называют каналом утечки информации. В канал утечки информации входит: источник сигнала, физическая среда его распространения, приемная аппаратура (средства разведки) на стороне злоумышленника (рис. 2). Движение информации в таком канале осуществляется только в одну сторону – от источника конфиденциальной информации к злоумышленнику.

Рис. 2. Схема появления канала утечки информации

Для возникновения (образования, установления) канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также соответствующие средства восприятия и фиксации информации на стороне злоумышленника.

Причинами образования технических каналов утечки информации являются:

- несовершенство (элементов, решений, технологии, монтажа);
- эксплуатационный износ (изменение характеристик, выход из строя, халатность);
- злоумышленные действия (перенастройка, авария, блокирование защиты).

Более полная классификация технических каналов утечки информации представлена на рис. 3. Наиболее часто на практике встречается электромагнитный канал утечки информации (электромагнитные волны безгранично распространяются и принимаются специальной аппаратурой с последующим усилением и раскодированием), а также электрический (прямое подключение к линии связи с последующим усилением сигнала), индукционный (регистрируются и усиливаются электромагнитные излучения линий связи), виброакустический (канал утечки возникает за счет преобразования акустических колебаний в электрические сигналы), акустический (речевой сигнал распространяется по воздуху и усиливается), акустоэлектрический (регистрируются колебания строительных конструкций под воздействием акустических), оптико-электронный (изменяются отражающие характеристики стекол под воздействием акустических колебаний) и параметрический (изменяются параметры электронных схем под воздействием акустических колебаний). Схемы представлены на рис. 4 и 5. Виды и схемы технических каналов утечки информации в ЭВМ представлены на рис. 3–6.

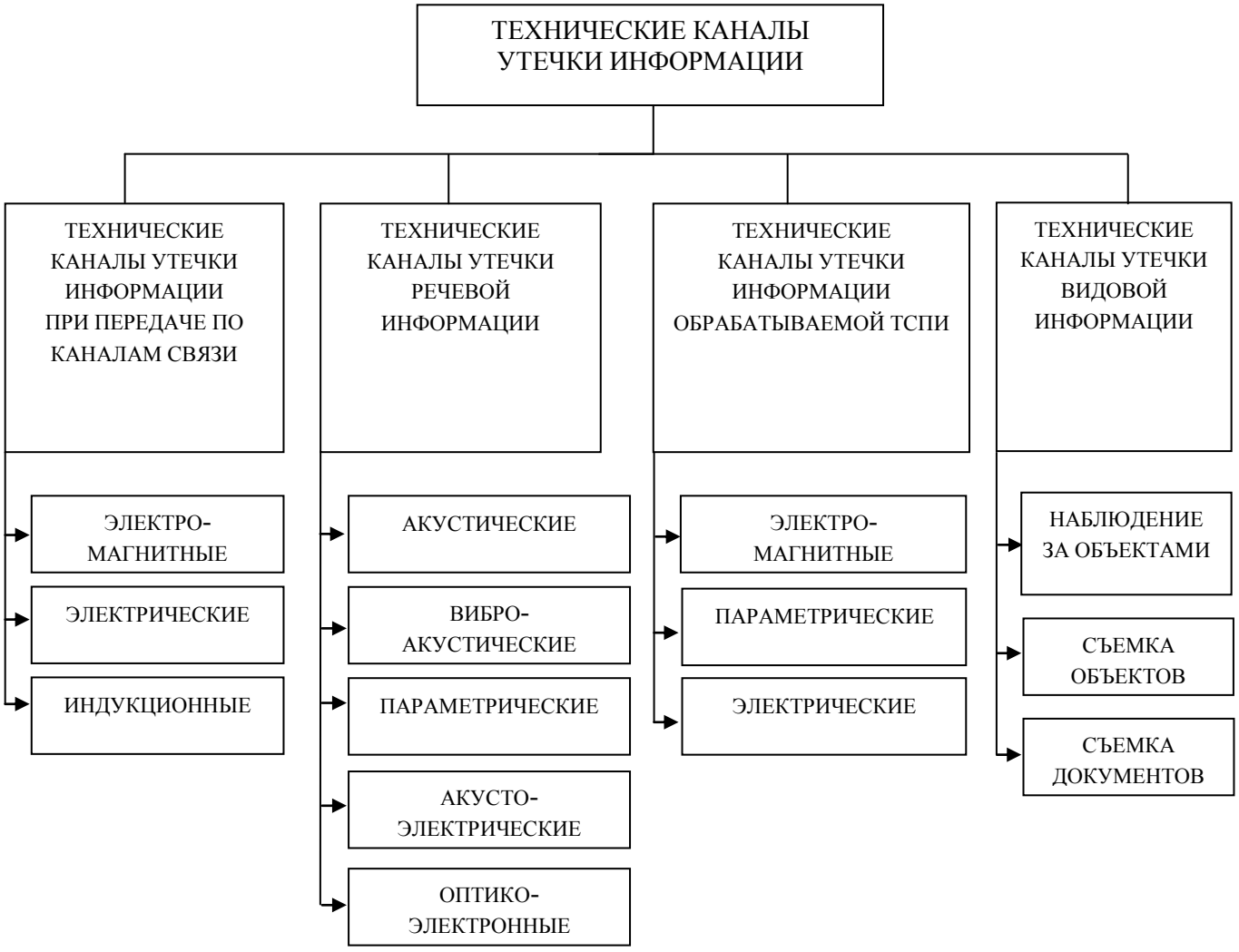

Рис. 3. Виды технических каналов утечки информации

Одним из актуальных каналов утечки информации является канал высокочастотного навязывания. Идея состоит в том, что злоумышленник, находясь на удаленном расстоянии от объекта разведки подает высокочастотный импульс на металлосодержащие элементы, например, персональные компьютеры, мониторы, батареи отопления и т. д. Человек, находясь в данном помещении, ведет конфиденциальный разговор, который модулирует высокочастотный сигнал разведчика, который тот, в свою очередь, принимает и демодулирует. Высокая вероятность перехвата информации по данному каналу утечки обусловлена тем, что практически все окружение современного человека имеет элементы, от которых может произойти переизлучение.

Не менее интересным каналом утечки информации является канал утечки побочных электромагнитных излучений и наводок. Этот канал утечки представляет собой электромагнитный информативный фон от технических устройств обработки информации, который может содержать сведения, которые обрабатываются в данных устройствах. При перехвате данного фона с достаточно средних расстояний, например около 300 метров, возможно восстановить информацию с высокой долей вероятности, разместившись, например, на парковке под окнами помещения, в котором обрабатывается информация ограниченного доступа. А наводки возможно снять, подключившись, например, к сети электропитания, единой с той, в которой происходит обработка информации.

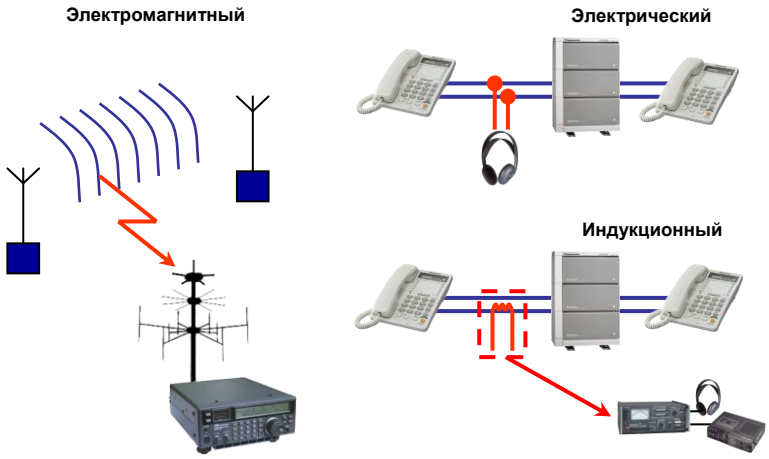

Рис. 4. Схемы создания электромагнитного, электрического и индукционного технических каналов утечки информации

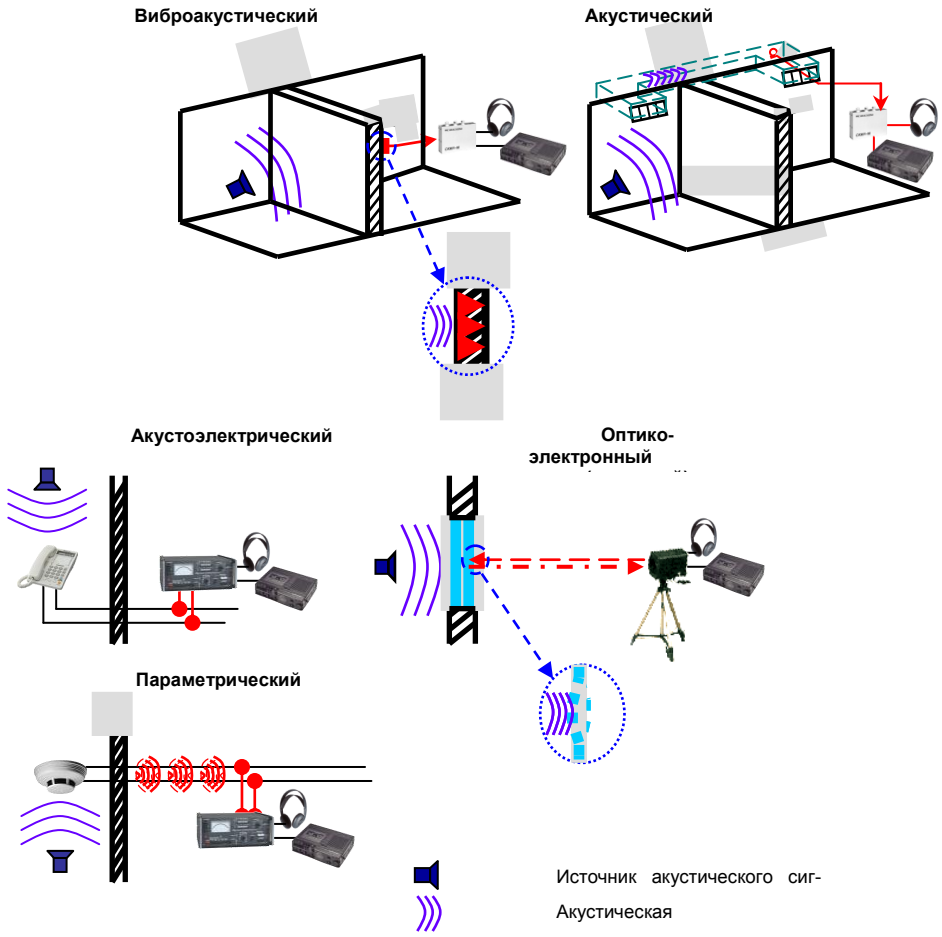

Рис. 5. Схемы создания виброакустического, акустического, акустоэлектрического, оптико-электронного и параметрического технических каналов утечки информации

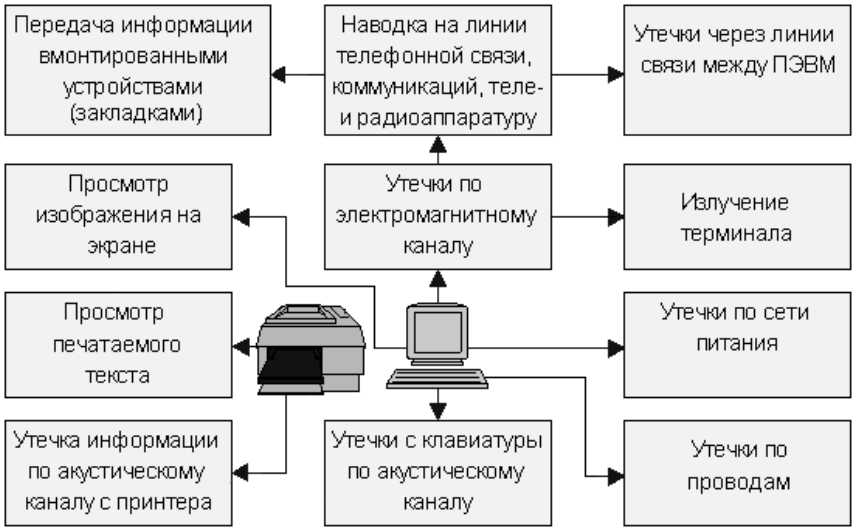

Рис. 6. Технические каналы утечки информации в ЭВМ

Основные направления инженерно-технической защиты информации

Приоритетными направлениями в защите информации является физическая и инженерно-техническая защита. Под физической защитой понимают все то, что препятствует доступу злоумышленников к информации и любым физическим воздействиям на информацию, носители информации, средства обработки информации, персонал, материальные средства и финансы. Под инженерно-технической защитой понимают системы, средства, приборы, устройства, приспособления, а также технические, конструкторские и дизайнерские решения, используемые в целях обеспечения информационной безопасности.

В систему физической и инженерно-технической защиты входят:

– сооружения и средства, препятствующие физическому проникновению на объекты защиты (строительные препятствия, здания, укрепленные стены, заборы, шлюзы, механические системы, колючая проволока, спирали из колючей ленты, системы ограждения и изоляции и т. п.);

– хранилища, сейфы;

– запирающие устройства, замки (механические, электромеханические, электронные);

– системы и средства связи;

– системы и средства видеонаблюдения (в т. ч. с функцией распознавания, обнаружения нарушителя или нарушающего воздействия);

– системы сигнализации (аварийной, охранной, противопожарной);

– системы контроля и управления доступом (с функцией досмотра);

– средства отображения и оценки обстановки, управления в аварийных и тревожных ситуациях;

– средства оповещения и связи в экстремальных ситуациях;

– системы электроснабжения;

– противопожарные системы;

– системы жизнеобеспечения (в т. ч. с учетом специальной подготовки выделенных помещений);

– технические средства защиты от перехвата информации (приборы, комплексы и системы поиска);

– технические средства нейтрализации каналов утечки информации: пассивные – средства экранирования помещений и активные – генераторы помех, генераторы шумов и т. п.;

– технические средства подготовки выделенных помещений (пол, окна, стены и т. п.);

– технические средства защиты информации от несанкционированного доступа (пломбы, замки разового пользования, защитные липкие ленты, защитные и голографические этикетки, специальные защитные упаковки, специальные средства для транспортировки и хранения физических носителей информации);

– специальные средства защиты от подделки документов;

– специальные пиротехнические средства для транспортировки, хранения и экстренного уничтожения физических носителей информации (бумага, фотопленка, аудио- и видеокассеты, лазерные диски и др.);

– антитеррористические средства (в т. ч. средства защиты от силового деструктивного воздействия по проводным и беспроводным каналам);

– персонал охраны системы и средства обеспечения личной безопасности персонала.

Для защиты объектов информатизации от утечки информации по техническим каналам могут быть применены следующие технические средства:

– устройства защиты от утечки информации по ПЭМИН (в т. ч. переносные);

– устройства защиты от утечки информации по электросети;

– устройства защиты от утечки информации по телефонным и слаботочным линиям;

– подавители GSM, 3G, WiFi, Bluetooth, GPS, Глонасс;

– подавители диктофонов;

– системы акустического и виброакустическго зашумления;

– помехоподавляющие сетевые фильтры;

– устройства уничтожения носителей информации;

– радиопоглощающие и экранирующие материалы;

– комплексы и системы защиты.

Пример некоторых сертифицированных технических средств защиты информации, используемых в органах внутренних дел: комплекс виброакустической защиты «Шелест-4К», специальный аппаратно-программный комплекс «Панцирь-М», система защиты информации от несанкционированного доступа (аппаратно-программный комплекс) «Страж NT», устройства защиты линий серии «Соната-ВК», генератор шума ГШ-1000М.

Лицензирование, сертификация, аттестация и специальные проверки объектов информатизации в сфере защиты информации

Действенными инструментами государственной системы защиты информации являются процедуры лицензирования деятельности организаций в области защиты информации, сертификации и средств защиты информации, аттестации объектов информатизации.

Лицензирование деятельности организаций в сфере защиты информации.

Лицензирование – процедура выдачи на определенный срок специальных разрешений (лицензий) на ведение соответствующих видов деятельности. Суть лицензирования заключается в разрешении юридическим лицам или индивидуальным предпринимателям (лицензиатам) заниматься определенными видами деятельности только при соблюдении обязательных требований и условий (устанавливаются соответствующими положениями о лицензировании конкретных видов деятельности). Осуществляют лицензионную деятельность (первоначальную проверку наличия у лицензиата соответствующих условий, выдачу лицензий и ведение соответствующих реестров, последующий контроль за соблюдением установленных требований и условий) лицензирующие органы – федеральные органы исполнительной власти и органы исполнительной власти субъектов федерации. Лицензии выдаются на определенный срок, на каждый конкретный вид деятельности. В случае выявления неоднократных или грубых нарушений лицензионных требований и условий лицензирующие органы вправе наложить административное взыскание и приостановить действие лицензии, установив срок устранения лицензиатом нарушений. Если в установленный срок лицензиат не

устранил указанные нарушения, лицензирующий орган обязан обратиться в суд с заявлением об аннулировании лицензии.

В области защиты информации обязательному лицензированию подлежат следующие виды деятельности:

– деятельность по распространению шифровальных (криптографических) средств;

– деятельность по техническому обслуживанию шифровальных (криптографических) средств;

– предоставление услуг в области шифрования информации;

– разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;

– деятельность по выявлению 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);

– деятельность по разработке и (или) производству средств защиты конфиденциальной информации;

– деятельность по технической защите 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.

Полномочия государственных органов по лицензированию перечисленных выше видов деятельности распределены следующим образом:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) лицензирует деятельность по технической защите конфиденциальной информации.

2. Федеральная служба безопасности РФ (ФСБ России) лицензирует деятельность:

– по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность;

– выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, когда указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

– распространению шифровальных (криптографических) средств;

– техническому обслуживанию шифровальных (криптографических) средств;

– предоставлению услуг в области шифрования информации;

– разработке и производству шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем.

Лицензированием деятельности по разработке и (или) производству средств защиты конфиденциальной информации занимается ФСТЭК России, а в части разработки и (или) производства таких средств, устанавливаемых на объектах высших органов государственной власти, – ФСБ России.

Еще один вид деятельности, подлежащий обязательному лицензированию, это деятельность, связанная с использованием и защитой сведений, составляющих государственную тайну (рис. 7).

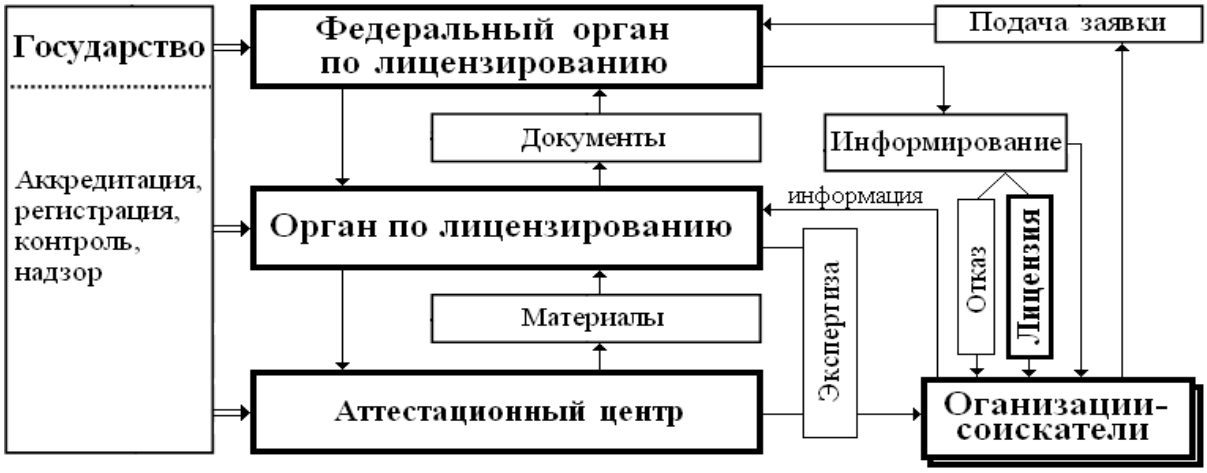

Рис. 7. Схема лицензирования организаций на право проведения работ и оказания услуг в области защиты государственной тайны

Сертификация средств защиты информации

Еще одним высокоэффективным средством государственного контроля является сертификация.

Сертификация – это подтверждение соответствия продукции, процессов производства, эксплуатации, работ, услуг или иных объектов установленным требованиям.

В области информационной безопасности нормы по сертификации средств защиты информации регламентируются Положением о сертификации средств защиты информации, утвержденным приказом ФСТЭК России от 3 апреля 2018 г. № 55. Данное положение утверждает основные правила по порядку получения, продления, приостановления сертификатов соответствия средств защиты информации.

В данной процедуре имеется две заинтересованные стороны – заявители и изготовители. При сертификации серийной партии изделий заявитель и изготовитель являются одним лицом. Но если в эксплуатации организации имеется средство защиты информации, которое необходимо сертифицировать и на которое отсутствуют заменяемые аналоги, то заявителем может стать организация, эксплуатирующая данное средство защиты.

Схема процесса сертификации представлена на рис. 8.

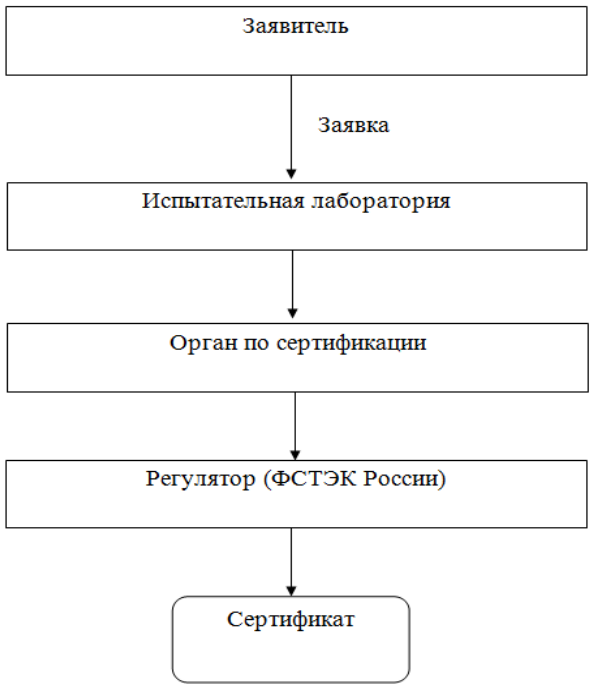

Рис. 8. Процесс получения сертификата соответствия

Процедуру сертификации осуществляет независимая от изготовителя (продавца, исполнителя) и потребителя (покупателя) организация – орган по сертификации, т. е. юридическое лицо или индивидуальный предприниматель, аккредитованные в установленном порядке для выполнения работ по сертификации. Органы сертификации, осуществляющие обязательную сертификацию, должны быть аккредитованы в порядке, устанавливаемом Правительством РФ.

В соответствии с п. 8 ст. 14 Федерального закона «Об информации, информационных технологиях и о защите информации», «технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации (СЗИ), должны соответствовать требованиям законодательства РФ о техническом регулировании».

Ст. 41 Федерального закона «О связи» устанавливает обязательную сертификацию средств связи, которую осуществляет Мининформсвязи России.

Одним из условий получения лицензии для осуществления работ со сведениями, составляющими государственную тайну, является наличие на предприятии сертифицированных средств защиты информации (технические, криптографические, программные и другие средства, а также средства, в которых они реализованы, и средства контроля эффективности защиты информации).

Организация сертификации средств защиты информации возлагается на ФСТЭК России, ФСБ России и Минобороны России согласно функциям, возложенным на них законодательством РФ. Сертификация осуществляется на основании требований государственных стандартов РФ и иных нормативных документов, утверждаемых Правительством РФ.

Подлежат сертификации: собственно средства защиты информации (технические, программно-технические, программные); средства, в которых реализованы СЗИ (т. е. защищенные технические программно-технические и программные средства); средства контроля эффективности защиты информации (технические, программно-технические, программные).

Координацию работ по организации сертификации средств защиты информации осуществляет Межведомственная комиссия по защите государственной тайны.

Обязательную сертификацию средств электронной цифровой подписи, используемых в открытых информационных системах, осуществляет ФСТЭК России.

Аттестация объектов информатизации

Аттестация объекта – официальное подтверждение наличия на объекте защиты необходимых и достаточных условий, обеспечивающих выполнение установленных требований руководящих документов по защите информации.

Аттестация объекта информатизации представляет процесс по обследованию объекта, установлению в нем отсутствия возможности утечки информации ограниченного доступа. Для данной цели применяется комплекс мер, направленных на исследование условий обработки информации.

Под аттестацией объекта информатизации по требованиям безопасности информации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа «Аттестат соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативных документов по защите информации, утвержденных ФСТЭК России (Гостехкомиссией).

Наличие на объекте информатизации действующего «Аттестата соответствия» дает право обработки информации с уровнем секретности (конфиденциальности) на период времени, установленным в «Аттестате соответствия».

Специальные проверки объектов информатизации

Специальная проверка – это проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств.

По сути дела, специальная проверка – это комплекс инженерно-технических мероприятий, проводимых с использованием контрольно-измерительной аппаратуры, в том числе и специализированных технических средств, направленных на исключение перехвата технической разведкой информации, содержащей сведения, составляющие государственную тайну, с помощью внедренных в защищаемые технические средства и изделия специальных электронных закладочных устройств.

Специальная проверка также может выполняться и для помещения для выявления факта наличия закладных устройств, так называемых «жучков». Проводится частичное освобождение площади помещения, зондируются нелинейным локатором стены, элементы интерьера, мебель. Принцип работы нелинейного локатора заключается в обнаружении нелинейных элементов, по аналогии принципа металлоискателя.

Требования по специальным проверкам регламентируются нормативно-правовыми актами регуляторов.

Вопросы и задания для самоконтроля

1. Каким образом можно классифицировать информационные угрозы по типу воздействия?
2. Как вы понимаете термин «Утечка информации»?
3. Поясните структуру системы связи.
4. Поясните причины образования технических каналов утечки информации.
5. Приведите классификацию технических каналов утечки информации.
6. Что входит в систему физической и инженерно-технической защиты?
7. Приведите примеры технических средств, которые могут быть применены для защиты объектов информатизации от утечки информации по техническим каналам связи.
8. Какие виды деятельности в области защиты информации подлежат обязательному лицензированию?
9. Поясните сертификацию средств защиты информации.
10. Поясните аттестацию объектов информатизации.

4. Защита информационных процессов в компьютерных системах

Основные проблемы в сфере защиты информации в КС

Все множество потенциальных угроз безопасности КС можно классифицировать следующим образом.

По воздействию извне угрозы безопасности КС подразделяются на естественные угрозы и искусственные угрозы.

Естественные угрозы – это угрозы, вызванные прямым или косвенным воздействием на КС силами природного характера, т. е. не человека. Например, наводнение, гроза и т. д.

Искусственные угрозы – это угрозы КС, реализованные человеком. Они подразделяются на умышленные угрозы и неумышленные угрозы.

Неумышленные угрозы – это угрозы, вызванные ошибками персонала, ошибками в программном обеспечении, то есть те угрозы, которые были осуществлены случайно, то есть непреднамеренно.

Умышленные угрозы – это целенаправленные действия, которые реализованы для того, чтобы осуществить преступный умысел: кража информации, блокирование или уничтожение.

Также угрозы можно классифицировать по источнику воздействия на внутренние угрозы и внешние угрозы.

Внутренние угрозы – реализуются, как правило, персоналом организации или иными лицами, допущенными к работе в КС.

Внешние угрозы могут быть реализованы лицом, не имеющим отношения к «атакуемой» организации, преследующим цель нанести определенный ущерб организации путем причинения вреда информационной безопасности.

Меры предотвращения угроз компьютерным системам

По способам воздействия все меры по минимизации угроз подразделяют на правовые, морально-этические, административные, физические, аппаратно-программные.

Перечисленные меры безопасности КС можно рассматривать как последовательность барьеров или рубежей защиты информации. Для того чтобы добраться до защищаемой информации, нужно последовательно преодолеть несколько рубежей защиты.

Первый рубеж защиты, встающий на пути человека, пытающегося осуществить НСД к информации, является чисто правовым. Этот аспект защиты информации связан с необходимостью соблюдения юридических норм при передаче и обработке информации. Эти нормы препятствуют несанкционированному использованию информации и являются сдерживающим фактором для потенциальных нарушителей.

Второй рубеж защиты образуют морально-этические меры. Этический момент в соблюдении требований защиты имеет весьма большое значение. Очень важно, чтобы люди, имеющие доступ к компьютерам, работали в здоровом морально-этическом климате. К морально-этическим мерам противодействия относятся всевозможные нормы поведения, которые традиционно сложились или складываются в обществе по мере распространения компьютеров.

Третьим рубежом, препятствующим неправомочному использованию информации, являются административные меры (организационные). Администраторы всех рангов с учетом правовых норм и социальных аспектов определяют соответствующие меры защиты информации. Эти меры регламентируют: процессы функционирования КС; использование ресурсов КС; деятельность ее персонала; порядок взаимодействия пользователей с системой, с тем, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности.

Четвертым рубежом являются физические меры защиты. Сюда относят разного рода устройства и сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации.

Пятым рубежом являются аппаратно-программные средства защиты. К ним относятся различные электронные устройства и специальные программы, которые реализуют самостоятельно или в комплексе с другими средствами следующие способы защиты:

- идентификацию (распознавание) и аутентификацию (проверка подлинности) субъектов (пользователей, процессов) КС;
- разграничение доступа к ресурсам КС;
- контроль целостности данных;
- обеспечение конфиденциальности данных;
- регистрацию и анализ событий, происходящих в КС;
- резервирование ресурсов и компонентов КС.

Криптографические методы защиты информации

Криптографические методы защиты основаны на возможности осуществления некоторой операции преобразования информации, которая может выполняться одним или несколькими пользователями АС, обладающими некоторым секретом, без знания которого (с вероятностью близкой к единице за разумное время) невозможно осуществить эту операцию.

К криптографическим методам зашиты информации, в общем случае, относятся:

- шифрование (расшифрование) информации;
- формирование и проверка цифровой подписи электронных документов.

Применение криптографических методов и средств позволяет обеспечить решение следующих задач по защите информации:

– предотвращение возможности несанкционированного ознакомления с информацией при ее хранении в компьютере или на отчуждаемых носителях, а также при передаче по каналам связи;

– подтверждение подлинности электронного документа, доказательство авторства документа и факта его получения от соответствующего источника информации;

– обеспечение имитостойкости (гарантий целостности) – исключение возможности необнаружения несанкционированного изменения информации;

– усиленная аутентификация пользователей системы – владельцев секретных ключей.

Основным достоинством криптографических методов защиты информации является то, что они обеспечивают высокую гарантированную стойкость защиты, которую можно рассчитать и выразить в числовой форме (средним числом операций или временем, необходимым для раскрытия зашифрованной информации или вычисления ключей).

К числу основных недостатков криптографических методов можно отнести следующие: большие затраты ресурсов (времени, производительности процессоров) на выполнение криптографических преобразований информации; трудности с совместным использованием зашифрованной информации; высокие требования к сохранности секретных ключей и защиты открытых ключей от подмены; трудности с применением в отсутствии надежных средств защиты открытой информации и ключей от НСД.

Криптографические средства защиты информации

Одним из надежнейших приемов защиты информации является применение криптографических приемов. Для понимания возможностей криптографии необходимо разбираться в основных ее положениях.

С момента появления письменности начинается история криптографии. Более того, первоначально письменность сама по себе была криптографической системой, т. к. в древних обществах ею владели только избранные. Священные книги Древнего мира тому примеры.

Криптография (греч. kryptos – тайный, скрытый и graho – пишу) – наука о методах защиты информации на основе ее преобразования с помощью различных шифров и сохранением достоверности семантического содержания. Криптография также представляет собой отрасль науки палеографии (а также египтологии), изучающей графику систем тайнописи. Исходя из современных позиций теории передачи информации и теории кодирования, криптография определяется как отрасль научных знаний о методах обеспечения секретности и достоверности данных при передаче по каналам связи и хранении в устройствах оперативной и долговременной памяти.

Криптография является составляющей такой науки как криптология (kryptos – тайный, logos – наука). Второе ее направление (с прямо противоположными целями) – криптоанализ.

Криптоанализ (греч. kryptos – тайный, скрытый и analysis – разложение) – наука о методах раскрытия и модификации данных. Это научное направление преследует две цели. Первая – исследование закриптографированной информации с целью восстановления семантического содержания исходного документа, вторая – на основе изучения и распознавания методов криптографирования производить фальсификацию исходных документов с целью передачи ложной информации.

В истории развития криптологии можно выделить три периода:

– первый период – донаучная криптология, период разработок, осуществляемых «искусными умельцами» и учеными различных фундаментальных и прикладных направлений, начиная от архитектуры и заканчивая фундаментальной математикой;

– второй период, начало которого условно определено с 1949 г., когда впервые появилась работа американского инженера и математика, одного из создателей теории информации, К. Э. Шеннона «Теория связи в секретных системах». Именно с этого периода криптология сформировалась как отрасль науки прикладной математики;

– третий период имеет свое начало с появлением работ У. Диффи и М. Хелмана «Новые направления в криптографии» (1976 г.), «Защищенность и имитостойкость: введение в криптографию» (1979 г.), которые показали возможности организации секретной связи без предварительной передачи секретного ключа (ключа дешифрования).

Дальнейшее развитие наука криптография как научно-прикладное направление современного развития многих научных и технических школ, особенно на этапе развития современных информационных технологий, получила в системах цифровой обработки информации. Это положение относится к организации обмена как в компьютерных системах, так и в системах передачи аналоговой информации цифровыми методами (аудио- и видеотехника, системы телеизмерений и т. д.).

В настоящее время выделяется четыре направления криптографии:

– шифрование с закрытым ключом (симметричное шифрование);

– шифрование с открытым ключом (ассиметричное шифрование);

– алгоритмы электронной подписи (например, хэш-функции);

– системы генерации ключей.

Следующим шагом целесообразно будет рассмотреть основные понятия, которые используются в современной криптографии.

Шифрование – это обратимый процесс преобразования информации с использованием открытых и закрытых ключей, а также определенного алфавита, с целью сокрытия информации, путем замены, перестановки и иных действий, затрудняющих возможное дешифрование зашифрованной информации.

Алфавит – это фиксированная последовательность символов, предназначенная для отображения информации.

Ключ – это обязательный элемент шифра, содержащий сведения, позволяющие дешифровать зашифрованное сообщение.

Дешифрование – это процесс обратный шифрованию, позволяющий преобразовать зашифрованное сообщение в исходное состояние, которое было изначально.

Электронной подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т. е. криптоанализу). Имеется несколько показателей криптостойкости, среди которых количество всех возможных ключей и среднее время, необходимое для криптоанализа.

Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

– зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

– число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;

– число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей, должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);

– знание алгоритма шифрования не должно влиять на надежность защиты;

– незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;

– структурные элементы алгоритма шифрования должны быть неизменными;

– дополнительные биты, вводимые в сообщение в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте;

– длина шифрованного текста должна быть равной длине исходного текста;

– не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования;

– любой ключ из множества возможных должен обеспечивать надежную защиту информации;

– алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

Основные алгоритмы шифрования

Метод шифровки-дешифровки называют шифром (cipher). Некоторые алгоритмы шифрования основаны на том, что сам метод шифрования (алгоритм) является секретным. Ныне такие методы представляют лишь исторический интерес и не имеют практического значения. Все современные алгоритмы используют ключ для управления шифровкой и дешифровкой; сообщение может быть успешно дешифровано, только если известен ключ. В общем случае ключ, используемый для дешифровки, может не совпадать с ключом, используемым для шифрования.

Алгоритмы с использованием ключа делятся на два класса: симметричные (или алгоритмы с секретным ключом) и асимметричные (или алгоритмы с открытым ключом). Разница в том, что симметричные алгоритмы используют один и тог же ключ для шифрования и для дешифрования (или же ключ для дешифровки просто вычисляется по ключу шифровки). В то время как асимметричные алгоритмы используют разные ключи и ключ для дешифровки не может быть вычислен по ключу шифровки.

Симметричные алгоритмы подразделяют на потоковые шифры и блочные шифры. Потоковые позволяют шифровать информацию побитово, в то время как блочные работают с некоторым набором битов данных (обычно размер блока составляет 64 бита) и шифруют этот набор как единое целое.

Асимметричные шифры (также именуемые алгоритмами с открытым ключом или в более общем плане криптографией с открытым ключом) допускают, чтобы открытый ключ был доступен всем (скажем, опубликован в газете). Это позволяет любому зашифровать сообщение. Однако расшифровать это сообщение сможет только нужный человек (тот, кто владеет ключом дешифровки). Ключ для шифрования называют открытым ключом, а ключ для дешифрования закрытым ключом или секретным ключом.

Современные алгоритмы шифровки-дешифровки достаточно сложны, и их невозможно проводить вручную. Настоящие криптографические алгоритмы разработаны для использования компьютерами или специальными аппаратными устройствами. В большинстве приложений криптография производится программным обеспечением и имеется множество доступных криптографических пакетов.

Вообще говоря, симметричные алгоритмы работают быстрее, чем асимметричные. На практике оба типа алгоритмов часто используются вместе: алгоритм с открытым ключом используется для того, чтобы передать случайным образом сгенерированный секретный ключ, который затем используется для дешифровки сообщения.

Многие качественные криптографические алгоритмы доступны широко – в книжном магазине, библиотеке, Интернете. К широко известным симметричным алгоритмам относятся DES и IDEA.

Таблица 2

Классификация криптографического закрытия информации
(А – аппаратный, П – программный)

Виды преобразований	Способы преобразований	Разновидности способа	Способ реализации
Шифрование	Замена (подстановка)	Простая (одноалфавитная)	П
		Многоалфавитная одноконтурная обыкновенная	П
		Многоалфавитная одноконтурная монофоническая	П
		Многоалфавитная многоконтурная	П
	Перестановка	Простая	П
		Усложненная по таблице	П
		Усложненная по маршрутам	П
	Аналитическое преобразование	По правилам алгебры матриц	П
		По особым зависимостям	П
	Гаммирование	С конечной короткой гаммой	АП
		С конечной длиной гаммой	АП
		С бесконечной гаммой	АП
	Комбинированные	Замена + перестановка	АП
		Замена + гаммирование	АП
		Перестановка + гаммирование	АП
		Гаммирование + гаммирование	АП
Кодирование	Смысловое	По специальным таблицам	П
	Символьное	По кодовому алфавиту	П
Другие виды	Рассечение-разнесение	Смысловое	АП
		Механическое	П
	Сжатие-расширение		

Секретность алгоритма принципиально не может обеспечить безусловной стойкости (т. е. невозможность чтения криптограммы противником, обладающим бесконечными вычислительными ресурсами). Поскольку секретные алгоритмы не могут быть проверены широкомасштабными криптоаналитическими исследованиями, то имеется значительно более высокая вероятность (по сравнению с открытыми алгоритмами) того, что будут найдены уязвимые места и эффективные способы доступа к зашифрованной информации. В связи с этими обстоятельствами в настоящее время наиболее широко используются открытые алгоритмы, прошедшие длительное тестирование и обсуждение в открытой криптографической литературе. Стойкость современных криптосистем основывается не на секретности алгоритма, а на секретности некоторой информации сравнительно малого размера, называемой ключом. Ключ используется для управления процессом криптографического преобразования (шифрования) и является легко сменяемым элементом криптосистемы. Ключ может быть заменен пользователями в произвольный момент времени, тогда как сам алгоритм шифрования является долговременным элементом криптосистемы и связан длительным этапом разработки и тестирования.

При прочих равных условиях секретность алгоритма шифрования существенно (при адекватной его реализации) затрудняет проведение криптоаналитической атаки. Поэтому были предложены современные криптосистемы, в которых непосредственно алгоритм шифрования является легко сменяемым элементом и секретным, но в то же время имеется возможность открытого обсуждения стойкости криптосистемы. Это реализуется в гибких криптосистемах, в которых алгоритм шифрования формируется по специальному алгоритму

предвычислений (инициализации) под управлением секретного ключа пользователя. Алгоритм инициализации является открытым, и сам алгоритм шифрования является секретным, так же как и ключ шифрования.

Прошли многие века, в течение которых криптография была предметом избранных (жрецы, правители, крупные военачальники, дипломаты). Несмотря на малую распространенность, использование криптографических методов и способов преодоления шифров противника оказывало существенное воздействие на исход важных исторических событий. Известен не один пример того, как переоценка используемых шифров приводила к военным и дипломатическим поражениям. Вопреки применению криптографических методов в важных областях, эпизодическое использование криптографии не могло даже близко подвести ее к той роли и значению, которые она имеет в современном обществе. Своим превращением в научную дисциплину криптография обязана потребностям практики, порожденным электронной информационной технологией.

Пробуждение значительного интереса к криптографии и ее развитие началось с XIX века, что связано с зарождением электросвязи. В XX столетии секретные службы большинства развитых стран стали относиться к этой дисциплине как к обязательному инструменту своей деятельности. Наряду с развитием криптографических систем совершенствовались и методы, позволяющие восстанавливать исходное сообщение, исходя только из шифртекста (криптоанализ). Успехи криптоанализа приводили к ужесточению требований к криптографическим алгоритмам.

Несмотря на то, что согласно современным требованиям к криптосистемам они должны выдерживать криптоанализ на основе известного алгоритма, большого объема известного открытого текста и соответствующего ему шифртекста, шифры, используемые специальными службами, сохраняются в секрете. Это обусловлено необходимостью иметь дополнительный запас прочности, поскольку в настоящее время создание криптосистем с доказуемой стойкостью является предметом развивающейся теории и представляет собой достаточно сложную проблему.

Чтобы избежать возможных слабостей, алгоритм шифрования должен быть построен на основе хорошо изученных и апробированных принципах и механизмах преобразования. Ни один серьезный современный пользователь не будет полагаться только па надежность сохранения в секрете своего алгоритма, поскольку крайне сложно гарантировать низкую вероятность того, что информация об алгоритме станет известной злоумышленнику.

Обоснование надежности используемых систем осуществляется, как правило, экспериментально при моделировании криптоаналитических нападений с привлечением группы опытных специалистов, которым предоставляются значительно более благоприятные условия по сравнению с теми, которые могут иметь место на практике в предполагаемых областях применения криптоалгоритма. Например, кроме шифртекста и алгоритма преобразований криптоаналитикам предоставляется весь или часть исходного текста, несколько независимых шифртекстов, полученных с помощью одного и того же ключа, или шифртексты, получаемые из данного открытого текста с помощью различных ключей. Оценивается стойкость испытываемой системы ко всем известным методам криптоанализа, разрабатываются новые подходы к раскрытию системы. Если в этих благоприятствующих взлому условиях криптосистема оказывается стойкой, то она рекомендуется для данного конкретного применения.

В современном криптоанализе рассматриваются следующие виды нападений на засекречивающие системы:

– криптоанализ на основе шифртекста;

– криптоанализ на основе известного открытого текста и шифртекста;

– криптоанализ на основе выбранного открытого текста;

– криптоанализ на основе выбранного шифртекста;

– криптоанализ на основе адаптированного открытого текста;
– криптоанализ на основе адаптированного шифртекста;
– криптоанализ на основе аппаратных ошибок.

Современные приложения криптографии

Значение криптографии выходит далеко за рамки обеспечения секретности данных. По мере все большей автоматизации передачи и обработки информации и интенсификации информационных потоков ее методы приобретают уникальное значение.

Отметим некоторые современные направления ее приложения:

– защита от несанкционированного чтения (обеспечение конфиденциальности информации);
– защита от навязывания ложных сообщений (умышленных и непреднамеренных);
– идентификация законных пользователей;
– контроль целостности информации;
– аутентификация информации;
– электронная цифровая подпись;
– системы тайного электронного голосования;
– электронная жеребьевка;
– защита от отказа факта приема сообщения;
– одновременное подписание контракта;
– защита документов и ценных бумаг от подделки.

Защита программ и баз данных от копирования.

Защита от копирования – особый вид защиты информации, применяемый в отношении программного обеспечения и других объектов интеллектуальной собственности в тех случаях, когда издатель желает сделать информацию доступной для чтения (воспроизведения, просмотра, запуска программ), но не хочет допускать несанкционированного копирования, тиражирования.

Способы защиты программ и баз данных от копирования

Так же, как в других случаях защиты информации действует принцип: абсолютной защиты не существует. Однако можно создать защиту, делающую нецелесообразным ее преодоление. Как правило, это касается продукции отечественного производства. На Западе гораздо меньше распространено программное «пиратство». Поэтому западные производители редко пользуются серьезной защитой от копирования. Ведь такая защита всегда создает некоторое неудобство для пользователя, а значит, снижает конкурентоспособность.

Основные методы защиты от копирования таковы:

1. Пароль на программу.

В этом случае, конечно, программу можно скопировать, но работать она будет лишь у того пользователя, который знает пароль. Понятно, что такой метод имеет смысл лишь тогда, когда пользователь программы не заинтересован в ее тиражировании. В связи с этим данный метод применяется ограниченно. Чаще всего при изготовлении некоей специализированной программы по индивидуальному заказу.

Разновидность данного метода часто используется в дистрибутивах продукции Microsoft и других западных производителей. Для инсталляции программы необходимо ввести индивидуальный код продукта (пользователя). Естественно, к нелицензионным (контрафактным) версиям продукта прилагается такой код, взятый с того экземпляра, который служил оригиналом. Часто можно ввести и какой-либо другой взятый наугад номер. Не с первой, так со второй-третьей попытки удается найти приемлемый.

Метод преодоления данного вида защиты – попробовать подобрать пароль, используя методы криптоанализа. Однако самое простое все же – узнать пароль у законного пользователя программы.

2. Ограничитель числа инсталляций.

Если дистрибутив программы поставляется на дискете (возможно, не весь дистрибутив, а лишь его часть), то возможно установить в программе-инсталляторе счетчик инсталляций. Установить программу иначе, чем при помощи инсталлятора нельзя, а он при каждой инсталляции изменяет свой счетчик и при исчерпании заданного числа инсталляций перестает работать.

3. Аппаратный ключ защиты.

Представляет собой электронный ключ (микросхему), подключаемый к параллельному или последовательному порту, а иногда – к специальному разъему компьютера. Программа будет работать только в том случае, если получит обусловленный отклик от установленного ключа. Ключ продается вместе с программой и гарантирует, что будет использоваться лишь одна ее копия.

Достаточно надежный способ защиты, т. к. изготовление копии ключа защиты или программного его эмулятора дорого.

4. Работа программы только с компакт-диска.

Когда программный продукт полностью или частично находится на компакт-диске, для исключения его распространения разработчик может потребовать, чтобы диск обязательно находился в дисководе во время работы программы.

В последнее время актуальность подобного метода ЗИ снизилась, ибо «пираты» да и простые пользователи без проблем изготавливают полную копию лицензионного компакт-диска. Все чаще встречаются устройства записи на CD. Понятно, что копирование компакт-диска происходит при помощи специального ПО, сохраняющего всю служебную информацию оригинала.

5. Ограничение срока действия программы.

Используется, как правило, в демоверсиях программ, но встречается и в лицензионных копиях, когда срок лицензии ограничен. С некоторой натяжкой данный метод можно отнести к методам защиты от копирования.

Суть метода понятна из названия. Реализуется это ограничение обычно через проверку текущей даты по таймеру компьютера. Иногда правильность показаний таймера может контролироваться другими способами.

Бывает, что ограничивается не календарный срок действия, а количество запусков программы. Тогда где-то в программе есть соответствующий счетчик.

Преодолевается метод иногда просто – переводом часов назад. Если нет – используются методы хакинга.

6. Недопущение повторной инсталляции.

Чтобы демоверсии не использовались неограниченное число раз, их разработчики вставляют проверку – не была ли данная демоверсия установлена на этом компьютере ранее. Практически все современные программы не могут переноситься с одного компьютера на другой в виде «развертки», а требуют инсталляции, т. е., установки на компьютер с дистрибутива. Процесс инсталляции кроме копирования файлов программы на диск также включает настройку параметров под данный компьютер и регистрацию программы и ее параметров в реестре операционной системы. Без этого сложная программа работать не может. Или не хочет.

При удалении (деинсталляции) программы отдельные ее файлы или записи в реестре могут остаться. К сожалению, современное программное обеспечение имеет привычку хозяйничать на компьютере, не спрашивая разрешения у пользователя на проведение каких-либо действий и даже не информируя его о таких действиях. При инсталляции программы, как правило, новые файлы записываются не только в каталог, указанный пользователем, но и в другие каталоги, чаще всего в системный каталог, в корневой, в каталог общих компонент (shared). Модуль инсталляции (install shield) пытается отследить все такие добавления, но это далеко не всегда возможно. Кроме простых добавлений файлов могут быть их изме-

нения, замещение других файлов. Кроме того, указанные действия могут производиться не только при инсталляции, но и во время работы программы. Также при инсталляции и работе программы обычно производятся изменения в реестре (registry), которые трудно отследить.

Понятно, что такую «пустившую корни» программу проблематично полностью «вычистить» с компьютера. Хотя имеются утилиты, помогающие пользователю отследить все изменения, они не слишком совершенны. Тем более, когда разработчик специально ставит себе задачу «оставить след» на данном компьютере при инсталляции продукта, он может обойти все проверки. При повторной инсталляции программа «узнает» компьютер, «вспоминает», что она здесь уже была. И, соответственно, отказывается работать.

7. Ограничение функций программы.

Демоверсия программы предоставляется пользователю бесплатно с тем, чтобы он, испробовав ее возможности, приобрел затем полную версию. Отличается от полной либо сроком действия (эта ситуация рассматривалась выше), либо набором функций. Набор выполняемых функций демоверсии, ее возможностей, объем доступных данных, число карт, сценариев и т. п. искусственно ограничены по сравнению с полной версией.

Разработка отдельной демоверсии – это дополнительные затраты. Поэтому обычно она делается из стандартной версии путем добавления нескольких команд в код программы, которые и реализуют ограничения. В таком случае возможен и обратный процесс – сделать из демоверсии полнофункциональную версию продукта.

8. Привязка к компьютеру.

В редких случаях, особенно когда разработчик имеет дело с конкретным заказчиком программного продукта, он может воспользоваться методом привязки программы к компьютеру.

Трудно найти совершенно одинаковые компьютеры. Они различаются не только внешне, но и «изнутри», т. е., с точки зрения программ. Прикладная программа может получить различную информацию об аппаратной конфигурации компьютера, параметрах его устройств. Эту информацию можно использовать для привязки.

Например, программа считывает содержимое BIOS, вычисляет его контрольную сумму. Если полученное число не соответствует тому компьютеру, для которого программа предназначена, она не будет работать. Разумеется, для настройки программы под конкретную машину разработчик должен иметь доступ к компьютеру заказчика или хотя бы возможность получить интересующую его информацию.

Процессоры снабжены индивидуальным номером, который выдается по запросу программы. Это облегчает привязку программ (а также создает дополнительные возможности для слежения за пользователями через сеть).

9. Организационные методы.

Многие хотели бы победить программное «пиратство». Но пока не удается. Однако ведущие производители программного обеспечения и их союзники не оставляют попыток воздействия с целью уменьшить число контрафактных копий. Кроме описанных выше программно-технических методов применяются и методы совершенно иного рода.

Во-первых, СМИ и другие средства пропаганды под влиянием крупных производителей ПО и других заинтересованных структур проводят кампанию по убеждению пользователей в аморальности программного «пиратства» и использования контрафактных продуктов.

Во-вторых, на органы государственной власти России оказывается влияние с целью побудить их усилить борьбу с нарушениями авторских прав. Результат такого влияния постепенно проявляется – все больше случаев привлечения «пиратов» к ответственности. В то же время, все понимают, что привлечь к какой-либо ответственности конечного пользователя ПО нереально. Таких попыток и не делается. В отношении конечных пользователей ставят на «сознательность», т. е., идеологическую обработку.

Третий метод борьбы с «пиратством» изобретен в России (полукриминальный). Он сразу же показал свою крайнюю действенность в определенных условиях. Одна из отечественных фирм, выпускающая игровые программы, несла огромные убытки от нелицензионного тиражирования ее продукции. И в то время, когда глава фирмы «Майкрософт» Билл Гейтс встречался с Премьер-министром России, прося его пресечь пиратское тиражирование его продукции, наши производители обратились в совершенно другие «инстанции»... К людям, занимающимся выпуском «пиратских» дисков, пришли «чисто конкретные пацаны» и в доступной форме попросили их больше не нарушать авторские права данной фирмы. Проблема была решена.

Еще один метод уменьшения потерь от «пиратства» состоит в такой организации работы, чтобы большинству конечных пользователей было выгоднее приобретать легальные копии. По этому пути пошла, например, фирма «Диалог-наука» – производитель антивирусных программ. Большая часть доходов у их поступает не от продажи ПО, а от оказания услуг, с ним связанных. А сами антивирусные программы каждый может получить бесплатно. К сожалению, такой метод применим далеко не всегда.

Вредоносные программы и антивирусное программное обеспечение

Вредоносная программа – любая программа, предназначенная для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного владельцем использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации и/или владельцу ЭВМ, и/или владельцу сети ЭВМ путем копирования, искажения, удаления или подмены информации.

Уголовный кодекс Российской Федерации (ст. 273) трактует понятие вредоносности чрезвычайно широко. Определение вредоносных программ выглядит следующим образом: «… программы для ЭВМ или внесение изменений в существующие программы, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети…».

Вредоносные программы могут иметь следующие названия:

– computer contaminant (computer – компьютер и contaminant – загрязнитель) – термин для обозначения вредоносного программного обеспечения, который используется в законодательстве США;

– badware (bad – плохое и (soft)ware – программное обеспечение) – плохое программное обеспечение;

– crimeware (crime – преступность) – класс вредоносных программ, специально созданный для автоматизации финансовых преступлений. Это не синоним термина malware (значение термина malware шире), но все программы, относящиеся к crimeware, являются вредоносными;

– malware (malicious (soft)ware – злонамеренное программное обеспечение – зловредная программа («зловред» на жаргоне антивирусных служб) – общепринятый термин для обозначения любого программного обеспечения, специально созданного для того, чтобы причинять ущерб отдельному компьютеру, серверу, или компьютерной сети, независимо от того, является ли оно вирусом, шпионской программой и т. д.

Классификация вредоносных программ

Единой классификации вредоносных программ не существует. У каждой компании-разработчика антивирусного программного обеспечения есть собственная корпоративная классификация и номенклатура вредоносных программ. Приведенная далее классификация основана на номенклатуре Лаборатории Касперского.

По вредоносной нагрузке:

– помехи в работе зараженного компьютера: начиная от открытия-закрытия поддона CD-ROM и заканчивая уничтожением данных и поломкой аппаратного обеспечения. Поломками известен, в частности, вирус Win32.CIH;

– блокировка антивирусных сайтов, антивирусного ПО и административных функций ОС с целью усложнить лечение;

– саботирование промышленных процессов, управляемых компьютером;

– инсталляция другого вредоносного ПО;

– загрузка из сети (downloader);

– распаковка другой вредоносной программы, уже содержащейся внутри файла (dropper);

– кража, мошенничество, вымогательство и шпионаж за пользователем. Для кражи может применяться сканирование жесткого диска, регистрация нажатий клавиш (Keylogger) и перенаправление пользователя на поддельные сайты, в точности повторяющие исходные ресурсы;

– похищение данных, представляющих ценность или тайну;

– кража аккаунтов различных служб (электронной почты, мессенджеров, игровых серверов…). Аккаунты применяются для рассылки спама. Также через электронную почту зачастую можно заполучить пароли от других аккаунтов, а виртуальное имущество в MMOG – продать;

– кража аккаунтов платежных систем;

– блокировка компьютера, шифрование файлов пользователя с целью шантажа и вымогательства денежных средств. В большинстве случаев после оплаты компьютер или не разблокируется, или вскоре блокируется второй раз;

– использование телефонного модема для совершения дорогостоящих звонков, что влечет за собой значительные суммы в телефонных счетах;

– платное ПО, имитирующее, например, антивирус, но ничего полезного не делающее (fraudware или scareware);

– прочая незаконная деятельность (получение несанкционированного (и/или дарового) доступа к ресурсам самого компьютера или третьим ресурсам, доступным через него, в том числе прямое управление компьютером. BackDoor («задняя дверь» или «черный ход» – тип троянов, дающий полный доступ к зараженному компьютеру; организация на компьютере общедоступных прокси-серверов; зараженный компьютер (в составе ботнета) может быть использован для проведения DDoS (Distributed Denial of Service) сетевых атак; сбор адресов электронной почты и распространение спама; накрутка электронных голосований, щелчков по рекламным баннерам; генерация монет платежной системы Bitcoin; использование эффекта 25-го кадра для зомбирования человека);

– файлы, не являющиеся истинно вредоносными, но чаще – нежелательные (шуточное ПО («злые шутки») (Bad-Joke, Hoax), делающее какие-либо беспокоящие пользователя вещи; Adware, Browser Hijackers – программное обеспечение, показывающее рекламу; Riskware – легальные программы (некоторые из них свободно продаются и широко используются в легальных целях), которые тем не менее в руках злоумышленника способны причинить вред пользователю и его данным); Spyware – программное обеспечение, посылающее через Интернет не санкционированную пользователем информацию; Pornware – утилиты, так или иначе связанные с показом пользователям информации порнографического характера; Flooder – хакерские утилиты используются для «забивания мусором» (бесполезными сообщениями) каналов Интернета – IRC-каналов, компьютерных пейджинговых сетей, электронной почты и т. д.; «Отравленные» документы, дестабилизирующие ПО, открывающее их (например, архив размером меньше мегабайта может содержать гигабайты данных и надолго «завесить» архиватор); программы удаленного администрирования (могут применять-

ся как для дистанционного управления компьютером, так и для неблаговидных целей); руткит (RootKit) нужен, чтобы скрывать другое вредоносное ПО от посторонних глаз; снифферы – программное обеспечение, которое позволяет просматривать содержимое сетевых пакетов, перехватывать трафик в сети и анализировать его; конструкторы (Constructor, VirTool) вирусов и троянских программ – это утилиты, предназначенные для изготовления новых компьютерных вирусов и «троянцев». Они позволяют генерировать исходные тексты вирусов (в т. ч. макро-вирусов), объектные модули, и/или непосредственно зараженные файлы; FileCryptor, PolyCryptor – хакерские утилиты, использующиеся для шифрования других вредоносных программ с целью скрытия их содержимого от антивирусной проверки; полиморфные генераторы (PolyEngine) Их главная функция – шифрование тела вируса и генерация соответствующего расшифровщика; иногда вредоносное ПО для собственного «жизнеобеспечения» устанавливает дополнительные утилиты: IRC-клиенты, программные маршрутизаторы, открытые библиотеки перехвата клавиатуры… Такое ПО вредоносным не является, но из-за того, что за ним часто стоит истинно вредоносная программа, детектируется антивирусами. Бывает даже, что вредоносным является только скрипт из одной строчки, а остальные программы вполне легитимны).

По методу размножения:

– эксплойт (exploit) – теоретически безобидный набор данных (например, графический файл или сетевой пакет), некорректно воспринимаемый программой, работающей с такими данными. Вред наносит не сам файл, а неадекватное поведение ПО с ошибкой. Также эксплойтом называют программу для генерации подобных «отравленных» данных;

– логическая бомба в программе срабатывает при определенном условии и неотделима от полезной программы-носителя;

– троянская программа («троян») не имеет собственного механизма размножения;

– компьютерный вирус размножается в пределах компьютера и через сменные диски. Размножение через сеть возможно, если пользователь сам выложит зараженный файл в сеть. Вирусы, в свою очередь, делятся по типу заражаемых файлов (файловые, загрузочные, макровирусы (в документах Microsoft Office), автозапускающиеся); по способу прикрепления к файлам (паразитирующие, «спутники» и перезаписывающие) и т. д.;

– сетевой червь способен самостоятельно размножаться по сети. Может быть: IRC-, почтовым, размножающимся с помощью эксплойтов и т. д.;

Вредоносное ПО может образовывать цепочки: например, с помощью эксплойта (1) на компьютере жертвы развертывается загрузчик (2), устанавливающий из Интернета червя (3).

Симптомы заражения:

– автоматическое открытие окон с незнакомым содержимым при запуске компьютера;

– блокировка доступа к официальным сайтам антивирусных компаний или же к сайтам, оказывающим услуги по «лечению» компьютеров от вредоносных программ;

– появление новых неизвестных процессов в окне «Процессы» (Windows);

– появление в ветках реестра, отвечающих за автозапуск, новых записей;

– запрет на изменение настроек компьютера в учетной записи администратора;

– невозможность запустить исполняемый файл (выдается сообщение об ошибке);

– появление всплывающих окон или системных сообщений с непривычным текстом, в том числе содержащих неизвестные веб-адреса и названия;

– перезапуск компьютера во время старта какой-либо программы;

– случайное и/или беспорядочное отключение компьютера;

– случайное аварийное завершение программ.

Однако следует учитывать, что, несмотря на отсутствие симптомов, компьютер может быть заражен вредоносными программами.

Методы защиты от вредоносных программ

Абсолютной защиты от вредоносных программ не существует: от «эксплойтов нулевого дня» наподобие Sasser или Conficker не застрахован никто. Но с помощью некоторых мер можно существенно снизить риск заражения вредоносными программами.

Наиболее эффективные меры для повышения безопасности:

– использовать современные операционные системы, не дающие изменять важные файлы без ведома пользователя;

– своевременно устанавливать обновления;

– если существует режим автоматического обновления, включить его;

– помимо антивирусных продуктов, использующих сигнатурные методы поиска вредоносных программ, использовать программное обеспечение, обеспечивающее проактивную защиту от угроз (необходимость использования проактивной защиты обуславливается тем, что сигнатурный антивирус не замечает новые угрозы, еще не внесенные в антивирусные базы). Однако его использование требует от пользователя большого опыта и знаний;

– постоянно работать на персональном компьютере исключительно под правами пользователя, а не администратора, что не позволит большинству вредоносных программ инсталлироваться на персональном компьютере. Но это не защитит от вредоносных программ, имеющих доступ к файлам пользователя, к которым ограниченная учетная запись имеет разрешение на запись и чтение;

– ограничить физический доступ к компьютеру посторонних лиц;

– использовать внешние носители информации только от проверенных источников;

– не открывать компьютерные файлы, полученные от ненадежных источников;

– использовать персональный межсетевой экран (аппаратный или программный), контролирующий выход в сеть Интернет с персонального компьютера на основании политик, которые устанавливает сам пользователь.

Антивирусное программное обеспечение

Антивирусная программа (антивирус) – любая программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики – предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Целевые платформы антивирусного программного обеспечения

На данный момент антивирусное программное обеспечение разрабатывается в основном для ОС семейства Windows, что вызвано большим количеством вредоносных программ именно под эту популярную платформу.

На сегодняшний день на рынке представлены самые различные программные продукты антивирусного плана. Производители разработали самый широкий спектр программного обеспечения, учитывающего всевозможные требования пользователей, а также требований нормативно-правовых актов. Помимо этого, в зависимости от комплектации программного обеспечения растет и цена. Но в то же время на рынке программных средств немало антивирусных продуктов, производитель которых распространяет их бесплатно. Таким образом, рядовые пользователи имеют возможность использовать не только платный продукт, но и бесплатные аналоги.

Помимо ОС для настольных компьютеров и ноутбуков, также существуют платформы и для мобильных устройств, такие как: Windows Mobile, Symbian, Apple iOS, BlackBerry, Android, Windows Phone 7 и др. Пользователи устройств на данных ОС также подвержены риску заражения вредоносным программным обеспечением, поэтому разработчики антивирусных программ выпускают продукты и для таких устройств.

Классификация антивирусных продуктов

Классифицировать антивирусные продукты можно сразу по нескольким признакам, таким как: используемые технологии антивирусной защиты, функционал продуктов, целевые платформы.

По используемым технологиям антивирусной защиты:

– классические антивирусные продукты (продукты, применяющие только сигнатурный метод детектирования);

– продукты проактивной антивирусной защиты (продукты, применяющие только проактивные технологии антивирусной защиты);

– комбинированные продукты (продукты, применяющие как классические, сигнатурные методы защиты, так и проактивные).

По функционалу продуктов:

– антивирусные продукты (продукты, обеспечивающие только антивирусную защиту);

– комбинированные продукты (продукты, обеспечивающие не только защиту от вредоносных программ, но и фильтрацию спама, шифрование и резервное копирование данных и другие функции).

По целевым платформам: для ОС семейства Windows, семейства *NIX (ОС BSD, Linux, Mac OS X и др.), мобильных платформ.

Антивирусные продукты для корпоративных пользователей можно также классифицировать по объектам защиты: рабочих станций; файловых и терминальных серверов; почтовых и Интернет-шлюзов; серверов виртуализации и др.

Работа антивируса

Обычно антивирус действует по схеме:

– поиск в базе данных антивирусного ПО сигнатур вирусов;

– если найден инфицированный код в памяти (оперативной и/или постоянной), запускается процесс карантина и процесс блокируется;

– зарегистрированная программа обычно удаляет вирус, незарегистрированная просит регистрации и оставляет систему уязвимой.

Базы антивирусов

Для использования антивирусов необходимы постоянные обновления так называемых баз антивирусов. Они представляют собой информацию о вирусах – как их найти и обезвредить. Поскольку вирусы пишут часто, то необходим постоянный мониторинг активности вирусов в сети. Для этого существуют специальные сети, которые собирают соответствующую информацию. После сбора этой информации производится анализ вредоносности вируса, анализируется его код, поведение, и после этого устанавливаются способы борьбы с ним. Чаще всего вирусы запускаются вместе с операционной системой. В таком случае можно просто удалить строки запуска вируса из реестра, и на этом в простом случае процесс может закончиться.

Более сложные вирусы используют возможность заражения файлов. Например, известны случаи, как некие даже антивирусные программы, будучи зараженными, сами становились причиной заражения других чистых программ и файлов. Поэтому более современные антивирусы имеют возможность защиты своих файлов от изменения и проверяют их на целостность по специальному алгоритму. Таким образом, вирусы усложнились, как и усложнились способы борьбы с ними. Сейчас можно увидеть вирусы, которые занимают уже не десятки килобайт, а сотни, а порой могут быть и размером в пару мегабайт. Обычно такие вирусы пишут в языках программирования более высокого уровня, поэтому их легче остановить.

Но по-прежнему существует угроза от вирусов, написанных на низкоуровневых машинных кодах наподобие ассемблера. Сложные вирусы заражают операционную систему,

после чего она становится уязвимой и нерабочей. К сожалению, по прогнозам специалистов, в ближайшем будущем работа антивирусных компаний сильно осложнится в связи с тем, что будут сильнее распространяться вирусы с защитой от копирования.

Вопросы и задания для самоконтроля

1. Дайте определения терминам: «Естественные угрозы», «Искусственные угрозы».
2. Поясните термин «Непреднамеренные искусственные угрозы», приведите примеры.
3. Поясните термин «Преднамеренные искусственные угрозы», приведите примеры.
4. Поясните криптографические методы защиты информации, приведите примеры.
5. Поясните криптографические средства защиты информации, приведите примеры.
6. Дайте определения терминам: «Криптография», «Криптоанализ», «Криптостойкость».
7. Дайте характеристику основным алгоритмам шифрования.
8. Каким образом осуществляется защита программ и баз данных от копирования?
9. Дайте определение терминам: «Вредоносная программа», «Антивирусное программное обеспечение».
10. Какие существуют методы защиты от вредоносных программ?

5. Защита информации в телекоммуникационных системах

Особенности защиты информации в телекоммуникационных системах

В настоящее время в геометрической прогрессии растет количество атак, производимых на телекоммуникационные системы, связано это в первую очередь, с широкомасштабной информатизацией общества: информационные технологии внедряются практически во все сферы общества, и лица, осуществляющие незаконную деятельность, эти пользуются. Одним из приоритетных факторов данных угроз является то, что их можно осуществить дистанционно, не имея физического доступа к телекоммуникационной системе, достаточно лишь системе иметь подключение к сети.

Основные угрозы, которые можно отметить, – это нарушение целостности информации, целенаправленное искажение содержимого информации, циркулирующей в информационной системе. Кража информации – деяние, направленное на получение доступа к информации, к которой не допущено атакующее лицо. Это может быть информация ограниченного доступа, разглашение которой может привести к неблагоприятным последствиям, начиная от ущербов коммерческой инфраструктуре до угрозы безопасности государства. Уничтожение информации – процесс, направленный на целенаправленную ликвидацию информационных ресурсов. Это может быть информация, необходимая для различных расчетов, отчетов, сведения, которые необходимо довести до широкой публики, и т. д.

Защита циркулирующей в телекоммуникационных системах информации требует осознания и выявления потенциальных угроз на всех этапах жизненного цикла (замысел, проектирование, создание, эксплуатация, модернизация, утилизация). Угрозы обычно делят на случайные и преднамеренные. Причинами случайных воздействий на элементы телекоммуникационных систем могут быть отказы и сбои аппаратуры, помехи в каналах связи, непреднамеренные ошибки обслуживающего персонала, схемные и системотехнические недочеты разработчиков, структурные, алгоритмические и программные ошибки, а также аварийные ситуации.

Круг преднамеренных угроз шире и опасней, т. к. обусловлен человеческой деятельностью. Большинство из них предусматривает несанкционированный доступ (НСД) посторонних лиц. Попытки реализации угроз такого вида именуются термином «информационные атаки» или просто называются атаками. Атаки на систему извне называются удаленными. Удаленные атаки бывают двух видов: на инфраструктуру сетей передачи данных и на теле-

коммуникационные службы. По характеру воздействия удаленные атаки могут быть пассивными (не оказывают непосредственного влияния на работу системы, но нарушают функционирование элементов безопасности), активными (наносят прямой ущерб) и условно-пассивными (подготавливают последующую атаку). Удаленные атаки также классифицируют по нескольким критериям: внутрисегментные и межсегментные; с обратной связью (с возможностью управления в реальном масштабе времени) и без обратной связи; разовые и долговременные; локальные и широкомасштабные (глобальные); с физическим доступом и без физического доступа (например, электромагнитные излучения или акустические волны).

В качестве защитного элемента в компьютерных сетях часто применяется межсетевой экран (Firewall или брандмауэр). Его задача – обеспечение безопасности при осуществлении электронного обмена информацией с другими взаимодействующими автоматизированными системами и внешними сетями, разграничение доступа между сегментами корпоративной сети, а также защита от проникновения и вмешательства в работу АС нарушителей из внешних систем.

Межсетевые экраны (МЭ), установленные в точках соединения с сетью Интернет, обеспечивают защиту внешнего периметра АС и защиту собственных Интернет-серверов, открытых для общего пользования, от несанкционированного доступа.

В общем случае межсетевой экран предназначен для того, чтобы защитить сетевые ресурсы от следующих видов атак:

– пассивное подслушивание / перехват пакетов – нападающий использует средства для прослушивания пакетов, чтобы получить критическую (конфиденциальную) информацию из потоков данных между двумя узлами сети или перехвата значений пароля или имени пользователя в приватной либо общедоступной сети;

– подмена IP-адресов – нападающий симулирует, что он работает с доверенного компьютера (маскируется под доверенного пользователя), используя IP-адрес из принятого диапазона адресов IP для внутренней сети;

– просмотр (сканирование) портов – это активный метод определения портов сетевого устройства, которые он слушает. После того, как нападающий обнаруживает «дырки» в МЭ, они могут концентрироваться на поиске вариантов атак, направленных на использование особенностей приложений, работающих по этим портам;

– атака «отказ в обслуживании» отличается из других типов атак тем, что вместо поиска доступа к ресурсам узлов сети нападающий пытается блокировать доступ законных пользователей к ресурсу или маршрутизатору;

– атака прикладного уровня может иметь много форм за счет использования слабостей (уязвимости) в программном обеспечении сервера, позволяющих получить доступ к критичным ресурсам путем присвоения прав пользователя, запустившего (выполняющего) данное приложение. Например, нападающий может использовать простейший протокол передачи почты для компрометации (поставить под угрозу) владельцев почтовых серверов, на которых работают устаревшие версии программ sendmail, путем использования известных им недокументированных команд в данных программах.

Внедрение «троянских коней» – ввод пользователя в заблуждение относительно назначения некоторой программы, содержащей вредоносную компоненту, и провоцирование на ее запуск. Более продвинутые варианты нападения прикладного уровня используют сложность новых технологий типа HTML, функциональных возможностей WEB-браузеров (навигаторов) и протокола передачи гипертекста (HTTP).

В межсетевых экранах применяются специальные, характерные только для данного вида средств, методы защиты:

– трансляция адресов для сокрытия структуры и адресации внутренней сети;

– фильтрация проходящего трафика;

– управление списками доступа на маршрутизаторах;

– дополнительная идентификация и аутентификация пользователей стандартных служб (на проходе);

– ревизия содержимого (вложений) информационных пакетов, выявление и нейтрализация компьютерных вирусов;

– виртуальные частные сети (для защиты потоков данных, передаваемых по открытым сетям – обеспечения конфиденциальности, применяются криптографические методы, рассмотренные выше);

– противодействие атакам на внутренние ресурсы.

К особенностям создания средств защиты сетей можно отнести разнообразие и высокую активность хакерских атак.

Аппаратно-программные средства защиты информации от несанкционированного доступа

Согласно требованиям нормативных документов, средства защиты информации от несанкционированного доступа (СЗИ НСД), отвечающие высокому уровню защиты, должны обеспечивать:

- дискреционный и мандатный принцип контроля доступа;
- очистку памяти;
- изоляцию модулей;
- маркировку документов;
- защиту ввода и вывода на отчуждаемый физический носитель информации;
- сопоставление пользователя с устройством;
- идентификацию и аутентификацию;
- гарантии проектирования;
- регистрацию;
- взаимодействие пользователя с комплексом средств защиты;
- надежное восстановление;
- целостность комплекса средств защиты;
- контроль модификации;
- контроль дистрибуции;
- гарантии архитектуры.

Комплексные СЗИ НСД должны сопровождаться пакетом следующих документов:

– руководство по СЗИ;

– руководство пользователя;

– тестовая документация;

– конструкторская (проектная) документация.

Таким образом, в соответствии с требованиями ФСТЭК России комплексные СЗИ НСД должны включать базовый набор подсистем. Конкретные возможности этих подсистем по реализации функций защиты информации определяют уровень защищенности средств вычислительной техники. Реальная эффективность СЗИ НСД определяется функциональными возможностями не только базовых, но и дополнительных подсистем, а также качеством их реализации.

Компьютерные системы и сети подвержены широкому спектру потенциальных угроз информации, что обусловливает необходимость предусмотреть большой перечень функций и подсистем защиты. Целесообразно в первую очередь обеспечить защиту наиболее информативных каналов утечки информации, каковыми являются следующие: возможность копирования данных с машинных носителей; каналы передачи данных; хищение ЭВМ или встроенных накопителей.

Проблема перекрытия этих каналов усложняется тем, что процедуры защиты данных не должны приводить к заметному снижению производительности вычислительных систем.

Эта задача может быть эффективно решена на основе технологии глобального шифрования информации.

Современная массовая система защиты должна быть эргономичной и обладать следующими свойствами, благоприятствующими широкому ее применению:

– комплексность – возможность установки разнообразных режимов защищенной обработки данных с учетом специфических требований различных пользователей и широкого перечня возможных действий предполагаемого нарушителя;

– совместимость – система должна быть совместимой со всеми программами, написанными для данной операционной системы, и должна обеспечивать защищенный режим работы компьютера в вычислительной сети;

– переносимость – возможность установки системы на различные типы компьютерных систем, включая портативные;

– удобство в работе – система должна быть проста в эксплуатации и не должна менять привычную технологию работы пользователей;

– работа в масштабе реального времени – процессы преобразования информации, включая шифрование, должны выполняться с большой скоростью;

– высокий уровень защиты информации;

– минимальная стоимость системы.

Под аппаратно-программными средствами обеспечения информационной безопасности обычно понимают программное обеспечение, а также различные устройства, блоки, блокировки, технические решения, обеспечивающие безопасность компьютерной информации и компьютерных систем.

Эти защитные средства условно подразделяют на три группы:

– программное обеспечение (отдельные программы или пакеты программ с необходимой документацией) – наиболее распространенное средство;

– собственно аппаратно-программные средства (специальные устройства и блоки с соответствующим программным обеспечением);

– аппаратные средства (электронные и электронно-механические устройства, блоки, блокировки, замки и т. п.).

На аппаратно-программные средства в соответствии с нормативными документами возлагается решение следующих основных задач по обеспечению внутренней и внешней безопасности автоматизированных (компьютерных) систем (АС):

– защита от вмешательства в процесс функционирования АС посторонних лиц (возможность использования АС и доступ к ее ресурсам могут иметь только зарегистрированные в установленном порядке пользователи);

– разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам АС (обеспечение возможности доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям АС для выполнения ими своих служебных обязанностей);

– регистрация действий пользователей при обращении к защищаемым ресурсам АС в системных журналах и периодический контроль действий пользователей системы путем анализа содержимого этих журналов сотрудниками, отвечающими за информационную безопасность;

– защита от несанкционированной модификации (обеспечение неизменности, целостности) используемых в АС программных средств, а также защита системы от внедрения несанкционированных программ, включая компьютерные вирусы и вредоносные программы-закладки;

– защита хранимой, обрабатываемой и передаваемой по каналам связи информации ограниченного распространения от несанкционированного разглашения, искажения, подмены или фальсификации;

– обеспечение аутентификации абонентов, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

– выявление источников угроз безопасности информации и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

– минимизация и локализация наносимого ущерба неправомерными действиями физических и юридических лиц.

Основными приемами (защитными механизмами), используемыми в технических средствах защиты компьютерных систем от несанкционированного доступа (НСД), являются следующие:

– идентификация и аутентификация пользователей системы;

– разграничение доступа пользователей к ресурсам системы и авторизация (присвоение полномочий) пользователей;

– регистрация и оперативное оповещение о событиях, происходящих в системе;

– криптографическое закрытие хранимых и передаваемых по каналам связи данных;

– контроль целостности и аутентичности данных;

– выявление и нейтрализация действий компьютерных вирусов;

– выявление уязвимости (слабых мест) системы;

– изоляция (защита периметра) компьютерных сетей (фильтрация трафика, скрытие внутренней структуры и адресации, противодействие атакам на ресурсы и т. д.);

– обнаружение атак (опасных действий нарушителей) и оперативное реагирование.

Перечисленные приемы (механизмы) защиты могут применяться в конкретных технических средствах и системах защиты в различных комбинациях и вариациях.

В целях обеспечения возможности разграничения доступа к ресурсам АС и возможности регистрации событий такого доступа каждый субъект (пользователь, процесс) и объект (ресурс) защищаемой автоматизированной системы должен быть однозначно идентифицируем. Для этого в системе должны храниться специальные признаки каждого субъекта и объекта, по которым их можно было бы однозначно опознать.

Аутентификация пользователей осуществляется обычно путем проверки знания ими паролей, владения ими какими-либо специальными устройствами с уникальными признаками или путем проверки уникальных физических характеристик и параметров (биометрических) самих пользователей. Средства идентификации и аутентификации должны быть устойчивыми к сетевым угрозам и обеспечивать концепцию единого входа в сеть.

Ввод пользователем своего идентификатора и пароля осуществляется чаще всего с клавиатуры. Однако многие современные СЗИ используют и другие типы идентификаторов – магнитные карточки, радиочастотные бесконтактные карточки, смарт-карты, электронные ключи и др. Использование биометрических средств позволяет осуществлять идентификацию и аутентификацию человека одновременно. Биометрические методы (например, сканирование отпечатков пальцев) характеризуются, с одной стороны, высоким уровнем достоверности опознавания пользователей, а с другой – возможностью ошибок распознавания первого и второго рода (пропуск или ложная тревога) и более высокой стоимостью реализующих их систем.

Программно-технические средства защиты информации можно классифицировать следующим образом:

– программы, обеспечивающие разграничение доступа к информации;

– программы идентификации и аутентификации терминалов и пользователей;

– программы проверки функционирования системы защиты информации и контроля целостности средства защиты от НСД;

– программы защиты различного вспомогательного назначения, в том числе антивирусные программы и программы защиты от закладок;

– программы защиты операционных систем персональных компьютеров (модульная программная интерпретация и т. п.);

– программы контроля целостности общесистемного и прикладного программного обеспечения;

– программы, сигнализирующие о нарушении использования ресурсов;

– программы уничтожения остаточной информации в запоминающих устройствах (оперативная память, видеопамять и т. п.) после завершения ее использования;

– программы контроля и восстановления файловой структуры данных;

– программы имитации работы системы или ее блокировки при обнаружении фактов НСД;

– программы определения фактов НСД и сигнализации (передачи сообщений) об их обнаружении;

– программно-технические средства защиты информации от несанкционированного копирования, в том числе средства защиты носителей данных и средства предотвращения копирования программного обеспечения, установленного на ПЭВМ;

– программно-технические средства криптографической и стенографической защиты информации (включая средства маскирования информации) при ее хранении на носителях данных и при передаче по каналам связи;

– программно-технические средства прерывания работы программы пользователя при нарушении им правил доступа, в том числе принудительное завершение работы программы и блокировка компьютера;

– программно-технические средства стирания данных (надежного удаления), в том числе стирание остаточной информации, возникающей в процессе обработки секретных данных в оперативной памяти, и стирание устаревшей информации с магнитных носителей;

– программно-технические средства выдачи сигнала тревоги при попытке несанкционированного доступа к информации, в том числе средства регистрации некорректных обращений пользователей к защищаемой информации и средства организации контроля за действиями пользователей персональных компьютеров;

– программно-технические средства обнаружения и локализации действия программных и программно-технических закладок.

Стеганографические средства защиты информации

Наряду с обычным шифрованием используется и такой способ сокрытия данных, как стеганография, т. е. внедрение конфиденциальной (секретной) информации в файл, не вызывающий подозрений. Таким образом, любой пользователь, севший за компьютер и, например, рассматривающий фотоальбом, не будет даже подозревать, что фотографии могут содержать какую-либо скрытую информацию (письма, инструкции, документы, персональные данные и т. п.).

Поскольку такой прием сокрытия может использоваться не только во благо, но и во зло (например, для связи террористов или наркодилеров), то сотрудники правоохранительных органов должны иметь достаточно знаний о стеганографии.

Вообще, слово стеганография в переводе с греческого буквально означает тайнопись (steganos – тайна, секрет; graphy – запись).

Стеганография представляет собой совокупность методов, основывающихся на различных принципах (отличных от криптографии), которые обеспечивают сокрытие самого факта существования секретной информации в той или иной среде, а также средств реализации этих методов (рис. 9). К ней можно отнести огромное множество секретных средств связи, таких как невидимые чернила, микрофотоснимки, условное расположение знаков, тайные (скрытые) каналы, средства связи с плавающими частотами и т. д. В настоящее время развиваются методы компьютерной стеганографии самостоятельного научного направления информационной безопасности, изучающей проблемы создания компонентов скрываемой информации в открытой информационной среде, которая может быть сформирована вычислительными системами и сетями.

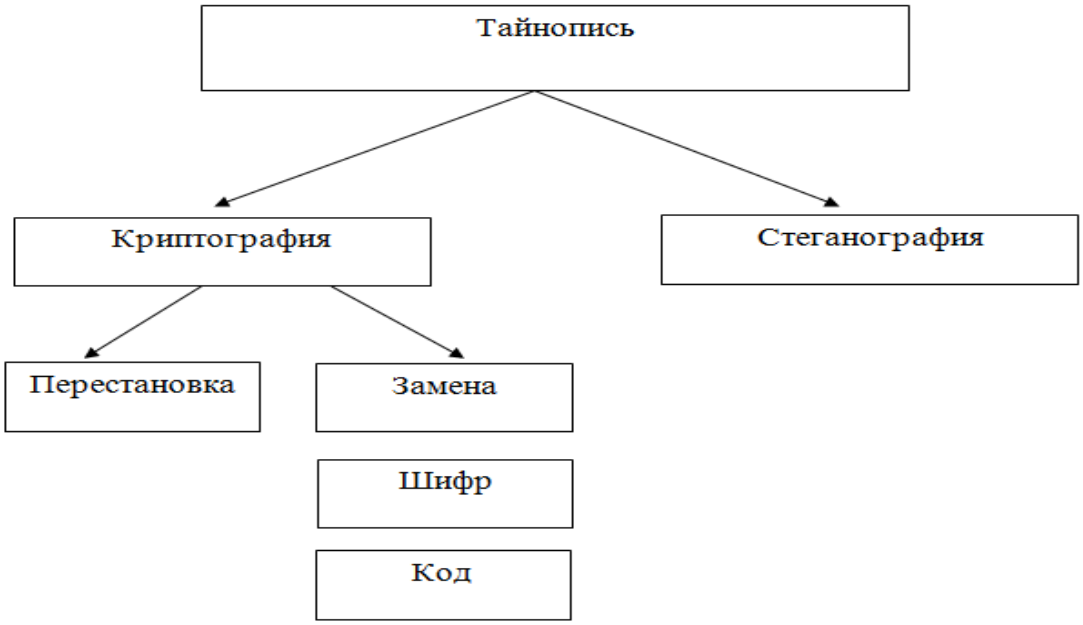

Рис. 9. Виды тайнописи

Особенностью стеганографического подхода является то, что он не предусматривает прямого оглашения факта существования защищаемой информации. Это обстоятельство позволяет в рамках традиционно существующих информационных потоков или информационной среды решать некоторые важные задачи защиты информации ряда прикладных областей. Основным определяющим моментом в стеганографии является стеганографическое преобразование. До недавнего времени стеганография как наука в основном изучала отдельные методы сокрытия информации и способы их технической реализации. Разнообразие принципов, заложенных в стеганографических методах, по существу тормозило развитие стеганографии как отдельной научной дисциплины и не позволило ей сформироваться в виде некоторой науки со своими теоретическими положениями и единой концептуальной системой, которая обеспечила бы формальное получение качественных и количественных оценок стеганометодов. В этом история развития стеганографии резко отличается от развития криптографии.

До конца XIX в. стеганография и криптография развивались в рамках единой науки о тайнописи. После формулирования знаменитого правила о том, что стойкость криптографического алгоритма должна определяется исключительно стойкостью ключа, криптография как отдельная наука отделилась от стеганографии. В основе многих подходов к решению задач стеганографии лежит общая с криптографией методическая база, заложенная Шенноном в теории тайнописи. Однако до сих пор теоретические основы стеганографии остаются мало разработанными.

Наблюдаемый в настоящее время интерес к стеганографии как совокупности методов сокрытия информации возник в большой мере благодаря интенсивному внедрению и широ-

кому распространению средств электронной вычислительной техники во все сферы деятельности человека. В рамках телекоммуникационных сетей возникли достаточно широкие возможности по оперативному обмену различной информацией в виде текстов, программ, звука, изображений между любыми участниками сетевых сеансов независимо от их территориального размещения. Это позволяет активно применять все преимущества, которые дают стеганографические методы защиты.

Стеганографические методы находят все большее применение в различных сферах деятельности (оборона, политика, коммерция, финансы и т. п.) в силу их легкой адаптируемости при решении задач защиты информации, а также отсутствия явно выраженных признаков средств защиты, использование которых может быть ограничено или запрещено (как, например, криптографических средств зашиты).

Сегодня стеганографические технологии активно используются для решения следующих основных задач:

- защиты информации с ограниченным доступом от НСД;
- защиты авторских прав на некоторые виды интеллектуальной собственности;
- преодоления систем мониторинга и управления сетевыми ресурсами;
- камуфляжа программного обеспечения;
- создания скрытых каналов утечки чувствительной информации от законного пользователя.

Использование стеганографических систем является наиболее эффективным при решении проблемы защиты информации с ограниченным доступом. Так, например, только одна секунда оцифрованного звука с частотой дискретизации 44 100 Гц и уровнем отсчета 8 бит в стереорежиме позволяет скрыть за счет замены младших разрядов на скрываемое сообщение около 10 Кбайт информации. При этом изменение значений отсчетов составляет менее 1 %. Такое изменение практически не обнаруживается при прослушивании файла большинством людей.

Кроме скрытой передачи сообщений, стеганография является одним из самых перспективных направлений для аутентификации и маркировки авторской продукции с целью защиты авторских прав на цифровые объекты от пиратского копирования. На компьютерные графические изображения, аудиопродукцию, литературные произведения (программы в том числе) наносится специальная метка, которая остается невидимой для глаз, но распознается; специальным программным обеспечением. Метка содержит скрытую информацию, подтверждающую авторство. Скрытая информация призвана обеспечить защиту интеллектуальной собственности. В качестве внедряемой информации можно использовать данные об авторе, дату и место создания произведения, номера документов, подтверждающих авторство, дату приоритета и т. п. Такие специальные сведения могут рассматриваться в качестве доказательств при рассмотрении споров об авторстве или для доказательств нелегального копирования.

Как и любые другие инструменты, стеганографические методы требуют к себе бережного отношения, т. к. они могут быть использованы как с целью защиты, так и в противоправных целях. Например, в конце 2001 г. под пристальным вниманием прессы оказались сведения о том, что один из опаснейших террористов мира Усама бен Ладен и члены его группировки широко используют Интернет для передач сообщений по организации террористических акций. Правительства некоторых стран предпринимают шаги с целью обуздания такой угрозы, пытаясь ввести ограничения на распространение программ, связанных с криптографическими и стеганографическими методами.

Однако стеганографические методы успешно применяются для противодействия системам мониторинга и управления сетевыми ресурсами промышленного шпионажа. С их помощь можно противостоять попыткам контроля над информационным пространством при

прохождении информации через серверы управления локальных и глобальных вычислительных сетей.

Нередко методы стеганографии используют для камуфлирования программного обеспечения. В тех случаях, когда использование программ незарегистрированными пользователями является нежелательным, оно может быть закамуфлировано под стандартные универсальные программные продукты (например, текстовые редакторы) или скрыто в файлах мультимедиа (например, в звуковом сопровождении компьютерных игр). Соответственно, если программное обеспечение нацелено на использование в серьезных автоматизированных системах, например, управления атомными электростанциями или управления пусками ракет, то необходима максимальная гарантия того факта, что в используемом программном обеспечении не будет различного рода закладок, которые по приказу извне могут взять управление на себя. Поэтому в данном случае необходимо использовать программное обеспечение, которому возможно доверить столь серьезные операции. Ввиду массового внедрения популярных операционных систем корпорация Microsoft внесла свои коррективы в данном вопросе, поскольку эта операционная система используется в достаточно широком секторе жизни общества и нет гарантии, что продукт не имеет различных закладочных механизмом деструктивного характера. На настоящий момент не представляется возможным на 100 процентов отказаться от продукции корпорации, оскольку необходимо определиться с видом используемого программного обеспечения, его возможностями, способностью воспроизводить программные продукты, используемые для повседневных задач. На сегодняшний день сделан большой шаг в этом направлении, имеется множество операционных систем российской разработки с достаточно широким функционалом. Более того, разработчики сертифицируют программное обеспечение не только для обработки сведений, составляющих конфиденциальную информацию, но и для работы с государственной тайной. Таким образом, положительная динамика в данной отрасли имеется и есть вероятность, что отечественные разработчики программного обеспечения займут прочную нишу на рынке с конкурентоспособной, функциональной, современной, оптимизированной операционной системой самого широкого функционала.

В современной стеганографии в целом можно выделить в два направления: технологическую стеганографию и информационную стеганографию (рис. 10).

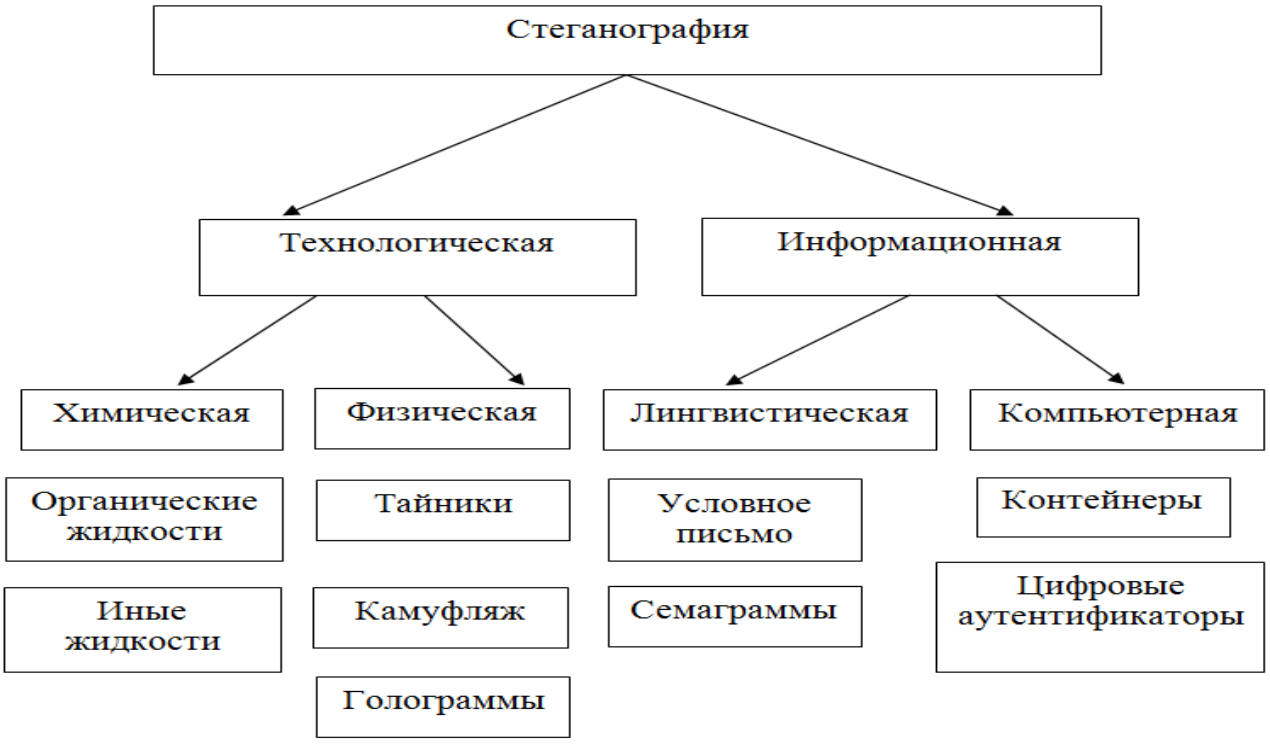

Рис. 10. Классификация видов стеганографии

К методам технологической стеганографии относятся методы, которые основаны на использовании химических или физических свойств различных материальных носителей информации. Химические методы стеганографии сводятся почти исключительно к применению невидимых чернил, к которым относятся органические жидкости (молоко, сок цитрусовых и т. п.) и симпатические химикалии.

К физическим методам можно отнести прокалывание иглой букв в текстах, микроточки (микрофототочки), различного вида тайники и методы камуфляжа. В настоящее время физические методы представляют интерес в области исследования различный носителей информации с целью записи на них данных, которые бы не выявлялись обычными методами считывания. Особый интерес имеется к стандартным носителям информации средств вычислительной, аудио- и видеотехники. Помимо этого, появился целый ряд новых технологий, которые, базируясь на традиционной стеганографии, используют последние достижения микроэлектроники (голограммы, кинеграммы).

К информационной стеганографии можно отнести методы лингвистической и компьютерной стеганографии. Лингвистические методы стеганографии подразделяются на две основные категории: условное письмо и семаграммы. Существуют три вида условного письма: жаргонный код, пустышечный шифр и геометрическая система. В жаргонном коде внешне безобидное слово имеет совершенно другое реальное значение, а текст составляется так, чтобы выглядеть как можно более невинно и правдоподобно. При применении пустышечного шифра в тексте имеют значение лишь некоторые определенные буквы или слова. Пустышечные шифры обычно выглядят еще более искусственно, чем жаргонный код. Третьим видом условного письма является геометрическая форма. При ее применении имеющие значение слова располагаются на странице в определенных местах или в точках пересечения геометрической фигуры заданного размера. Вторую категорию лингвистических методов составляют семаграммы – тайные сообщения, в которых шифрообозначениями являются любые символы, кроме букв и цифр. Эти сообщения могут быть переданы, например, в рисунке, содержащем точки и тире для чтения по коду Морзе.

Стеганографические методы в их проекции на инструментарий и среду, которая реализуется на основе компьютерной техники и программного обеспечения в рамках отдельных вычислительных или управляющих систем, корпоративных или глобальных вычислительных сетей, составляют предмет изучения сравнительно нового научного направления информационной безопасности – компьютерной стеганографии.

В рамках компьютерной стеганографии рассматриваются вопросы, связанные с сокрытием информации, которая хранится на носителях или передается по сетям телекоммуникаций, с организацией скрытых каналов в компьютерных системах и сетях, а также с технологиями цифровых водяных знаков и отпечатка пальца.

Существуют определенные отличия между технологиями цифровых водяных знаков и отпечатка пальца с одной стороны и собственно стеганографическими технологиями сокрытия секретной информации для ее последующей передачи или хранения. Самое главное отличие – это то, что цифровые водные знаки и отпечатки имеют целью защиту самого цифрового объекта (программы, изображения, музыкального файла и т. п.), куда они внедряются, обеспечивают доказательство прав собственности на данный объект.

При использовании методов компьютерной стеганографии должны учитываться следующие условия:

– противник может иметь полное представление о стеганографической системе и деталях ее реализации. Единственная информация, которая должна оставаться ему неизвестной, – это ключ, с помощью которого можно установить факт присутствия скрытого сообщения и его содержание;

– если противнику каким-то образом удалось узнать о факте существования скрытого сообщения, то это не должно позволить ему извлечь подобные сообщения из других стеганограмм до тех пор, пока ключ хранится в тайне;

– потенциальный противник должен быть лишен каких-либо технических и иных преимуществ в распознавании или раскрытии содержания тайных сообщений.

Основная идея стеганографического сокрытия состоит в том, что добавление «секретного» сообщения в файл-контейнер должно вызывать лишь незначительные изменения последнего (не улавливаются органами чувств человека).

Рис. 11. Схема стеганографического преобразования при тайной передаче сообщения по компьютерной сети

Для стеганографического преобразования необходимы:

– исходный скрываемый файл (текст);

– программа (бесплатный или условно бесплатный программный продукт);

– файл-контейнер (приемник) данных достаточно большого размера (графический, аудио- или видеофайл).

К средствам стеганографического сокрытия данных можно отнести: OutGuess, JSTEG, JPHS, Gifshuffle, Hide-and-Seek, Steganos, Steghide, DC-Stegano, Invisible Secrets, Hide4PGP, StegoDOS, FFEncode, Contraband, Isteg, Winstorm, StegoWav, Steaghan, MP3Stego, S-Tools, WNS, Covert_TCP, UnderMP3 Cover, Securengine.

Пользование большинством из программ достаточно просто и сводится к нажатию нескольких кнопок в окнах диалога. На определенном этапе вводится пароль (ключ).

Вопросы и задания для самоконтроля

1. Дайте определение термину «Межсетевой экран» и поясните его назначение.
2. Что понимают под аппаратно-программными средствами обеспечения информационной безопасности?
3. Какие задачи по обеспечению внутренней и внешней безопасности автоматизированных (компьютерных) систем возлагаются на аппаратно-программные средства?
4. Поясните основные приемы, используемые в технических средствах защиты компьютерных систем от несанкционированного доступа.
5. Каким образом можно классифицировать программно-технические средства защиты информации?
6. Дайте определение термину «Стеганография».
7. Для решения какого рода (типа) задач используются стеганографические технологии?
8. Дайте определение термину «Компьютерная стеганография».
9. Поясните процедуру стеганографического преобразования информации.
10. Приведите примеры программного обеспечения, которое можно отнести к средствам стеганографического сокрытия информации.

Заключение

В учебном пособии «Основы информационной безопасности в органах внутренних дел» изложен теоретический материал, охватывающий темы рабочей программы учебной дисциплины «Основы информационной безопасности в органах внутренних дел» для обучающихся по специальностям 40.05.01 Правовое обеспечение национальной безопасности, 40.05.02 Правоохранительная деятельность, 38.05.01 Экономическая безопасность, по которым предусмотрены аудиторные занятия, а именно:

– тема 1 «Основные понятия информационной безопасности органов внутренних дел»;

– тема 2 «Обеспечение информационной безопасности в органах внутренних дел»;

– тема 3 «Защита информации от утечки на объектах информатизации органов внутренних дел»;

– тема 4 «Защита информационных процессов в компьютерных системах»;

– тема 5 «Защита информации в телекоммуникационных системах».

Работа с учебным пособием также предполагает самостоятельное изучение обучающимися учебного материала (в рамках самостоятельной работы обучающихся) для подготовки:

– к учебным занятиям;

– к промежуточной аттестации.

Список использованных источников

1. Об электронной подписи: федеральный закон от 06.04.2011 № 63-ФЗ [Электронный ресурс]. – URL: http://www.garant.ru/

2. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ [Электронный ресурс]. – URL: http://www.garant.ru/

3. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ [Электронный ресурс]. – URL: http://www.garant.ru/

4. О связи: Федеральный закон от 07.07.2003 № 126-ФЗ [Электронный ресурс]. – URL: http://www.garant.ru/

5. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ [Электронный ресурс]. – URL: http://www.garant.ru/

6. О государственной тайне: Закон Российской Федерации от 21.07.1993 № 5485-1 [Электронный ресурс]. – URL: http://www.garant.ru/

7. О Стратегии национальной безопасности Российской Федерации: указ Президента Российской Федерации от 31.12.2015 № 683 [Электронный ресурс]. – URL: http://www.garant.ru/

8. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента Российской Федерации от 05.12.2016 № 646 [Электронный ресурс]. – URL: http://www.garant.ru/

9. Постановление Правительства Российской Федерации от 15.04.1995 № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» [Электронный ресурс]. – URL: http://www.garant.ru/

10. Защита информации. Основные термины и определения. ГОСТ Р 50922-2006 [Электронный ресурс]. – URL: http://www.garant.ru/

11. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием

скрытых каналов. Часть 1. Общие положения ГОСТ Р 53113.1-2008 [Электронный ресурс]. – URL: http://www.garant.ru/

12. Об утверждении Положения о системе сертификации средств защиты информации: приказ ФСТЭК России от 03.04.2018 № 55 [Электронный ресурс]. – URL: http://www.garant.ru/

13. *Костюченко К. Л.* Основы информационной безопасности в органах внутренних дел: учеб. пособие / К. Л. Костюченко, С. В. Мухачев. – Екатеринбург: Уральский юридический институт МВД России, 2015. – 156 с.

14. *Скрипник Д. А.* Общие вопросы технической защиты информации [Электронный ресурс]: учеб. пособие / Д. А. Скрипник. – 3-е изд. – Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. – 424 с. – URL: http://www.iprbookshop.ru/89451.html/

15. *Фаронов А. Е.* Основы информационной безопасности при работе на компьютере [Электронный ресурс]: учеб. пособие / А. Е. Фаронов. – 3-е изд. – Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. – 154 с. – URL: http://www.iprbookshop.ru/89453.html/

Перечень использованных ресурсов
информационно-телекоммуникационной сети Интернет

1. URL: http://www.iprbookshop.ru/ – Электронно-библиотечная система IPRbooks.

2. URL: http://www.garant.ru/ – Информационно-правовое обеспечение «Гарант».

3. URL: http://www.consultant.ru/ – Справочная правовая система «КонсультантПлюс».

4. URL: http://www.pravo.gov.ru/ – Официальный интернет-портал правовой информации. Государственная система правовой информации.

5. URL: http://www.fstec.ru/ – Официальный сайт Федеральной службы по техническому и экспортному контролю.

Содержание

ГИЗАТУЛЛИН Марат Галимянович
ФАЙСХАНОВ Ирек Фоатович

Основы информационной безопасности в органах внутренних дел

Учебное пособие

Редактура *Г. Р. Кудояровой*
Компьютерная верстка *И. Б. Бебих*

Подписано в печать 08.07.2020. Формат 60х84 1/16
Печать трафаретная. Бумага офисная
Усл. печ. л. 3,0. Уч.-изд. л. 3,2
Тираж 135 экз. Заказ № 41

Типография научно-исследовательского
и редакционно-издательского отдела
Уральского юридического института МВД России

620057, Екатеринбург, ул. Корепина, 66