Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет телекоммуникаций

Кафедра защиты информации

Т. А. Пулко

ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

Рекомендовано УМО по образованию в области информатики и радиоэлектроники в качестве учебно-методического пособия для практических работ для специальности 1-98 01 02 «Защита информации в телекоммуникациях»

Минск БГУИР 2016

УДК 004.056(076)
ББК 32.973.202я73
П88

Р е ц е н з е н т ы:

кафедра телекоммуникационных систем учреждения образования «Белорусская государственная академия связи» (протокол №6 от 05.01.2015);

начальник научно-исследовательского отдела (защиты информации) государственного учреждения «Научно-исследовательский институт Вооруженных Сил Республики Беларусь», кандидат технических наук, доцент Л. Л. Утин

Пулко, Т. А.

П88 Введение в информационную безопасность : учеб.-метод. пособие / Т. А. Пулко. – Минск : БГУИР, 2016. – 156 с. : ил.

ISBN 978-985-543-194-8.

Рассмотрены приоритетные направления обеспечения безопасности Республики Беларусь в информационной сфере, их политическая и социальная значимость. Приводится описание основных угроз информационной безопасности и методы физического, технического и программного обеспечения информационной безопасности. Раскрыты вопросы обеспечения безопасности в компьютерных и беспроводных сетях.

УДК 004.056(076)
ББК 32.973.202я73

ISBN 978-985-543-194-8

СОДЕРЖАНИЕ

ПРАКТИЧЕСКАЯ РАБОТА №1
МЕЖДУНАРОДНЫЕ СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель работы: изучить международные стандарты, определяющие требования к системам управления информационной безопасностью, управление рисками, метрики и измерения, а также руководство по внедрению.

1.1. Теоретическая часть

В соответствии с международными и национальными стандартами обеспечение информационной безопасности в любой компании предполагает следующее:

- определение целей обеспечения информационной безопасности компьютерных систем;
- создание эффективной системы управления информационной безопасностью;
- расчет совокупности детализированных качественных и количественных показателей для оценки соответствия информационной безопасности поставленным целям;
- применение инструментария обеспечения информационной безопасности и оценки ее текущего состояния;
- использование методик управления безопасностью, позволяющих объективно оценить защищенность информационных активов и управлять информационной безопасностью компании.

Рассмотрим наиболее известные международные стандарты в области защиты информации [22].

Стандарты ISO/IEC 17799:2002 (BS 7799:2000)

Международный стандарт ISO/IEC 17799:2000 (BS 7799-1:2000) «Управление информационной безопасностью – Информационные технологии» является одним из наиболее известных стандартов в области защиты информации. Данный стандарт был разработан на основе первой части британского стандарта BS 7799–1:1995 «Практические рекомендации по управлению информационной безопасностью» и относится к новому поколению стандартов информационной безопасности компьютерных информационных систем (КИС).

Текущая версия стандарта ISO/IEC 17799:2000 (BS 7799–1:2000) рассматривает следующие актуальные вопросы обеспечения информационной безопасности организаций и предприятий:

- необходимость обеспечения информационной безопасности;
- основные понятия и определения информационной безопасности;
- политика информационной безопасности компании;
- организация информационной безопасности на предприятии;

• классификация и управление корпоративными информационными ресурсами;

• кадровый менеджмент и информационная безопасность;

• физическая безопасность;

• администрирование безопасности;

• управление доступом;

• управление бизнес-процессами компании с точки зрения информационной безопасности;

• внутренний аудит информационной безопасности компании.

Вторая часть стандарта BS 7799–2:2000 «Спецификации систем управления информационной безопасностью» определяет возможные функциональные спецификации корпоративных систем управления информационной безопасностью с точки зрения их проверки на соответствие требованиям первой части. В соответствии с положениями второй части данного стандарта также регламентируется процедура аудита КИС.

Дополнительные рекомендации по управлению информационной безопасностью содержат руководства Британского института стандартов – British Standards Institution (BSI), изданные в 1995–2003 гг. в виде следующих серий:

• «Введение в проблему управления информационной безопасностью»;

• «Возможности сертификации на требования стандарта BS 7799»;

• «Руководство BS 7799 по оценке и управлению рисками»;

• «Руководство для проведения аудита на требования стандарта»;

• «Практические рекомендации по управлению безопасностью информационных технологий».

В 2002 г. международный стандарт ISO 17799 (BS 7799) был пересмотрен и существенно дополнен. В новом варианте большое внимание уделено вопросам повышения культуры защиты информации в различных международных компаниях. По мнению специалистов, обновление международного стандарта ISO 17799 (BS 7799) позволит не только повысить культуру защиты информационных активов компании, но и скоординировать действия различных ведущих государственных и коммерческих структур в области защиты информации.

Германский стандарт BSI

В отличие от ISO 17799 германское «Руководство по защите информационных технологий для базового уровня защищенности» посвящено детальному рассмотрению частных вопросов управления информационной безопасностью компании.

В германском стандарте BSI представлены:

• общая методика управления информационной безопасностью (организация менеджмента в области информационной безопасности, методология использования руководства);

• описания компонентов современных информационных технологий (ИТ);

• описания основных компонентов организации режима информационной безопасности (организационный и технический уровни защиты данных, планирование действий в чрезвычайных ситуациях, поддержка непрерывности бизнеса);

• характеристики объектов информатизации (здания, помещения, кабельные сети, контролируемые зоны);

• характеристики основных информационных активов компании (в том числе аппаратное и программное обеспечение, например, рабочие станции и серверы под управлением операционной системы (ОС) семейства DOS, Windows и UNIX);

• характеристики компьютерных сетей на основе различных сетевых технологий, например, сети NovellNetWare, сети UNIX и Windows;

• характеристика активного и пассивного телекоммуникационного оборудования ведущих поставщиков, например Cisco Systems;

• подробные каталоги угроз безопасности и мер контроля (более 600 наименований в каждом каталоге).

Вопросы защиты приведенных информационных активов компании рассматриваются по определенному сценарию: общее описание информационного актива компании – возможные угрозы и уязвимости безопасности – возможные меры, средства контроля и защиты.

Международный стандарт ISO 15408 «Общие критерии безопасности информационных технологий»

Одним из главных результатов стандартизации в сфере систематизации требований и характеристик защищенных информационных комплексов стала система международных и национальных стандартов безопасности информации, которая насчитывает более сотни различных документов. Важное место в этой системе стандартов занимает стандарт ISO 15408, известный как «Common Criteria».

В 1990 г. Международная организация по стандартизации (ISO) приступила к разработке международного стандарта по критериям оценки безопасности ИТ для общего использования. В разработке участвовали: Национальный институт стандартов и технологии и Агентство национальной безопасности (США), Учреждение безопасности коммуникаций (Канада), Агентство информационной безопасности (Германия), Агентство национальной безопасности коммуникаций (Голландия), органы исполнения Программы безопасности и сертификации ИТ (Англия), Центр обеспечения безопасности систем (Франция), которые опирались на свой солидный задел.

За десятилетие разработки лучшими специалистами мира документ неоднократно редактировался. Первые две версии были опубликованы соответственно в январе и мае 1998 г. Версия 2.1 этого стандарта утверждена 8 июня 1999 г. Международной организацией по стандартизации (ISO) в качестве международного стандарта информационной безопасности ISO/IEC 15408 под названием «Общие критерии оценки безопасности информационных технологий», или «Common Criteria».

Общие критерии (ОК) обобщили содержание и опыт использования Оранжевой книги, развили европейские и канадские критерии и воплотили в реальные структуры концепцию типовых профилей защиты федеральных критериев США. В ОК проведена классификация широкого набора требований безопасности ИТ, определены структуры их группирования и принципы использования. Главные достоинства ОК – полнота требований безопасности и их систематизация, гибкость в применении и открытость для последующего развития.

Ведущие мировые производители оборудования ИТ сразу стали поставлять заказчикам средства, полностью отвечающие требованиям ОК.

Общие критерии обеспечивают нормативную поддержку процесса выбора ИТ-продукта, к которому предъявляются требования функционирования в условиях действия определенных угроз, служат руководящим материалом для разработчиков таких систем, а также регламентируют технологию их создания и процедуру оценки обеспечиваемого уровня безопасности.

Общие критерии рассматривают информационную безопасность как совокупность конфиденциальности и целостности информации, обрабатываемой ИТ-продуктом, а также доступности ресурсов ВС и ставят перед средствами защиты задачу противодействия угрозам, актуальным для среды эксплуатации этого продукта и реализации политики безопасности, принятой в этой среде эксплуатации. Поэтому в концепцию ОК входят все аспекты процесса проектирования, производства и эксплуатации ИТ-продуктов, предназначенных для работы в условиях действия определенных угроз безопасности.

Стандарт ISO 15408 поднял стандартизацию ИТ на межгосударственный уровень. Возникла реальная перспектива создания единого безопасного информационного пространства, в котором сертификация безопасности систем обработки информации будет осуществляться на глобальном уровне, что предоставит возможности для интеграции национальных ИС, что в свою очередь откроет новые сферы применения ИТ.

Стандарты информационной безопасности в Интернете

По оценке Комитета ООН по предупреждению преступности и борьбе с ней, компьютерная преступность вышла на уровень одной из международных проблем. Поэтому чрезвычайно важно добиваться эффективного решения проблем обеспечения безопасности коммерческой информации в глобальной сети Интернет и смежных интранет-сетях, которые по своей технической сущности не имеют принципиальных отличий и различаются в основном масштабами и открытостью.

Рассмотрим особенности стандартизации процесса обеспечения безопасности коммерческой информации в сетях с протоколом передачи данных IP/TCP и с акцентом на защиту телекоммуникаций. Обеспечение безопасности ИТ особенно актуально для открытых систем коммерческого применения, обрабатывающих информацию ограниченного доступа, не

содержащую государственную тайну. Под открытыми системами понимают совокупности всевозможного вычислительного и телекоммуникационного оборудования разного производства, совместное функционирование которого обеспечивается соответствием требованиям международных стандартов. Термин «открытые системы» подразумевает также, что если вычислительная система соответствует стандартам, то она будет открыта для взаимосвязи с любой другой системой, которая соответствует тем же стандартам. Это, в частности, относится и к механизмам криптографической защиты информации или к защите от несанкционированного доступа (НСД) к информации.

В Интернете уже давно существует ряд комитетов, в основном из организаций-добровольцев, которые осторожно проводят предлагаемые технологии через процесс стандартизации. Эти комитеты, составляющие основную часть Рабочей группы инженеров Интернета IETF (Internet Engineering Task Force), провели стандартизацию нескольких важных протоколов, ускоряя их внедрение в Интернет. Непосредственными результатами усилий IETF являются такие протоколы, как семейство TCP/IP для передачи данных, SMTP (Simple Mail Transport Protocol) и POP (Post Office Protocol) для электронной почты, а также SNMP (Simple Network Management Protocol) для управления сетью.

В Интернете популярны протоколы безопасной передачи данных, а именно SSL, SET, IPSec. Перечисленные протоколы появились в Интернете сравнительно недавно как необходимость защиты ценной информации и сразу стали стандартами де-факто.

Протокол SSL (Secure Socket Layer) – популярный сетевой протокол с шифрованием данных для безопасной передачи по сети. Он позволяет устанавливать защищенное соединение, производить контроль целостности данных и решать различные сопутствующие задачи. Протокол SSL обеспечивает защиту данных между сервисными протоколами (HTTP, FTP и др.) и транспортными протоколами (TCP/IP) с помощью современной криптографии.

Протокол SET (Security Electronics Transaction) – перспективный стандарт безопасных электронных транзакций в сети Интернет, предназначенный для организации электронной торговли через сеть Интернет. Протокол SET основан на использовании цифровых сертификатов по стандарту X.509.

Протокол выполнения защищенных транзакций SET является стандартом, разработанным компаниями MasterCard и Visa при значительном участии IBM, GlobeSet и других партнеров. Он позволяет покупателям приобретать товары через Интернет, используя защищенный механизм выполнения платежей. Протокол SET является открытым стандартным многосторонним протоколом для проведения безопасных платежей с использованием пластиковых карточек в Интернете, обеспечивает кросс-аутентификацию счета держателя карты, продавца и банка продавца для проверки готовности оплаты, а также целостность и секретность сообщения, шифрование ценных и уязвимых данных.

Как упоминалось ранее, базовыми задачами защиты информации являются обеспечение ее доступности, конфиденциальности, целостности и юридической значимости. Протокол SET, в отличии от других протоколов, позволяет решать указанные задачи защиты информации в целом. В частности, он обеспечивает выполнение следующих специальных требований защиты операций электронной коммерции:

• секретность данных об оплате и конфиденциальность информации о заказе, переданной наряду с данными об оплате;

• сохранение целостности данных о платежах, которая обеспечивается с помощью цифровой подписи;

• специальную криптографию с открытым ключом для проведения аутентификации;

• аутентификацию держателя по кредитной карте, которая обеспечивается применением цифровой подписи и сертификатов держателя карт;

• аутентификацию продавца и его возможность принимать платежи по пластиковым картам с применением цифровой подписи и сертификатов продавца;

• аутентификацию того, что банк продавца является действующей организацией, которая может принимать платежи по пластиковым картам через связь с процессинговой карточной системой; аутентификация банка продавца обеспечивается использованием цифровой подписи и сертификатов банка продавца;

• готовность оплаты транзакций в результате аутентификации сертификата с открытым ключом для всех сторон;

• безопасность передачи данных посредством преимущественного использования криптографии.

Основное преимущество SET по сравнению с другими существующими системами обеспечения информационной безопасности заключается в использовании цифровых сертификатов (стандарт X.509, версия 3), которые ассоциируют держателя карты, продавца и банк продавца с банковскими учреждениями платежных систем Visa и MasterCard. Кроме того, SET позволяет сохранить существующие отношения между банком, держателями карт и продавцами и интегрируется с существующими системами.

Протокол IPSec. Спецификация IPSec входит в стандарт IP v.6 и является дополнительной по отношению к текущей версии протоколов TCP/IP. Она разработана Рабочей группой IP Security IETF. В настоящее время IPSec включает 3 алгоритмо-независимые базовые спецификации, представляющие соответствующие RFC-стандарты. Протокол IPSec обеспечивает стандартный способ шифрования трафика на сетевом (третьем) уровне IP и защищает информацию посредством сквозного шифрования (т. е. независимо от работающего приложения), при этом шифруется каждый пакет данных, проходящий по каналу. Это позволяет организациям создавать в Интернете виртуальные частные сети.

Инфраструктура управления открытыми ключами PKI (Public Key Infrastructure) предназначена для защищенного управления криптографическими ключами электронного документооборота, основанного на применении криптографии с открытыми ключами. Эта инфраструктура подразумевает использование цифровых сертификатов, удовлетворяющих рекомендациям международного стандарта X.509 и развернутой сети центров сертификации, обеспечивающих выдачу и сопровождение цифровых сертификатов для всех участников электронного обмена документами.

1.2. Практическая часть

Задание 1

Открыть программный модуль «Введение в информационную безопасность. Практические работы», расположенный на диске /D лабораторного компьютера. Перейти по вкладке «Разделы» в раздел «Практическая работа №1». Пройти тестирование по материалу изученной темы в разделе «Тест».

Задание 2

Пользуясь инструкцией к выполнению задания в разделе «Практика» программного модуля, выполнить задание.

ПРАКТИЧЕСКАЯ РАБОТА №2
ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ЧАСТЬ 1

Цель работы: изучить законы Республики Беларусь по определению правовых и организационных основ отнесения сведений к государственным секретам и их защите, государственное регулирование и управление в области информации, информатизации и защиты информации.

2.1. Теоретические сведения

Приведены главы 1–11 Закона Республики Беларусь от 19 июля 2010 г. №170-З «О государственных секретах» [6].

Настоящий Закон определяет правовые и организационные основы отнесения сведений к государственным секретам, защиты государственных секретов, осуществления иной деятельности в сфере государственных секретов в целях обеспечения национальной безопасности Республики Беларусь.

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Основные термины, используемые в настоящем Законе, и их определения. В настоящем Законе используются следующие основные термины и их определения:

государственные секреты (сведения, составляющие государственные секреты) – сведения, отнесенные в установленном порядке к государственным секретам, защищаемые государством в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь;

гриф секретности – реквизит, проставляемый на носителе государственных секретов и (или) сопроводительной документации к нему, свидетельствующий о степени секретности содержащихся на этом носителе государственных секретов;

допуск к государственным секретам – право гражданина Республики Беларусь, иностранного гражданина, лица без гражданства (далее, если не указано иное, – гражданин) или государственного органа, иной организации на осуществление деятельности с использованием государственных секретов;

доступ к государственным секретам – ознакомление гражданина с государственными секретами или осуществление им иной деятельности с использованием государственных секретов;

носитель государственных секретов – материальный объект, на котором государственные секреты содержатся в виде символов, образов, сигналов и (или) технических решений и процессов, позволяющих их распознать и идентифицировать;

средства защиты государственных секретов – технические, программные, криптографические и другие средства, используемые для защиты

государственных секретов, а также средства контроля эффективности защиты государственных секретов;

степень секретности – показатель важности государственных секретов, определяющий меры и средства защиты государственных секретов.

Статья 2. Законодательство Республики Беларусь о государственных секретах. Законодательство Республики Беларусь о государственных секретах основывается на Конституции Республики Беларусь и состоит из настоящего Закона, других актов законодательства Республики Беларусь, в том числе международных договоров Республики Беларусь о защите государственных секретов.

ГЛАВА 2. ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ И УПРАВЛЕНИЕ В СФЕРЕ ГОСУДАРСТВЕННЫХ СЕКРЕТОВ

Статья 3. Государственное регулирование и управление в сфере государственных секретов. Государственное регулирование и управление в сфере государственных секретов осуществляются Президентом Республики Беларусь, Советом Министров Республики Беларусь, а также Межведомственной комиссией по защите государственных секретов при Совете Безопасности Республики Беларусь, уполномоченным государственным органом по защите государственных секретов, органами государственной безопасности, Оперативно-аналитическим центром при Президенте Республики Беларусь.

Статья 4. Полномочия Президента Республики Беларусь. Президент Республики Беларусь в сфере государственных секретов:

определяет государственную политику;

утверждает государственные программы;

утверждает Положение о Межведомственной комиссии по защите государственных секретов при Совете Безопасности Республики Беларусь и ее состав;

создает, реорганизует и упраздняет уполномоченный государственный орган по защите государственных секретов;

утверждает перечень государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам, перечень сведений, подлежащих отнесению к государственным секретам;

ведет переговоры и подписывает межгосударственные договоры Республики Беларусь о защите государственных секретов;

принимает решения о передаче государственных секретов иностранным государствам, международным организациям, межгосударственным образованиям, если иное не установлено настоящим Законом;

устанавливает порядок предоставления допуска к государственным секретам иностранным гражданам и лицам без гражданства, а также гражданам Республики Беларусь, постоянно проживающим за пределами Республики Беларусь;

осуществляет иные полномочия в соответствии с настоящим Законом и другими законодательными актами Республики Беларусь.

Статья 5. Полномочия Совета Министров Республики Беларусь. Совет Министров Республики Беларусь в сфере государственных секретов:

организует разработку проектов государственных программ, перечня государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам, перечня сведений, подлежащих отнесению к государственным секретам, и представляет их на утверждение Президенту Республики Беларусь, принимает меры по выполнению государственных программ;

организует разработку проектов актов законодательства Республики Беларусь, в том числе международных договоров Республики Беларусь о защите государственных секретов, принимает в пределах своей компетенции акты законодательства Республики Беларусь;

заключает межправительственные договоры Республики Беларусь о защите государственных секретов, принимает меры по реализации международных договоров Республики Беларусь о защите государственных секретов;

утверждает положение об экспертных комиссиях в сфере государственных секретов, перечень особо режимных и режимных объектов, положение об особо режимных и режимных объектах, порядок создания и деятельности подразделений по защите государственных секретов;

принимает решения о создании межведомственных экспертных комиссий в сфере государственных секретов;

устанавливает порядок определения тяжести последствий, которые наступили или могут наступить, размера вреда, который причинен или может быть причинен в результате разглашения или утраты государственных секретов;

устанавливает порядок предоставления гражданам допуска к государственным секретам, если иное не установлено настоящим Законом;

устанавливает с учетом положений настоящего Закона порядок осуществления гражданами доступа к государственным секретам;

устанавливает с учетом положений настоящего Закона порядок отнесения сведений к государственным секретам, засекречивания, рассекречивания, а также защиты государственных секретов;

устанавливает с учетом положений настоящего Закона порядок передачи государственных секретов государственным органам и иным организациям;

устанавливает с учетом положений настоящего Закона порядок передачи государственных секретов иностранным государствам, международным организациям, межгосударственным образованиям;

устанавливает размеры надбавок к тарифным ставкам (окладам) гражданам на период доступа к государственным секретам в зависимости от степени секретности, а также компенсационных выплат гражданам на период действия временного ограничения их права на выезд из Республики Беларусь, если они осведомлены о государственной тайне, и надбавок к тарифным ставкам (окладам) работникам подразделений по защите государственных

секретов за стаж работы в указанных подразделениях, а также порядок их выплат;

определяет порядок материально-технического и финансового обеспечения деятельности в сфере государственных секретов;

осуществляет иные полномочия в соответствии с настоящим Законом и другими законодательными актами Республики Беларусь.

Статья 6. Полномочия Межведомственной комиссии по защите государственных секретов при Совете Безопасности Республики Беларусь. Межведомственная комиссия по защите государственных секретов при Совете Безопасности Республики Беларусь в сфере государственных секретов:

координирует деятельность государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам;

осуществляет подготовку предложений Президенту Республики Беларусь и Совету Безопасности Республики Беларусь о формировании государственной политики и совершенствовании защиты государственных секретов;

рассматривает проекты государственных программ, актов законодательства Республики Беларусь, в том числе международных договоров Республики Беларусь о защите государственных секретов;

осуществляет иные полномочия в соответствии с законодательными актами Республики Беларусь.

Статья 7. Полномочия уполномоченного государственного органа по защите государственных секретов. Уполномоченный государственный орган по защите государственных секретов в сфере государственных секретов:

координирует деятельность государственных органов и иных организаций по защите государственных секретов;

разрабатывает предложения о формировании государственной политики и совершенствовании защиты государственных секретов;

осуществляет государственный контроль;

разрабатывает проекты государственных программ, актов законодательства Республики Беларусь, в том числе международных договоров Республики Беларусь о защите государственных секретов, принимает в пределах своей компетенции акты законодательства Республики Беларусь;

проводит проверочные мероприятия в государственных органах и иных организациях в связи с предоставлением им допуска к государственным секретам;

устанавливает порядок выдачи разрешений на осуществление деятельности с использованием государственных секретов, выдает, приостанавливает, возобновляет и аннулирует разрешения на осуществление деятельности с использованием государственных секретов государственным органам и иным организациям, за исключением государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам;

согласовывает перечни сведений, подлежащих засекречиванию, номенклатуры должностей работников, подлежащих допуску к государственным секретам;

согласовывает предоставление гражданам допуска к государственным секретам, а также осуществление доступа к государственным секретам граждан, являющихся представителями иностранных государств, международных организаций, межгосударственных образований;

создает экспертные комиссии в сфере государственных секретов для рассмотрения материалов о возможности передачи государственных секретов иностранным государствам, международным организациям, межгосударственным образованиям, выносит заключения о возможности передачи государственных секретов иностранным государствам, международным организациям, межгосударственным образованиям;

осуществляет государственную регистрацию информационных систем, содержащих государственные секреты;

организует повышение квалификации, подготовку и переподготовку руководителей, ответственных за обеспечение защиты государственных секретов, и других работников государственных органов и иных организаций, осуществляющих деятельность с использованием государственных секретов;

оказывает методическую и практическую помощь государственным органам и иным организациям, осуществляющим деятельность с использованием государственных секретов, по вопросам защиты государственных секретов;

осуществляет иные полномочия в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь.

Статья 8. Полномочия органов государственной безопасности. Органы государственной безопасности в сфере государственных секретов:

организуют обеспечение государственных органов и иных организаций средствами шифрованной, других видов специальной связи, координируют их применение, осуществляют контроль за использованием указанных средств;

координируют применение государственными органами и иными организациями криптографических средств защиты государственных секретов, осуществляют контроль за их использованием;

осуществляют в пределах своих полномочий контроль за защитой государственных секретов, в том числе контроль при использовании криптографических средств защиты государственных секретов;

осуществляют подтверждение соответствия средств шифрованной, других видов специальной связи и криптографических средств защиты государственных секретов требованиям технических нормативных правовых актов Республики Беларусь в области технического нормирования и стандартизации и выдают сертификаты соответствия;

организуют применение технических мер защиты государственных секретов в своей деятельности, осуществляют контроль за их использованием;

разрабатывают проекты актов законодательства Республики Беларусь, в том числе технических нормативных правовых актов, принимают в пределах своей компетенции акты законодательства Республики Беларусь;

согласовывают создание, реорганизацию и ликвидацию государственными органами и иными организациями подразделений по защите государственных секретов, а также назначение на должности и освобождение от должностей руководителей этих подразделений;

проводят в пределах своей компетенции проверочные мероприятия в отношении граждан в связи с предоставлением им допуска к государственным секретам, осуществлением ими деятельности в сфере государственных секретов;

вносят предложения в государственные органы и иные организации, осуществляющие деятельность с использованием государственных секретов, о временном ограничении права граждан, осведомленных о государственной тайне, на выезд из Республики Беларусь;

вносят предписания в государственные органы и иные организации, осуществляющие деятельность с использованием государственных секретов, о прекращении допуска к государственным секретам граждан;

осуществляют иные полномочия в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь.

Статья 9. Полномочия Оперативно-аналитического центра при Президенте Республики Беларусь. Оперативно-аналитический центр при Президенте Республики Беларусь в сфере государственных секретов:

координирует применение технических мер защиты государственных секретов в государственных органах и иных организациях, осуществляющих деятельность с использованием государственных секретов, за исключением применения технических мер защиты государственных секретов в системах шифрованной, других видов специальной связи и при использовании криптографических средств защиты государственных секретов, осуществляет контроль за применением указанных мер в порядке, установленном этим центром;

разрабатывает проекты актов законодательства Республики Беларусь о применении технических мер защиты государственных секретов, за исключением применения технических мер защиты государственных секретов в системах шифрованной, других видов специальной связи и при использовании криптографических средств защиты государственных секретов, а также проекты технических нормативных правовых актов Республики Беларусь в области технического нормирования и стандартизации средств защиты государственных секретов, за исключением систем шифрованной, других видов специальной связи и криптографических средств защиты государственных секретов, принимает в пределах своей компетенции акты законодательства Республики Беларусь;

осуществляет подтверждение соответствия средств защиты государственных секретов требованиям технических нормативных правовых

актов Республики Беларусь в области технического нормирования и стандартизации, за исключением средств шифрованной, других видов специальной связи и криптографических средств защиты государственных секретов, и выдает сертификат соответствия;

осуществляет методическое руководство повышением квалификации, подготовкой и переподготовкой руководителей, ответственных за обеспечение защиты государственных секретов, и других работников государственных органов и иных организаций, осуществляющих деятельность с использованием государственных секретов, по применению технических мер защиты государственных секретов, определяет порядок их аттестации;

осуществляет иные полномочия в соответствии с актами законодательства Республики Беларусь.

ГЛАВА 3. ОСУЩЕСТВЛЕНИЕ ДЕЯТЕЛЬНОСТИ С ИСПОЛЬЗОВАНИЕМ ГОСУДАРСТВЕННЫХ СЕКРЕТОВ

Статья 10. Осуществление деятельности с использованием государственных секретов. Деятельность с использованием государственных секретов осуществляют государственные органы и иные организации, наделенные полномочием по отнесению сведений к государственным секретам, другие государственные органы, иные организации и граждане.

Условием осуществления деятельности с использованием государственных секретов является наличие у государственных органов, иных организаций и граждан допуска к государственным секретам, предоставленного в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь.

Статья 11. Полномочия государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам. Государственные органы и иные организации, наделенные полномочием по отнесению сведений к государственным секретам, в сфере государственных секретов:

относят в сфере своей деятельности сведения к государственным секретам, разрабатывают и утверждают перечни сведений, подлежащих засекречиванию;

организуют и осуществляют в сфере своей деятельности защиту государственных секретов;

вносят в Совет Министров Республики Беларусь предложения о формировании перечня сведений, подлежащих отнесению к государственным секретам, перечня особо режимных и режимных объектов, а также предложения о создании межведомственных экспертных комиссий в сфере государственных секретов;

передают государственные секреты другим государственным органам и иным организациям;

принимают решения о передаче служебной тайны иностранным государствам, международным организациям, межгосударственным

образованиям при наличии международного договора Республики Беларусь о защите государственных секретов;

осуществляют контроль за защитой государственных секретов в подчиненных организациях, а также в государственных органах и иных организациях, которым в связи с проведением работ с использованием государственных секретов передаются ими государственные секреты;

согласовывают создание, реорганизацию и ликвидацию подразделений по защите государственных секретов в подчиненных организациях, а также в других государственных органах и иных организациях, которым в связи с проведением работ с использованием государственных секретов передаются ими государственные секреты;

создают, реорганизуют и ликвидируют подразделения по защите государственных секретов, обеспечивают их функционирование;

определяют руководителей, ответственных за обеспечение защиты государственных секретов;

создают условия для осуществления деятельности с использованием государственных секретов;

разрабатывают и утверждают номенклатуры должностей работников, подлежащих допуску к государственным секретам;

принимают в пределах своей компетенции решения о создании экспертных комиссий в сфере государственных секретов;

обеспечивают повышение квалификации, подготовку и переподготовку руководителей, ответственных за обеспечение защиты государственных секретов, и других работников, осуществляющих деятельность с использованием государственных секретов;

осуществляют иные полномочия в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь.

Статья 12. Полномочия других государственных органов и иных организаций. Другие государственные органы и иные организации, осуществляющие деятельность с использованием государственных секретов, в сфере государственных секретов:

организуют и осуществляют защиту государственных секретов, находящихся в их пользовании;

осуществляют полномочия, предусмотренные абзацами седьмым – четырнадцатым статьи 11 настоящего Закона;

вносят в государственные органы и иные организации, наделенные полномочием по отнесению сведений к государственным секретам, предложения о формировании перечня сведений, подлежащих отнесению к государственным секретам, перечней сведений, подлежащих засекречиванию, перечня особо режимных и режимных объектов, а также предложения о создании экспертных комиссий в сфере государственных секретов;

осуществляют иные полномочия в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь.

Статья 13. Права и обязанности граждан. Граждане в сфере государственных секретов имеют право:

на осуществление деятельности с использованием государственных секретов с соблюдением требований, предусмотренных настоящим Законом и другими актами законодательства Республики Беларусь о государственных секретах;

на получение надбавок к тарифным ставкам (окладам) на период их доступа к государственным секретам в зависимости от степени секретности, а также компенсационных выплат на период действия временного ограничения их права на выезд из Республики Беларусь, если они осведомлены о государственной тайне, и надбавок к тарифным ставкам (окладам) за стаж работы в подразделениях по защите государственных секретов;

ознакомиться с законодательством Республики Беларусь о государственных секретах в необходимом объеме;

осуществлять иные права, предусмотренные настоящим Законом и другими актами законодательства Республики Беларусь.

Граждане обязаны выполнять требования, предусмотренные настоящим Законом и другими актами законодательства Республики Беларусь о государственных секретах.

ГЛАВА 4. СВЕДЕНИЯ, КОТОРЫЕ МОГУТ БЫТЬ ОТНЕСЕНЫ ЛИБО НЕ МОГУТ БЫТЬ ОТНЕСЕНЫ К ГОСУДАРСТВЕННЫМ СЕКРЕТАМ

Статья 14. Сведения, которые могут быть отнесены к государственным секретам. К государственным секретам могут быть отнесены:

сведения в области политики:

о стратегии и тактике внешней политики, а также внешнеэкономической деятельности;

о подготовке, заключении, содержании, выполнении, приостановлении или прекращении действия международных договоров Республики Беларусь;

об экспорте и импорте вооружения и военной техники;

о содержании или объемах экономического сотрудничества с иностранными государствами в военное время;

сведения в области экономики и финансов:

о содержании планов подготовки экономики к отражению возможной военной агрессии;

о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники;

о планах (заданиях) государственного оборонного заказа, об объемах выпуска и поставках вооружения и военной техники, военно-технического имущества;

об объемах финансирования из республиканского бюджета Вооруженных Сил Республики Беларусь, других войск и воинских формирований,

правоохранительных и иных государственных органов, обеспечивающих национальную безопасность Республики Беларусь;

о технологии изготовления системы защиты, применяемой при производстве денежных знаков, бланков ценных бумаг и других документов с определенной степенью защиты, обеспечиваемых государством;

сведения в области науки и техники:

о содержании государственных и других программ, концепций по направлениям, определяющим национальную безопасность Республики Беларусь;

о проведении научно-исследовательских, опытно-технологических и опытно-конструкторских работ в интересах национальной безопасности Республики Беларусь;

сведения в военной области:

о планах строительства Вооруженных Сил Республики Беларусь, содержании основных направлений (программ) развития вооружения и военной техники;

о тактико-технических характеристиках и возможностях боевого применения вооружения и военной техники;

о системе управления Вооруженными Силами Республики Беларусь;

о содержании стратегических или оперативных планов, планов территориальной обороны, документов боевого управления по подготовке и проведению операций, стратегическому развертыванию Вооруженных Сил Республики Беларусь, других войск и воинских формирований, их боевой, мобилизационной готовности и мобилизационных ресурсах;

о назначении, местонахождении, степени защищенности, системе охраны особо режимных и режимных объектов, пунктов управления государством в военное время или их проектировании, строительстве, эксплуатации, степени готовности;

сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности:

об организации, тактике, силах, средствах, объектах, методах, планах разведывательной, контрразведывательной и оперативно-розыскной деятельности, в том числе по обеспечению собственной безопасности в органах, осуществляющих такую деятельность;

о финансировании мероприятий, проводимых органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;

о гражданах, сотрудничающих (сотрудничавших) на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность, а также о штатных негласных сотрудниках и сотрудниках этих органов, в том числе внедренных в организованные группы, выполняющих (выполнявших) специальные задания;

сведения в информационной и иных областях национальной безопасности Республики Беларусь:

о содержании, организации или результатах основных видов деятельности Совета Безопасности Республики Беларусь, государственных органов, обеспечивающих национальную безопасность Республики Беларусь;

об организации, силах, средствах и методах обеспечения безопасности охраняемых граждан и защиты охраняемых объектов;

о финансировании мероприятий, проводимых в целях обеспечения безопасности охраняемых граждан и защиты охраняемых объектов;

о системе, методах и средствах защиты государственных секретов, состоянии защиты государственных секретов;

о шифрах, системах шифрованной, других видов специальной связи;

иные сведения в области политики, экономики, финансов, науки, техники, в военной области, области разведывательной, контрразведывательной, оперативно-розыскной деятельности, информационной и иных областях национальной безопасности Республики Беларусь, которые включаются в перечень сведений, подлежащих отнесению к государственным секретам.

Статья 15. Сведения, которые не могут быть отнесены к государственным секретам. К государственным секретам не могут быть отнесены сведения:

являющиеся общедоступной информацией, доступ к которой, распространение и (или) предоставление которой не могут быть ограничены в соответствии с законодательными актами Республики Беларусь;

находящиеся в собственности иностранных государств, международных организаций, межгосударственных образований и переданные Республике Беларусь.

ГЛАВА 5. КАТЕГОРИИ ГОСУДАРСТВЕННЫХ СЕКРЕТОВ. СТЕПЕНИ СЕКРЕТНОСТИ. ГРИФЫ СЕКРЕТНОСТИ

Статья 16. Категории государственных секретов. Государственные секреты подразделяются на две категории: государственную тайну (сведения, составляющие государственную тайну) и служебную тайну (сведения, составляющие служебную тайну).

Государственная тайна – сведения, в результате разглашения или утраты которых могут наступить тяжкие последствия для национальной безопасности Республики Беларусь.

Служебная тайна – сведения, в результате разглашения или утраты которых может быть причинен существенный вред национальной безопасности Республики Беларусь.

Служебная тайна может являться составной частью государственной тайны, не раскрывая ее в целом.

Статья 17. Степени секретности. Для государственных секретов в зависимости от тяжести последствий, которые наступили или могут наступить,

размера вреда, который причинен или может быть причинен в результате их разглашения или утраты, устанавливаются следующие степени секретности:

для государственной тайны – «Особой важности», «Совершенно секретно»;

для служебной тайны – «Секретно».

Статья 18. Грифы секретности. На носителях государственных секретов и (или) сопроводительной документации к ним в зависимости от степени секретности государственных секретов проставляются следующие грифы секретности:

на носителях государственной тайны и (или) сопроводительной документации к ним – «Особой важности», «Совершенно секретно»;

на носителях служебной тайны и (или) сопроводительной документации к ним – «Секретно».

ГЛАВА 6. ОТНЕСЕНИЕ СВЕДЕНИЙ К ГОСУДАРСТВЕННЫМ СЕКРЕТАМ. ЗАСЕКРЕЧИВАНИЕ. РАССЕКРЕЧИВАНИЕ

Статья 19. Отнесение сведений к государственным секретам. Отнесение сведений к государственным секретам осуществляется посредством определения сведений, которые подлежат защите в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь.

Отнесение сведений к государственным секретам осуществляется государственными органами и иными организациями, наделенными полномочием по отнесению сведений к государственным секретам, с учетом перечня сведений, подлежащих отнесению к государственным секретам.

Государственные органы и иные организации, наделенные полномочием по отнесению сведений к государственным секретам, в сфере своей деятельности разрабатывают и утверждают перечни сведений, подлежащих засекречиванию.

Сведения, полученные государственными органами и иными организациями, а также гражданами при осуществлении деятельности, не связанной с использованием государственных секретов, собственниками которых они являются, могут быть отнесены к государственным секретам после передачи их этими государственными органами и иными организациями, а также гражданами по договору государственному органу и иной организации, наделенным полномочием по отнесению сведений к государственным секретам. Договор о передаче таких сведений заключается в соответствии с Гражданским кодексом Республики Беларусь и должен содержать указание на условия передачи этих сведений.

До принятия решения об отнесении к государственным секретам сведений, указанных в части четвертой настоящей статьи, государственными органами и иными организациями, а также гражданами осуществляется их защита.

Статья 20. Определение и изменение степени секретности. Определение и изменение степени секретности осуществляются государственными органами и иными организациями, наделенными

полномочием по отнесению сведений к государственным секретам, в сфере своей деятельности.

Статья 21. Засекречивание. Засекречивание осуществляется на основании перечня сведений, подлежащих засекречиванию, посредством установления ограничений на распространение и (или) предоставление сведений и применения иных мер защиты в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь.

При засекречивании на носителе государственных секретов и (или) сопроводительной документации к нему проставляется гриф секретности.

Статья 22. Срок засекречивания, изменение срока засекречивания. Для государственных секретов, как правило, устанавливаются следующие сроки засекречивания:

для государственной тайны – до тридцати лет;

для служебной тайны – до десяти лет.

Срок засекречивания исчисляется с даты засекречивания.

Изменение срока засекречивания осуществляется на основании решений государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам.

Статья 23. Рассекречивание. Рассекречивание осуществляется посредством снятия ограничений на распространение и (или) предоставление государственных секретов и прекращения иных мер защиты.

Рассекречивание осуществляется на основании решений государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам.

При рассекречивании на носителях государственных секретов и (или) сопроводительной документации к ним аннулируется гриф секретности.

ГЛАВА 7. ПРАВО СОБСТВЕННОСТИ НА ГОСУДАРСТВЕННЫЕ СЕКРЕТЫ. ВЛАДЕНИЕ, ПОЛЬЗОВАНИЕ И РАСПОРЯЖЕНИЕ ГОСУДАРСТВЕННЫМИ СЕКРЕТАМИ

Статья 24. Право собственности на государственные секреты. Государственные секреты являются собственностью Республики Беларусь.

Статья 25. Владение, пользование и распоряжение государственными секретами. Государственные органы и иные организации, наделенные полномочием по отнесению сведений к государственным секретам, в сфере своей деятельности осуществляют владение, пользование и распоряжение государственными секретами в соответствии с актами законодательства Республики Беларусь.

Другие государственные органы и иные организации, осуществляющие деятельность с использованием государственных секретов, реализуют право пользования государственными секретами, а также в пределах полномочий, предоставленных им государственными органами и иными организациями, наделенными полномочием по отнесению сведений к государственным секретам, распоряжаются государственными секретами.

Статья 26. Передача государственных секретов государственным органам и иным организациям. Государственные секреты передаются государственным органам и иным организациям в целях осуществления ими своих полномочий либо в связи с проведением работ с использованием государственных секретов в объеме, необходимом для осуществления этих полномочий либо проведения таких работ.

Передача государственных секретов государственным органам и иным организациям осуществляется на основании решений государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам.

Статья 27. Передача государственных секретов иностранным государствам, международным организациям, межгосударственным образованиям. Передача государственных секретов иностранным государствам, международным организациям, межгосударственным образованиям осуществляется на основании решений Президента Республики Беларусь или руководителей государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам, в пределах их компетенции с учетом заключения уполномоченного государственного органа по защите государственных секретов о возможности их передачи.

Решение о передаче государственных секретов иностранным государствам, международным организациям, межгосударственным образованиям принимается Президентом Республики Беларусь при наличии обязательства иностранного государства, международной организации, межгосударственного образования о защите государственных секретов.

Решение о передаче служебной тайны иностранным государствам, международным организациям, межгосударственным образованиям принимается руководителями государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам, при наличии международного договора Республики Беларусь о защите государственных секретов.

ГЛАВА 8. ЗАЩИТА ГОСУДАРСТВЕННЫХ СЕКРЕТОВ

Статья 28. Организация защиты государственных секретов в государственных органах и иных организациях. Организация защиты государственных секретов в государственных органах и иных организациях возлагается на их руководителей.

Защита государственных секретов осуществляется посредством применения правовых, организационных, технических мер, в том числе посредством использования сертифицированных средств защиты государственных секретов, и иных мер в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь в целях предотвращения тяжких последствий или существенного вреда национальной безопасности Республики Беларусь.

В государственных органах и иных организациях, наделенных полномочием по отнесению сведений к государственным секретам, должны быть созданы подразделения по защите государственных секретов.

Другие государственные органы и иные организации по решению их руководителей создают подразделения по защите государственных секретов или заключают договор об оказании услуг по защите государственных секретов с государственным органом и иной организацией, имеющими подразделение по защите государственных секретов, по согласованию с государственным органом и иной организацией, которые передают им государственные секреты.

Государственные органы и иные организации в случае их реорганизации или ликвидации, а также прекращения деятельности с использованием государственных секретов обязаны в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь принять меры по защите находящихся у них государственных секретов.

Статья 29. Защита государственных секретов иностранных государств, международных организаций, межгосударственных образований. Защита государственных секретов иностранных государств, международных организаций, межгосударственных образований, переданных Республике Беларусь на основании международных договоров Республики Беларусь либо в связи с ее членством в этих международных организациях, межгосударственных образованиях, а также сведений, образовавшихся при их использовании, осуществляется в соответствии с настоящим Законом, другими актами законодательства Республики Беларусь, в том числе международными договорами Республики Беларусь о защите государственных секретов, с учетом требований иностранных государств, международных организаций, межгосударственных образований, передавших государственные секреты.

ГЛАВА 9. ДОПУСК К ГОСУДАРСТВЕННЫМ СЕКРЕТАМ. ДОСТУП К ГОСУДАРСТВЕННЫМ СЕКРЕТАМ

Статья 30. Условия предоставления допуска к государственным секретам государственным органам и иным организациям. Допуск к государственным секретам государственным органам и иным организациям предоставляется при соблюдении ими законодательства Республики Беларусь о государственных секретах, а также, если:

в их структуре имеется подразделение по защите государственных секретов, состоящее из работников, количество и уровень квалификации которых достаточны для защиты государственных секретов, или ими заключен договор об оказании услуг по защите государственных секретов с государственным органом и иной организацией, имеющими подразделение по защите государственных секретов;

разработана и утверждена номенклатура должностей работников, подлежащих допуску к государственным секретам;

их руководители, ответственные за обеспечение защиты государственных секретов, имеют допуск к государственным секретам;

приняты иные меры защиты государственных секретов, предусмотренные законодательством Республики Беларусь о государственных секретах.

Статья 31. Допуск к государственным секретам государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам. Допуск к государственным секретам государственным органам и иным организациям, наделенным полномочием по отнесению сведений к государственным секретам, предоставляется на основании включения их в перечень государственных органов и иных организаций, наделенных полномочием по отнесению сведений к государственным секретам, утвержденный Президентом Республики Беларусь.

Государственные органы и иные организации, наделенные полномочием по отнесению сведений к государственным секретам, осуществляют деятельность с использованием государственных секретов при наличии в их структуре подразделения по защите государственных секретов и выполнении условий, предусмотренных абзацами первым, третьим – пятым статьи 30 настоящего Закона. Информация о состоянии защиты государственных секретов в государственных органах и иных организациях, наделенных полномочием по отнесению сведений к государственным секретам, учитывается при проведении в соответствии с актами законодательства Республики Беларусь аттестации их руководителей.

Статья 32. Допуск к государственным секретам других государственных органов и иных организаций. Допуск к государственным секретам другим государственным органам и иным организациям предоставляется на основании разрешения на осуществление деятельности с использованием государственных секретов, выданного уполномоченным государственным органом по защите государственных секретов по результатам проверочных мероприятий.

Разрешение на осуществление деятельности с использованием государственных секретов выдается после выполнения другими государственными органами и иными организациями условий, предусмотренных статьей 30 настоящего Закона, и аттестации их руководителей, ответственных за обеспечение защиты государственных секретов.

Статья 33. Условия предоставления гражданам допуска к государственным секретам. Допуск к государственным секретам гражданам предоставляется, если:

граждане ознакомлены с правами и обязанностями, предусмотренными настоящим Законом и другими актами законодательства Республики Беларусь о государственных секретах, с возможным временным ограничением их права на выезд из Республики Беларусь, а также с законодательными актами Республики Беларусь, устанавливающими ответственность за нарушение законодательства Республики Беларусь о государственных секретах;

имеется письменное согласие граждан на проведение в отношении их проверочных мероприятий в связи с предоставлением им допуска к государственным секретам;

гражданами представлены их персональные данные;

гражданами приняты письменные обязательства перед государством о соблюдении законодательства Республики Беларусь о государственных секретах;

имеется согласование уполномоченным государственным органом по защите государственных секретов предоставления им допуска к государственным секретам;

проведены проверочные мероприятия в отношении граждан в связи с предоставлением им допуска к государственным секретам.

Допуск к государственным секретам гражданам Республики Беларусь, указанным в статье 35 настоящего Закона, предоставляется без согласования с уполномоченным государственным органом по защите государственных секретов и проведения в отношении их проверочных мероприятий в связи с предоставлением им допуска к государственным секретам.

Допуск к государственным секретам гражданам, оказывающим на конфиденциальной основе содействие органам, осуществляющим разведывательную, контрразведывательную и оперативно-розыскную деятельность, а также гражданам Республики Беларусь, являющимся штатными негласными сотрудниками указанных органов, предоставляется без согласования с уполномоченным государственным органом по защите государственных секретов.

Гражданам, достигшим шестнадцатилетнего возраста, но не достигшим восемнадцатилетнего возраста, предоставляется допуск к служебной тайне.

Проверочные мероприятия в отношении граждан в связи с предоставлением им допуска к государственным секретам проводятся органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность, в пределах их компетенции.

Статья 34. Допуск к государственным секретам граждан. Допуск к государственным секретам предоставляется:

гражданам Республики Беларусь, постоянно проживающим в Республике Беларусь, являющимся работниками государственных органов и иных организаций, осуществляющих деятельность с использованием государственных секретов, – на основании решений руководителей государственных органов и иных организаций, принимаемых ими с учетом обязанностей, исполняемых работниками по месту работы (службы);

гражданам Республики Беларусь, постоянно проживающим в Республике Беларусь, не являющимся работниками государственных органов и иных организаций, осуществляющих деятельность с использованием государственных секретов, – на основании решений руководителей государственных органов и иных организаций о привлечении их к проведению работ с использованием государственных секретов;

гражданам Республики Беларусь, указанным в статье 35 настоящего Закона, – на основании решений об избрании (назначении) их на соответствующие должности, о признании их полномочий;

участникам уголовного, гражданского, хозяйственного, административного процесса, не имеющим допуска к государственным секретам, – на основании решений органов, ведущих соответственно уголовный, гражданский, хозяйственный или административный процесс;

иностранным гражданам и лицам без гражданства, а также гражданам Республики Беларусь, постоянно проживающим за пределами Республики Беларусь (за исключением граждан, являющихся представителями иностранных государств, международных организаций, межгосударственных образований, участвующих в реализации заключенных договоров (контрактов), предусматривающих использование государственных секретов), – на основании решений об использовании в интересах Республики Беларусь их профессиональных навыков и квалификации, принимаемых с учетом заключения уполномоченного государственного органа по защите государственных секретов о предоставлении им допуска к государственным секретам;

гражданам, оказывающим на конфиденциальной основе содействие органам, осуществляющим разведывательную, контрразведывательную и оперативно-розыскную деятельность, а также гражданам Республики Беларусь, являющимся штатными негласными сотрудниками указанных органов, – на основании решений, принимаемых органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность.

Решение о предоставлении гражданам допуска к государственным секретам принимается в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь.

Статья 35. Допуск к государственным секретам граждан Республики Беларусь в связи с их избранием (назначением) на должность. Допуск к государственным секретам в связи с избранием (назначением) на должность предоставляется:

Президенту Республики Беларусь – с момента вступления его в должность;

Премьер-министру Республики Беларусь – с даты назначения его на должность;

депутатам Палаты представителей, членам Совета Республики Национального собрания Республики Беларусь, депутатам местных Советов депутатов – с даты признания их полномочий;

судьям – с даты назначения (избрания) их на должность.

Статья 36. Формы допуска к государственным секретам. В зависимости от степени секретности устанавливаются три формы допуска к государственным секретам:

форма №1 – форма допуска к государственной тайне, имеющей степень секретности «Особой важности»;

форма №2 – форма допуска к государственной тайне, имеющей степень секретности «Совершенно секретно»;

форма №3 – форма допуска к служебной тайне, имеющей степень секретности «Секретно».

Статья 37. Основания для отказа в предоставлении гражданам допуска к государственным секретам. Основаниями для отказа в предоставлении гражданину допуска к государственным секретам являются:

невыполнение условий предоставления допуска к государственным секретам;

признание судом гражданина недееспособным;

наличие у гражданина заболевания, препятствующего работе с государственными секретами, согласно перечню, утвержденному Министерством здравоохранения Республики Беларусь.

В предоставлении гражданину допуска к государственным секретам может быть отказано при:

возбуждении в отношении этого гражданина уголовного дела либо привлечении его в качестве подозреваемого или обвиняемого по уголовному делу, возбужденному в отношении других граждан, либо по факту совершения преступления;

наличии в уголовном, гражданском, хозяйственном или административном процессе дела, связанного с нарушением этим гражданином законодательства Республики Беларусь о государственных секретах;

наличии у гражданина неснятой или непогашенной судимости за совершение умышленного преступления;

оформлении гражданином документов для постоянного проживания за пределами Республики Беларусь;

представлении гражданином заведомо ложных его персональных данных.

Решение об отказе в предоставлении гражданам допуска к государственным секретам принимается в соответствии с настоящим Законом и другими актами законодательства Республики Беларусь и может быть обжаловано в вышестоящий государственный орган (вышестоящую организацию) и (или) в суд.

Статья 38. Прекращение допуска к государственным секретам граждан. Допуск к государственным секретам граждан прекращается в случае:

прекращения гражданами трудовых отношений с государственными органами и иными организациями, осуществляющими деятельность с использованием государственных секретов;

завершения участия граждан в проведении работ с использованием государственных секретов либо прекращения проведения таких работ;

прекращения полномочий граждан Республики Беларусь, указанных в статье 35 настоящего Закона;

завершения участия граждан в уголовном, гражданском, хозяйственном или административном процессе, которым допуск к государственным секретам был предоставлен по решению органа, ведущего уголовный, гражданский, хозяйственный или административный процесс;

завершения использования в интересах Республики Беларусь профессиональных навыков и квалификации граждан;

завершения оказания гражданами на конфиденциальной основе содействия органам, осуществляющим разведывательную, контрразведывательную и оперативно-розыскную деятельность, или исполнения обязанностей штатного негласного сотрудника указанных органов;

внесения органом государственной безопасности в государственные органы и иные организации, осуществляющие деятельность с использованием государственных секретов, предписаний о прекращении допуска к государственным секретам граждан.

Прекращение допуска к государственным секретам граждан не освобождает их от соблюдения законодательства Республики Беларусь о государственных секретах, в том числе от возможного временного ограничения их права на выезд из Республики Беларусь, если они осведомлены о государственной тайне.

Статья 39. Доступ к государственным секретам граждан. Доступ к государственным секретам осуществляется гражданами на основании предоставленного им допуска к государственным секретам после их ознакомления в необходимом объеме с законодательством Республики Беларусь о государственных секретах.

Руководители государственных органов и иных организаций, осуществляющих деятельность с использованием государственных секретов, создают условия для осуществления гражданами доступа к государственным секретам, при которых граждане будут иметь доступ только к тем государственным секретам и в таком объеме, которые необходимы им для исполнения их обязанностей.

Доступ к государственным секретам, имеющим степени секретности «Особой важности», «Совершенно секретно» и «Секретно», осуществляется при наличии допуска к государственным секретам формы №1.

Доступ к государственным секретам, имеющим степени секретности «Совершенно секретно» и «Секретно», осуществляется при наличии допуска к государственным секретам формы №2.

Доступ к государственным секретам, имеющим степень секретности «Секретно», осуществляется при наличии допуска к государственным секретам формы №3.

Доступ к государственным секретам осуществляется:

гражданами Республики Беларусь, постоянно проживающими в Республике Беларусь, – в период исполнения ими обязанностей по месту работы (службы) либо в связи с привлечением их к проведению работ с использованием государственных секретов;

гражданами Республики Беларусь, указанными в статье 35 настоящего Закона, — в период осуществления ими полномочий в связи с избранием (назначением) их на соответствующие должности;

участниками уголовного, гражданского, хозяйственного или административного процесса – в соответствии с процессуальным законодательством Республики Беларусь;

иностранными гражданами и лицами без гражданства, а также гражданами Республики Беларусь, постоянно проживающими за пределами Республики Беларусь (за исключением граждан, являющихся представителями иностранных государств, международных организаций, межгосударственных образований, участвующих в реализации заключенных договоров (контрактов), предусматривающих использование государственных секретов), — в период использования в интересах Республики Беларусь их профессиональных навыков и квалификации;

гражданами, являющимися представителями иностранных государств, международных организаций, межгосударственных образований, участвующими в реализации заключенных договоров (контрактов), предусматривающих использование государственных секретов, при наличии международных договоров Республики Беларусь о защите государственных секретов и по согласованию с уполномоченным государственным органом по защите государственных секретов – в период их участия в реализации заключенных договоров (контрактов), предусматривающих использование государственных секретов;

гражданами, оказывающими на конфиденциальной основе содействие органам, осуществляющим разведывательную, контрразведывательную и оперативно-розыскную деятельность, а также гражданами Республики Беларусь, являющимися штатными негласными сотрудниками указанных органов, — в период оказания ими содействия на конфиденциальной основе или исполнения обязанностей штатного негласного сотрудника этих органов.

ГЛАВА 10. ЗАЩИТА ПРАВ И ЗАКОННЫХ ИНТЕРЕСОВ ГОСУДАРСТВЕННЫХ ОРГАНОВ, ИНЫХ ОРГАНИЗАЦИЙ И ГРАЖДАН В СФЕРЕ ГОСУДАРСТВЕННЫХ СЕКРЕТОВ

Статья 40. Защита прав и законных интересов государственных органов, иных организаций и граждан в сфере государственных секретов. Защита прав и законных интересов государственных органов, иных организаций и граждан в сфере государственных секретов осуществляется в соответствии с настоящим Законом и другими законодательными актами Республики Беларусь.

Статья 41. Временное ограничение прав граждан. Граждане временно ограничиваются в праве на неприкосновенность личной жизни в период проведения в отношении их проверочных мероприятий в связи с предоставлением им допуска к государственным секретам.

Граждане, осведомленные о государственной тайне, могут быть временно ограничены в праве на выезд из Республики Беларусь в соответствии с законодательными актами Республики Беларусь.

Статья 42. Предоставление гражданам надбавок и компенсационных выплат. Гражданам, осуществляющим либо осуществлявшим доступ к государственным секретам, устанавливаются надбавки к тарифным ставкам (окладам) на период их доступа к государственным секретам в зависимости от степени секретности, а также компенсационные выплаты на период действия временного ограничения их права на выезд из Республики Беларусь, если они осведомлены о государственной тайне. Работникам подразделений по защите государственных секретов в государственных органах и иных организациях, осуществляющих деятельность с использованием государственных секретов, дополнительно к установленным частью первой настоящей статьи надбавкам и компенсационным выплатам устанавливаются за стаж работы в указанных подразделениях надбавки к тарифным ставкам (окладам).

ГЛАВА 11. НАДЗОР, КОНТРОЛЬ И ОТВЕТСТВЕННОСТЬ В СФЕРЕ ГОСУДАРСТВЕННЫХ СЕКРЕТОВ. ФИНАНСИРОВАНИЕ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ГОСУДАРСТВЕННЫХ СЕКРЕТОВ

Статья 43. Надзор за исполнением законодательства Республики Беларусь о государственных секретах. Надзор за точным и единообразным исполнением законодательства Республики Беларусь о государственных секретах осуществляют Генеральный прокурор Республики Беларусь и подчиненные ему прокуроры в пределах предоставленных им полномочий.

Статья 44. Государственный контроль в сфере государственных секретов. Государственный контроль в сфере государственных секретов осуществляется уполномоченным государственным органом по защите государственных секретов в порядке, установленном Президентом Республики Беларусь.

Статья 45. Контроль за защитой государственных секретов. Контроль за защитой государственных секретов в пределах полномочий осуществляется органами государственной безопасности, государственными органами и иными организациями, наделенными полномочием по отнесению сведений к государственным секретам, другими государственными органами и иными организациями, осуществляющими деятельность с использованием государственных секретов, в порядке, установленном Советом Министров Республики Беларусь.

Статья 46. Ответственность в сфере государственных секретов. Нарушение законодательства Республики Беларусь о государственных секретах влечет ответственность, установленную законодательными актами Республики Беларусь. Ответственность за организацию защиты государственных секретов в государственных органах и иных организациях, осуществляющих деятельность с использованием государственных секретов, возлагается на их руководителей.

Статья 47. Финансирование мероприятий по защите государственных секретов. Финансирование мероприятий по защите

государственных секретов осуществляется за счет средств республиканского и местных бюджетов, а также иных источников, не запрещенных актами законодательства Республики Беларусь.

2.2. Практическая часть

Задание 1

Открыть программный модуль «Введение в информационную безопасность. Практические работы», расположенный на диске /D лабораторного компьютера. Перейти по вкладке «Разделы» в раздел «Практическая работа №2». Пройти тестирование по материалу изученной темы в разделе «Тест».

Задание 2

Пользуясь инструкцией к выполнению задания в разделе «Практика» программного модуля, выполнить задание.

ПРАКТИЧЕСКАЯ РАБОТА №3
ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ЧАСТЬ 2

Цель работы: изучить вопросы, связанные с разрешением спорных вопросов по защите объектов промышленной собственности, с защитой авторского права и смежных прав, а также меры борьбы с пиратством.

3.1. Теоретические сведения

Приведены главы 1–8 Закона Республики Беларусь от 10 ноября 2008 г. №455-З «Об информации, информатизации и защите информации» [5].

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Основные термины, применяемые в настоящем Законе, и их определения. В настоящем Законе применяются следующие основные термины и их определения:

база данных – совокупность структурированной и взаимосвязанной информации, организованной по определенным правилам на материальных носителях;

банк данных – организационно-техническая система, включающая одну или несколько баз данных и систему управления ими;

владелец программно-технических средств, информационных ресурсов, информационных систем и информационных сетей – субъект информационных отношений, реализующий права владения, пользования и распоряжения программно-техническими средствами, информационными ресурсами, информационными системами и информационными сетями в пределах и порядке, определенных их собственником в соответствии с законодательством Республики Беларусь;

государственная информационная система – информационная система, создаваемая и (или) приобретаемая за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц;

государственный информационный ресурс – информационный ресурс, формируемый или приобретаемый за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц;

документированная информация – информация, зафиксированная на материальном носителе с реквизитами, позволяющими ее идентифицировать;

доступ к информации – возможность получения информации и пользования ею;

доступ к информационной системе и (или) информационной сети – возможность использования информационной системы и (или) информационной сети;

защита информации – комплекс правовых, организационных и технических мер, направленных на обеспечение целостности (неизменности), конфиденциальности, доступности и сохранности информации;

информатизация – организационный, социально-экономический и научно-технический процесс, обеспечивающий условия для формирования и использования информационных ресурсов и реализации информационных отношений;

информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

информационная сеть – совокупность информационных систем либо комплексов программно-технических средств информационной системы, взаимодействующих посредством сетей электросвязи;

информационная система – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств;

информационная технология – совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и защиты информации;

информационная услуга – деятельность по осуществлению поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также защиты информации;

информационные отношения – отношения, возникающие при поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, пользовании информацией, защите информации, а также при применении информационных технологий;

информационный посредник – субъект информационных отношений, предоставляющий информационные услуги обладателям и (или) пользователям информации;

информационный ресурс – организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах;

комплекс программно-технических средств – совокупность программных и технических средств, обеспечивающих осуществление информационных отношений с помощью информационных технологий;

конфиденциальность информации – требование не допускать распространения и (или) предоставления информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами Республики Беларусь;

обладатель информации – субъект информационных отношений, получивший права обладателя информации по основаниям, установленным актами законодательства Республики Беларусь, или по договору;

оператор информационной системы – субъект информационных отношений, осуществляющий эксплуатацию информационной системы и (или) оказывающий посредством ее информационные услуги;

пользователь информации – субъект информационных отношений, получающий, распространяющий и (или) предоставляющий информацию, реализующий право на пользование ею;

пользователь информационной системы и (или) информационной сети – субъект информационных отношений, получивший доступ к информационной системе и (или) информационной сети и пользующийся ими;

предоставление информации – действия, направленные на ознакомление с информацией определенного круга лиц;

распространение информации – действия, направленные на ознакомление с информацией неопределенного круга лиц;

собственник программно-технических средств, информационных ресурсов, информационных систем и информационных сетей – субъект информационных отношений, реализующий права владения, пользования и распоряжения программно-техническими средствами, информационными ресурсами, информационными системами и информационными сетями.

Статья 2. Сфера действия настоящего Закона. Настоящим Законом регулируются общественные отношения, возникающие при:

поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, а также пользовании информацией;

создании и использовании информационных технологий, информационных систем и информационных сетей, формировании информационных ресурсов;

организации и обеспечении защиты информации.

Законодательством Республики Беларусь могут быть установлены особенности правового регулирования информационных отношений, связанных со сведениями, составляющими государственные секреты, с персональными данными, рекламой, научно-технической, статистической, правовой и иной информацией.

Действие настоящего Закона не распространяется на общественные отношения, связанные с деятельностью средств массовой информации и охраной информации, являющейся объектом интеллектуальной собственности.

Статья 3. Законодательство об информации, информатизации и защите информации. Законодательство об информации, информатизации и защите информации основывается на Конституции Республики Беларусь и состоит из настоящего Закона, актов Президента Республики Беларусь, иных актов законодательства Республики Беларусь.

Если международным договором Республики Беларусь установлены иные правила, чем те, которые предусмотрены настоящим Законом, то применяются правила международного договора.

Статья 4. Принципы правового регулирования информационных отношений. Правовое регулирование информационных отношений осуществляется на основе следующих принципов:

свободы поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией;

установления ограничений распространения и (или) предоставления информации только законодательными актами Республики Беларусь;

своевременности предоставления, объективности, полноты и достоверности информации;

защиты информации о частной жизни физического лица и персональных данных;

обеспечения безопасности личности, общества и государства при пользовании информацией и применении информационных технологий;

обязательности применения определенных информационных технологий для создания и эксплуатации информационных систем и информационных сетей в случаях, установленных законодательством Республики Беларусь.

Статья 5. Субъекты информационных отношений. Субъектами информационных отношений могут являться:

Республика Беларусь, административно-территориальные единицы Республики Беларусь;

государственные органы, другие государственные организации (далее – государственные органы);

иные юридические лица, организации, не являющиеся юридическими лицами (далее – юридические лица);

физические лица, в том числе индивидуальные предприниматели (далее – физические лица);

иностранные государства, международные организации.

Субъекты информационных отношений в соответствии с настоящим Законом могут выступать в качестве:

обладателей информации;

пользователей информации, информационных систем и (или) информационных сетей;

собственников и владельцев программно-технических средств, информационных ресурсов, информационных систем и информационных сетей;

информационных посредников;

операторов информационных систем.

Статья 6. Право на информацию. Государственные органы, физические и юридические лица вправе осуществлять поиск, получение, передачу, сбор, обработку, накопление, хранение, распространение и (или) предоставление информации, пользование информацией в соответствии с настоящим Законом и иными актами законодательства Республики Беларусь.

Государственные органы, общественные объединения, должностные лица обязаны предоставлять гражданам Республики Беларусь возможность ознакомления с информацией, затрагивающей их права и законные интересы, в порядке, установленном настоящим Законом и иными актами законодательства Республики Беларусь.

Гражданам Республики Беларусь гарантируется право на получение, хранение и распространение полной, достоверной и своевременной информации о деятельности государственных органов, общественных объединений, о политической, экономической, культурной и международной жизни, состоянии окружающей среды в порядке, установленном настоящим Законом и иными актами законодательства Республики Беларусь.

Право на информацию не может быть использовано для пропаганды войны или экстремистской деятельности, а также для совершения иных противоправных деяний.

ГЛАВА 2. ГОСУДАРСТВЕННОЕ РЕГУЛИРОВАНИЕ И УПРАВЛЕНИЕ В ОБЛАСТИ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЫ ИНФОРМАЦИИ

Статья 7. Государственное регулирование в области информации, информатизации и защиты информации. Государственное регулирование в области информации, информатизации и защиты информации включает:

обеспечение условий для реализации и защиты прав государственных органов, физических и юридических лиц;

создание системы информационной поддержки решения задач социально-экономического и научно-технического развития Республики Беларусь;

создание условий для развития и использования информационных технологий, информационных систем и информационных сетей на основе единых принципов технического нормирования и стандартизации, оценки соответствия требованиям технических нормативных правовых актов в области технического нормирования и стандартизации;

формирование и осуществление единой научной, научно-технической, промышленной и инновационной политики в области информации, информатизации и защиты информации с учетом имеющегося научно-производственного потенциала и современного мирового уровня развития информационных технологий;

создание и совершенствование системы привлечения инвестиций и механизма стимулирования разработки и реализации проектов в области информации, информатизации и защиты информации;

содействие развитию рынка информационных технологий и информационных услуг, обеспечение условий для формирования и развития всех видов информационных ресурсов, информационных систем и информационных сетей;

обеспечение условий для участия Республики Беларусь, административно-территориальных единиц Республики Беларусь,

государственных органов, физических и юридических лиц в международном сотрудничестве, включая взаимодействие с международными организациями, обеспечение выполнения обязательств по международным договорам Республики Беларусь;

разработку и обеспечение реализации целевых программ создания информационных систем, применения информационных технологий;

совершенствование законодательства Республики Беларусь об информации, информатизации и защите информации;

иное государственное регулирование.

Статья 8. Осуществление государственного регулирования и управления в области информации, информатизации и защиты информации. Государственное регулирование и управление в области информации, информатизации и защиты информации осуществляются Президентом Республики Беларусь, Советом Министров Республики Беларусь, Национальной академией наук Беларуси, Оперативно-аналитическим центром при Президенте Республики Беларусь, Министерством связи и информатизации Республики Беларусь, иными государственными органами в пределах их компетенции.

Статья 9. Полномочия Президента Республики Беларусь в области информации, информатизации и защиты информации. Президент Республики Беларусь в соответствии с Конституцией Республики Беларусь, настоящим Законом и иными законодательными актами Республики Беларусь определяет единую государственную политику и осуществляет иное государственное регулирование в области информации, информатизации и защиты информации.

Статья 10. Полномочия Совета Министров Республики Беларусь в области информации, информатизации и защиты информации. Совет Министров Республики Беларусь в области информации, информатизации и защиты информации:

обеспечивает проведение единой государственной политики;

координирует, направляет и контролирует работу республиканских органов государственного управления и иных государственных организаций, подчиненных Правительству Республики Беларусь;

утверждает государственные программы, если иное не предусмотрено законодательными актами Республики Беларусь, и обеспечивает их реализацию;

осуществляет иные полномочия, возложенные на него Конституцией Республики Беларусь, настоящим Законом, иными законами Республики Беларусь и актами Президента Республики Беларусь.

Статья 11. Полномочия Национальной академии наук Беларуси в области информации, информатизации и защиты информации. Национальная академия наук Беларуси в области информации, информатизации и защиты информации:

осуществляет научно-методическое обеспечение развития информатизации, реализации государственных программ;

участвует в разработке проектов нормативных правовых актов;

осуществляет иные полномочия в соответствии с настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 12. Полномочия Оперативно-аналитического центра при Президенте Республики Беларусь в области защиты информации. Оперативно-аналитический центр при Президенте Республики Беларусь в области защиты информации:

определяет приоритетные направления технической защиты информации, содержащей сведения, составляющие государственные секреты, или иные сведения, охраняемые в соответствии с законодательством Республики Беларусь;

координирует деятельность по технической защите информации;

осуществляет в пределах своих полномочий контроль за деятельностью по обеспечению технической защиты информации;

участвует в разработке проектов нормативных правовых актов в области технической защиты информации;

осуществляет иные полномочия в соответствии с настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 13. Полномочия Министерства связи и информатизации Республики Беларусь в области информатизации. Министерство связи и информатизации Республики Беларусь в области информатизации:

реализует единую государственную политику;

разрабатывает и реализует государственные программы;

участвует в разработке проектов нормативных правовых актов;

координирует работу по формированию и государственной регистрации информационных ресурсов;

устанавливает требования совместимости информационных ресурсов, информационных систем и информационных сетей;

разрабатывает и утверждает правила эксплуатации и взаимодействия информационных ресурсов, информационных систем и информационных сетей;

организует работы по техническому нормированию и стандартизации, подтверждению соответствия создания, использования и эксплуатации информационных ресурсов, информационных систем и информационных сетей требованиям технических нормативных правовых актов в области технического нормирования и стандартизации;

стимулирует создание информационных технологий, информационных систем и информационных сетей;

осуществляет международное сотрудничество, включая взаимодействие с международными организациями, обеспечение выполнения обязательств по международным договорам Республики Беларусь;

осуществляет иные полномочия в соответствии с настоящим Законом и иными актами законодательства Республики Беларусь.

Статья 14. Полномочия иных государственных органов в области информации, информатизации и защиты информации. Иные государственные органы в пределах своих полномочий в области информации, информатизации и защиты информации:

участвуют в реализации единой государственной политики;

формируют и используют информационные ресурсы;

создают и развивают информационные системы и информационные сети, обеспечивают их совместимость и взаимодействие в информационном пространстве Республики Беларусь;

осуществляют техническое нормирование и стандартизацию в области информационных технологий, информационных ресурсов, информационных систем и информационных сетей;

осуществляют подтверждение соответствия информационных технологий, информационных ресурсов, информационных систем и информационных сетей требованиям технических нормативных правовых актов в области технического нормирования и стандартизации;

осуществляют иные полномочия в соответствии с настоящим Законом и иными актами законодательства Республики Беларусь.

ГЛАВА 3. ПРАВОВОЙ РЕЖИМ ИНФОРМАЦИИ

Статья 15. Виды информации. В зависимости от категории доступа информация делится на:

общедоступную информацию;

информацию, распространение и (или) предоставление которой ограничено.

Статья 16. Общедоступная информация. К общедоступной информации относится информация, доступ к которой, распространение и (или) предоставление которой не ограничены.

Не могут быть ограничены доступ к информации, распространение и (или) предоставление информации:

о правах, свободах и законных интересах физических лиц, правах и законных интересах юридических лиц и о порядке реализации прав, свобод и законных интересов;

о деятельности государственных органов, общественных объединений;

о правовом статусе государственных органов, за исключением информации, доступ к которой ограничен законодательными актами Республики Беларусь;

о чрезвычайных ситуациях, экологической, санитарно-эпидемиологической обстановке, гидрометеорологической и иной информации, отражающей состояние общественной безопасности;

о состоянии здравоохранения, демографии, образования, культуры, сельского хозяйства;

о состоянии преступности, а также о фактах нарушения законности;

о льготах и компенсациях, предоставляемых государством физическим и юридическим лицам;

о размерах золотого запаса;

об обобщенных показателях по внешней задолженности;

о состоянии здоровья должностных лиц, занимающих должности, включенные в перечень высших государственных должностей Республики Беларусь;

накапливаемой в открытых фондах библиотек и архивов, информационных системах государственных органов, физических и юридических лиц, созданных (предназначенных) для информационного обслуживания физических лиц.

Статья 17. Информация, распространение и (или) предоставление которой ограничено. К информации, распространение и (или) предоставление которой ограничено, относится:

информация о частной жизни физического лица и персональные данные;

сведения, составляющие государственные секреты;

информация, составляющая коммерческую и профессиональную тайну;

информация, содержащаяся в делах об административных правонарушениях, материалах и уголовных делах органов уголовного преследования и суда до завершения производства по делу;

иная информация, доступ к которой ограничен законодательными актами Республики Беларусь.

Правовой режим информации, распространение и (или) предоставление которой ограничено, определяется настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 18. Информация о частной жизни физического лица и персональные данные. Никто не вправе требовать от физического лица предоставления информации о его частной жизни и персональных данных, включая сведения, составляющие личную и семейную тайну, тайну телефонных переговоров, почтовых и иных сообщений, касающиеся состояния его здоровья, либо получать такую информацию иным образом помимо воли данного физического лица, кроме случаев, установленных законодательными актами Республики Беларусь.

Сбор, обработка, хранение информации о частной жизни физического лица и персональных данных, а также пользование ими осуществляются с согласия данного физического лица, если иное не установлено законодательными актами Республики Беларусь.

Порядок получения, передачи, сбора, обработки, накопления, хранения и предоставления информации о частной жизни физического лица и персональных данных, а также пользования ими устанавливается законодательными актами Республики Беларусь.

Статья 19. Документирование информации. Документирование информации осуществляется ее обладателем в соответствии с требованиями делопроизводства, установленными законодательством Республики Беларусь.

Порядок документирования информации, обработки, хранения, распространения и (или) предоставления документированной информации, а также пользования ею устанавливается актами законодательства Республики Беларусь, в том числе техническими нормативными правовыми актами.

ГЛАВА 4. РАСПРОСТРАНЕНИЕ И (ИЛИ) ПРЕДОСТАВЛЕНИЕ ИНФОРМАЦИИ

Статья 20. Распространение и (или) предоставление информации. Распространяемая и (или) предоставляемая информация должна содержать достоверные сведения о ее обладателе, а также о лице, распространяющем и (или) предоставляющем информацию, в форме и объеме, достаточных для идентификации таких лиц.

При использовании для предоставления информации технических средств, позволяющих ознакомить с информацией определенный круг лиц, обладатель информации и информационный посредник обязаны обеспечить пользователям информации возможность свободного отказа от получения предоставляемой таким способом информации.

Если обладателем информации либо информационным посредником или владельцем информационной сети получено уведомление о нежелании конкретного пользователя информации получать распространяемую и (или) предоставляемую информацию, они обязаны принять меры по предотвращению получения такой информации пользователем информации.

При распространении и (или) предоставлении информации по почте, сетям электросвязи лица, распространяющие и (или) предоставляющие информацию, обязаны соблюдать требования законодательства Республики Беларусь о почтовой связи, об электросвязи и о рекламе.

Случаи и требования обязательного распространения и (или) предоставления информации, в том числе предоставления обязательных экземпляров документов, устанавливаются законодательными актами Республики Беларусь и постановлениями Совета Министров Республики Беларусь.

Порядок распространения и (или) предоставления информации, за исключением информации, указанной в части пятой настоящей статьи и части первой статьи 17 настоящего Закона, определяется соглашением субъектов соответствующих информационных отношений, если иное не установлено законодательными актами Республики Беларусь.

Статья 21. Предоставление общедоступной информации по запросу. Предоставление общедоступной информации может осуществляться по запросу заинтересованного государственного органа, физического или юридического лица.

Запросы о получении общедоступной информации могут быть адресованы ее обладателям в форме:

устного запроса;

письменного запроса.

Предоставление заинтересованному государственному органу, физическому или юридическому лицу общедоступной информации по запросу может осуществляться посредством:

устного изложения содержания запрашиваемой информации;

ознакомления с документами, содержащими запрашиваемую информацию;

предоставления копии документа, содержащего запрашиваемую информацию, или выписок из него;

предоставления письменного ответа (справки), содержащего (содержащей) запрашиваемую информацию.

Порядок осуществления устных и письменных запросов о получении общедоступной информации, а также порядок их рассмотрения определяются законодательными актами Республики Беларусь.

Статья 22. Порядок распространения и (или) предоставления общедоступной информации о деятельности государственных органов.

Распространение и (или) предоставление общедоступной информации о деятельности государственных органов могут осуществляться посредством ее:

распространения в средствах массовой информации;

размещения в государственном органе в общедоступных местах;

размещения в информационных сетях;

предоставления на основании запросов заинтересованных государственных органов, физических и юридических лиц;

распространения и (или) предоставления иными способами.

Государственные органы обязаны посредством размещения в государственном органе в общедоступных местах распространять, а также могут иными способами распространять и (или) предоставлять следующую информацию:

официальное наименование государственного органа;

адрес места нахождения государственного органа, контактный телефон (факс);

организационную структуру государственного органа (руководство, отделы (управления), контактные телефоны), за исключением информации, доступ к которой ограничен законодательными актами Республики Беларусь;

режим работы государственного органа и время приема физических лиц;

нормативные правовые акты, регламентирующие деятельность государственного органа, за исключением информации, доступ к которой ограничен законодательными актами Республики Беларусь;

официальное наименование, адрес места нахождения и режим работы вышестоящего государственного органа и время приема физических лиц в этом органе.

Кроме информации, указанной в части второй настоящей статьи, в информационных сетях государственные органы обязаны распространять и (или) предоставлять общедоступную информацию о нормативных правовых актах, в том числе технических нормативных правовых актах, принятых данным государственным органом, и иную информацию в соответствии с законодательством Республики Беларусь.

Распространение и (или) предоставление общедоступной информации о деятельности государственных органов осуществляются на безвозмездной основе, если иное не установлено законодательными актами Республики Беларусь.

ГЛАВА 5. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

Статья 23. Виды информационных ресурсов. Правовой режим информационных ресурсов. Информационные ресурсы делятся на государственные и негосударственные.

Состав государственных информационных ресурсов, порядок их формирования, а также пользования документированной информацией из государственных информационных ресурсов определяются Советом Министров Республики Беларусь.

Порядок формирования негосударственных информационных ресурсов определяется собственниками информационных ресурсов.

Статья 24. Государственная регистрация информационных ресурсов. Государственная регистрация информационных ресурсов осуществляется в целях создания единой системы учета и сохранности информационных ресурсов, создания условий для их передачи на государственное архивное хранение, информирования государственных органов, физических и юридических лиц о составе и содержании информационных ресурсов в Республике Беларусь.

Государственная регистрация информационных ресурсов осуществляется Министерством связи и информатизации Республики Беларусь путем внесения сведений об информационных ресурсах в Государственный регистр информационных ресурсов.

Порядок государственной регистрации информационных ресурсов, за исключением информационных ресурсов, указанных в части четвертой настоящей статьи, и порядок ведения Государственного регистра информационных ресурсов определяются Советом Министров Республики Беларусь.

Порядок регистрации информационных ресурсов, формируемых органами государственной безопасности Республики Беларусь, определяется Комитетом государственной безопасности Республики Беларусь.

Государственной регистрации подлежат государственные информационные ресурсы.

Негосударственные информационные ресурсы регистрируются в Государственном регистре информационных ресурсов на добровольной основе.

ГЛАВА 6. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ИНФОРМАЦИОННЫЕ СЕТИ

Статья 25. Создание и использование информационных технологий, информационных систем и информационных сетей. Создание информационных технологий, информационных систем и информационных сетей осуществляется государственными органами, физическими и юридическими лицами.

Информационные системы делятся на государственные и негосударственные.

Государственные информационные системы создаются в целях предоставления общедоступной информации, обеспечения ее объективности, полноты и достоверности, оказания информационных услуг, оптимизации деятельности государственных органов и обеспечения информационного обмена между ними.

Государственные информационные системы создаются в порядке и на условиях, определенных законодательством Республики Беларусь.

Порядок использования государственных информационных систем определяется Советом Министров Республики Беларусь.

Негосударственные информационные системы создаются физическими и юридическими лицами в целях удовлетворения своих информационных потребностей и (или) оказания информационных услуг.

Порядок создания и использования негосударственных информационных систем определяется их собственниками или уполномоченными ими лицами.

Порядок включения информационных систем в информационные сети, а также правила обмена информацией в них устанавливаются их собственниками или уполномоченными ими лицами.

Порядок использования информационных систем и информационных сетей в случае, когда собственниками программно-технических средств и информационных систем являются разные лица, определяется соглашением между этими лицами.

Идентификация лиц, участвующих в информационном обмене с использованием информационных систем и информационных сетей, осуществляется в случаях, установленных актами законодательства Республики Беларусь.

Статья 26. Государственная регистрация информационных систем. Государственная регистрация информационных систем осуществляется в целях создания единой системы учета информационных систем, обеспечения их сохранности, а также информирования государственных органов, физических и юридических лиц об информационных системах в Республике Беларусь.

Государственная регистрация информационных систем, за исключением информационных систем, указанных в части четвертой настоящей статьи, осуществляется Министерством связи и информатизации Республики Беларусь путем внесения сведений об информационных системах в Государственный регистр информационных систем.

Порядок государственной регистрации информационных систем, за исключением информационных систем, указанных в части четвертой настоящей статьи, и порядок ведения Государственного регистра информационных систем определяются Советом Министров Республики Беларусь.

Порядок государственной регистрации информационных систем, содержащих государственные секреты, определяется Комитетом государственной безопасности Республики Беларусь.

Государственной регистрации подлежат государственные информационные системы.

Негосударственные информационные системы регистрируются в Государственном регистре информационных систем на добровольной основе.

ГЛАВА 7. ЗАЩИТА ИНФОРМАЦИИ

Статья 27. Цели защиты информации. Целями защиты информации являются:

обеспечение национальной безопасности, суверенитета Республики Беларусь;

сохранение информации о частной жизни физических лиц и неразглашение персональных данных, содержащихся в информационных системах;

обеспечение прав субъектов информационных отношений при создании, использовании и эксплуатации информационных систем и информационных сетей, использовании информационных технологий, а также формировании и использовании информационных ресурсов;

недопущение неправомерного доступа, уничтожения, модификации (изменения), копирования, распространения и (или) предоставления информации, блокирования правомерного доступа к информации, а также иных неправомерных действий.

Статья 28. Основные требования по защите информации. Защите подлежит информация, неправомерные действия в отношении которой могут причинить вред ее обладателю, пользователю или иному лицу.

Требования по защите общедоступной информации могут устанавливаться только в целях недопущения ее уничтожения, модификации (изменения), блокирования правомерного доступа к ней.

Требования по защите информации в государственных информационных системах, а также информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено, определяются законодательством Республики Беларусь.

Информация, распространение и (или) предоставление которой ограничено, а также информация, содержащаяся в государственных информационных системах, должны обрабатываться в информационных системах с применением системы защиты информации, аттестованной в порядке, установленном Советом Министров Республики Беларусь.

Не допускается эксплуатация государственных информационных систем без реализации мер по защите информации.

Обеспечение целостности и сохранности информации, содержащейся в государственных информационных системах, осуществляется путем установления и соблюдения единых требований по защите информации от неправомерного доступа, уничтожения, модификации (изменения) и блокирования правомерного доступа к ней, в том числе при осуществлении доступа к информационным сетям.

Для создания системы защиты информации используются средства защиты информации, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы, порядок проведения которой определяется Советом Министров Республики Беларусь.

Физические и юридические лица, занимающиеся созданием средств защиты информации и реализацией мер по защите информации, осуществляют свою деятельность в этой области на основании специальных разрешений (лицензий), выдаваемых государственными органами, уполномоченными Президентом Республики Беларусь, в соответствии с законодательством Республики Беларусь о лицензировании.

Статья 29. Меры по защите информации. К правовым мерам по защите информации относятся заключаемые обладателем информации с пользователем информации договоры, в которых ставятся условия пользования информацией, а также ответственность сторон по договору за нарушение указанных условий.

К организационным мерам по защите информации относятся обеспечение особого режима допуска на территории (в помещения), где может быть осуществлен доступ к информации (материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации.

К техническим (программно-техническим) мерам по защите информации относятся меры по использованию средств защиты информации, в том числе криптографических, а также систем контроля доступа и регистрации фактов доступа к информации.

Государственные органы и юридические лица, осуществляющие обработку информации, распространение и (или) предоставление которой ограничено, определяют соответствующие структурные подразделения или должностных лиц, ответственных за обеспечение защиты информации.

Статья 30. Организация защиты информации. Защита информации организуется:

в отношении общедоступной информации – лицом, осуществляющим распространение и (или) предоставление такой информации;

в отношении информации, распространение и (или) предоставление которой ограничено, – собственником или оператором информационной

системы, содержащей такую информацию, либо обладателем информации, если такая информация не содержится в информационных системах;

иными лицами в случаях, определенных настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 31. Права и обязанности субъектов информационных отношений по защите информации. Обладатель информации, собственник программно-технических средств, информационных ресурсов, информационных систем и информационных сетей или уполномоченные ими лица вправе:

запрещать или приостанавливать обработку информации и (или) пользование ею в случае невыполнения требований по защите информации;

обращаться в государственные органы, определенные Президентом Республики Беларусь и (или) Советом Министров Республики Беларусь, для оценки правильности выполнения требований по защите их информации в информационных системах, проведения экспертизы достаточности мер по защите их программно-технических средств, информационных ресурсов, информационных систем и информационных сетей, а также для получения консультаций.

Владелец информационных систем и информационных сетей обязан уведомить их собственника, а также обладателя информации о всех фактах нарушения требований по защите информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Республики Беларусь, обязаны:

обеспечить защиту информации, а также постоянный контроль за соблюдением требований по защите информации;

установить порядок предоставления информации пользователю информации и определить необходимые меры по обеспечению условий доступа к информации пользователя информации;

не допускать воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

обеспечивать возможность незамедлительного восстановления информации, модифицированной (измененной) или уничтоженной вследствие неправомерного (несанкционированного) доступа к ней.

Статья 32. Защита персональных данных. Меры по защите персональных данных от разглашения должны быть приняты с момента, когда персональные данные были предоставлены физическим лицом, к которому они относятся, другому лицу либо когда предоставление персональных данных осуществляется в соответствии с законодательными актами Республики Беларусь.

Последующая передача персональных данных разрешается только с согласия физического лица, к которому они относятся, либо в соответствии с законодательными актами Республики Беларусь.

Меры, указанные в части первой настоящей статьи, должны приниматься до уничтожения персональных данных, либо до их обезличивания, либо до

получения согласия физического лица, к которому эти данные относятся, на их разглашение.

Субъекты информационных отношений, получившие персональные данные в нарушение требований настоящего Закона и иных законодательных актов Республики Беларусь, не вправе пользоваться ими.

ГЛАВА 8. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТОВ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ

Статья 33. Права и обязанности обладателя информации. Обладатель информации в отношении информации, которой он обладает, имеет право:

распространять и (или) предоставлять информацию, пользоваться ею;

разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа в соответствии с законодательными актами Республики Беларусь;

требовать указания себя в качестве источника информации, ставшей общедоступной по его решению, при ее распространении и (или) предоставлении другими лицами;

определять условия обработки информации и пользования ею в информационных системах и информационных сетях;

передавать права на пользование информацией в соответствии с законодательством Республики Беларусь или по договору;

защищать в установленном законодательством Республики Беларусь порядке свои права в случае незаконного получения информации или незаконного пользования ею иными лицами;

осуществлять меры по защите информации;

осуществлять иные действия в соответствии с настоящим Законом и иными актами законодательства Республики Беларусь.

Права обладателя информации, содержащейся в информационном ресурсе, подлежат охране независимо от авторских и иных прав на информационный ресурс. Права обладателя информации не распространяются на программно-технические средства, информационные системы и информационные сети, принадлежащие собственнику, с помощью которых осуществляются поиск, получение, передача, сбор, обработка, накопление, хранение, распространение и (или) предоставление информации, пользование информацией.

Обладатель информации обязан:

соблюдать права и законные интересы иных лиц при распространении и (или) предоставлении информации, которой он обладает, а также при пользовании ею;

принимать меры по защите информации, если такая обязанность установлена законодательными актами Республики Беларусь;

распространять и (или) предоставлять информацию, в отношении которой законодательными актами Республики Беларусь установлена обязательность ее распространения и (или) предоставления;

предоставлять достоверную, полную информацию в установленный срок;

ограничивать и (или) запрещать доступ к информации, если такая обязанность установлена законодательными актами Республики Беларусь;

обеспечивать сохранность информации, распространение и (или) предоставление которой ограничено;

исполнять другие обязанности в соответствии с настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 34. Права и обязанности пользователя информации. Пользователь информации имеет право:

получать, распространять и (или) предоставлять информацию;

использовать информационные технологии, информационные системы и информационные сети;

знакомиться со своими персональными данными;

осуществлять иные действия в соответствии с настоящим Законом и иными актами законодательства Республики Беларусь.

Пользователь информации обязан:

соблюдать права и законные интересы других лиц при использовании информационных технологий, информационных систем и информационных сетей;

принимать меры по защите информации, если такая обязанность установлена законодательными актами Республики Беларусь;

обеспечивать сохранность информации, распространение и (или) предоставление которой ограничено, и не передавать ее полностью или частично третьим лицам без согласия обладателя информации;

исполнять другие обязанности в соответствии с настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 35. Права и обязанности пользователя информационной системы и (или) информационной сети

Пользователь информационной системы и (или) информационной сети имеет право:

использовать информационную систему и (или) информационную сеть для доступа к информационным ресурсам;

получать, распространять и (или) предоставлять информацию, содержащуюся в информационной системе и (или) информационной сети;

осуществлять иные действия в соответствии с настоящим Законом и иными актами законодательства Республики Беларусь.

Пользователь информационной системы и (или) информационной сети обязан:

соблюдать права других лиц при использовании информационной системы и (или) информационной сети;

исполнять другие обязанности в соответствии с настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 36. Права и обязанности собственника информационных ресурсов. Собственник информационных ресурсов, если иное не предусмотрено настоящим Законом и иными законодательными актами Республики Беларусь, имеет право:

предоставлять права владения и пользования информационными ресурсами иному лицу;

определять правила обработки информации, использования информационных ресурсов;

определять условия распоряжения документированной информацией в случае ее распространения и (или) предоставления по договору;

осуществлять иные действия в соответствии с настоящим Законом и иными актами законодательства Республики Беларусь.

Собственник информационных ресурсов обязан:

определять условия владения и пользования информационными ресурсами в случае, предусмотренном абзацем вторым части первой настоящей статьи;

осуществлять меры по защите информационных ресурсов, если такая обязанность установлена законодательными актами Республики Беларусь;

исполнять другие обязанности в соответствии с настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 37. Права и обязанности собственника программно-технических средств, информационных систем и информационных сетей. Собственником программно-технических средств, используемых для создания информационной системы, и собственником информационной системы, образующих информационную сеть, могут являться как одно, так и несколько лиц.

Собственник программно-технических средств, информационных систем и информационных сетей вправе передать иному лицу права владения и пользования программно-техническими средствами, информационными системами и информационными сетями.

Права на информацию, включенную в состав информационных систем, определяются соглашением между обладателями информации и собственниками информационных систем.

Правомочия собственника государственной информационной системы осуществляет заказчик по государственному контракту на выполнение подрядных работ для государственных нужд по созданию такой информационной системы, если иное не указано в решении о ее создании.

Собственник информационной системы вправе, если иное не установлено обладателем информации, запретить или ограничить передачу, распространение и (или) предоставление информации.

Собственник программно-технических средств, информационных систем и информационных сетей обладает другими правами в соответствии с

настоящим Законом и иными актами законодательства Республики Беларусь, исполняет обязанности в соответствии с настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 38. Права и обязанности владельца программно-технических средств, информационных ресурсов, информационных систем и информационных сетей. Владелец программно-технических средств, информационных ресурсов, информационных систем и информационных сетей имеет право:

определять условия их использования с соблюдением исключительных прав на объекты интеллектуальной собственности;

осуществлять иные действия в соответствии с настоящим Законом и иными актами законодательства Республики Беларусь.

Владелец программно-технических средств, информационных ресурсов, информационных систем и информационных сетей обязан:

осуществлять меры по защите информации;

исполнять другие обязанности в соответствии с настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 39. Права и обязанности информационного посредника. Информационный посредник обладает правами в соответствии с настоящим Законом и иными актами законодательства Республики Беларусь.

Информационный посредник обязан обеспечить предоставление информационных услуг обладателю и (или) пользователю информации по их запросам или в соответствии с условиями договора между информационным посредником и обладателем или пользователем информации либо уполномоченными ими лицами.

Информационному посреднику запрещается распространять и (или) предоставлять третьим лицам информацию, полученную при предоставлении информационных услуг, кроме случаев, предусмотренных законодательством Республики Беларусь.

Информационный посредник исполняет другие обязанности в соответствии с настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 40. Права и обязанности оператора информационной системы. Оператор информационной системы имеет право:

осуществлять эксплуатацию информационной системы в порядке и на условиях, определенных договором, заключенным с ее владельцем;

определять порядок эксплуатации информационной системы в случае, если он является ее владельцем;

осуществлять иные действия в соответствии с настоящим Законом и иными актами законодательства Республики Беларусь.

Оператор информационной системы обязан:

обеспечить целостность и сохранность информации, содержащейся в информационной системе;

принимать меры по предотвращению разглашения, утраты, искажения, уничтожения, модификации (изменения) информации и блокирования правомерного доступа к ней, а при необходимости – меры по восстановлению утраченной информации;

- исполнять другие обязанности в соответствии с настоящим Законом и иными законодательными актами Республики Беларусь.

Статья 41. Ответственность за нарушение законодательства об информации, информатизации и защите информации. Нарушение законодательства об информации, информатизации и защите информации влечет ответственность в соответствии с законодательными актами Республики Беларусь.

3.2. Вопросы для самоконтроля

1. Что определяет Закон «О государственных секретах Республики Беларусь»?
2. Какими правами обладают граждане Республики Беларусь в сфере государственных секретов?
3. Какие сведения не могут быть отнесены к государственным секретам?
4. Определите условия предоставления гражданам Республики Беларусь допуска к государственным секретам.
5. Какова сфера деятельности Закона «Об информации, информатизации и защите информации»?
6. Что в себя включает государственное регулирование в области информации, информатизации и защиты информации?
7. Какова ответственность граждан Республики Беларусь за нарушение требований законодательства об информации, информатизации и защите информации?

3.3. Практическая часть

Задание 1

Открыть программный модуль «Введение в информационную безопасность. Практические работы», расположенный на диске /D лабораторного компьютера. Перейти по вкладке «Разделы» в раздел «Практическая работа №3». Пройти тестирование по материалу изученной темы в разделе «Тест».

Задание 2

Пользуясь инструкцией к выполнению задания в разделе «Практика» программного модуля, выполнить задание.

ПРАКТИЧЕСКАЯ РАБОТА №4
ТЕХНИЧЕСКИЙ РЕГЛАМЕНТ РЕСПУБЛИКИ БЕЛАРУСЬ

Цель работы: изучить область применения технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY), требования к информационной безопасности различных объектов, с сертификацией и других средств защиты информации.

4.1. Теоретические сведения

Рассмотрим статьи 1–8 Постановления Совета Министров Республики Беларусь от 15 мая 2013 г. №375 «Технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) [13].

Статья 1. Область применения

1. Технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) распространяется на выпускаемые в обращение на территории Республики Беларусь средства защиты информации независимо от страны происхождения, за исключением средств шифрованной, других видов специальной связи и криптографических средств защиты государственных секретов.

2. Настоящим техническим регламентом устанавливаются требования к средствам защиты информации в целях защиты жизни и здоровья человека, имущества, а также предупреждения действий, вводящих в заблуждение потребителей (пользователей) относительно назначения, информационной безопасности и качества средств защиты информации.

3. До введения в действие настоящего технического регламента в отношении средств защиты информации, подлежащих согласно законодательству обязательному подтверждению соответствия, применяются правила, установленные Национальной системой подтверждения соответствия Республики Беларусь.

Статья 2. Термины и их определения

В настоящем техническом регламенте применяются следующие термины и их определения:

государственная информационная система – информационная система, создаваемая и (или) приобретаемая за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц;

защита информации – комплекс правовых, организационных и технических мер по обеспечению целостности, конфиденциальности, доступности и сохранности информации;

заявитель на подтверждение соответствия (далее – заявитель) – юридическое лицо Республики Беларусь, иностранное или международное юридическое лицо (организация, не являющаяся юридическим лицом), индивидуальный предприниматель, зарегистрированный в Республике Беларусь, иностранный гражданин или лицо без гражданства, обратившиеся с заявкой на получение сертификата соответствия, либо изготовитель (продавец), обратившийся с заявкой о регистрации принятой им декларации о соответствии;

изготовитель (продавец) – юридическое лицо Республики Беларусь или индивидуальный предприниматель, осуществляющие производство и (или) реализацию средств защиты информации либо представляющие на основании договора интересы иностранного или международного юридического лица (организации, не являющейся юридическим лицом), осуществляющего производство и (или) реализацию средств защиты информации, или интересы иностранного гражданина либо лица без гражданства, постоянно проживающих за пределами Республики Беларусь и осуществляющих производство и (или) реализацию продукции, в части обеспечения соответствия производимой и (или) реализуемой ими продукции требованиям технических нормативных правовых актов в области технического нормирования и стандартизации, либо открытое в установленном порядке на территории Республики Беларусь представительство иностранной организации, осуществляющей производство и (или) реализацию продукции;

импортер – резидент Республики Беларусь, который заключил с нерезидентом Республики Беларусь внешнеторговый договор на передачу средств защиты информации, осуществляет их реализацию и несет ответственность за их соответствие требованиям информационной безопасности;

испытательная лаборатория (центр) – юридическое лицо, аккредитованное для проведения испытаний продукции в определенной области аккредитации;

критические параметры – параметры, связанные с обеспечением безопасности, несанкционированное раскрытие или модификация которых снижает безопасность средства защиты информации или защищаемой им информации;

носитель информации – материальный объект, в котором информация находит свое отображение и (или) хранится;

обращение средств защиты информации на рынке – движение средств защиты информации от изготовителя к потребителю (пользователю), охватывающее все процессы, которые проходят средства защиты информации после завершения их производства;

объект информатизации – средства электронной вычислительной техники вместе с программным обеспечением, в том числе автоматизированные системы различного уровня и назначения, вычислительные сети и центры,

автономные стационарные и персональные электронные вычислительные машины, используемые для обработки информации;

применение по назначению – использование средств защиты информации в соответствии с назначением, указанным в эксплуатационных документах;

средства защиты информации – технические, программные, программно-аппаратные средства, предназначенные для защиты информации, а также средства контроля эффективности ее защищенности;

уполномоченный представитель изготовителя – резидент Республики Беларусь, назначенный изготовителем на осуществление действий от его имени при подтверждении соответствия и размещении средств защиты информации на рынке.

Статья 3. Правила размещения на рынке или ввода в эксплуатацию средств защиты информации

Средства защиты информации выпускаются в обращение на рынке в установленном порядке при их соответствии настоящему техническому регламенту, а также другим техническим регламентам, действие которых на них распространяется.

Средства защиты информации, соответствие которых требованиям настоящего технического регламента не подтверждено, не должны быть маркированы знаком соответствия техническому регламенту согласно ТКП 5.1.08-2012 «Национальная система подтверждения соответствия Республики Беларусь. Знаки соответствия. Описание и порядок применения» (далее – ТКП 5.1.08-2012) и не допускаются к выпуску в обращение на рынке.

Статья 4. Требования информационной безопасности

1. Средства защиты информации должны быть разработаны и изготовлены таким образом, чтобы, применяя их по назначению и выполняя требования к эксплуатации и техническому обслуживанию, они обеспечивали:

выполнение функций в соответствии с эксплуатационными документами;

защиту от несанкционированного раскрытия и (или) модификации критических параметров;

контроль целостности конфигурации;

самотестирование;

контроль доступа к функциям управления и настройкам;

сохранение работоспособности при обработке некорректных данных.

2. Наименование и (или) обозначение средств защиты информации (тип, марка, модель), их параметры и характеристики, наименование и (или) товарный знак изготовителя, наименование страны-изготовителя должны быть нанесены непосредственно на средства защиты информации либо их носители, а также указаны в прилагаемых к ним эксплуатационных документах.

3. Если сведения, приведенные в пункте 2 настоящей статьи, невозможно нанести непосредственно на средства защиты информации или их носители, то они могут указываться только в эксплуатационных документах, прилагаемых к средствам защиты информации. При этом наименование изготовителя и (или)

его товарный знак, наименование и обозначение средств защиты информации (тип, марка, модель) должны быть нанесены на упаковку.

4. Маркировка средств защиты информации должна быть разборчивой и нанесена на доступную для осмотра поверхность средств защиты информации или их носители.

5. Эксплуатационные документы средств защиты информации должны включать:

информацию, перечисленную в пункте 2 настоящей статьи;

информацию о назначении средств защиты информации;

основные потребительские свойства или характеристики;

правила и условия безопасной эксплуатации (использования);

правила и условия хранения, перевозки, реализации, монтажа и утилизации (при необходимости установления требований к ним);

информацию о мерах, которые следует предпринять при обнаружении неисправности;

местонахождение изготовителя, информацию для связи с ним;

наименование и местонахождение уполномоченного представителя изготовителя, импортера, информацию для связи с ним;

дату изготовления средств защиты информации;

обязательства изготовителя (уполномоченного представителя изготовителя) по установке, сопровождению и поддержке средств защиты информации.

6. Маркировка и эксплуатационные документы выполняются на государственных языках Республики Беларусь – белорусском и (или) русском.

Статья 5. Обеспечение соответствия требованиям информационной безопасности

1. Соответствие средств защиты информации настоящему техническому регламенту обеспечивается выполнением требований информационной безопасности технического регламента непосредственно либо выполнением требований взаимосвязанных государственных стандартов.

2. Перечень взаимосвязанных с настоящим техническим регламентом государственных стандартов (далее – перечень стандартов) определяет Оперативно-аналитический центр при Президенте Республики Беларусь.

3. Методы исследований (испытаний) средств защиты информации устанавливаются в государственных стандартах, включенных в перечень стандартов, содержащих правила и методы исследований (испытаний), в том числе правила отбора образцов, необходимые для применения и исполнения требований настоящего технического регламента и осуществления оценки (подтверждения) соответствия продукции.

Статья 6. Подтверждение соответствия требованиям информационной безопасности

1. Процедуры подтверждения соответствия средств защиты информации требованиям информационной безопасности выполняются согласно требованиям Национальной системы подтверждения соответствия Республики Беларусь.

2. Перед выпуском в обращение на рынке средства защиты информации должны быть подвергнуты процедуре подтверждения соответствия требованиям информационной безопасности настоящего технического регламента в форме сертификации или декларирования соответствия.

3. Подтверждению соответствия требованиям информационной безопасности настоящего технического регламента путем сертификации подлежат средства защиты информации, которые будут использоваться для:

технической защиты государственных секретов;

создания систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено;

создания систем безопасности критически важных объектов информатизации;

обеспечения целостности и подлинности электронных документов в государственных информационных системах.

Требования информационной безопасности настоящего технического регламента, на соответствие которым осуществляется сертификация, определяются Оперативно-аналитическим центром при Президенте Республики Беларусь в зависимости от специфики средств защиты информации.

4. Подтверждение соответствия требованиям информационной безопасности настоящего технического регламента средств защиты информации, за исключением указанных в пункте 3 настоящей статьи, осуществляется изготовителем – юридическим лицом Республики Беларусь или уполномоченным представителем изготовителя, зарегистрированным в установленном порядке на территории Республики Беларусь, или импортером путем декларирования соответствия.

5. Сертификацию средств защиты информации, указанных в пункте 3 настоящей статьи, проводит аккредитованный орган по сертификации согласно схемам:

схема 1с – для серийно выпускаемой продукции;

схема 2с – для серийно выпускаемой продукции при наличии у изготовителя сертифицированных в Национальной системе подтверждения соответствия Республики Беларусь системы управления качеством и (или) системы управления безопасностью продукции;

схема 3с – для партии продукции;

схема 4с – для единичного изделия.

6. Средства защиты информации для подтверждения соответствия представляет заявитель.

7. При проведении аккредитованным органом по сертификации работ по подтверждению соответствия средств защиты информации, указанных в пункте 3 настоящей статьи:

7.1. аккредитованный орган по сертификации:

проводит анализ документов, представленных заявителем;

заключает договор на проведение работ по подтверждению соответствия;

проводит идентификацию средств защиты информации и отбор образцов для испытаний;

организует проведение испытаний образца (образцов) средств защиты информации в аккредитованной испытательной лаборатории на соответствие требованиям настоящего технического регламента и взаимосвязанных с настоящим техническим регламентом государственных стандартов (при сертификации на соответствие СТБ 34.101.1-2004 «Информационные технологии и безопасность».

Критерии оценки безопасности информационных технологий.

Часть 1. «Введение и общая модель» (далее – СТБ 34.101.1-2004), СТБ 34.101.2-2004 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий».

Часть 2. «Функциональные требования безопасности» (далее – СТБ 34.101.2-2004), СТБ 34.101.3-2004 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий».

Часть 3. Гарантийные требования безопасности (далее – СТБ 34.101.3-2004) в качестве основы для оценки средств защиты информации используется задание по безопасности);

проводит анализ состояния производства (схема 1с) или рассмотрение документов, подтверждающих наличие сертифицированных в Национальной системе подтверждения соответствия Республики Беларусь системы управления качеством и (или) системы управления безопасностью продукции (схема 2с);

выдает сертификат соответствия настоящему техническому регламенту в рамках Национальной системы подтверждения соответствия Республики Беларусь;

заключает с заявителем соглашение по сертификации (схемы 1с, 2с);

осуществляет инспекционный контроль за сертифицированной продукцией (схемы 1с, 2с);

7.2. заявитель:

подает заявку на проведение работ по сертификации продукции с комплектом документов, который включает:

технические условия (при наличии);

задание по безопасности и протокол его оценки в испытательной лаборатории (при сертификации на соответствие требованиям СТБ 34.101.1-2004, СТБ 34.101.2-2004, СТБ 34.101.3-2004);

эксплуатационные документы;

перечень взаимосвязанных с настоящим техническим регламентом государственных стандартов, требованиям которых соответствует средство защиты информации (при их применении изготовителем);

протокол (протоколы) испытаний, проведенных в аккредитованных испытательных лабораториях;

копии сертификатов на систему управления качеством и (или) систему управления безопасностью продукции (при наличии);

заключает договор на проведение работ по сертификации продукции;

предоставляет продукцию для проведения идентификации (схемы 1с, 2с, 3с, 4с) и отбора образцов для испытаний (схемы 1с, 3с);

создает условия для проведения анализа состояния производства (схема 1с);

заключает с аккредитованным органом по сертификации соглашение по сертификации (схемы 1с, 2с);

создает условия для проведения инспекционного контроля за сертифицированной продукцией (схемы 1с, 2с);

7.3. аккредитованная испытательная лаборатория:

заключает договор на проведение испытаний;

проводит испытания продукции.

Аккредитованный орган по сертификации имеет право запросить дополнительную техническую (конструкторскую) документацию (тексты и описания программных средств, методики и программы испытаний, спецификации, сборочные чертежи, чертежи сборочных единиц и деталей, электрические схемы или иные документы, согласно которым изготавливается средство защиты информации), необходимую для подтверждения соответствия средства защиты информации требованиям информационной безопасности настоящего технического регламента.

8. Подтверждение соответствия средств защиты информации, указанных в пункте 4 настоящей статьи, проводится путем декларирования соответствия по одной из схем:

при принятии заявителем декларации о соответствии на основании собственных доказательств:

схема 1д – для серийно выпускаемой продукции;

схема 2д – для партии продукции (единичного изделия);

при принятии заявителем декларации о соответствии на основании собственных доказательств и доказательств, полученных с участием аккредитованного органа по сертификации и (или) аккредитованной испытательной лаборатории:

схема 3д – для серийно выпускаемой продукции;

схема 4д – для партии продукции (единичного изделия);

схема 6д – для серийно выпускаемой продукции при наличии у изготовителя сертифицированных в Национальной системе подтверждения соответствия Республики Беларусь системы управления качеством и (или) системы управления безопасностью продукции.

Применяя указанные схемы:

8.1. аккредитованный орган по сертификации:

заключает договор на проведение работ по подтверждению соответствия (регистрация декларации о соответствии);

проводит анализ представленной заявителем декларации о соответствии;

регистрирует декларацию о соответствии;

8.2. заявитель:

формирует документы, подтверждающие соответствие продукции установленным требованиям и правомочность принятия декларации о соответствии;

осуществляет контроль в процессе производства продукции (схемы 1д, 3д, 6д);

проводит испытания продукции (схемы 1д, 2д, 6д);

принимает декларацию о соответствии;

предоставляет продукцию для испытаний (схемы 3д, 4д, 6д);

подает заявление на регистрацию декларации о соответствии;

заключает договор на проведение работ по подтверждению соответствия (регистрация декларации о соответствии) (схемы 1д, 2д, 3д, 4д, 6д) и испытаний (схемы 3д, 4д, 6д);

8.3. аккредитованная испытательная лаборатория:

заключает договор на проведение испытаний (схемы 3д, 4д, 6д);

проводит испытания продукции (схемы 3д, 4д, 6д).

9. Изготовитель осуществляет производственный контроль и принимает все необходимые меры, для того чтобы процесс производства обеспечивал соответствие средств защиты информации требованиям настоящего технического регламента.

Требования к процессам производства и контроля, а также результаты их контроля должны быть оформлены документально.

10. На территории Республики Беларусь должен храниться комплект документов на:

средства защиты информации – у изготовителя (уполномоченного изготовителем лица) в течение не менее 10 лет со дня снятия с производства (прекращения производства) средств защиты информации;

партию средств защиты информации – у импортера в течение не менее 10 лет со дня реализации последнего изделия из партии.

Комплект документов должен предоставляться органам государственного надзора по их требованию согласно законодательству.

Статья 7. Маркировка знаком соответствия

1. Средства защиты информации, соответствующие требованиям информационной безопасности и прошедшие процедуру подтверждения соответствия согласно статье 6 настоящего технического регламента, должны маркироваться знаком соответствия техническому регламенту согласно ТКП 5.1.08-2012.

2. Маркировка средств защиты информации знаком соответствия техническому регламенту осуществляется перед их выпуском в обращение на рынке.

3. Знак соответствия техническому регламенту наносится любым способом, обеспечивающим четкое и ясное изображение в течение всего срока службы средств защиты информации, на:

каждую единицу технических и программно-аппаратных средств защиты информации;

каждый носитель информации программных средств защиты информации;

упаковку.

4. Маркировка средств защиты информации знаком соответствия техническому регламенту свидетельствует о соответствии данных средств требованиям всех технических регламентов, распространяющих на них свое действие и предусматривающих нанесение этого знака соответствия.

Статья 8. Государственный надзор за соблюдением настоящего технического регламента

Государственный надзор за соблюдением настоящего технического регламента осуществляется в порядке, установленном законодательством.

4.2. Вопросы для самоконтроля

1. Какие требования к средствам защиты информации устанавливаются техническим регламентом Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY)?
2. Какие параметры называются критическими?
3. Что относится к средствам защиты информации и что они должны обеспечивать?
4. Что должны включать в себя эксплуатационные документы средств защиты информации?
5. Какие средства защиты информации подлежат подтверждению соответствия требованиям информационной безопасности настоящего технического регламента?

4.3. Практическая часть

Задание 1

Используя программный модуль «Введение в информационную безопасность. Практические работы», выполнить предлагаемый тест в разделе «Тест» и задание в разделе «Практика». Открыть программный модуль «Введение в информационную безопасность. Практические работы», расположенный на диске /D лабораторного компьютера. Перейти по вкладке «Разделы» в раздел «Практическая работа №4». Пройти тестирование по материалу изученной темы в разделе «Тест».

Задание 2

Согласно полученному варианту, указанному в табл. 1, провести анализ средств защиты информации и определить их соответствие установленным требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY).

В соответствии с заданием определить:

- соответствие требованиям информационной безопасности (ст.4 ТР 2013/027/BY);
- необходимость подтверждения соответствия требованиям информационной безопасности путем сертификации (ст.6 ТР 2013/027/BY).

Таблица 1

Варианты для выполнения задания 2

Номер варианта	Наименование продукции	Дополнительные сведения
1	2	3
1	Антивирусное программное обеспечение ESET NOD32 Business Edition версии 4.2 для операционных систем Microsoft Windows 7 (32- и 64-разрядные версии) и XP (32- и 64-разрядные версии), Microsoft Windows Server 2003, 2008	Разработано и изготовлено в соответствии со всеми требованиями эксплуатации и ТО. Требуемая маркировка, параметры и характеристики указаны только в эксплуатационной документации, которая представлена в полном объеме на русском языке
2	Устройство защиты цепей электросети и заземления «ГНОМ-3Мс»	Разработано и изготовлено в соответствии со всеми требованиями эксплуатации и ТО. Требуемая маркировка, параметры и характеристики указаны на внутренней поверхности устройства
3	Модуль шифрования IP-пакетов «IPSecVPN.sys» (РБ.КМАС.00035-02) программного средства криптографической защиты информации BelIPSec v2.0 (РБ.КМАС.00023-02)	Разработано и изготовлено в соответствии со всеми требованиями эксплуатации и ТО. Предполагается использовать для серийного выпуска, поэтому заявитель не предоставил условия для проведения инспекционного контроля за сертифицированной продукцией
4	«Средства программные. Пакет прикладных программ КАНЦЛЕР», версия 4.0	Разработано и изготовлено в соответствии со всеми требованиями эксплуатации и ТО. Требуемая маркировка, параметры и характеристики указаны только в эксплуатационной документации, которая представлена в полном объеме на русском языке, отсутствуют обязательства изготовителя по сопровождению СЗИ
5	Фильтр-ограничитель	Разработано и изготовлено в соответствии со всеми требованиями эксплуатации и ТО. Требуемая маркировка, параметры и характеристики указаны только на поверхности устройства на русском языке

Продолжение табл. 1

1	2	3
6	Программный комплекс электронной цифровой подписи, используемый в автоматизированной системе межбанковских расчетов. Библиотека AvAsSign (РБ.ЮСКИ.09040-02)	Разработано и изготовлено в соответствии со всеми требованиями эксплуатации и ТО. В заявленных документах отсутствует перечень заявленных государственных стандартов, которым соответствует средство ЗИ
7	Программное средство криптографической защиты информации «En_TMS54_crypto» (РБ.АСРМ.00150-01)	Разработано и изготовлено в соответствии со всеми требованиями эксплуатации и ТО. Требуемая маркировка, параметры и характеристики указаны в эксплуатационной документации, которая представлена в полном объеме на английском языке
8	Антивирусное программное средство «Kaspersky Internet Security 2011» для операционной системы Windows 7	Разработано и изготовлено в соответствии со всеми требованиями эксплуатации и ТО. Требуемая маркировка, параметры и характеристики указаны только в эксплуатационной документации, которая представлена в полном объёме на русском языке. Требует подтверждения соответствия требованиям ИБ настоящего технического регламента
9	Фильтр сетевой помехоподавляющий ФПГ-2	Разработано и изготовлено в соответствии со всеми требованиями эксплуатации и ТО. Требуемая маркировка, параметры и характеристики указаны на поверхности СЗИ на русском языке. Предполагается использование на критически важных объектах информатизации
10	Программный комплекс «InfoWatch Traffic Monitor Enterprise Editor»	Разработано и изготовлено в соответствии со всеми требованиями эксплуатации и ТО. Требуемая маркировка, параметры и характеристики указаны только в эксплуатационной документации, которая представлена в полном объёме на английском языке. Предполагается использование в качестве единичного изделия

Окончание табл. 1

1	2	3
11	Генератор линейного зашумления «Рокот»	Разработано и изготовлено в соответствии со всеми требованиями эксплуатации и ТО. Требуемая маркировка, параметры и характеристики указаны только в эксплуатационной документации, которая представлена в полном объеме на русском языке. Заявитель требует проведения испытания продукции
12	Программное средство электронной цифровой подписи и шифрования «AvCrypt.DLL ver.4.0» (РБ.ЮСКИ.06011-01)	Разработано и изготовлено в соответствии со всеми требованиями эксплуатации и ТО. Требуемая маркировка, параметры и характеристики указаны только в эксплуатационной документации, которая представлена в полном объеме на русском языке
13	Программный продукт «Библиотека криптографических преобразований CRYPTOCONT» (СЮИК.00318-01)	Разработано и изготовлено в соответствии со всеми требованиями эксплуатации и ТО. У заявителя отсутствует договор на проведение работ по сертификации продукции
14	Многофункциональное устройство Cisco Adaptive Securite Appliance 5525-X (ASA 5525-X) с программным обеспечением Cisco Adaptive Securite Appliance Software версии 9.0	Разработано и изготовлено в соответствии со всеми требованиями эксплуатации и ТО. Требуемая маркировка, параметры и характеристики указаны только в эксплуатационной документации, которая представлена в полном объеме на английском языке
15	Маршрутизатор HP MSR20-20 Router	Разработано и изготовлено в соответствии со всеми требованиями эксплуатации и ТО. Требуемая маркировка, параметры и характеристики указаны только в эксплуатационной документации, которая представлена в полном объеме на русском языке. Предполагается выпуск в серийное производство

ПРАКТИЧЕСКАЯ РАБОТА №5
КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ОБЪЕКТОВ

Цель работы: изучить угрозы информационной безопасности для различных объектов информатизации; научиться анализировать угрозы безопасности для объекта информатизации в соответствии с заданием преподавателя.

5.1. Теоретические сведения

Информационный объект – это среда, в которой информация создается, обрабатывается, хранится и передается.

Под угрозой информационной безопасности объекта понимаются возможные воздействия на него, приводящие к ущербу.

По своей общей направленности угрозы информационной безопасности Республики Беларусь подразделяются на следующие виды:

1. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению Республики Беларусь. Этими угрозами являются:

- принятие органами государственной власти субъектов Республики Беларусь нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;
- создание монополий на формирование, получение и распространение информации в Республике Беларусь, в том числе с использованием телекоммуникационных систем;
- противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;
- нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;
- противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;
- неисполнение федеральными органами государственной власти, органами государственной власти субъектов Республики Беларусь, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;
- неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Республики Беларусь, органов

местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации;

- дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;

- нарушение конституционных прав и свобод человека и гражданина в области массовой информации;

- вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни Республики Беларусь от зарубежных информационных структур;

- девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в нашем обществе;

- снижение духовного, нравственного и творческого потенциала населения Республики Беларусь, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;

- манипулирование информацией (дезинформация, сокрытие или искажение информации).

2. Угрозы информационному обеспечению государственной политики Республики Беларусь:

- монополизация информационного рынка Республики Беларусь, его отдельных секторов отечественными и зарубежными информационными структурами;

- блокирование деятельности государственных средств массовой информации по информированию аудитории;

- низкая эффективность информационного обеспечения государственной политики Республики Беларусь вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

3. Угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов:

- противодействие доступу Республики Беларусь к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости Республики Беларусь в области современных информационных технологий;

- закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;

- вытеснение с отечественного рынка белорусских производителей средств информатизации, телекоммуникации и связи;

- увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

4. Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории Республики Беларусь. Ими могут являться:

- противоправные сбор и использование информации;

- нарушения технологии обработки информации;

- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств или систем обработки информации, телекоммуникации и связи;

- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации, компрометация ключей и средств криптографической защиты информации;

- утечка информации по техническим каналам;

- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;

- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;

- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии белорусской информационной инфраструктуры;

- несанкционированный доступ к информации, находящейся в банках и базах данных;

- нарушение законных ограничений на распространение информации.

Источники угроз информационной безопасности

Носителями угроз безопасности информации являются источники угроз. В качестве источников угроз могут выступать как субъекты (личность) так и объективные проявления.

Все источники угроз информационной безопасности можно разделить на три основные группы (рис. 1).

I. Обусловленные действиями субъекта (антропогенные источники), которые могут привести к нарушению безопасности информации. Данные действия могут быть квалифицированы как умышленные (преднамеренные) или случайные (непреднамеренные) преступления.

1. Непреднамеренные угрозы на объект информатизации (ОИ):

- неумышленные действия, приводящие к частичному или полному отказу или разрушению технических, программных, информационных ресурсов ОИ;
- неумышленная порча оборудования, удаление, искажение файлов с защищаемой информацией или программ, в том числе системных;
- неправомерное отключение оборудования или изменение режимов работы устройств и программ;
- неумышленная порча носителей информации;
- запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности ОИ или его компонент (зависания или зацикливания) или осуществляющих необратимые изменения (форматирование или реструктуризацию машинных носителей информации (МНИ), удаление данных и т. п.);
- нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
- заражение ПЭВМ компьютерными вирусами;
- неосторожные действия, приводящие к разглашению защищаемой информации или делающие ее общедоступной;
- разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей, идентификационных карточек, пропусков и т. п.);
- проектирование архитектуры объекта информатизации (ОИ), технологии обработки данных, разработка прикладных программ с использованием возможностей, представляющих опасность для работоспособности ОИ и средств защиты информации (СЗИ) от несанкционированного доступа (НСД);
- игнорирование организационных ограничений (установленных правил) при работе на ОИ;
- вход в локально-вычислительные сети (ЛВС) в обход средств защиты (например, загрузка посторонней операционной системы со сменных МНИ);

- некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;

- пересылка данных по ошибочному адресу абонента (устройства);

- ввод ошибочных данных;

- неумышленное повреждение информационных линий связи.

2. Преднамеренные угрозы на ОИ:

- физическое разрушение ОИ (путем взрыва, поджога и т. п.) или вывод из строя отдельных наиболее важных компонент (устройств, носителей важной системной информации и т. п.);

- отключение или вывод из строя подсистем обеспечения функционирования ОИ (электропитания, охлаждения и вентиляции, линий связи);

- действия по дезорганизации функционирования ОИ (изменение режимов работы устройств или программ);

- вербовка (путем подкупа, шантажа и т. п.) персонала или отдельных пользователей ОИ, имеющих определенные полномочия;

- применение устройств дистанционной фото- и видеосъемки;

- перехват данных, передаваемых по информационным линиям связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения на ОИ;

- хищение технических средств и носителей информации (системных блоков ПЭВМ, МНИ, запоминающих устройств);

- несанкционированное копирование носителей информации, включая МНИ;

- хищение производственных отходов (распечаток, записей, списанных МНИ);

- чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств ПЭВМ;

- чтение информации из областей оперативной памяти, используемых операционной системой (в том числе СЗИ от НСД) или другими пользователями, в асинхронном режиме благодаря недостаткам многозадачных операционных систем и систем программирования;

- незаконное получение паролей и других реквизитов разграничения доступа (из-за халатности пользователей, путем подбора, путем имитации интерфейса обмена) с последующей маскировкой под зарегистрированного пользователя («маскарад»);

- несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи;

- внедрение вредоносного программного кода («закладок», «вирусов», «троянских коней», «кейлогеров», «жучков»), т. е. такого исполняемого кода, который не нужен для осуществления заявленных функций, но позволяет преодолевать систему защиты, скрытно и незаконно осуществлять доступ к

системным ресурсам с целью регистрации и передачи защищаемой информации или дезорганизации функционирования ОИ;

- незаконное подключение к информационным линиям связи с целью работы «между строк», с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;

- незаконное подключение к информационным линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в ЛВС и успешной аутентификации с последующим вводом и навязыванием ложных сообщений;

- воздействие на технические и программные средства в целях нарушения пути доставки и своевременности информационного обмена в ЛВС.

Источники, действия которых могут привести к нарушению безопасности информации, бывают как внешними, так и внутренними. Данные источники можно спрогнозировать и принять адекватные меры.

II. Обусловленные техническими средствами (техногенные источники). Эти источники угроз менее прогнозируемы и напрямую зависят от свойств техники и поэтому требуют особого внимания. Данные источники угроз информационной безопасности также могут быть как внутренними, так и внешними.

III. Стихийные источники. Данная группа объединяет обстоятельства, составляющие непреодолимую силу (стихийные бедствия или другие обстоятельства, которые невозможно предусмотреть или предотвратить или возможно предусмотреть, но невозможно предотвратить). Эти обстоятельства носят объективный и абсолютный характер, распространяющийся на всех. Такие источники угроз совершенно не поддаются прогнозированию, и поэтому меры против них должны применяться всегда. Стихийные источники как правило, являются внешними по отношению к защищаемому объекту и под ними, как правило, понимаются природные катаклизмы.

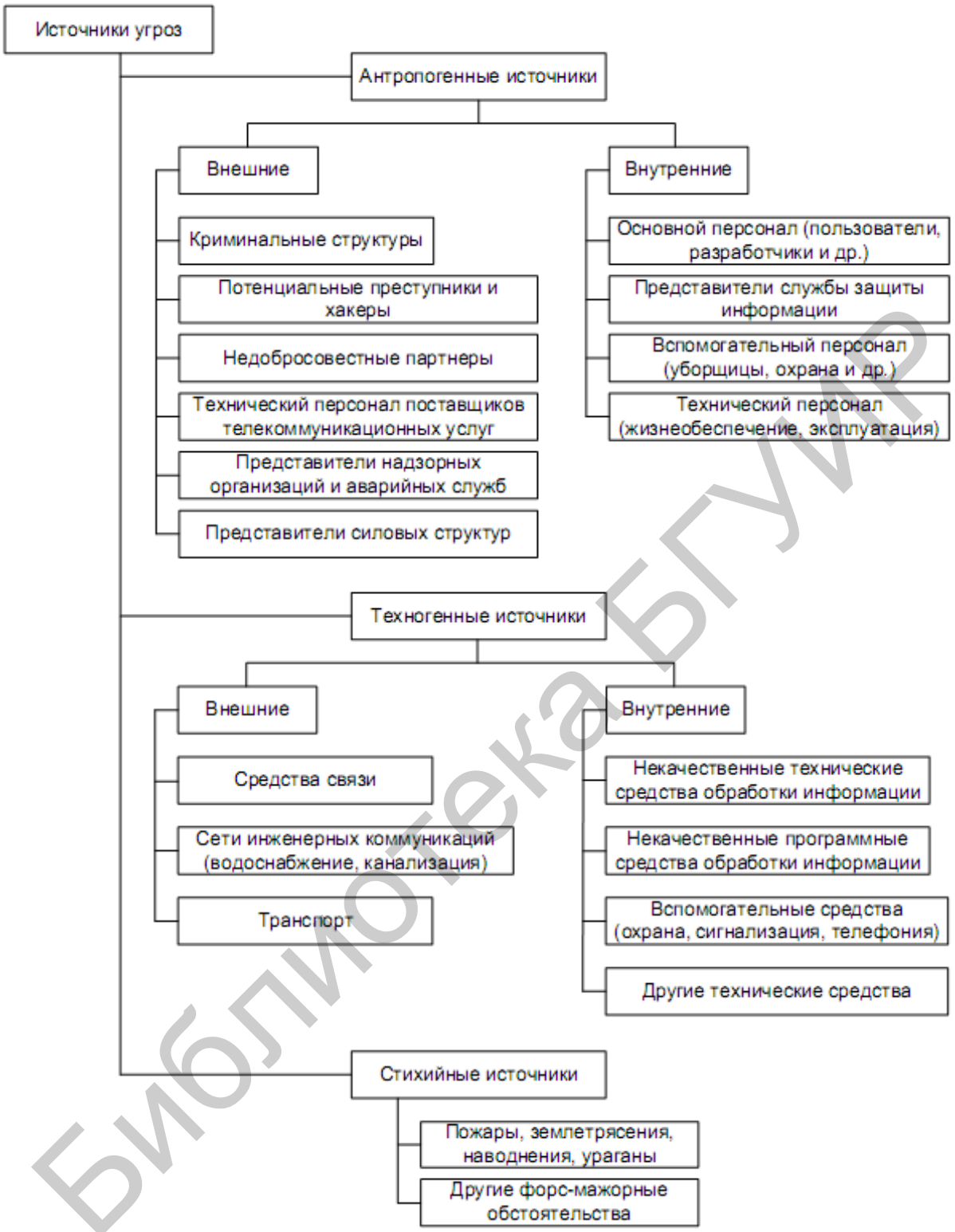

Рис. 1. Классификация источников угроз

5.2. Контрольные вопросы

1. Что принято называть угрозой информационной безопасности?
2. Какова классификация методов защиты информации, в том числе по характеру проводимых мероприятий?
3. Какова классификация угроз информационной безопасности?
4. Что понимается под термином «информационный объект»?
5. Что представляет собой угроза права собственности?

5.3. Практическая часть

Задание 1

Используя программный модуль «Введение в информационную безопасность. Практические работы», выполнить предлагаемый тест в разделе «Тест» и задание в разделе «Практика». Открыть программный модуль «Введение в информационную безопасность. Практические работы», расположенный на диске /D лабораторного компьютера. Перейти по вкладке «Разделы» в раздел «Практическая работа №5». Пройти тестирование по материалу изученной темы в разделе «Тест».

Задание 2

Используя программный модуль «Введение в информационную безопасность. Практические работы», выполнить предлагаемый тест в разделе «Практическая работа №5».

ПРАКТИЧЕСКАЯ РАБОТА №6
ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Цель работы: получить практические навыки по созданию сценария инженерно-технической защиты информации в кабинете руководителя организации.

6.1. Теоретическая часть

Сценарий инженерно-технической защиты информации в кабинете руководителя организации

Сценарий предназначен для формирования на практических занятиях навыков по обеспечению защиты информации в кабинете руководителя организации. Рассматриваются все основные этапы и процедуры защиты информации:

- описание кабинета руководителя как наиболее сложного объекта защиты;
- описание угроз информации в кабинете руководителя организации;
- выбор рациональных мер по защите информации в кабинете руководителя организации.

I. Описание кабинета руководителя организации как наиболее сложного объекта защиты

1. Выбор кабинета как объекта защиты обусловлен следующими факторами:

- в кабинете руководителя циркулирует наиболее ценная информация организации;
- кабинет посещают сотрудники организации всех должностных категорий по служебным и личным вопросам, а также посетители организации;
- в кабинете, как правило, размещаются различные радио- и электрические приборы, которые могут быть источниками побочных электромагнитных излучений и наводок;
- в кабинете во время докладов и совещаний проводится демонстрация продукции, документов, плакатов, аудио- и видеоматериалов;
- в кабинете много элементов интерьера и мебели, в которой легко спрятать закладные устройства.

Кабинет руководителя, как правило, граничит с приемной и другими служебными помещениями. В приемной возможно длительное присутствие посторонних лиц (сотрудников и посетителей), ожидающих приема. В результате недостаточной защиты информации в кабинете (например из-за слабой звукоизоляции стены), относительно частого открывания двери в кабинет, продолжения в приемной разговора на служебные темы выходящих из кабинета людей, работа секретаря с документами в присутствии находящихся в

приемной людей могут создать реальные предпосылки для утечки информации из приемной.

Во время совещания с участием представителей других организаций или беседы руководителя с посетителями последние могут попытаться записать конфиденциальный разговор с помощью скрытой записи на диктофон или закладного устройства с целью последующего использования этой информации во вред руководителю организации или организации в целом.

Здание, в котором находится кабинет, как правило, окружено другими административными и жилыми домами, через окна или с крыши которых возможно наблюдение за источниками информации в кабинете, а также возможен перехват из кабинета радиосигналов закладных устройств и побочных электромагнитных излучений и наводок.

Следовательно, кабинет представляет собой объект защиты, в котором, с одной стороны, циркулирует наиболее ценная информация, а с другой стороны, возможен доступ в него всех категорий сотрудников и посетителей, в том числе тех, которые могут заниматься добыванием информации.

2. Характеристика информации, защищаемой в кабинете руководителя

Виды информации в кабинете руководителя

В кабинете руководителя на различных носителях могут находиться почти все виды защищаемой в организации информации, в том числе:

- семантическая информация в документах, с которыми работает руководитель или которые приносят его заместители, другие сотрудники, представители других организаций, а также на чертежах и плакатах, развешиваемых на стенах или проецируемых во время докладов или совещаний;
- семантическая информация во время конфиденциального разговора руководителя с посетителями и выступлений участников совещания;
- информация о видовых признаках VIP-персон, посещающих руководителя и по характеру деятельности которых можно определить тематику обсуждаемых вопросов;
- видовые демаскирующие признаки продукции, макетов и опытных образцов, которые демонстрируются руководителю на разных этапах их производства, а также их изображения на плакатах, экранах видеопроектора или телевизора;
- демаскирующие признаки веществ, приносимых руководителю для демонстрации соответствующей продукции, а также образцы исходных материалов.

Таким образом, основными видами информации в кабинете руководителя являются: речевая информация, семантическая, информация на плакатах, экране видеопроектора, информация о видовых демаскирующих признаках продукции.

Источники информации в кабинете руководителя

Основными источниками информации в кабинете руководителя являются:

- руководитель организации;
- должностные лица организации, посещающие кабинет;
- представители других организаций, с которыми руководитель обменивается секретной (конфиденциальной) информацией в ходе встреч или совещаний;
- посетители во время приема по личным вопросам, разговор с которыми может содержать сведения, содержащие коммерческую или иную тайну;
- документы на столах, плакаты на стенах, аудио- и видеодокументы;
- приносимая в кабинет продукция, сведения о которой и ее демаскирующие признаки содержат государственную, коммерческую или иную тайну;
- приносимые в кабинет материалы и продукция в виде веществ, информация о составе и технологии изготовления которых защищается.

Характеристика информации и ее источников дана в табл. 2.

Продукция, сигналы которой содержат защищаемые сигнальные признаки, во время ее демонстрации в кабинете не включается во избежание утечки информации. Поэтому информация о сигнальных демаскирующих признаках разрабатываемой продукции в сценарии не рассматривается.

При определении цены защищаемой в кабинете руководителя информации используется шкала с 5 градациями: очень высокая, высокая, средняя, низкая, очень низкая. Для понимания значений шкалы уточним граничные значения:

- очень высокая – цена информации, утечка которой может нанести государству очень большой ущерб или привести к банкротству фирмы;
- очень низкая – цена информации, потеря которой не имеет последствий.

С учетом этого остальные значения цены информации обозначают следующее:

- высокая – цена информации, утечка которой может нанести государству большой ущерб или заметно ухудшить финансовое состояние фирмы;
- средняя – цена информации, потеря которой может привести к существенным для государства и фирмы финансово-экономическим потерям, но может компенсироваться внутренними резервами фирмы;
- низкая – цена информации, утечка которой приводит к малым потерям.

Виды информации в кабинете и соответствующие им значения цены указаны в табл. 2.

Таблица 2

Характеристика информации и ее источников

Вид информации в кабинете	Источник информации	Максимальная цена информации	Место нахождения информации в кабинете
Семантическая документальная	Документы	Очень высокая	В сейфе, на столах, стене, плакатах, доске, экране монитора или видеопроектора
Семантическая речевая акустическая	Люди	Очень высокая	В кабинете
Семантическая речевая, читаемая по губам	Люди	Средняя	В кабинете
Видовые признаки	Продукция	Средняя	На столе, стене, плакатах, доске, экране монитора или видеопроектора
То же	Люди	Низкая	В кабинете
»	Вещества и материалы	Очень низкая	На столах
Вещественные признаки	Продукция химического производства	Средняя	На столах
	Продукция других производств	Низкая	На столах
То же	Материалы	Очень низкая	На столах

Для государственных структур признаком цены информации может служить ее гриф секретности: «чрезвычайной важности» – чрезвычайно высокая, «совершенно секретно» – очень высокая, «секретно» – высокая, для «служебного пользования» – низкая.

Наибольшую цену имеет семантическая документальная информация. Цена информации о видовых или вещественных признаках зависит от их информативности. На предприятиях химической и смежных сфер промышленности цена информации о вещественных признаках продукции может быть высокой, т. к. состав веществ и технология их изготовления для этих предприятий является основной государственной или коммерческой тайной. Для машиностроительных предприятий цена такой информации низкая. Но могут быть исключения, например, если существенное улучшение параметров продукции достигнуто за счет применения новых материалов.

При формировании табл. 2 очень важно указать все места нахождения источников информации в кабинете, т. к. они могут существенно влиять на величину угрозы канала утечки. Например, если документ находится на столе, то возможности его наблюдения через окно весьма ограничены; если он в виде плаката повешен на стену напротив окна, то риск наблюдения резко возрастает.

II. Описание угроз информации в кабинете руководителя организации

Информация в кабинете подвергается угрозам воздействия и утечки. Эти потенциальные угрозы существуют всегда, но возможность их резко возрастает, когда злоумышленник пытается проникнуть в организацию или вербует сотрудника, возникает очаг пожара или проявляются достаточно информативные признаки технических каналов утечки информации.

1. Описание угроз воздействия на источники информации

При описании угроз воздействия прогнозируются маршруты движения злоумышленника из нулевого состояния вне территории организации к источникам информации в кабинете руководителя, оцениваются параметры (вероятность и время реализации) участков маршрутов (дуг семантической сети). По ним оценивается ущерб и ранг угроз.

Способы проникновения злоумышленника в кабинет руководителя зависят от «квалификации» злоумышленника, модели объектов защиты и времени проникновения.

В данном сценарии рассматривается вариант проникновения «квалифицированного» злоумышленника, который имеет в организации сообщника без специальной подготовки.

Время проникновения целесообразно разделить на рабочее и нерабочее время организации. Рабочее время характеризуется следующими условиями: пропуск людей и автотранспорта производится через контрольно-пропускной пункт (КПП) по пропускам, извещатели технических средств охраны на территории и в здании выключаются, входная дверь в административное здание, в котором размещается кабинет руководителя, открывается для свободного прохода.

В рабочее время несанкционированное проникновение в организацию возможно через КПП по фальшивым документам и через забор. Хотя второй способ проникновения в рабочее время маловероятен, полностью исключить его нельзя. В рабочее время проникнуть в кабинет может как «чужой» злоумышленник, так и сотрудник организации. Очевидно, что сотруднику сделать это проще. Проникновение возможно при открытых и закрытых дверях кабинета и приемной, но наиболее легкий вариант для злоумышленника – обе двери открыты. Такой вариант в принципе возможен, когда руководитель уходит или выходит из кабинета, а секретарь выходит из приемной, не закрыв оба кабинета. Более частый вариант – дверь кабинета закрыта, а в приемную – открыта.

Во внерабочее время проникновение злоумышленника в организацию возможно через забор, а также через окно и дверь здания, примыкающего к тротуару.

Если злоумышленник имеет предварительную информацию о расположении и типах средств охраны и видеоконтроля, он может попытаться проникнуть в кабинет во внерабочее время путем скрытого преодоления в ночное время рубежей и зон безопасности или спрятавшись в конце рабочего

дня в одном из незакрываемых помещений организации. Возможные варианты проникновения злоумышленника в кабинет представлены в виде семантической цепи на рис. 2.

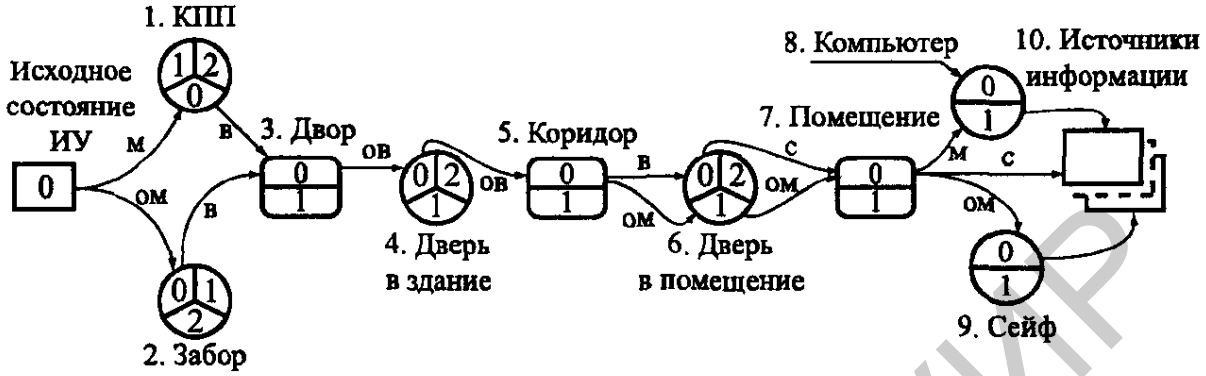

Рис. 2. Семантическая цепь представления вариантов проникновения злоумышленника в кабинет руководителя с градацией вероятностей перехода: ом – очень малая; м – малая; с – средняя; в – высокая; ов – очень высокая

2. Описание технических каналов утечки информации

Описание выявленных технических каналов утечки информации предполагает определение показателей их угроз.

Описание оптических каналов утечки информации

Возможны следующие оптические каналы утечки информации из кабинета руководителя:

- объект наблюдения в кабинете – окно кабинета – окно противоположного дома – оптический прибор злоумышленника;
- объект наблюдения в кабинете – приоткрытая дверь – злоумышленник;
- объект наблюдения в кабинете – телевизионное закладное устройство – проводной или радиоканал – телевизионный приемник злоумышленника.

Вероятность обнаружения объектов наблюдения в кабинете и их распознавания зависит от количества и информативности видовых демаскирующих признаков. Эти признаки получают из изображения объекта наблюдения на сетчатке глаза, фотоснимке, фоточувствительной поверхности оптического приемника. Количество признаков зависит от:

- разрешающей способности оптического приемника;
- масштаба изображения относительно реального объекта.

Минимальные размеры элемента изображения объекта наблюдения в виде точки на светочувствительном элементе, определяются как $\Delta h \approx D/Rf$, где D – дальность от светоприемника до объекта наблюдения; f – фокусное расстояние объектива оптического приемника.

В качестве технического средства наблюдения за объектами в кабинете через его окна рассматривается фотоаппарат ФС-122 («Фотоснайпер») с объективом Таир-30, фокусное расстояние которого равно 300 мм, а

разрешающая способность объектива $R_0 \approx 50$ лин/мм. Такой фотоаппарат размещается в удобном для скрытого переноса портфеле типа «кейс». При использовании фотопленки с разрешающей способностью $R_{фп} = 100$ лин/мм разрешение фотоаппарата (объектив – пленка) $R = 33$ лин/мм. Для D=50 м размеры элемента объекта, отображаемого на светочувствительном элементе в виде точки-пикселя, соответствуют $\Delta h \approx 10$ мм. Минимальные линейные размеры объекта, который можно распознать с вероятностью 0,9, составляют 5–6 см. Такие минимальные размеры могут иметь буквы и цифры на плакатах, иллюстрирующих выступления докладчиков на ответственных совещаниях.

При полученных значениях разрешения могут быть также распознаны лица людей и внешний вид достаточно крупной продукции. Однако прочитать документ формата А4, рассмотреть изображение на экране компьютера и телевизора, прочитать произносимые слова по губам нельзя. Следовательно, риск рассмотренного оптического канала утечки информации, содержащейся в изображении плакатов, людей и крупногабаритной продукции, велик, а утечки информации, содержащейся в изображениях документов формата А4, очень мал.

Другой оптический канал утечки информации может возникнуть при приоткрытой двери кабинета или заглядывании в кабинет посторонних лиц. В этом случае могут быть прочитаны тексты не только на плакатах, но и на столах и экранах светопроектора и телевизора. Но при наличии бдительного секретаря в приемной возможностью такого наблюдения очень мала.

Наконец, возможность реализации угрозы наблюдения с помощью видео закладного устройства также мала, т. к. установка телевизионной камеры в кабинете – серьезная разведывательная операция. Однако пренебрегать такой возможностью нельзя.

На основании перечисленных данных риск утечки информации при наблюдении можно оценить следующим образом:

- очень высокий – семантической документальной информации, отображаемой на плакатах;
- очень малый – остальной документальной информации;
- средний – о видовых признаках людей;
- малый – о видовых признаках продукции;
- очень малый – о видовых признаках веществ и материалов.

Описание акустических каналов утечки информации

Утечка речевой информации возможна по следующим акустическим техническим каналам:

- источник речевого сигнала – стена в соседнее помещение – акустический приемник злоумышленника;
- источник речевого сигнала – приоткрытая дверь в приемную – акустический приемник;

- источник речевого сигнала – закладное устройство – радиоканал – радиоприемник злоумышленника;

- источник речевого сигнала – стекло окна – модулированный лазерный луч – фотоприемник лазерной системы подслушивания;

- источник речевого сигнала – воздухопровод – акустический приемник;

- источник речевого сигнала – случайный акустоэлектрический преобразователь в техническом средстве – побочное излучение технического средства – радиоприемник;

- источник речевого сигнала – случайный акустоэлектрический преобразователь в техническом средстве – проводные кабели, выходящие за пределы контролируемой зоны;

- источник речевого сигнала – воздушная среда помещения – диктофон у злоумышленника.

Для оценки угроз речевой информации необходимо оценить уровень акустического сигнала в возможных местах размещения акустического приемника злоумышленника. Такими местами являются:

- приемная;
- коридор;
- смежные с кабинетом помещения;
- помещения с трубами отопления, проходящими через кабинет;
- помещения, акустически связанные с кабинетом через воздуховоды вентиляции.

Кроме того, речевая информация в кабинете может ретранслироваться по радиоканалу или проводам телефонной линии и электропитания закладными устройствами и побочными электромагнитными излучениями основных и вспомогательных технических средств и систем, а также средствами лазерного подслушивания. Так как носителями информации при ретрансляции являются электромагнитная волна в радиодиапазоне и электрический ток, то угрозы и меры по предотвращению перехвата рассматриваются в радиоэлектронном канале утечки информации. Также акустическая информация может быть получена с помощью лазерного средства подслушивания, установленного в помещении противоположного дома. Характеристика акустических каналов утечки информации дана в табл. 3.

Таблица 3

Характеристика акустических каналов утечки информации

Характеристика речи	Громкость, дБ	Основной элемент среды распространения, дБ	Величина звукоизоляции, дБ	Место нахождения акустического приемника	Уровень шума, дБ
Спокойный разговор	50–60	Стена и дверь в приемную	27	Приемная	≈30
Громкая речь	60–70	Стена в коридор	51	Коридор	35–40
Шумное совещание	70–80	Стена в смежную комнату	40	Соседнее помещение	20–25
То же	70–80	Межэтажное перекрытие	50	Помещения на верхнем и нижнем этажах	25–30
»	70–80	Вентиляционный короб	0,2 дБ/м 3–7 дБ на изгиб	В вентиляционном отверстии другого помещения	30
»	70–80	Трубы отопления	25–35	На трубе отопления	30

В качестве критерия защищенности речевой информации используется отношение сигнал/шум, при котором качество подслушиваемой речевой информации ниже допустимого уровня. В соответствии с существующими нормами понимание речи невозможно, если отношение помеха/сигнал равно 6–8, а акустический сигнал не воспринимается человеком как речевой, если отношение помеха/сигнал превышает 8–10. Следовательно, для гарантированной защищенности речевой информации отношение сигнал/шум должно быть не более 0,1 или –10 дБ. Оценка угрозы утечки информации по акустическому каналу при подслушивании человеком производится по формуле $L_п = L_и - Q_{ог} - L_ш$. При применении технического акустического приемника значение этой величины повышается на 6 дБ.

Уровни громкости речевой информации в возможных местах размещения акустического приемника злоумышленника при громкости источника 70 дБ и оценка риска подслушивания указаны в табл. 4.

Таблица 4

Уровни громкости речевой информации

Место размещения акустического приемника злоумышленника	Уровень громкости, дБ	Оценка риска подслушивания
Приемная	5–10	Очень высокий
Коридор	–15– (–20)	Отсутствует
Соседнее помещение	≈(–5)	Низкий
Верхнее (нижнее) помещение	–15– (–10)	Отсутствует
Вентиляционный короб	0–5	Средний
Трубы отопления	0–5	Средний

Как следует из данных табл. 4, наибольшую угрозу создает канал утечки, приемник которого расположен в приемной и в коробе вентиляции. Каналом утечки, приемник которого расположен в коридоре, можно пренебречь.

Моделирование радиоэлектронных каналов утечки информации

Радиоэлектронные каналы утечки информации из кабинета руководителя представляют собой простые каналы и части составных акусто- радиоэлектронных каналов утечки информации. Простые каналы образованы побочными электромагнитными излучениями и наводками радиосредств и электрических приборов, размещенных в кабинете, в том числе:

- компьютера при обработке на нем закрытой информации;
- видеодвойки (в случае просмотра видеокассет с закрытой информацией).

Кроме того, опасные сигналы случайных акустоэлектрических преобразователей в радиосредствах и электрических приборах могут добавить к простым оптическим и акустическим каналам радиоэлектронные каналы утечки информации и создать акустоэлектронные каналы утечки. Источниками радиоэлектронных каналов утечки в составе акустоэлектронных составных являются:

- коммутационное оборудование и кабели внутренней АТС;
- электрические приборы в кабинете (вторичные часы единого времени, вентилятор, громкоговоритель оперативного оповещения);
- передатчики акустических и телевизионных закладных устройств.

Если в кабинете установлено телевизионное закладное устройство, например, в типовых папках (скоросшивателях) с отверстием в торце, то составной оптико-электронный канал утечки информации содержит радиоэлектронный канал утечки информации с элементами: телевизионная камера – телевизионный приемник – видеомагнитофон или злоумышленник-наблюдатель.

Побочные НЧ- и ВЧ-излучения основных технических средств и систем (ОТСС) имеют очень широкий диапазон частот: доли герцев – тысячи мегагерцев (длины волн: сотни метров – десятки сантиметров). Помещение кабинета с учетом его размеров, представляет собой ближнюю, переходную и дальнюю зоны побочного излучения ОТСС. На частотах до 30 МГц помещение

образует ближнюю зону. В зависимости от вида излучателя в ближайшей зоне может преобладать электрическое или магнитное поле.

Информация в помещении находится в безопасности, если уровни ее носителей в виде электрических сигналов и напряженности поля не превышают нормативы. Следовательно, для предотвращения подслушивания путем перехвата опасных сигналов необходимо определить эти уровни на границе контролируемой зоны (периметра кабинета) и в случае недопустимо больших значений определить рациональные меры по их уменьшению.

Уменьшение затухания электромагнитной волны в железобетонных стенах с повышением ее частоты вызвано снижением экранирующего эффекта металлической арматуры железобетона. На частоте 1 ГГц длина волны равна 30 см, что соизмеримо с размерами ячеек арматуры.

При ослаблении электромагнитной волны стенами здания на 20 дБ дальность ее распространения уменьшается на 1 порядок. Учитывая, что окна кабинета выходят на улицу, риск перехвата радиоизлучений ПЭВМ из кабинета руководителя организации можно оценить значением «средний», а электрических сигналов акустоэлектрических преобразований – «низкий».

Таким образом, наибольший ущерб информации, содержащейся в кабинете руководителя, могут нанести следующие угрозы:

- наблюдение из окна противоположного дома текста и изображений на плакатах экрана, укрепленных на стенах кабинета;
- подслушивание разговора в кабинете через приоткрытую дверь в приемную руководителя;
- подслушивание громкого разговора через стену, разделяющую кабинет и коридор;
- наблюдение через окно противоположного дома за участниками совещания;
- наблюдение через открытую дверь за участниками совещания;
- перехват побочных электромагнитных излучений радиоэлектронных средств и электрических приборов, размещенных и работающих в кабинете во время разговора;
- перехват опасных сигналов, содержащих речевую информацию, распространяющихся по проводам телефонных линий связи, трансляции, часов единого времени, электропитания и заземления;
- подслушивание с помощью стетоскопа речевой информации акустических сигналов, распространяющихся по трубам отопления;
- подслушивание речевой информации акустических сигналов, распространяющихся по воздухопроводам;
- подслушивание с помощью акустических закладных устройств, установленных в кабинете;
- скрытое наблюдение с помощью предварительно установленных телевизионных камер;
- скрытное проникновение к источникам информации, хранящимся в ящиках стола, компьютере, сейфе.

III. Нейтрализация угроз информации в кабинете руководителя организации

Меры по предотвращению доступа злоумышленника к источникам информации

Так как проникновение злоумышленника возможно через дверь в приемную, то в ночное время необходимо создать дополнительный рубеж и контролируемую зону в приемной. Для этого на двери из коридора в приемную устанавливается магнитоконтактный извещатель типа СМК-3 или более современные ИО-104-2-4. Эти извещатели обеспечивают замыкание или размыкание контактов геркона при приближении магнита на расстояние не более 10 мм и удалении не более 45 мм. Аналогичный извещатель устанавливается на дверях кабинета.

Для обнаружения злоумышленника в кабинете необходимо установить объемный извещатель (пассивный оптико-электронный, ультразвуковой, радиоволновой, комбинированный). Выбор производится исходя из помехоустойчивости, объема кабинета и затрат на приобретение и эксплуатацию. В отличие от приемной, средства охраны которой в рабочее время отключаются, средства охраны кабинета при отсутствии на рабочем месте руководителя организации целесообразно сохранять во включенном состоянии. Для обеспечения такого режима необходимо использовать отдельный шлейф.

Учитывая небольшую площадь кабинета, целесообразно применять или пассивные оптико-электронные извещатели или активные волновые с регулируемой мощностью излучения. В качестве таких средств могут использоваться следующие извещатели: оптико-электронный «Фотон-5», создающий «занавес» с максимальной дальностью 12 м; ультразвуковой «Эхо-2» для площади 30 м^2; радиоволновой объемный «Волна-5» с регулируемой дальностью 2–16 м и комбинированный «Сокол-2», совмещающий пассивный инфракрасный и радиоволновой принципы обнаружения. Последний обеспечивает дальность действия: минимальную – 3–5 м, максимальную – 12 м. Он может крепиться к стене или на потолке, имеет высокую помехоустойчивость. Наиболее доступным извещателем с требуемыми функциональными возможностями является оптико-электронный извещатель «Фотон-5». По критерию «эффективность – стоимость» лучшие показатели имеет комбинированный извещатель «Сокол-2».

Кроме рассмотренных средств целесообразно установить локальные извещатели для охраны сейфа и компьютера. Для охраны сейфа можно использовать охранный поверхностный емкостный извещатель «Пик» с регулируемой чувствительностью на приближение человека на расстояние до 0,2 м.

Для защиты информации, содержащейся в компьютере, от действий злоумышленника (хищения информации путем копирования или изъятия винчестера) можно использовать емкостный извещатель «Пик», антенна

которого соединена с корпусом сейфа. Для механической защиты системный блок с винчестером может быть размещен в специальном сейфе под приставным столиком или может использоваться съемный винчестер, помещаемый в сейф.

Защита информации в кабинете руководителя от наблюдения

Для защиты информации от наблюдения применяют методы энергетического скрытия путем увеличения затухания среды распространения. Для прекращения функционирования оптического канала утечки информации «окно кабинета – окно противоположного жилого дома» можно применить следующие средства:

- шторы на окнах;
- жалюзи;
- тонированные пленки на стеклах.

Шторы – традиционное средство для предотвращения скрытого наблюдения через окно кабинета, но они существенно ухудшают естественную освещенность кабинета и накапливают пыль.

Тонированные пленки на стеклах исключают возможность наблюдения за объектами защиты в кабинете, незначительно уменьшают освещенность кабинета, но позволяют легко выявить окна помещений с повышенными требованиями к безопасности информации, что из-за соображений скрытности защиты не рекомендуется использовать. Для обеспечения скрытости защиты применять пленку надо на всех окнах по крайней мере этажа, а лучше – здания.

Наиболее приемлемый вариант защиты – применение жалюзи на окнах. Они не только исключают возможность наблюдения через окно, но и эффективны по основному назначению – защите от солнечных лучей.

Для предотвращения наблюдения через приоткрытую дверь применяют доводчик двери, который плавно закрывает дверь после ее открытия.

Меры по обнаружению и локализации скрытно установленной в кабинете телевизионной камеры предпринимаются периодически и перед проведением совещания. Исключить установку камеры между проверками нельзя. Телевизионное изображение может передаваться в реальном масштабе времени или записываться на пленочный или цифровой видеомагнитофон с последующей ускоренной передачей. Однако кинематический видеомагнитофон имеет большие, чем телевизионная камера размеры и энергопотребление, поэтому его практическое применение в настоящее время ограничено. В будущем следует ожидать появление бескинематических цифровых видеомагнитофонов для скрытой записи. Основным демаскирующим признаком телевизионной камеры и видеомагнитофона является излучение. Поэтому для обнаружения и локализации телевизионной камеры применяются средства поиска радиоизлучающих зарядных устройств: индикаторы поля, специальные радиоприемники, автоматизированные комплексы для радиомониторинга и др. Перед совещанием во время «чистки» кабинета применяются также нелинейные локаторы и металлодетекторы.

Меры по защите речевой информации от подслушивания

Для защиты от подслушивания речевой информации в приемной необходимо существенно повысить звукоизоляцию дверей и стен до 55 дБ на частоте 1000 Гц. Такая звукоизоляция обеспечивается двойной дверью с тамбуром шириной не менее 20 см с уплотнителями по периметру дверных полотен. Для предотвращения утечки информации через ограждения кабинета возможны 3 варианта:

- повышение поверхностной плотности ограждения;
- установление дополнительной перегородки;
- зашумление ограждения.

Так как звукоизоляция пропорциональна поверхностной плотности среды распространения акустической волны, то при недостаточной звукоизоляции утолщают стены. Звукоизоляция стен между кабинетом и приемной, кабинетом и коридором, кабинетом и смежным помещением повышается путем утолщения стен и крепления к ним дополнительных перегородок. Наиболее удобным строительным материалом для этого является кирпич, который укладывают на ширину половины или длины целого кирпича вплотную к стенке. Утолщенная стена из качественного кирпича обеспечивает повышение звукоизоляции с 48 до 53 дБ. Кладка утолщенной стены с зазором между стенками 40 мм увеличивает звукоизоляцию еще примерно на 4–5 дБ. Утолщение стены целесообразно проводить со стороны приемной, так как это позволит уменьшить выступ двойной двери с тамбуром в приемную.

Возможно также укрепление на стене строительных материалов (многослойной фанеры различной толщины, стеклопластика, пемзобетонных плит и др.). В качестве дополнительных перегородок используются асбестоцементные, гипсокартонные, древесностружечные, древесноволокнистые плиты толщиной 10–20 мм. Они крепятся к стене с помощью деревянных реек и брусков толщиной 40–50 мм по периметру и поверхности стены. По периметру между перегородкой и другими ограждениями устанавливаются упругие (из губчатой резины) прокладки. Между перегородкой и стеной может быть размещен звукопоглощающий пористый материал.

В качестве меры, повышающей энергетическое скрытие речевой информации в кабинете, на стенах могут быть укреплены виброакустические излучатели акустических генераторов помех. Для исключения утечки информации через батареи и трубы отопления перед батареями устанавливают резонаторные экраны в виде деревянных перегородок с отверстиями. Для предотвращения утечки информации через вентиляционное отверстие перед ним укрепляют экран и (или) размещают глушитель звука.

В качестве мер предотвращения подслушивания рекомендуется:

- установка двойной двери с уплотнительными прокладками и тамбуром глубиной 30 см;
- увеличение толщины стены между кабинетом и приемной, а также соседними помещениями на половину длины кирпича;
- установка на батареи отопления резонаторных экранов или излучателей генератора виброакустического зашумления;
- закрытие окон плотными шторами, установка на стекла окон излучателей генератора виброакустического зашумления (для предотвращения лазерного подслушивания при закрытых окнах);
- установка перед воздухозаборниками воздухопроводов акустических экранов;
- установка датчиков комплекса обнаружения скрыто работающего диктофона PDRT-18 под столешницу стола руководителя возле стула для посетителя и стола заседаний;
- применение устройств для подавления сигналов скрыто работающего диктофона.

Примечание. Установка двойной двери повышает звукоизоляцию с 18 до 48 дБ, утолщение стены увеличивает звукоизоляцию примерно на 20 дБ.

Предотвращение перехвата электрических и радиосигналов

Предотвращение утечки информации из кабинета по радиоэлектронному каналу обеспечивается:

- выключением во время разговора всех радиосредств и электрических приборов, в которых нет необходимости;
- установкой в разрыв цепей электропитания возле стен сетевых фильтров для исключения ВЧ-навязывания;
- установкой средств подавления сигналов акустоэлектрических преобразователей телефонных аппаратов типа «Корунд» и «Гранит-VIII», ограничителей малых амплитуд с фильтрам от ВЧ-навязывания;
- установкой НЧ-фильтров в цепь вторичных часов единого времени (устройство МП-4);
- установкой буфера в цепь громкоговорителя системы оповещения (устройство МП-5);
- использованием в кабинете генератора пространственного электромагнитного зашумления, включаемого во время проведения совещания по тематике, содержащей тайну;
- установкой в свободный слот системной платы компьютера плат генератора помех.

Кроме того, информация на компьютере в кабинете руководителя организации может защищаться путем:

- использования защитных ПЭВМ;
- размещения системного блока в специальном сейфе;
- установки винчестера в съемный кожух и хранения его в сейфе;

- программной защиты доступа к компьютеру и отдельным папкам;
- криптографического шифрования информации, хранящейся на машинных носителях.

Кроме того, после проведения капитального ремонта и перед проведением совещания производится чистка помещения с целью обнаружения закладных устройств.

6.2. Практическая часть

Создать сценарий инженерно-технической защиты информации в кабинете руководителя организации.

Пример

План кабинета как объекта защиты

Кабинет размещен на 3-м этаже 5-этажного кирпичного здания, примыкающего к тротуару улицы. Окна кабинета выходят на улицу. Ширина улицы составляет около 50 м. На противоположной стороне улицы расположены жилые 12-этажные дома. Территория организации обнесена бетонным забором высотой 2 м, соединенным с наружной стеной административного здания. Вход людей в организацию обеспечивается через контрольно-пропускной пункт, въезд автотранспорта – через ворота, вход в здание – через дверь, открываемую во двор. Окна 1-го этажа укреплены стальными решетками.

Схема расположения организации представлена на рис. 3.

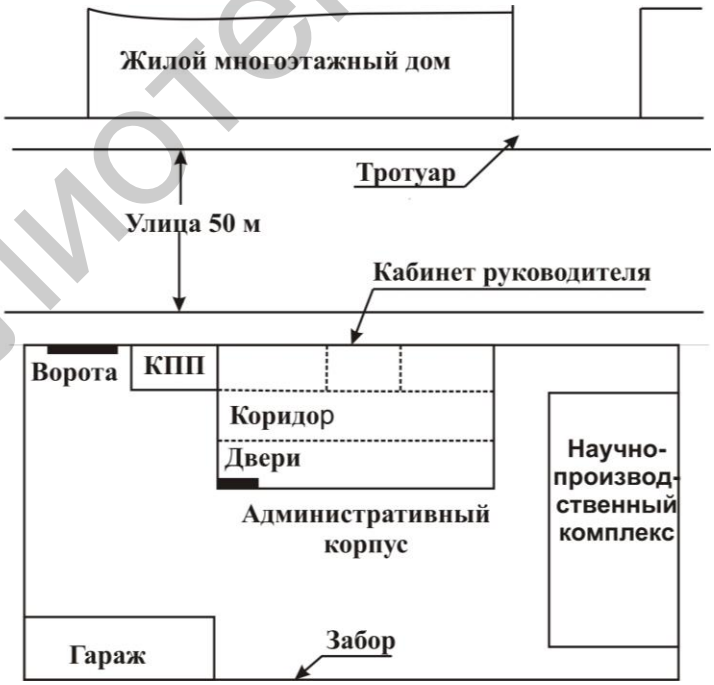

Рис. 3. Примерный план расположения организации

Кабинет руководителя имеет два окна, выходящие на улицу, и дверь в приемную. Площадь кабинета составляет около 30 м^2, приемной – 20 м^2. Схематический чертеж варианта кабинета приведен на рис. 4.

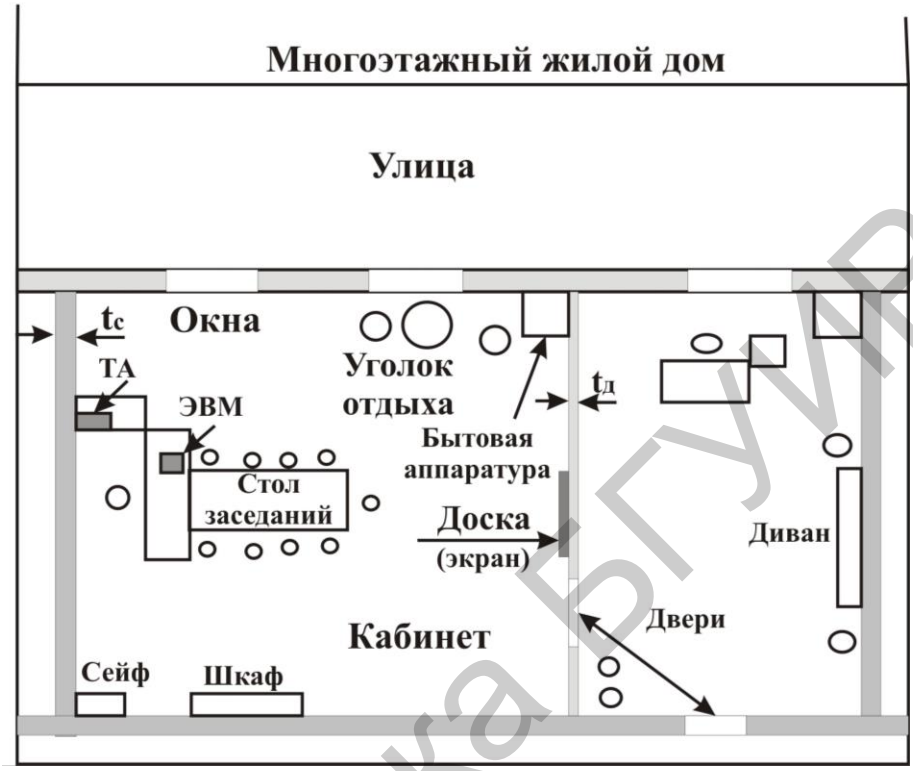

Рис. 4. Примерный план кабинета руководителя

Для описания фактов, влияющих на защищенность информации в кабинете, проводится его обследование. Описание помещения содержит 5 групп факторов:

- общая характеристика помещения;
- ограждения;
- предметы мебели и интерьера;
- радиоэлектронные средства и электрические приборы;
- средства коммуникаций.

Результаты обследования помещены в табл. 5.

Таблица 5

Результат обследования защищаемого помещения

№ п/п	Факторы влияния	Параметры	Примечание
1	2	3	4
	1. Общая характеристика		
1.1	Этаж	3-й	
1.2	Площадь, м^2	30 м^2	
1.3	Смежные помещения	Справа – приемная; слева – кабинет заместителя; сверху – служебное помещение организации	
	2. Ограждения		
2.1	Стены	*Наружная* – железобетонная толщиной 400 мм, на стене укреплены 2 чугунные батареи отопления, соединенные металлическими трубами с трубами в боковых стенах; *смежная с коридором* – железобетонная толщиной 140 мм; 2 вентиляционных отверстия; *смежная с приемной* – кирпичная толщиной в 1 кирпич (270 мм); *смежная с кабинетом заместителя* – железобетонная толщиной 140 мм	
2.2	Потолок	Железобетонная плита толщиной 400 мм, окрашенная водо-эмульсионной краской	
2.3	Пол	Железобетонная плита толщиной 400 мм, покрытая паркетом и ковролином	
2.4	Окна	Количество – 2, двухрамные, обращены на улицу, толщина стекла –3 мм	
2.5	Дверь	Типовая щитовая, без доводчика, выход в приемную	
	3. Предметы мебели и интерьера		
3.1	Картина	Размеры рамы 700×500 мм, расположена под углом к стене, смежной с коридором	
3.2	Шкаф книжный	Дверцы стеклянные, на 4 полках книги и папки с документами	
3.3	Сейф напольный	Замок механический кодовый	
3.4	Стол приставной	Имеет под столешницей полку	
3.5	Столик под телевизионную аппаратуру	1 шт.	

Окончание табл. 5

1	2	3	4
3.6	Доска-экран	Размер 2000×1200 мм, из белого пластика	
3.7	Кресло кожаное вращающееся	1 шт.	
3.8	Кожаные кресла для отдыха	2 шт.	
3.9	Журнальный столик	1 шт.	
3.10	Стол для заседаний	Рассчитан на 10 человек	
3.11	Стулья	Деревянные полужесткие, 10 шт.	
	4. Радиоэлектронные средства и электрические приборы		
4.1	Компьютер	Состав: системный блок, монитор, мышь, клавиатура, 2 динамика, на письменном столе	
4.2	Телефон закрытой связи (ЗАС)	На приставном столике	
4.3	Видеодвойка (телевизор+видеомагнитофон)	В случае просмотра видеокассет с закрытой информацией	
4.4	Телефон городской АТС	На приставном столике	
4.5	Телефон внутренней АТС	На приставном столике	
4.6	Концентратор	Под столешницей приставного столика	
4.7	Видеодвойка	Просмотр видеокассет с открытой информацией	
4.8	Вентилятор	На письменном столе	
4.9	Вторичные часы единого времени	На стене, смежной с приемной	
4.10	Громкоговоритель оповещения	На стене, смежной с коридором	
4.11	Настольная лампа	1 шт.	
4.12	Люстра из 5 рожков	1 шт. на потолке	
4.13	Извещатели пожарные	2 шт. на потолке	
	5. Средства коммуникаций		
5.1	Розетки электропитания	Одна – возле письменного стола, другая – возле видеодвойки	
5.2	Телефонные розетки	2 шт. возле письменного стола	
5.3	Электропроводка	Скрытая в стенах	
5.4	Кабели телефонных линий	Наружные, на стене возле письменного стола	
5.5	Кабель локальной сети	Витая пара, укрепленная на стене	
5.6	Шлейф пожарной сигнализакции	Наружный, на потолке и стене возле письменного стола	

Примечание. Характеристики ограждений, указанные в этой таблице, занижены по сравнению с типовыми реальными значениями с целью выявления большего количества угроз подслушивания.

ПРАКТИЧЕСКАЯ РАБОТА №7
ПРИЗНАКИ ПОЯВЛЕНИЯ ВИРУСОВ. МЕТОДЫ ЗАЩИТЫ. АНТИВИРУСНОЕ ПО

Цель работы: изучить основные проявления вирусов на компьютерах, классификацию вирусов, антивирусное программное обеспечение.

7.1. Теоретическая часть

7.1.1. Компьютерные вирусы

Компьютерный вирус – это специально написанная, как правило, небольшая по размерам программа, которая может записывать свои копии в компьютерные программы, расположенные в исполнимых файлах, системных областях дисков, драйверах, документах и т. д., причем эти копии сохраняют возможность к «размножению». Процесс внедрения вирусом своей копии в другую программу (системную область диска и т. д.) называется заражением, а программа или иной объект, содержащий вирус – зараженным.

Сегодня науке известно около 30 тыс. компьютерных вирусов. Как и обычным вирусам, вирусам компьютерным для «размножения» нужен «носитель» – здоровая программа или документ, в которых они прячут участки своего программного кода. В тот момент, когда пользователь, ничего не подозревая, запускает на своем компьютере зараженную программу или открывает документ, вирус активизируется и заставляет компьютер следовать инструкциям вируса. Это приводит к удалению какой-либо информации, причем чаще всего – безвозвратно. Кроме этого, современные вирусы могут испортить не только программы, но и компьютер. Например, уничтожают содержимое BIOS материнской платы или повреждают жесткий диск.

Первые компьютерные вирусы были простыми и неприхотливыми: от пользователей не скрывались, «скрашивали» свое разрушительное действие (удаление файлов, разрушение логической структуры диска) выводимыми на экран картинками и предупреждениями («Назовите точную высоту горы Килиманджаро в миллиметрах! При введении неправильного ответа все данные на вашем винчестере будут уничтожены!»). Выявить такие вирусы было нетрудно – они «приклеивались» к исполняемым (*.com или *.exe) файлам, изменяя их оригинальные размеры.

Позднее вирусы стали прятать свой программный код так, что ни один антивирус не мог его обнаружить. Такие вирусы назывались невидимками.

В 90-е гг. XX в. вирусы стали мутировать – постоянно изменять свой программный код, при этом пряча его в различных участках жесткого диска. Такие вирусы-мутанты стали называться полиморфными.

Весомый вклад в распространение вирусов внес Интернет. Впервые внимание общественности к проблеме интернет-вирусов было привлечено после появления знаменитого «червя Морриса» – относительно безобидного

экспериментального вируса, распространившегося по всей мировой сети в результате неосторожности его создателя. А к 1996–1998 гг. Интернет стал главным поставщиком вирусов. Возник даже целый класс интернет-вирусов, названных троянскими. Эти программы не причиняли вреда компьютеру и хранящейся в нем информации, зато с легкостью могли «украсть» пароль и логин для доступа к сети, а также другую секретную информацию.

В 1995 г. после появления операционной системы Windows 95 были зарегистрированы вирусы, работающие под Windows 95. Примерно через полгода были обнаружены вирусы, которые действовали на документах, подготовленных в популярных программах из комплекта Microsoft Office. Дело в том, что в текстовый редактор Microsoft Word и табличный редактор Microsoft Excel был встроен язык программирования Visual Basic for Applications (VBA), предназначенный для создания специальных дополнений к редакторам – макросов. Эти макросы сохранялись в теле документов Microsoft Office и легко могли быть заменены вирусами. После открытия зараженного файла вирус активировался и заражал все документы Microsoft Office. Первоначально *макровирусы* наносили вред только текстовым документам, позднее они стали уничтожать информацию.

В течение 1998–1999 гг. мир потрясли несколько разрушительных вирусных атак: в результате деятельности вирусов Melissa, Win95.CIH и Chernobyl были выведены из строя около миллиона компьютеров во всех странах мира. Вирусы портили жесткий диск и уничтожали BIOS материнской платы.

Опасные и неопасные вирусы. Большинство вирусов не выполняет каких-либо действий, кроме своего распространения (заражения других программ, дисков и т. д.) и иногда выдачи каких-либо сообщений или иных эффектов, придуманных автором вируса: игры, музыки, перезагрузки компьютера, выдачи на экран разных рисунков, блокировки или изменения функций клавиш клавиатуры, замедления работы компьютера и т. д. Однако сознательной порчи информации эти вирусы не осуществляют. Такие вирусы условно называются *неопасными*. Впрочем, и эти вирусы способны причинить большие неприятности (например, перезагрузки каждые несколько минут будут мешать работе пользователя).

Однако около трети всех видов вирусов портят данные на дисках – или сознательно, или из-за содержащихся в вирусах ошибок, скажем, из-за не вполне корректного выполнения некоторых действий. Если порча данных происходит лишь эпизодически и не приводит к тяжелым последствиям, то вирусы называются *опасными*. Если же порча данных происходит часто или вирусы причиняют значительные разрушения (форматирование жесткого диска, систематическое изменение данных на диске и т. д.), то вирусы называются *очень опасными*.

Классификация вирусов по типам заражаемых объектов. Компьютерные вирусы отличаются друг от друга по тому, в какие объекты они

внедряются, т. е. что они заражают. Некоторые вирусы могут заражать сразу несколько видов объектов.

Большинство вирусов распространяются, заражая *исполнимые файлы,* т. е. файлы с расширением имени .COM и .EXE, а также различные вспомогательные файлы, загружаемые при выполнении других программ. Такие вирусы называются *файловыми*. Вирус в зараженных исполнимых файлах начинает свою работу при запуске той программы, в которой он находится.

Еще один распространенный вид вирусов внедряется в начальный сектор дискет или логических дисков, где находится загрузчик операционной системы, или в начальный сектор жестких дисков, где находится таблица разбиения жесткого диска и небольшая программа, осуществляющая загрузку с одного из разделов, указанных в этой таблице. Такие вирусы называются загрузочными, или бутовыми (от слова boot – загрузчик). Эти вирусы начинают свою работу при загрузке компьютера с зараженного диска. Загрузочные вирусы являются резидентными и заражают вставляемые в компьютер дискеты. Встречаются загрузочные вирусы, заражающие также и файлы, – файлово-загрузочные вирусы.

Некоторые вирусы умеют заражать драйверы, т. е. файлы, указываемые в предложении DEVICE или DEVICEHIGH файла CONFIG.SYS. Вирус, находящийся в драйвере, начинает свою работу при загрузке данного драйвера из файла CONFIG.SYS при начальной загрузке компьютера. Обычно заражающие драйверы вирусы заражают также исполнимые файлы или сектора дискет, поскольку иначе им не удавалось бы распространяться – ведь драйверы очень редко переписывают с одного компьютера на другой.

Очень редко встречаются вирусы, заражающие системные файлы DOS (IO.SYS или MSDOS.SYS). Эти вирусы активизируются при загрузке компьютера. Обычно такие вирусы заражают также загрузочные сектора дискет, поскольку иначе им не удавалось бы распространяться.

Очень редкой разновидностью вирусов являются вирусы, заражающие командные файлы. Обычно эти вирусы формируют на диске исполнимый файл с помощью команд командного файла, запускают этот файл, он выполняет размножение вируса, после чего данный файл стирается. Вирус в зараженных командных файлах начинает свою работу при выполнении командного файла, в котором он находится. Иногда вызов зараженного командного файла вставляется в файл AUTOEXE.BAT.

Долгое время заражение вирусами файлов документов считалось невозможным, т. к. документы не содержали исполнимых программ. Однако программисты фирмы Microsoft встроили в документы Word для Windows мощный язык макрокоманд WordBasic, на котором стало возможно писать вирусы. Запуск вируса происходит при открытии для редактирования зараженных документов. При этом макрокоманды вируса записываются в глобальный шаблон NORMAL.DOT, так что при новых сеансах работы с Word для Windows вирус будет автоматически активирован.

Возможно заражение и других объектов, содержащих программы в какой-либо форме, – текстов программ, электронных таблиц и т. д. Например, вирус AsmVirus.238 заражает файлы программ на языке ассемблера (.ASM-файлы), вставляя туда ассемблерные команды, которые при трансляции порождают код вируса. Однако число пользователей, программирующих на языке ассемблера, невелико, поэтому широкое распространение такого вируса невозможно.

Электронные таблицы содержат макрокоманды, в том числе и те, которые автоматически выполняются при открытии таблицы. Поэтому для них могут быть созданы вирусы, аналогичные вирусам для документов Word для Windows. Пока что такие вирусы были созданы для таблиц табличного процессора Excel.

Вирус является программой, поэтому объекты, не содержащие программ и не подлежащие преобразованию в программы, заражены вирусом быть не могут. Не содержащие программ объекты вирус может только испортить, но не заразить. К числу таких объектов относятся текстовые файлы (кроме командных файлов и текстов программ), документы простых редакторов документов типа ЛЕКСИКОН или Multi-Edit, информационные файлы баз данных и т.д.

Особые виды вирусов. Некоторые виды вирусов требуют особого отношения, поскольку стандартные методы их лечения могут привести к потере информации (вирусы семейства DIR) или не излечивают от вируса (вирусы семейства ЗАРАЗА).

Вирусы семейства DIR

В 1991 г. появились вирусы нового типа – вирусы, меняющие файловую систему на диске (семейство DIR). Такие вирусы прячут свое тело в некоторый участок диска (обычно – в последний кластер диска) и помечают его в таблице размещения файлов (FAT) как конец файла или как дефектный участок. Для всех .COM- и .EXE-файлов указатели на первый участок файла, содержащиеся в соответствующих элементах каталога, заменяются ссылкой на участок диска, содержащий вирус, а правильный указатель в закодированном виде прячется в неиспользуемой части элемента каталога. Поэтому при запуске любой программы в память загружается вирус, после чего он остается в памяти резидентно, подключается к программам DOS для обработки файлов на диске и при всех обращениях к элементам каталога выдает правильные ссылки.

Таким образом, при работающем вирусе файловая система на диске кажется совершенно нормальной. При поверхностном просмотре зараженного диска на «чистом» компьютере также ничего странного не наблюдается. Только при попытке прочесть или скопировать с зараженной дискеты программные файлы из них будут прочтены или скопированы только 512 или 1024 байта, даже если файл гораздо длиннее. А при запуске любой исполнимой программы с зараженного таким вирусом диска этот диск начинает казаться исправным (неудивительно, ведь компьютер при этом становится зараженным).

Особая опасность вирусов семейства DIR состоит в том, что повреждения файловой структуры, сделанные этими вирусами, не следует исправлять

программами типа ScanDisk или NDD – при этом диск окажется безнадежно испорченным. Для исправления надо применять только антивирусные программы.

Вирусы семейства ЗАРАЗА

Еще один необычный тип вирусов – это вирусы, заражающие системный файл IO.SYS. Семейство этих вирусов обычно называется ЗАРАЗА, потому что первый такой вирус выводил сообщение «В BOOT СЕКТОРЕ – ЗАРАЗА!».

Данные вирусы являются файлово-загрузочными и используют рассогласование между механизмом начальной загрузки DOS и обычным механизмом работы с файлами. При начальной загрузке MS DOS проверяется, что имена двух первых элементов в корневом каталоге загрузочного диска – IO.SYS и MSDOS.SYS, но атрибуты этих элементов не проверяются. Если имена совпадают, то программа начальной загрузки считывает в память первый кластер элемента с именем IO.SYS и передает ему управление. Из-за этого несовершенства программа начальной загрузки при заражении жестких дисков производит следующие действия:

- копирует содержимое файла IO.SYS в конец логического диска;
- сдвигает элементы корневого каталога, начиная с третьего, на один элемент к концу каталога;
- копирует первый элемент корневого каталога (соответствующий файлу IO.SYS) в освободившийся третий элемент корневого каталога и устанавливает в нем номер начального кластера, указывающий на место, куда было скопировано содержимое файла IO.SYS;
- записывает свое тело в место, где находится файл IO.SYS (как правило, в начало области данных логического диска);
- у первого элемента корневого каталога диска устанавливает признак «метка тома».

В корневом каталоге появляются два элемента с именем IO.SYS, один из которых помечен атрибутом «метка тома». Но при начальной загрузке это не вызывает сбоев – программа начальной загрузки, проверив, что первые два элемента каталога имеют имена IO.SYS и MSDOS.SYS, загрузит кластер, указанный в первом элементе оглавления (на обычном диске это начало файла IO.SYS, а на зараженном – код вируса), и передаст ему управление. Вирус загрузит себя в оперативную память, после чего загрузит начало исходного файла IO.SYS и передаст ему управление. Далее начальная загрузка идет как обычно.

Опасность вирусов семейства ЗАРАЗА состоит в следующем: даже если загрузить компьютер с «чистой» системной дискеты и ввести команду SYS C:, вирус не будет удален с диска. Команда SYS, как и остальные программы DOS, проигнорирует указывающий на вирус первый элемент корневого каталога, посчитав его описанием метки. Перезаписан будет лишь «файл-дублер» IO.SYS, описанный в третьем элементе корневого каталога. Причем если программа SYS запишет файл IO.SYS в новое место на диске, то система перестанет загружаться с жесткого диска, т. к. вирус в своем теле хранит адрес

начального сектора исходного файла IO.SYS. Поэтому обеззараживать диски, инфицированные вирусами семейства ЗАРАЗА, командой SYS не следует, это надо делать антивирусными программами.

Методы маскировки вирусов. Чтобы предотвратить свое обнаружение, многие вирусы применяют довольно хитрые приемы маскировки. Многие резидентные вирусы предотвращают свое обнаружение тем, что перехватывают обращения операционной системы к зараженным файлам и областям диска и выдают их в исходном (незараженном) виде. Такие вирусы называются невидимыми, или стелс-вирусами. Разумеется, эффект «невидимости» наблюдается только на зараженном компьютере – на «чистом» компьютере изменения в файлах и загрузочных областях диска можно легко обнаружить. Некоторые антивирусные программы могут обнаруживать «невидимые» вирусы даже на зараженном компьютере. Для этого они выполняют чтение диска, не пользуясь услугами DOS. Примером таких программ являются антивирусы семейства ADinf фирмы «Диалог-Наука», Norton AntiVirus и др.

Вирусы часто содержат внутри себя различные сообщения, что позволяет заподозрить неладное при просмотре содержащих вирус файлов или областей дисков. Чтобы затруднить свое обнаружение, некоторые вирусы шифруют свое содержимое, так что при просмотре зараженных ими объектов никаких подозрительных текстовых строк пользователь не увидит.

Еще один способ, применяемый вирусами для того чтобы укрыться от обнаружения, – модификация своего тела. Это затрудняет нахождение таких вирусов программами-детекторами – в теле таких вирусов не имеется ни одной постоянной цепочки байтов, по которой его можно было бы идентифицировать. Такие вирусы называются полиморфными, или самомодифицирующимися. Имеются программы-детекторы, способные обнаруживать полиморфные вирусы, например Dr.Web фирмы «Диалог-Наука».

Как уберечься от вируса. При активизации зараженного вирусом файла управление сразу передается на вирус, который выполняет свои разрушительные действия, а также параллельно приписывается к другим программам и файлам. Затем технологически происходит возврат к тем действиям, которые выполнялись на компьютере. При высоком быстродействии компьютера подобное «отвлечение» от регламентированного хода работ для пользователя остается абсолютно незамеченным. Нанесенный ущерб может обнаружиться не сразу. Внешние проявления присутствия вируса в компьютере могут быть самыми различными, например:

- мерцание экрана;
- появление на экране непредусмотренного сообщения;
- непредусмотренное требование снять защиту записи с дискеты;
- изменение даты и времени создания зараженных файлов;
- зависание компьютера и невозможность преодолеть эту проблему;
- опадание букв на экране (иногда с музыкальным сопровождением);
- исчезновение некоторых программных файлов по пятницам, приходящихся на 13 число месяца;

- необычное аварийное завершение работы;
- уничтожение информационных файлов или их частичное разрушение;
- замедление работы компьютера;
- блокирование ввода с клавиатуры;
- звучание музыки;
- поворот символов на экране;
- блокировка записи на жесткий диск;
- другие виды необычного «поведения» компьютера.

Особенно опасным для пользователя является такое действие вируса, как форматирование жесткого диска, что сопряжено с быстрой потерей всей хранящейся там информации. Поскольку от проникновения вируса не застрахован ни один пользователь, то можно по крайней мере сократить до минимума возможные последствия от присутствия в компьютере вируса. Для этого необходимо соблюдать несколько простых правил:

1) каждую свою дискету, если она «побывала» на другом компьютере, следует обязательно проверить любой доступной антивирусной программой, что поможет не только обнаружить вирус, но и «вылечить» дискету, особенно это касается игровых программ, т. к. большинство вирусов распространяется именно через них;

2) аналогичные проверки необходимо устраивать для файлов, полученных через сеть Интернет;

3) антивирусная программа очень быстро морально стареет, поэтому рекомендуется ее периодически обновлять новой версией; период обновления программ такого рода составляет от одной недели до одного квартала;

4) не снимать защиту записи с дискеты в ходе повседневных работ, если это не предусмотрено технологией решения задач;

5) при обнаружении вируса не предпринимать необдуманных действий, т. к. это может привести к потере той информации, которую еще можно было бы спасти. Самое правильное в такой ситуации – это выключить компьютер, чтобы блокировать деятельность вируса. Затем загрузить компьютер с эталонной дискеты операционной системой. После этого запустить антивирусную программу, в функциях которой предусмотрено не только обнаружение инфицированных файлов, но и их лечение. Далее выполнить антивирусную программу повторно. Если все операции по удалению вируса были сделаны правильно, то результатом ее работы должно быть информирование пользователя о полном отсутствии вирусов. Но следует помнить, что программа не должна быть морально устаревшей.

В последнее время при работе в сетях, особенно при пользовании электронной почтой, участилось проникновение вирусов в компьютер пользователя посредством чтения почтовых сообщений. Поэтому здесь также следует соблюдать несколько простых правил:

1) не открывать прикрепленные к письму файлы, кроме случая, когда есть предварительная договоренность с отправителем об их отправке;

2) не открывать прикрепленные к письму файлы, пришедшие от антивирусных лабораторий, компании Microsoft и прочих (компании никогда не занимаются рассылкой файлов);

3) не открывать прикрепленные к письму файлы, если тема письма и само письмо пустые;

4) удалять все подозрительные письма;

5) при длительном отсутствии следует прервать подписку на различные электронные рассылки.

Антивирусные программы. Данные программы можно классифицировать по пяти основным группам: фильтры, детекторы, ревизоры, доктора и вакцинаторы.

Антивирусы-фильтры – резидентные программы, которые оповещают пользователя обо всех попытках какой-либо программы записаться на диск, а уж тем более отформатировать его, а также о других подозрительных действиях. При этом выводится запрос о разрешении или запрещении данного действия. Принцип работы этих программ основан на перехвате соответствующих векторов прерываний. К преимуществу программ этого класса по сравнению с программами-детекторами можно отнести универсальность по отношению как к известным, так и неизвестным вирусам, тогда как детекторы пишутся под конкретные, известные на данный момент программисту виды. Это особенно актуально сейчас, когда появилось множество вирусов-мутантов, не имеющих постоянного кода. Однако программы-фильтры не могут отслеживать вирусы, обращающиеся непосредственно к BIOS, а также BOOT-вирусы, активизирующиеся еще до запуска антивируса, в начальной стадии загрузки DOS. К недостаткам также можно отнести частую выдачу запросов на осуществление какой-либо операции. При установке некоторых антивирусов-фильтров могут возникать конфликты с другими резидентными программами, использующими те же прерывания, которые просто перестают работать.

Наибольшее распространение в нашей стране получили программы-детекторы, а вернее программы, объединяющие в себе функции детектора и доктора. Наиболее известные представители этого класса – Aidstest, Doctor Web, MicroSoft AntiVirus – далее будут рассмотрены подробнее. Антивирусы-детекторы рассчитаны на конкретные вирусы и основаны на сравнении последовательности кодов, содержащихся в теле вируса, с кодами проверяемых программ. Многие программы-детекторы позволяют также лечить зараженные файлы или диски, удаляя из них вирусы (разумеется, лечение поддерживается только для вирусов, известных программе-детектору). Такие программы нужно регулярно обновлять, т. к. они быстро устаревают и не могут обнаруживать новые виды вирусов.

Ревизоры – это программы, которые анализируют текущее состояние файлов и системных областей диска и сравнивают его с информацией, сохраненной ранее в одном из файлов данных ревизора. При этом проверяется состояние BOOT-сектора, таблицы FAT, а также длина файлов, их время

создания, атрибуты, контрольная сумма. Анализируя сообщения программы-ревизора, пользователь может решить, вызваны ли изменения вирусом. При выдаче такого рода сообщений не следует предаваться панике, т. к. причиной изменений, например длины программы, может быть и не вирус.

К еще одной группе относятся самые неэффективные антивирусы – вакцинаторы. Они записывают в вакцинируемую программу признаки конкретного вируса так, что вирус считает ее уже зараженной.

Aidstest. Особую популярность приобрели антивирусные программы, совмещающие в себе функции детектора и доктора. Самой известной из них является программа Aidstest Д. Н. Лозинского. Эта программа была написана в 1988 г., и с тех пор она постоянно совершенствуется и пополняется. Одна из последних версий обнаруживает более 1500 вирусов.

Программа Aidstest предназначена для исправления программ, зараженных обычными (неполиморфными) вирусами, не меняющими свой код. Это ограничение вызвано тем, что поиск вирусов этой программой ведется по опознавательным кодам. Зато при этом достигается очень высокая скорость проверки файлов.

Aidstest для своего нормального функционирования требует, чтобы в памяти не было резидентных антивирусов, блокирующих запись в программные файлы, поэтому их следует выгрузить, либо указать опцию выгрузки самой резидентной программы, либо воспользоваться соответствующей утилитой.

При запуске Aidstest проверяет оперативную память на наличие известных ему вирусов и обезвреживает их. При этом парализуются только функции вируса, связанные с размножением, а другие побочные эффекты могут оставаться. Поэтому программа после окончания обезвреживания вируса в памяти выдает запрос о перезагрузке. Следует обязательно последовать этому совету, если оператор ПЭВМ не является системным программистом, занимающимся изучением свойств вирусов. Причем следует перезагрузиться кнопкой RESET, т. к. при «теплой перезагрузке» некоторые вирусы могут сохраняться. Причем лучше запустить машину и Aidstest с защищенной от записи дискетой, т. к. при запуске с зараженного диска вирус может записаться в память резидентом и препятствовать лечению.

Aidstest тестирует свое тело на наличие известных вирусов, а также по искажениям в своем коде судит о своем заражении неизвестным вирусом. При это возможны случаи ложной тревоги, например при сжатии антивируса упаковщиком. Программа не имеет графического интерфейса, и режимы ее работы задаются с помощью ключей. Указав путь, можно проверить не весь диск, а отдельный подкаталог.

Недостатки программы Aidstest:

- не распознает полиморфные вирусы;
- не снабжена эвристическим анализатором, позволяющим находить неизвестные ей вирусы;
- не умеет проверять и лечить файлы в архивах;

- не распознает вирусы в программах, обработанных упаковщиками исполнимых файлов типа EXEPACK, DIET, PKLITE и т. д.

Достоинства Aidstest:

- легка в использовании;
- работает очень быстро;
- распознает значительную часть вирусов;
- хорошо интегрирована с программой-ревизором Adinf;
- работает практически на любом компьютере.

Doctor Web. В последнее время стремительно растет популярность другой антивирусной программы – Doctor Web, которую предлагает фирма «Диалог-Наука». Эта программа была создана в 1994 г. И. А. Даниловым. Она так же, как и Aidstest, относится к классу детекторов-докторов, но в отличие от последней имеет так называемый «эвристический анализатор» – алгоритм, позволяющий обнаруживать неизвестные вирусы. «Лечебная паутина», как переводится с английского название программы, стала ответом отечественных программистов на нашествие самомодифицирующихся вирусов-мутантов, которые при размножении модифицируют свое тело так, что не остается ни одной характерной цепочки байтов, присутствовавшей в исходной версии вируса. В пользу этой программы говорит тот факт, что крупную лицензию (на 2000 компьютеров) приобрело Главное управление информационных ресурсов при Президенте Российской Федерации, а второй по величине покупатель «паутины» – «Инкомбанк».

Управление режимами так же, как и в Aidtest, осуществляется с помощью ключей. Пользователь может указать программе тестировать как весь диск, так и отдельные подкаталоги или группы файлов, либо же отказаться от проверки дисков и тестировать только оперативную память. В свою очередь можно тестировать либо только базовую память, либо расширенную. Как и Aidstest, Doctor Web может создавать отчет о работе, загружать знакогенератор кириллицы, поддерживать работу с программно-аппаратным комплексом Sheriff.

Тестирование винчестера программой Dr.Web занимает намного больше времени, чем программой Aidstest, поэтому не каждый пользователь может себе позволить тратить столько времени на ежедневную проверку всего жесткого диска. Таким пользователям можно посоветовать более тщательно проверять принесенные извне дискеты. Если информация на дискете находится в архиве (а в последнее время программы и данные переносятся с машины на машину только в таком виде; даже фирмы-производители программного обеспечения, например Borland, пакуют свою продукцию), следует распаковать его в отдельный каталог на жестком диске и сразу же, не откладывая, запустить программу Dr.Web, задав ей в качестве параметра вместо имени диска полный путь к этому подкаталогу. И все же нужно хотя бы раз в две недели производить полную проверку винчестера на вирусы с заданием максимального уровня эвристического анализа.

Так же как и в случае с Aidstest, при начальном тестировании не стоит разрешать программе лечить файлы, в которых она обнаружит вирус, т. к. нельзя исключить, что последовательность байтов, принятая в антивирусе за шаблон может встретиться в здоровой программе.

В отличие от Aidstest программа Dr.Web обладает следующими возможностями:

- распознавание полиморфных вирусов;
- проведение эвристического анализа;
- проверка и лечение файлов в архивах;
- тестирование файлов, вакцинированных CPAV, а также упакованных LZEXE, PKLITE, DIET.

Фирма «Диалог-Наука» предлагает разные версии программы Dr.Web для DOS. Как известно, имеются две версии для DOS, которые традиционно называются *16-разрядной* и *32-разрядной*. В этих названиях (16- и 32-разрядная) полностью отражена суть различия версий для DOS, однако непосредственно из названий она очевидна лишь специалистам. Лишь 32-разрядная версия обладает всеми функциональными возможностями, присущими другим современным версиям Doctor Web (в частности версиям для Windows).

16-разрядная версия в силу ограничений по объему доступной памяти, накладываемых операционной системой, не обладает некоторыми крайне важными на сегодняшний день «умениями», например, в нее не включены (и в силу указанных ограничений по памяти не могут быть включены):

- модули «обслуживания» известных вирусов современных типов (в частности речь идет о макро- и стелс-вирусах);
- модули эвристического анализатора для обнаружения неизвестных вирусов современных типов;
- модули распаковки современных типов архивов и упакованных Windows-программ.

Таким образом, хотя 16-разрядная версия использует ту же вирусную базу (VDB-файлы), что и 32-разрядные версии, отсутствие в ней некоторых модулей делает обработку соответствующих вирусов невозможной. Кроме того, в силу тех же причин 16-разрядная версия не поддерживает некоторые современные программные и аппаратно-технические средства, что может сделать ее работу неустойчивой или некорректной. Поскольку 32-разрядная версия является полнофункциональной и, как видно из другого ее названия – Doctor Web для DOS/386, может использоваться при работе в DOS на компьютерах с процессором не ниже 386, всем пользователям, нуждающимся в версии Doctor Web для DOS, лучше использовать именно ее. Что же касается 16-разрядной версии, то она продолжает выпускаться, поскольку еще существует парк старых машин на платформе 86/286, где 32-разрядная версия работать не может.

AVSP. Эта программа сочетает в себе функции детектора, доктора и ревизора, а также имеет некоторые функции резидентного фильтра (запрет

записи в файлы с атрибутом READ ONLY). Антивирус может лечить как известные, так и неизвестные вирусы, причем о способе лечения последних программе может сообщить сам пользователь. К тому же AVSP может лечить самомодифицирующиеся и стелс-вирусы (невидимки).

При запуске AVSP появляется система окон с меню и информация о состоянии программы. Очень удобна контекстная система подсказок, которая дает пояснения к каждому пункту меню. Она вызывается классически, клавишей F1, и меняется при переходе от пункта к пункту. Также немаловажным достоинством в наш век Windows является поддержка мыши. Существенный недостаток интерфейса AVSP – отсутствие возможности выбора пунктов меню нажатием клавиши с соответствующей буквой, хотя это несколько компенсируется возможностью выбрать пункт, нажав ALT и цифру, соответствующую номеру этого пункта.

В состав пакета AVSP входит также *резидентный драйвер AVSP.SYS*, который позволяет обнаруживать большинство невидимых вирусов (кроме вирусов типа Ghost-1963 или DIR), дезактивировать вирусы на время своей работы, а также запрещает изменять файлы READ ONLY.

Еще одна функция AVSP.SYS – *отключение на время работы AVSP.EXE резидентных вирусов*, правда вместе с вирусами драйвер отключает и некоторые другие резидентные программы. При первом запуске AVSP следует протестировать систему на наличие известных вирусов. При этом проверяется оперативная память, BOOT-сектор и файлы. В ряде случаев можно восстанавливать даже файлы, испорченные неизвестным вирусом. Можно установить проверку размеров файлов, их контрольных сумм, наличие в них вирусов либо все это вместе. Также можно указать, что именно проверять (Boot-сектор, память, или файлы). Как и в большинстве антивирусных программ, здесь пользователю предоставляется возможность выбрать между скоростью и качеством. Суть скоростной проверки заключается в том, что просматривается не весь файл, а только его начало; при этом удается обнаружить большинство вирусов. Если же вирус пишется в середину либо файл заражен несколькими вирусами (при этом «старые» вирусы как бы оттесняются в середину «молодым»), то программа его и не заметит. Поэтому следует установить оптимизацию по качеству, тем более что в AVSP качественное тестирование занимает не намного больше времени, чем скоростное.

При автоматическом определении новых вирусов AVSP может допустить множество ошибок. Так что при автоматическом определении шаблона следует проверить, действительно ли это вирус и не будет ли этот шаблон встречаться в здоровых программах.

Если в процессе AVSP обнаружит известный вирус, то следует предпринять те же действия, как и при работе с Aidstest и Dr.Web: скопировать файл на диск, перезагрузиться с резервной дискеты и запустить AVSP. Желательно также, чтобы при этом в память был загружен драйвер AVSP.SYS, т. к. он помогает основной программе лечить стелс-вирусы.

Еще одной полезной функцией является *встроенный дизассемблер*. С его помощью можно разобраться, есть ли в файле вирус или при проверке диска произошло ложное срабатывание AVSP. Кроме того, можно попытаться выяснить способ заражения, принцип действия вируса, а также место, куда он «спрятал» замещенные байты файла (если мы имеем дело с таким типом вируса). Все это позволит написать процедуру удаления вируса и восстановить испорченные файлы. Еще одна полезная функция – выдача *наглядной карты изменений*. Карта изменений позволяет оценить, соответствуют ли эти изменения вирусу или нет, а также сузить область поиска тела вируса при дизассемблировании.

В программе AVSP есть два алгоритма нейтрализации стелс-вирусов («невидимок») и оба они работают только при наличии активного вируса в памяти. Вот, что происходит при реализации этих алгоритмов: все файлы копируются в файлы данных, а потом стираются. Спасаются только файлы с атрибутом SYSTEM. В Adinf процесс удаления стелс-вирусов реализован гораздо проще.

Программа AVSP контролирует также и состояние загрузочных секторов. Если заражен BOOT-сектор на дискете и антивирус не может его вылечить, то следует стереть загрузочный код. Дискета при этом станет несистемной, но данные при этом не потеряются. С винчестером так поступать нельзя. При обнаружении изменений в одном из BOOT-секторов жесткого диска AVSP предложит его сохранить в некотором файле, а затем попытается удалить вирус.

Microsoft Antivirus. В состав современных версий MS-DOS (например 6.22) входит антивирусная программа Microsoft Antivirus (MSAV). Этот антивирус может работать в режимах детектора-доктора и ревизора, имеет *интерфейс в стиле MS-Windows*. Хорошо реализована *контекстная помощь:* подсказка есть практически к любому пункту меню, к любой ситуации. Универсально реализован доступ к пунктам меню: для этого можно использовать клавиши управления курсором, ключевые клавиши (F1–F9), клавиши, соответствующие одной из букв названия пункта, а также мышь. Серьезным неудобством при использовании программы является то, что она сохраняет таблицы с данными о файлах не в одном файле, а разбрасывает их по всем директориям.

При первой проверке MSAV создает в каждой директории, содержащей исполнимые файлы, файлы CHKLIST.MS, в которые записывает информацию о размере, дате, времени, атрибутах, а также контрольную сумму контролируемых файлов. При последующих проверках программа будет сравнивать файлы с информацией в CHKLIST.MS-файлах. Если изменились размер и дата, то программа сообщит об этом пользователю и запросит дальнейшие действия: обновить информацию (Update), установить дату и время в соответствии с данными в CHKLIST.MS (Repair), продолжить, не обращая внимания на изменения в данном файле (Continue), прервать проверку (Stop).

В меню Options можно сконфигурировать программу по собственному желанию. Здесь можно установить режим поиска вирусов-невидимок (Anti-Stealth), проверки всех (а не только исполнимых) файлов (Check All Files), а также разрешить или запретить создавать таблицы CHKLIST.MS (Create New Checksums). К тому же можно задать режим сохранения отчета о проделанной работе в файле. Если установить опцию Create Backup, то перед удалением вируса из зараженного файла его копия будет сохранена с расширением VIR.

Находясь в основном меню, можно просмотреть список вирусов, известных программе MSAV, нажав клавишу F9. При этом выведется окно с названиями вирусов. Чтобы посмотреть более подробную информацию о вирусе, нужно подвести курсор к его имени и нажать ENTER. Можно быстро перейти к интересующему вирусу, набрав первые буквы его имени. Информацию о вирусе можно вывести на принтер, выбрав соответствующий пункт меню.

ADinf (Advanced Diskinfoscope). Относится к классу программ-ревизоров. Эта программа была создана Д. Ю. Мостовым в 1991 г. Семейство программ ADinf – это ревизоры дисков, предназначенные для работы на персональных компьютерах под управлением операционных систем MS-DOS, MS-Windows 3.xx, Windows 95/98 и Windows NT/2000. Работа программ основана на регулярном отслеживании изменений, происходящих на жестких дисках. В случае появления вируса ADinf обнаруживает его по тем модификациям, которые он выполняет в файловой системе и/или загрузочном секторе диска и информирует об этом пользователя. В отличие от антивирусов-сканеров ADinf не использует в своей работе «портреты» (сигнатур) конкретных вирусов. Поэтому ADinf особенно эффективен для обнаружения новых вирусов, противоядие для которых еще не придумано.

Особенно следует отметить, что для контроля дисков ADinf не использует функции операционной системы. Он читает диск по секторам и самостоятельно разбирает структуру файловой системы, что позволяет ему обнаруживать так называемые вирусы-невидимки (стелс-вирусы).

Если в системе установлен лечащий блок ADinf (*ADinf Cure Module*), то этот тандем способен не только обнаруживать, но и успешно удалять вирус. Тестирование показало, что ADinf Cure Module способен успешно справиться с 97 % вирусов, восстановив поврежденные файлы с точностью до байта.

Полезные свойства ADinf не ограничиваются только лишь борьбой с вирусами. По сути ADinf является системой, позволяющей следить за сохранностью информации на дисках и обнаруживать любые, даже малозаметные изменения в файловой системе, а именно: изменения системных областей, изменения файлов, создание и удаление каталогов, создание, удаление, переименование и перемещение файлов из каталога в каталог. Состав контролируемой информации гибко настраивается, что позволяет ставить под контроль только то, что нужно.

Первая версия программы вышла в 1991 г. и с тех пор ADinf заслуженно является самым популярным ревизором в России и странах бывшего СССР.

Сегодня уже трудно сосчитать число легальных и нелегальных пользователей ADinf. Более 2500 корпоративных подписчиков антивирусного комплекта фирмы «Диалог-Наука», в составе которого поставляется ADinf, защищают им свои компьютеры. Программа ADinf получила сертификаты в Системе сертификации ГОСТ Р, Системе сертификации средств защиты информации Министерства обороны и Сертификат Государственной технической комиссии при Президенте Российской Федерации (в составе антивирусного комплекта фирмы «Диалог-Наука»). Программа постоянно совершенствуется и все время находится на острие современных технологий. Сейчас существует семейство совместимых между собой ревизоров для различных операционных систем.

Итак, программа ADinf:

- имеет высокую скорость работы;
- способна с успехом противостоять вирусам, находящимся в памяти;
- позволяет контролировать диск, читая его по секторам через BIOS и не используя системные прерывания DOS, которые может перехватить вирус;
- может обрабатывать до 32 000 файлов на каждом диске;
- в отличие от AVSP, когда пользователю приходится самому анализировать, заражена ли машина стелс-вирусом, загружаясь сначала с винчестера, а потом с эталонной дискеты, в ADinf эта операция происходит автоматически;
- в отличие от других антивирусов Advanced Diskinfoscope не требует загрузки с эталонной, защищенной от записи дискеты, т. к. при загрузке с винчестера надежность защиты не уменьшается;
- имеет хорошо выполненный дружественный интерфейс, который в отличие от AVSP реализован не в текстовом, а в графическом режиме;
- при инсталляции ADinf в систему имеется возможность изменить имя основного файла ADINF.EXE и имя таблиц, при этом пользователь может задать любое имя. Это очень полезная функция, т. к. в последнее время появилось множество вирусов, «охотящихся» за антивирусами (например, есть вирус, который изменяет программу Aidstest так, что она вместо заставки фирмы «Диалог-Наука» пишет: «Лозинский – пень»), в том числе и за ADinf.

Существует несколько вариантов ревизора ADinf для различных операционных систем. Каждый из них имеет свои особенности.

Ревизор *ADinf* предназначен для операционных систем MS-DOS и Windows 95/98. Это развитие первого варианта ревизора, созданного еще в 1991 г. Сегодня ADinf это самое надежное средство для обнаружения как известных, так и новых неизвестных вирусов. Это единственный в мире ревизор, проверяющий файловую систему чтением по секторам напрямую через BIOS компьютера.

Ревизор *ADinf Pro* предназначен для контроля за сохранностью особо ценной информации, например баз данных или документов, в среде различных операционных систем. Особенностью этого варианта программы является использование 64-битной хэш-функции для контроля целостности файлов, разработанной известной российской фирмой ЛАН-Крипто. Использование

этой хэш-функции гарантирует не только обнаружение случайных изменений файлов или изменений, вызванных вирусами, но и делает невозможным преднамеренную незаметную модификацию данных на диске.

Следует заметить, что программа ADinf хорошо интегрирована с другими программами комплекта DSAV фирмы «Диалог-Наука». Так, ADinf создает список новых и измененных файлов на диске, а Aidstest и Dr.Web могут проверять файлы из этого списка, что значительно сокращает время работы этих программ.

AVP (AntiViral Toolkit Pro). Данная программа была создана ЗАО «Лаборатория Касперского». AVP обладает одним из самых совершенных механизмов обнаружения вирусов. Сегодня AVP практически ни в чем не уступает западным аналогам.

AVP предоставляет пользователям максимум сервиса: возможность обновления антивирусных баз через Интернет, возможность задания параметров автоматического сканирования и лечения зараженных файлов. Обновления на сайте AVP появляются практически еженедельно, а база данных включает описания уже почти 40 000 вирусов.

AVP состоит из нескольких важных модулей:

1) *AVP-сканер* проверяет жесткие диски на предмет заражения вирусами. Можно задать полный поиск, при котором программа будет проверять все файлы подряд, а также задать режим проверки архивированных файлов. Одно из главных преимуществ AVP – *борьба с макровирусами*. Пользователь может выбрать специальный режим, при котором будут проверяться документы, созданные в формате Microsoft Office. После обнаружения вирусов или зараженных файлов AVP предлагает на выбор несколько вариантов: удалить вирусы из файлов, удалить сами зараженные файлы или переместить их в специальную папку.

2) *AVP-Monitor.* Эта программа автоматически загружается при запуске Windows, автоматически проверяет все запускаемые на компьютере файлы и открываемые документы и в случае вирусной атаки сигнализирует об этом пользователю. Более того, в большинстве случаев AVP Monitor просто не дает зараженному файлу запуститься, блокируя процесс его выполнения. Эта функция программы очень полезна для тех, кто постоянно имеет дело со множеством новых файлов, например, для активных пользователей сети Интернет (т. к. каждые пять минут запускать AVP для проверки скачанных файлов невозможно, на помощь приходит AVP Monitor).

3) *AVP-Inspector* – последний и очень важный модуль комплекта AVP, позволяющий отлавливать даже неизвестные вирусы. Программа использует метод контроля изменения размера файлов. Внедряясь в файл, вирус неизбежно увеличивает его объем, и AVP-Inspector легко его обнаруживает.

Кроме всего перечисленного существует так называемый *Центр Управления AVP* – «пульт управления» всеми программами комплекса AVP. Самая важная функция этой программы – встроенный «Планировщик задач», позволяющий осуществлять оперативную проверку (а если понадобится – и

лечение системы) в автоматическом режиме, без участия пользователя, но в заданное им время.

7.1.2. Методы обнаружения вирусов и защиты от них

Существуют основные признаки наличия вирусов в компьютере, к которым относят:

- достаточно заметное замедление работы самого компьютера;
- проявления неисправностей в работе операционной системы в виде систематически появляющихся сообщений об ошибках, невозможности совершить какое-либо действие и т. д.;
- некорректная работа ранее нормально функционирующих программ, а также неожиданное завершение их работы;
- нехватка свободной оперативной памяти, вплоть до беспричинного уменьшения ее общего объема;
- приостановки, зависания, сбои в работе операционной системы;
- некорректная, долгая загрузка операционной системы, вплоть до невозможности ее загрузки;
- невозможность отображения каких-либо данных, изменение свойств файлов;
- увеличение количества файлов на жестком диске;
- незапланированная перезагрузка операционной системы;
- отображение на экране каких-либо сообщений и изображений, связанных с оплатой счетов, переводом денег и т. д.

Проявлений, признаков деятельности компьютерных вирусов существует много, но самый главный признак – операционная система стала работать отлично от той работы, которая вас устраивала.

В зависимости от проявлений компьютерных вирусов компьютерный мастер должен принять грамотное решение по устранению последствий работы этих вирусов, удалению самих вирусов, а также созданию таких условий работы компьютера, при которых возможность заражения была бы наиболее низкой.

Программно-технические методы обнаружения вирусов. Основным средством борьбы с вирусами были и остаются антивирусные программы. Можно использовать антивирусные программы (антивирусы), не имея представления о том, как они устроены. Однако без понимания принципов устройства антивирусов, знания типов вирусов, а также способов их распространения нельзя организовать надежную защиту компьютера. Как результат, компьютер может быть заражен, даже если на нем установлены антивирусы.

Сегодня используется несколько основополагающих методик обнаружения и защиты от вирусов:

- сканирование;
- эвристический анализ;

- использование антивирусных мониторов;
- обнаружение изменений;
- использование антивирусов, встроенных в BIOS компьютера.

Кроме того, практически все антивирусные программы обеспечивают автоматическое восстановление зараженных программ и загрузочных секторов. Конечно, если это возможно.

Сканирование. Самая простая методика поиска вирусов заключается в том, что антивирусная программа последовательно просматривает проверяемые файлы в поиске сигнатур известных вирусов. Под сигнатурой понимается уникальная последовательность байтов, принадлежащая вирусу и не встречающаяся в других программах.

Антивирусные программы-сканеры способны найти только уже известные и изученные вирусы, для которых была определена сигнатура. Применение простых программ-сканеров не защищает компьютер от проникновения новых вирусов.

Для шифрующихся и полиморфных вирусов, способных полностью изменять свой код при заражении новой программы или загрузочного сектора, невозможно выделить сигнатуру. Поэтому простые антивирусные программы-сканеры не могут обнаружить полиморфные вирусы.

Эвристический анализ. Эвристический анализ позволяет обнаруживать ранее неизвестные вирусы, причем для этого не надо предварительно собирать данные о файловой системе.

Антивирусные программы, реализующие метод эвристического анализа, проверяют программы и загрузочные секторы дисков и дискет, пытаясь обнаружить в них код, характерный для вирусов. Эвристический анализатор может обнаружить, например, что проверяемая программа устанавливает резидентный модуль в памяти или записывает данные в исполнимый файл программы.

Практически все современные антивирусные программы реализуют собственные методы эвристического анализа. На рис. 5 показана одна из таких программ – сканер McAffee VirusScan, запущенный вручную для антивирусной проверки диска.

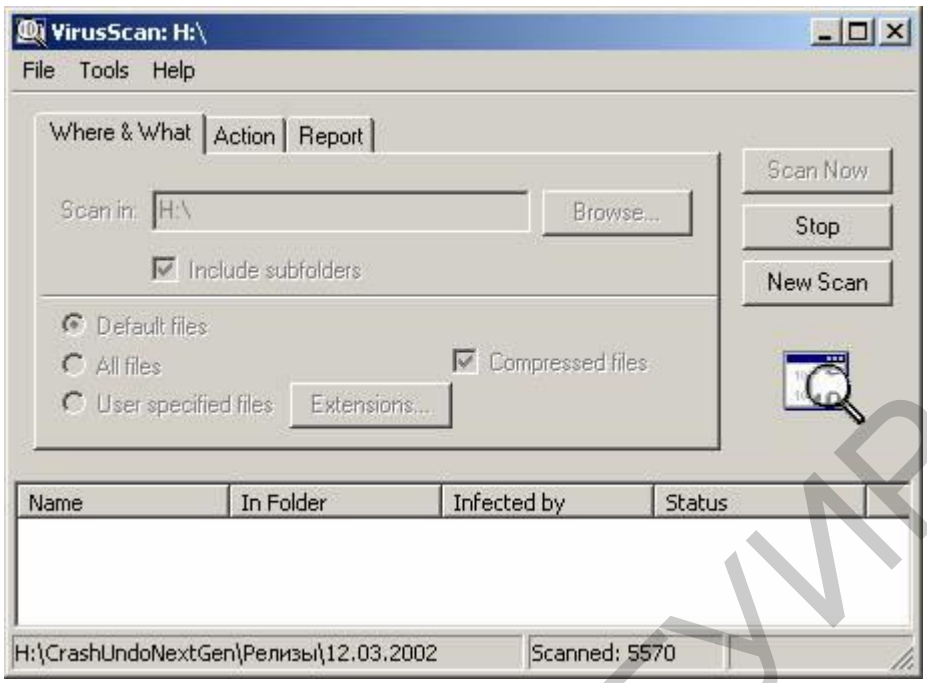

Рис. 5. Сканер McAffee VirusScan проверяет диск

Когда антивирус обнаруживает зараженный файл, он обычно выводит сообщение на экране монитора и делает запись в собственном или системном журнале. В зависимости от настроек антивирус может также направлять сообщение об обнаруженном вирусе администратору сети.

Если это возможно, антивирус вылечивает файл, восстанавливая его содержимое. В противном случае предлагается только одна возможность – удалить зараженный файл и затем восстановить его из резервной копии.

Антивирусные мониторы. Существует еще целый класс антивирусных программ, которые постоянно находятся в памяти компьютера и отслеживают все подозрительные действия, выполняемые другими программами. Такие программы носят название антивирусных мониторов, или сторожей.

Монитор автоматически проверяет все запускаемые программы, создаваемые, открываемые и сохраняемые документы, файлы программ и документов, полученные через Интернет или скопированные на жесткий диск с дискеты или компакт-диска. Антивирусный монитор сообщит пользователю, если какая-либо программа попытается выполнить потенциально опасное действие.

В комплект одного из наиболее совершенных сканеров Doctor Web (рис. 6), разработанных Игорем Даниловым (http://www.drweb.ru), входит сторож Spider Guard, выполняющий функции антивирусного монитора.

Рис. 6. Сканер Doctor Web

Обнаружение изменений. Когда вирус заражает компьютер, он изменяет содержимое жесткого диска, например, дописывает свой код в файл программы или документа, добавляет вызов программы-вируса в файл AUTOEXEC.BAT, изменяет загрузочный сектор, создает файл-спутник. Таких изменений, однако, не делают «бестелесные» вирусы, обитающие не на диске, а в памяти процессов ОС.

Антивирусные программы, называемые ревизорами диска, не выполняют поиск вирусов по сигнатурам. Они запоминают предварительно характеристики всех областей диска, которые подвергаются нападению вируса, а затем периодически проверяют их (отсюда происходит название «программы-ревизоры»). Ревизор может найти изменения, сделанные известным или неизвестным вирусом.

В качестве примеров ревизоров диска можно привести программы Advanced Diskinfoscope (ADinf) производства ЗАО «Диалог-Наука» (http://www.dials.ru, http://www.adinf.ru) и AVP Inspector производства ЗАО «Лаборатория Касперского» (http://www.kaspersky.ru).

Вместе с ADinf применяется лечащий модуль ADinf Cure Module (ADinfExt), который использует собранную ранее информацию о файлах для восстановления их после поражения неизвестными вирусами. Ревизор AVP Inspector также имеет в своем составе лечащий модуль, способный удалять вирусы.

Защита, встроенная в BIOS компьютера. В системные платы компьютеров тоже встраивают простейшие средства защиты от вирусов. Эти средства позволяют контролировать все обращения к главной загрузочной записи жестких дисков, а также к загрузочным секторам дисков и дискет. Если

какая-либо программа попытается изменить содержимое загрузочных секторов, срабатывает защита и пользователь получает соответствующее предупреждение.

Однако эта защита не очень надежна. Существуют вирусы (например Tchechen.1912 и Tchechen.1914), которые пытаются отключить антивирусный контроль BIOS, изменяя некоторые ячейки в энергонезависимой памяти (CMOS-памяти) компьютера.

Особенности защиты корпоративной интрасети. Корпоративная интрасеть может насчитывать сотни и тысячи компьютеров, играющих роль рабочих станций и серверов. Эта сеть обычно подключена к Интернету и в ней имеются почтовые серверы, серверы систем автоматизации документооборота, такие как Microsoft Exchange и Lotus Notes, а также нестандартные информационные системы.

Для надежной защиты корпоративной интрасети необходимо установить антивирусы на все рабочие станции и серверы. При этом на файл-серверах, серверах электронной почты и серверах систем документооборота следует использовать специальное серверное антивирусное программное обеспечение. Что же касается рабочих станций, их можно защитить обычными антивирусными сканерами и мониторами.

Разработаны специальные антивирусные прокси-серверы и брандмауэры, сканирующие проходящий через них трафик и удаляющие из него вредоносные программные компоненты. Эти антивирусы часто применяются для защиты почтовых серверов и серверов систем документооборота.

Защита файловых серверов. Защита файловых серверов должна осуществляться с использованием антивирусных мониторов, способных автоматически проверять все файлы сервера, к которым идет обращение по сети. Антивирусы, предназначенные для защиты файловых серверов, выпускают все антивирусные компании, поэтому на рынке предлагается широкий выбор.

Защита почтовых серверов. Антивирусные мониторы неэффективны для обнаружения вирусов в почтовых сообщениях. Для этого необходимы специальные антивирусы, способные фильтровать трафик SMTP, POP3 и IMAP, исключая попадание зараженных сообщений на рабочие станции пользователей.

Для защиты почтовых серверов можно приобрести антивирусы, специально предназначенные для проверки почтового трафика, или подключить к почтовому серверу обычные антивирусы, допускающие работу в режиме командной строки.

Домен антивируса Doctor Web можно интегрировать со всеми наиболее известными почтовыми серверами и системами, такими как Doctor Commini Gate Pro, Sendmail, Postfix, Exim, QMail и Zmailer. Аналогичные средства предоставляются и Лабораторией Касперского в составе пакета Kaspersky Corporate Suite.

Почтовый сервер MERAK Mail Server допускает подключение внешних антивирусов различных типов, имеющих интерфейс командной строки. Некоторые почтовые серверы (например EServ) поставляются со встроенным антивирусом.

Можно также дополнительно проверять трафик POP3 и на рабочих станциях пользователей. Это позволяет сделать, например, антивирусный прокси-сервер SpIDer Mail для протокола POP3, который можно приобрести вместе с антивирусом Doctor Web.

Защита серверов систем документооборота. Серверы систем документооборота, такие как Microsoft Exchange и Lotus Notes, хранят документы в базах данных собственного формата. Поэтому использование обычных файловых сканеров для антивирусной проверки документов не даст никаких результатов.

Существует ряд антивирусных программ, специально предназначенных для антивирусной защиты подобных систем. Это Trend MicroScanMail для Lotus Notes, McAfee GroupScan и McAfee GroupShield, Norton Antivirus для Lotus Notes, антивирус Касперского Business Optimal для MS Exchange Server и некоторые другие.

Эти программы сканируют почту и файлы вложений, удаляя в реальном времени все вредоносные программы, обнаруживают макрокомандные вирусы и троянские программы в формах и макросах файлов сценариев и объектов OLE. Проверка выполняется в режиме реального времени, а также по требованию.

Защита нестандартных информационных систем. Для антивирусной защиты нестандартных информационных систем, хранящих данные в собственных форматах, необходимо либо встраивать антивирусное ядро в систему, либо подключать внешний сканер, работающий в режиме командной строки.

Например, ядро антивируса Doctor Web было использовано ФГУП «НПО машиностроения» для защиты системы документооборота, созданной на базе собственной технологии Sapiens (http://www.npomit.ru). Вся информация, сохраняемая этой системой в базе данных, проверяется антивирусным ядром Doctor Web.

Как разработчики информационных систем для ответственного применения, предприятие «НПО машиностроения» снабдило антивирусной защитой такие свои разработки, как Sapiens Регистрация и Контроль Исполнения Документов, Sapiens Мониторинг Вычислительных Ресурсов, Sapiens Электронный Архив Конструкторской Документации.

Сетевой центр управления антивирусами. Если интрасеть насчитывает сотни и тысячи компьютеров, то необходимо централизованное удаленное управление антивирусными программами и контроль их работы. Выполнение в «ручном» режиме таких операций, как отслеживание обновлений антивирусной базы данных и загрузочных модулей антивирусных программ, контроль эффективности обнаружения вирусов на рабочих станциях и серверах и т. п.,

малоэффективно, если в сети имеется большое количество пользователей или если сеть состоит из территориально удаленных друг от друга сегментов.

Если же не обеспечить своевременное и эффективное выполнение перечисленных выше операций, технология антивирусной защиты корпоративной сети обязательно будет нарушена, что рано или поздно приведет к вирусному заражению. Например, пользователи могут неправильно настроить автоматическое обновление антивирусной базы данных или просто выключать свои компьютеры в то время, когда такое обновление выполняется. В результате автоматическое обновление не будет выполнено и возникнет потенциальная угроза заражения новыми вирусами.

В современных антивирусных системах реализованы следующие функции удаленного управления и контроля:

- установка и обновление антивирусных программ, а также антивирусных баз данных;
- централизованная дистанционная установка и настройка антивирусов;
- автоматическое обнаружение новых рабочих станций, подключенных к корпоративной сети, с последующей автоматической установкой на эти станции антивирусных программ;
- планирование заданий для немедленного или отложенного запуска (обновление программ или антивирусной базы данных, сканирование файлов и т. п.) на любых компьютерах сети;
- отображение в реальном времени процесса работы антивирусов на рабочих станциях и серверах сети.

Все перечисленные выше функции или многие из них реализованы в сетевых центрах управления ведущих корпоративных антивирусных продуктов, созданных компаниями Sophos, Symantec, Network Associates и Лаборатория Касперского.

Сетевые центры управления позволяют управлять антивирусной защитой всей сети с одной рабочей станции системного администратора. При этом для ускорения процесса установки антивирусов в удаленных сетях, подключенных к основной сети медленными каналами связи, создаются собственные локальные дистрибутивные каталоги.

При использовании клиент-серверной архитектуры основой сетевого центра управления является антивирусный сервер, установленный на одном из серверов корпоративной сети. С ним взаимодействуют, с одной стороны, программы-агенты, установленные вместе с антивирусами на рабочих станциях сети, а с другой стороны, – управляющая консоль администратора антивирусной защиты (рис. 7).

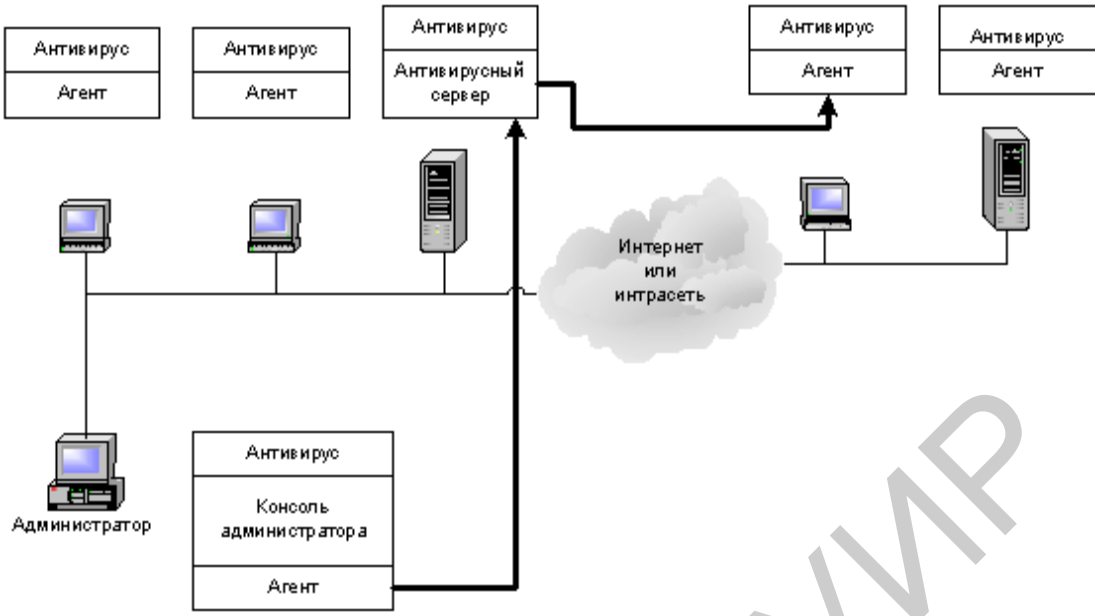

Рис. 7. Взаимодействие консоли администратора, агентов и антивирусного сервера

Антивирусный сервер выполняет управляющие и координирующие действия. Он хранит общий журнал событий, имеющих отношение к антивирусной защите и возникающих на всех компьютерах сети, список и расписание выполнения заданий. Антивирусный сервер отвечает за прием от агентов и передачу администратору антивирусной защиты сообщений о возникновении тех или иных событий в сети, выполняет периодическую проверку конфигурации сети с целью обнаружения новых рабочих станций или рабочих станций с изменившейся конфигурацией антивирусных средств и т. д.

Помимо агентов на каждой рабочей станции и сервере корпоративной сети устанавливается антивирус, выполняющий сканирование файлов и их проверку при открытии (функции сканера и антивирусного монитора). Результаты работы антивируса передаются через агентов антивирусному серверу, который их анализирует и протоколирует в журнале событий.

Управляющая консоль может представлять собой стандартное приложение Microsoft Windows с оконным интерфейсом или апплет управляющей консоли Control Panel операционной системы Microsoft Windows. Первый подход реализован, например, в управляющей системе антивирусов Sophos, а второй – в управляющей системе Norton AntiVirus.

Пользовательский интерфейс управляющей консоли позволяет просматривать древовидную структуру корпоративной сети, получая при необходимости доступ к отдельным компьютерам тех или иных групп пользователей или доменов.

Многоуровневые системы с Web-интерфейсом. Архитектура многоуровневых систем с Web-интерфейсом предполагает использование Web-сервера в качестве ядра системы. Задачей этого ядра является организация

диалогового интерактивного взаимодействия, с одной стороны, с пользователем, а с другой, – с программными модулями той или иной системы.

Преимущества такого подхода заключаются в унификации способов управления различными системами сети, а также в отсутствии необходимости устанавливать на рабочую станцию администратора какие-либо управляющие программы или консоли. Администрирование может выполняться с любого компьютера сети, а если сеть подключена к Интернету, то из любого места земного шара, где есть Интернет и компьютер с браузером.

Для защиты управляющей информации при ее передаче по Интернету или корпоративной интрасети применяются протоколы SSH или другие аналогичные средства (например, собственные защищенные модификации протокола HTTP).

На рис. 8 изображена структурная схема системы антивирусной защиты с Web-интерфейсом Trend Virus Control System. Эта система позволяет полностью управлять и контролировать работу корпоративной системы антивирусной защиты с одной рабочей станции через браузер, даже если отдельные фрагменты сети находятся в разных странах или на разных континентах.

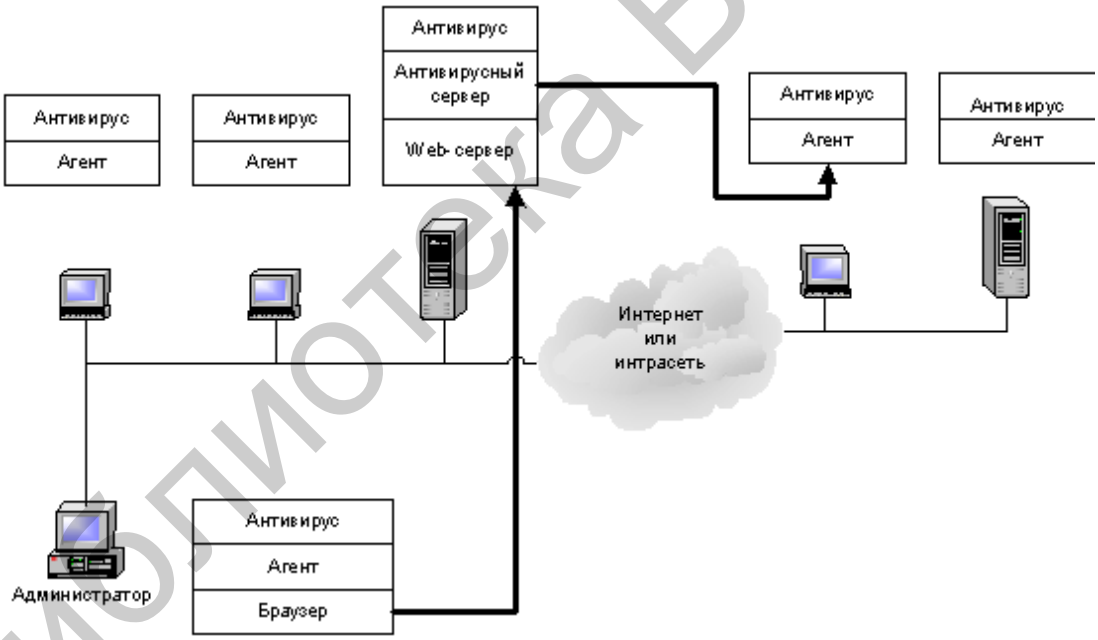

Рис. 8. Антивирусная система с Web-интерфейсом

Эта схема аналогична схеме, показанной на рис. 7, однако администратор антивирусной защиты управляет ее работой через браузер, а не через консольное приложение.

На рабочих станциях устанавливается антивирус, например PC-cillin, Server Protect, InterScan VirusWall, ScanMail и т. д., который управляется антивирусным сервером через агента.

На компьютере, играющем роль антивирусного сервера, устанавливается Web-сервер Microsoft IIS. Специальное Web-приложение, работающее на этом

сервере, управляет антивирусным сервером. Оно также предоставляет администратору пользовательский интерфейс для управления системой антивирусной защиты.

С целью обеспечения максимальной независимости от компьютерных платформ сервер Trend VCS Server и клиентское приложение написаны на языке программирования Java и других языках, применяющихся для разработки приложений Интернета.

Что же касается извещений о возникновении событий в корпоративной системе антивирусной защиты, то они передаются программами-агентами серверу Trend VCS Server и рассылаются по электронной почте через системы SMS и т. п.

Административно-технологические методы защиты. Для того чтобы антивирусные программы эффективно выполняли свои функции, необходимо строго соблюдать рекомендации по их применению, описанные в документации. Особое внимание следует обратить на необходимость регулярного обновления вирусных баз данных и программных компонент антивирусов. Современные антивирусы умеют загружать файлы обновлений через Интернет или по локальной сети, но для этого их необходимо настроить соответствующим образом.

Однако даже без применения антивирусных программ можно постараться предотвратить проникновение вирусов в компьютер и уменьшить вред, который они нанесут в случае заражения. Вот что следует для этого сделать в первую очередь:

- блокируйте возможные каналы проникновения вирусов: не подключайте компьютер к Интернету и локальной сети компании, если в этом нет необходимости, отключите устройства внешней памяти, такие как дисководы для дискет и устройства CD-ROM;
- настройте параметры BIOS таким образом, чтобы загрузка ОС выполнялась только с жесткого диска, но не с дискет;
- запретите программное изменение содержимого энергонезависимой памяти BIOS;
- изготовьте системную загрузочную дискету, записав на нее антивирусы и другие системные утилиты для работы с диском, а также диск аварийного восстановления Microsoft Windows;
- проверяйте все программы и файлы документов, записываемые на компьютер, а также дискеты с помощью антивирусных программ новейших версий;
- устанавливайте программное обеспечение только с лицензионных компакт-дисков;
- установите на всех дискетах защиту от записи и снимайте ее только в случае необходимости;
- ограничьте обмен программами и дискетами;
- регулярно выполняйте резервное копирование данных;

- устанавливайте минимально необходимые права доступа к каталогам файлового сервера, защищайте от записи каталоги дистрибутивов и программных файлов;

- составьте инструкцию для пользователей по антивирусной защите, описав в ней правила использования антивирусов, правила работы с файлами и электронной почтой, а также действия, которые следует предпринять при обнаружении вирусов.

Проблема домашних компьютеров. Часто сотрудники компаний работают не только в офисе, но и дома, обмениваясь файлами между домашним компьютером и офисной рабочей станцией. Системный администратор компании не в состоянии защитить от вирусов все домашние компьютеры сотрудников, т. к. вирусы могут попасть из Интернета, а также в результате обмена игровыми программами. Зачастую это происходит, если к домашнему компьютеру имеют доступ другие члены семьи и дети.

Все файлы, которые сотрудники приносят из дома на работу, следует рассматривать как потенциально опасные. В особо важных случаях такой обмен следует полностью запретить либо сильно ограничить. Потенциально опасные «домашние» файлы необходимо проверять перед открытием антивирусными программами.

Установка персональных брандмауэров. Корпоративная сеть, подключенная к Интернету, должна быть защищена от атак хакеров при помощи брандмауэра. Однако помимо этого можно дополнительно защитить рабочие станции и серверы сети, установив на них персональные брандмауэры, такие как AtGuard (рис. 9).

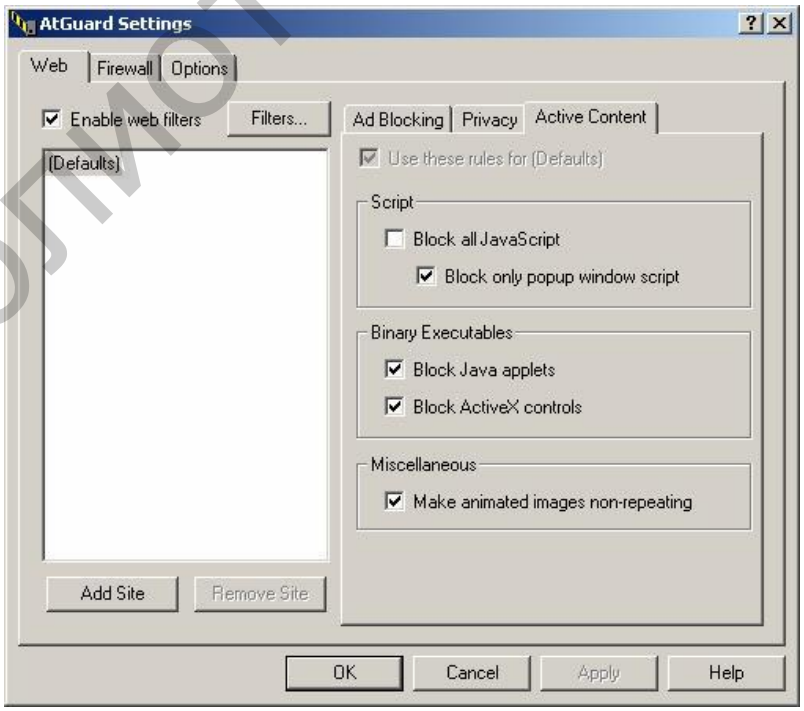

Рис. 9. Настройка персонального брандмауэра AtGuard

Помимо фильтрации нежелательного трафика, некоторые персональные брандмауэры способны защитить компьютер от троянских апплетов Java и элементов управления ActiveX. Такие компоненты могут быть встроены в почтовые сообщения формата HTML и в страницы троянских Web-сайтов.

Персональные брандмауэры, находящиеся в так называемом режиме обучения, могут оказать помощь в обнаружении трафика от троянских программ, логических бомб и других нежелательных вредоносных компонентов. Когда такой компонент попытается установить связь с компьютером хакера, брандмауэр отобразит на экране предупреждающее сообщение.

Следует заметить, что в настройках браузера можно отключить активные компоненты, такие как аплеты Java и элементы управления ActiveX. Однако персональные брандмауэры более универсальны и позволяют блокировать использование названных компонентов любыми программами, например почтовыми клиентами.

При работе с современным персональным компьютером пользователя (особенно начинающего) может подстерегать множество неприятностей: потеря данных, зависание системы, выход из строя отдельных частей компьютера и др. Одной из причин этих проблем наряду с ошибками в программном обеспечении и неумелыми действиями самого оператора ПЭВМ могут быть проникшие в систему компьютерные вирусы.

Сегодня самой распространенной группой вирусов стали макровирусы, заражающие не программы, а документы, созданные в Microsoft Word и Microsoft Excel.

Путей распространения вирусов существует множество. Вирус может попасть в компьютер пользователя вместе с дискетой, пиратским компакт-диском или сообщением электронной почты. Чтобы этого не случилось, каждому пользователю следует хорошо знать принципы защиты от компьютерных вирусов. Ведь нет никакой надежды на то, что с приходом нового тысячелетия вирусы исчезнут. Так же как и нет надежды справиться с ними окончательно в какие-то обозримые сроки, т. к. таланту авторов антивирусных программ противостоит фантазия компьютерных графоманов.

7.1.3 Антивирусная проверка электронной почты

Если на заре развития компьютерных технологий основным каналом распространения вирусов был обмен файлами программ через дискеты, то сегодня «пальма первенства» принадлежит электронной почте. Каждый день по ее каналам передаются миллионы и миллионы сообщений, причем многие из них заражены вирусами.

К сожалению, файлы вложений, передаваемые вместе с электронными сообщениями, также могут оказаться чрезвычайно опасными для «здоровья» компьютера. В чем опасность файлов вложения? В качестве такого файла пользователю могут прислать вирусную или троянскую программу либо

документ в формате Microsoft Office (*.doc, *.xls), зараженные компьютерным вирусом. Запустив полученную программу на выполнение или открыв для просмотра документ, пользователь может инициировать вирус или установить на свой компьютер троянскую программу. Более того, из-за неправильных настроек почтовой программы или имеющихся в ней ошибок файлы вложений могут открываться автоматически при просмотре содержимого полученных писем. В этом случае, если не предпринимать никаких защитных мер, проникновение вирусов или других вредоносных программ на ваш компьютер – дело времени.

Возможны и другие попытки проникновения вирусов в компьютер через электронную почту. Например, могут прислать сообщение в виде документа HTML, в который встроен троянский элемент управления ActiveX. Открыв такое сообщение, вы можете загрузить этот элемент на свой компьютер, после чего тот немедленно начнет делать свое дело.

Защита от вирусов, распространяющихся по электронной почте. Помимо чисто административных мер, для борьбы с вирусами и другими вредоносными программами необходимо использовать специальное антивирусное программное обеспечение (антивирусы).

Для защиты от вирусов, распространяющихся по электронной почте, можно установить антивирусы на компьютерах отправителя и получателя. Однако такой защиты часто оказывается недостаточно. Обычные антивирусы, установленные на компьютерах пользователей Интернета, рассчитаны на проверку файлов и не всегда умеют анализировать поток данных электронной почты. Если антивирус не выполняет автоматическую проверку всех открываемых файлов, то вирус или троянская программа может легко просочиться сквозь защиту на диск компьютера.

Кроме того, эффективность антивирусов очень сильно зависит от соблюдения правил их применения: необходимо периодически обновлять антивирусную базу данных, использовать правильные настройки антивирусного сканера и т. д. К сожалению, многие владельцы компьютеров не умеют правильно пользоваться антивирусами или не обновляют антивирусную базу данных, что неизбежно приводит к вирусному заражению.

Антивирусы для почтовых серверов. Понимая актуальность проблемы распространения вирусов по электронной почте, многие компании предлагают специальные программы-антивирусы для защиты почтовых серверов. Такие антивирусы анализируют поток данных, проходящий через почтовый сервер, не допуская передачи сообщений с зараженными файлами вложений. Существует и другое решение – подключение к почтовым серверам обычных антивирусов, предназначенных для проверки файлов.

Антивирусная защита почтовых серверов SMTP и POP3 намного эффективнее антивирусной защиты компьютеров пользователей. Как правило, настройкой антивирусов на сервере занимается опытный администратор, который не ошибется при настройке и к тому же включит режим автоматического обновления базы данных через Интернет. Пользователи

защищенных серверов SMTP и POP3 могут не беспокоиться по поводу основного канала распространения вирусов – к ним будут приходить сообщения, уже очищенные от вирусов.

Действия, выполняемые почтовыми серверами при отправке и получении зараженных писем, зависят от настройки антивируса и самого почтового сервера. Например, когда отправитель пытается послать сообщение с зараженным файлом, защищенный почтовый сервер SMTP откажет ему в этом, а почтовая программа выведет на экран предупреждающее сообщение. Если же кто-то пошлет на ваш адрес письмо с зараженным файлом вложения, то при использовании защищенного сервера POP3 вместо него придет только сообщение об обнаружении вируса.

Несмотря на постоянно растущую популярность платформы Microsoft Windows, сегодня большинство серверов Интернета работает под управлением операционных систем Linux, FreeBSD и аналогичных UNIX-подобных систем. Основное преимущество Linux – очень низкая стоимость приобретения. Каждый может загрузить через Интернет дистрибутив Linux и установить его на любое количество компьютеров. В составе этого дистрибутива есть все, что нужно для создания узла Интернета, в том числе и серверы электронной почты.

Среди други преимуществ Linux и подобных ОС следует отметить открытость, доступность исходных текстов, наличие огромного сообщества добровольных разработчиков, готовых помочь в сложных ситуациях, простое удаленное управление с помощью текстовой консоли и т. д. Для ОС этой серии было создано всего несколько десятков вирусов, что говорит о ее высокой защищенности.

Doctor Web для UNIX-систем. Для защиты почтовых серверов, работающих под управлением операционных систем Linux, FreeBSD и Solaris, с успехом можно использовать антивирусную программу Doctor Web Игоря Данилова. В комплект антивируса входят *программа-домен* Dr.WebD и *программа-сканер* Dr.Web, а также решения для интеграции с почтовыми системами: CommuniGate Pro, Sendmail, Qmail, Exim, Postfix.

Домен Dr.WebD снабжен открытым документированным интерфейсом и может использоваться практически во всех системах обработки данных в качестве подключаемого внешнего антивирусного фильтра. Открытые исходные тексты некоторых компонентов интеграции позволяют проводить аудит, модифицировать интерфейсные компоненты для более полного удовлетворения требованиям разработчика. Кроме того, эти исходные тексты могут служить примером для написания собственных компонентов интеграции. В процессе своей работы домен Dr.WebD автоматически проверяет все сообщения электронной почты, проходящие через сервер. При этом проверяются файлы вложений (даже упакованные), а также все объекты, встроенные в документы.

При обнаружении вируса в почтовом сообщении тело вируса изымается и перемещается в зону «карантина», после чего получателю сообщения и администратору сервера посылается извещение. Таким образом пользователи

Sendmail будут надежно защищены от вредоносных программ, распространяющихся через электронную почту. Аналогичный механизм взаимодействия предусмотрен и для других почтовых серверов.

Doctor Web автоматически загружает через Интернет обновления антивирусных баз данных, что необходимо для надежной антивирусной защиты.

Помимо антивирусной проверки домен может выполнять фильтрацию сообщений по содержимому различных полей заголовков, что может быть использовано для защиты от несанкционированной рассылки сообщений – спама.

Одним из несомненных достоинств программы является высокая производительность работы домена Dr.WebD и сканера Dr.Web, достигнутая благодаря использованию совершенных алгоритмов. Это имеет особое значение в том случае, когда сервер обладает малой вычислительной мощностью. Кроме того, домен, почтовый фильтр и почтовый сервер могут работать на разных компьютерах, что позволяет при необходимости балансировать нагрузку на серверы и сетевые интерфейсы.

«Антивирус Касперского» для проверки электронной почты. Специально для защиты почтовых систем была создана программа «Антивирус Касперского (AVP) для Sendmail/Qmail/Postfix». Выполняя в реальном времени или по требованию пользователей централизованную фильтрацию всех сообщений, проходящих через почтовый сервер, эта программа удаляет вирусы из электронной почты до того, как они достигнут адресата.

При обнаружении вирусов в файлах вложений программа удаляет их и пересылает само сообщение, а также предупреждение об обнаружении вируса на заранее заданный адрес. Это позволяет администратору определять источник вирусов или других вредоносных программ. В программе реализована функция «карантин» для зараженных и подозрительных объектов. «Антивирус Касперского» может проверять не только вложенные файлы, но и встроенные в документы объекты, упакованные архивы файлов всех основных форматов, а также содержимое вложенных почтовых сообщений любого уровня вложенности. Среди других достоинств программы заслуживают упоминания возможность проверки личных и публичных папок, автоматическое обновление антивирусных баз данных через Интернет, изменение списка защищаемых ящиков без перезагрузки сервера, встроенная система рассылки предупреждений о случаях вирусных атак, а также удобная система управления, обновления и конфигурирования программы.

7.2. Практическая часть

Задание 1

Используя программный модуль «Введение в информационную безопасность. Практические работы», выполнить предлагаемый тест в разделе «Тест» и задание в разделе «Практика». Открыть программный модуль

«Введение в информационную безопасность. Практические работы», расположенный на диске /D лабораторного компьютера. Перейти по вкладке «Разделы» в раздел «Практическая работа №7». Пройти тестирование по материалу изученной темы в разделе «Тест».

Задание 2

Используя программный модуль «Введение в информационную безопасность. Практические работы», выполнить предлагаемый тест в разделе «Практическая работа №7».

ПРАКТИЧЕСКАЯ РАБОТА №8
ВЫЯВЛЕНИЕ И ФИКСАЦИЯ СЛЕДОВ ПРОТИВОПРАВНОЙ ДЕЯТЕЛЬНОСТИ, СВЯЗАННОЙ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНОЙ ТЕХНИКИ

Цель работы: систематизировать и закрепить знания о характеристике преступлений в сфере информационной безопасности и их выявлении; проконтролировать усвоение знаний, полученных на лекциях и в ходе самостоятельной подготовки студентов.

8.1. Теоретическая часть

8.1.1. Законодательная база. Действующий с 2001 г. новый Уголовный кодекс Республики Беларусь содержит ряд статей, предусматривающих ответственность за преступления против собственности (ст. 212 УК) и информационной безопасности (ст. 349–355 УК), совершенные с использованием компьютерных технологий. Впервые в перечень введены шесть преступлений, связанных с посягательством на компьютерные информацию:

- несанкционированный доступ к компьютерной информации (ст. 349);
- модификация компьютерной информации (ст. 350);
- компьютерный саботаж (ст. 351);
- неправомерное завладение компьютерной информацией (ст. 352);
- разработка, использование либо распространение вредоносных программ (ст. 354);
- нарушение правил эксплуатации компьютерной системы или сети (ст. 355).

Осознавая реальность потенциальной угрозы использования информационных технологий в противоправных целях, МВД последовательно реализует комплексную систему мер противодействия данным преступным посягательствам, которая планомерно создавалась с 2001 г. Так, в системе МВД созданы специализированные оперативно-розыскные подразделения по борьбе с киберпреступлениями. В настоящее время эти задачи решаются управлением по раскрытию преступлений в сфере высоких технологий МВД и его подразделениями на местах. В 2006 г. в структуре Главного управления предварительного расследования МВД создано управление по расследованию преступлений в сфере высоких технологий и интеллектуальной собственности. Таким образом, по линии МВД организационно завершено построение системы противодействия киберпреступности в стране. Это особенно актуально в связи с тем, что в настоящее время в Республике Беларусь реализуется широкий комплекс мер по развитию и широкому применению информационно-телекоммуникационных систем в различных сферах деятельности и отраслях экономики.

Во исполнение поручения Президента Республики Беларусь от 27 мая 2002 г. разработана Государственная программа информатизации

Республики Беларусь «Электронная Беларусь». Ее реализация создаст необходимые условия для приведения стандартов республики в сфере ИТС в соответствие с мировой системой стандартов, будет способствовать расширению присутствия Беларуси в сети Интернет и развитию электронной торговли.

8.1.2. Методика раскрытия и расследования компьютерных преступлений

В ходе расследования несанкционированного доступа к компьютерной информации необходимо последовательно установить:

1) факт неправомерного доступа к информации в компьютерной системы или сети;

2) место несанкционированного проникновения в компьютерную систему или сеть;

3) время совершения преступления;

4) надежность средств защиты компьютерной информации;

5) способ несанкционированного доступа;

6) личностей, совершивших неправомерный доступ, их виновность и мотивы преступления;

7) вредные последствия преступления;

8) обстоятельства, способствовавшие преступлению.

На признаки несанкционированного доступа или подготовки к нему могут указывать следующие обстоятельства:

- появление в компьютере фальшивых данных;
- необновление в течение длительного времени в автоматизированной информационной системе кодов, паролей и других защитных средств;
- частые сбои в процессе работы компьютеров;
- участившиеся жалобы клиентов компьютерной системы или сети;
- осуществление сотрудником сверхурочных работ без необходимости;
- немотивированные отказы некоторых сотрудников, обслуживающих компьютерные системы или сети, от отпусков;
- неожиданное приобретение сотрудником домашнего дорогостоящего компьютера;
- чистые дискеты либо диски, принесенные на работу сотрудниками компьютерной системы под сомнительным предлогом перезаписи программ для компьютерных игр;
- участившиеся случаи перезаписи отдельных данных без необходимости;
- чрезмерный интерес отдельных сотрудников к содержанию чужих распечаток (листингов), выходящих из принтеров.

Определить место и время непосредственного применения технических средств при удаленном несанкционированном доступе (не входящих в данную компьютерную систему или сеть) на практике бывает достаточно трудно. Для установления этих данных необходимо привлекать специалистов.

Способ несанкционированного доступа может быть установлен путем проведения информационно-технической судебной экспертизы. Перед экспертом следует поставить вопрос: «Каким способом мог быть совершен несанкционированный доступ в данную компьютерную систему?». Целесообразно представить эксперту всю проектную документацию на исследуемую систему (если таковая имеется), а также имеющиеся данные о ее сертификации.

Несанкционированный доступ к закрытой компьютерной системе или сети является технологически весьма сложным действием. Совершить такую акцию могут только специалисты, имеющие достаточно высокую квалификацию. Поэтому поиск подозреваемых следует начинать с технического персонала пострадавших компьютерных систем или сетей (разработчиков соответствующих систем, их руководителей, операторов, программистов, инженеров связи, специалистов по защите информации и др.).

Следственная практика показывает, что чем сложнее в техническом отношении способ проникновения в компьютерную систему или сеть, тем легче выделить подозреваемого, поскольку круг специалистов, обладающих соответствующими способностями, обычно весьма ограничен.

При расследовании преступления, предусматривающего создание, использование и распространение вредоносных программ для ЭВМ, наиболее целесообразной представляется следующая последовательность решений основных задач:

1. Установление факта и способа создания вредоносной программы для ЭВМ.
2. Установление факта использования и распространения вредоносной программы.
3. Установление лиц, виновных в создании, использовании и распространении вредоносных программ для ЭВМ.
4. Установление вреда, причиненного данным преступлением.
5. Установление обстоятельств, способствовавших совершению расследуемого преступления.

При расследовании нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети необходимо прежде всего доказать факт нарушения определенных правил, повлекший уничтожение, блокирование или модификацию охраняемой законом компьютерной информации и причинивший существенный вред. Кроме того, необходимо установить и доказать:

- место и время (период времени) нарушения правил эксплуатации ЭВМ;
- характер компьютерной информации, подвергшейся уничтожению, блокированию или модификации вследствие нарушения правил эксплуатации компьютерной системы или сети;
- способ и механизм нарушения правил;
- характер и размер ущерба, причиненного преступлением;
- факт нарушения правил определенным лицом;
- виновность лица, допустившего преступное нарушение правил эксплуатации ЭВМ;

- обстоятельства, способствовавшие совершению расследуемого преступления.

Помимо этого, следователю необходимо знать, что существует много особенностей, которые должны учитываться при производстве отдельных следственных действий. Например, если следователь (лицо, проводящее дознание) располагает информацией, что на объекте обыска находятся средства компьютерной техники, расшифровка данных которых может предоставить доказательства по делу, он должен заранее подготовиться к их изъятию и обеспечить участие в ходе обыска специалиста по компьютерной технике. По прибытии на место обыска следует сразу же принять меры по обеспечению сохранности ЭВМ и имеющихся на них данных и ценной информации. Для этого необходимо:

- запретить лицам, работающим на объекте обыска или находящимся здесь по другим причинам (персоналу), прикасаться к ЭВМ с какой-либо целью;

- запретить персоналу выключать электроснабжение на объекте обыска;

- в случае если на момент начала обыска электроснабжение объекта выключено, то до его восстановления следует отключить от электросети всю компьютерную технику, находящуюся на объекте;

- не производить самостоятельно никаких манипуляций со средствами компьютерной техники, если результат этих манипуляций заранее неизвестен.

После принятия указанных неотложных мер можно приступать к непосредственному обыску помещения и изъятию средств компьютерной техники. При этом следует принять во внимание следующие неблагоприятные факторы:

- возможные попытки со стороны персонала повредить ЭВМ с целью уничтожения информации и ценных данных;

- возможное наличие на компьютерах специальных средств защиты от несанкционированного доступа, которые, не получив в установленное время специальный код, автоматически уничтожат всю информацию;

- возможное наличие на ЭВМ новых средств защиты от несанкционированного доступа в связи с постоянным совершенствованием компьютерной техники, следствием чего может быть наличие на объекте программно-технических средств, незнакомых следователю.

В целях недопущения вредных последствий перечисленных факторов следователь (лицо, проводящее дознание) может придерживаться следующих рекомендаций:

1. Перед выключением питания по возможности корректно закрыть все используемые программы, а в сомнительных случаях просто отключить компьютер (в некоторых случаях некорректное отключение компьютера – путем перезагрузки или выключения питания без предварительного выхода из программы и записи информации на постоянный носитель – приводит к потере информации в оперативной памяти и даже к стиранию информационных ресурсов на данном компьютере).

2. При наличии средств защиты ЭВМ от несанкционированного доступа принять меры к установлению ключей доступа (паролей, алгоритмов и т. д.).

3. Корректно выключить питание всех ЭВМ, находящихся на объекте (в помещении).

4. Не пытаться на месте просматривать информацию, содержащуюся в компьютерах.

5. В затруднительных случаях не обращаться за консультацией (помощью) к персоналу, а вызывать специалиста, не заинтересованного в исходе дела.

6. Следует изъять все ЭВМ, обнаруженные на объекте.

7. При обыске не подносить ближе чем на 1 м к компьютерной технике металлоискатели и другие источники магнитного поля, в том числе сильные осветительные приборы и некоторую спецаппаратуру.

8. Поскольку многие, особенно неквалифицированные, пользователи записывают процедуру входа-выхода, работы с компьютерной системой, а пароли доступа на отдельных бумажных листках, следует изъять также все записи, относящиеся к работе с ЭВМ.

9. Так как многие коммерческие и государственные структуры прибегают к услугам нештатных и временно работающих специалистов по обслуживанию средств компьютерной техники, следует записать паспортные данные всех лиц, находящихся на объекте, независимо от их объяснений цели пребывания на объекте.

10. При изъятии средств компьютерной техники необходимо обеспечить строгое соблюдение требований действующего уголовно-процессуального законодательства. Для этого следует акцентировать внимание понятых на всех производимых действиях и их результатах, давая им при необходимости пояснения, поскольку многим участникам следствия могут быть непонятны производимые действия.

11. Кроме того, следует опечатывать ЭВМ так, чтобы исключить возможность работы с ними, разукомплектовки и физического повреждения основных рабочих компонентов в отсутствие владельца или эксперта.

12. При опечатывании компьютерных устройств следует положить один лист бумаги на разъем электропитания, расположенный на задней панели, второй – на переднюю панель вверху с захлестом на верхнюю панель и закрепить их края густым клеем. На листах бумаги должны быть подписи следователя, понятых и представителя персонала.

13. При изъятии магнитных носителей машинной информации нужно помнить, что они должны перемещаться в пространстве и храниться только в специальных опломбированных и экранированных контейнерах или в стандартных дискетных или иных алюминиевых футлярах заводского изготовления, исключающих разрушающее воздействие различных электромагнитных и магнитных полей и «наводок», направленных излучений. В случае когда необходимо сослаться непосредственно на определенный физический носитель, следует указать в протоколе его серийный (заводской)

номер, тип, название (если есть) или провести его точное описание (размеры, цвет, класс, надписи, физические повреждения). При отсутствии четких внешних признаков физический носитель запечатывается в отдельную коробку (ящик, конверт), о чем обязательно делается отметка в протоколе проведения следственного действия.

14. В случае невозможности изъятия и приобщения к делу в качестве вещественного доказательства средства компьютерной техники (например, если компьютер является сервером или рабочей станцией компьютерной сети) в обязательном порядке после его осмотра необходимо блокировать не только соответствующее помещение, но и отключить источники энергопитания аппаратуры или в крайнем случае создать условия лишь для приема информации с одновременным опломбированием всех необходимых узлов, деталей, частей и механизмов компьютерной системы.

15. Если же возникла необходимость изъятия информации из оперативной памяти компьютера (непосредственно из ОЗУ), то сделать это возможно только путем копирования соответствующей машинной информации на физический носитель с использованием стандартных паспортизированных программных средств с соответствующим документальным приложением и в порядке, установленном следующими нормативными документами: Государственным стандартом (ГОСТ) 6104-84 от 01.07.87 «УСД. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения» и Постановлением Госстандарта №2781 от 24.09.86 «Методические указания по внедрению и применению ГОСТ 6104-84». Только с использованием указанных нормативных документов машинная информация будет относиться к разряду «документированной информации», как требует того закон. К сожалению, практика работы многих следователей (представителей СИБ) показывает, что вышеуказанные рекомендации в большинстве случаев следователями не применяются в практической деятельности по расследованию преступлений. В результате неправильного изъятия средств компьютерной техники добытая информация зачастую не может являться доказательством в судебном процессе.

Типичные следственные ситуации и следственные действия первоначального этапа. Типовые ситуации – наиболее часто встречающиеся ситуации расследования, предопределяющие особенности методики расследования. Они включают в себя типовые следственные версии, типовые задачи расследования и методы и средства их решения.

Анализ отечественного и зарубежного опыта показывает, что можно выделить три типичные следственные ситуации:

1. Собственник информационной системы собственными силами выявил нарушение целостности/конфиденциальности информации в системе, обнаружил виновное лицо и заявил об этом в правоохранительные органы.

2. Собственник информационной системы собственными силами выявил нарушение целостности/конфиденциальности информации в системе, не смог обнаружить виновное лицо и заявил об этом в правоохранительные органы.

3. Данные о нарушении целостности/конфиденциальности информации в информационной системе и виновном лице стали общеизвестными или непосредственно обнаружены органом дознания (например, в ходе проведения оперативно-розыскных мероприятий по другому делу).

При наличии заподозренного виновного лица первоначальная задача следствия заключается в сборе с помощью собственника информационной системы и процессуальной фиксации следующих доказательств:

- нарушения целостности/конфиденциальности информации в системе;
- наличия ущерба, причиненного нарушением целостности/конфиденциальности информации и его размера;
- причинной связи между действиями, образующими способ нарушения, и наступившими последствиями путем детализации способа нарушения целостности/конфиденциальности информации в системе и характера совершенных виновным действий;
- отношения виновного лица к совершенным действиям и наступившим последствиям.

Для ситуации, когда преступник задержан на месте совершения преступления или сразу же после его совершения, характерны следующие первоначальные следственные действия:

- личный обыск задержанного;
- допрос задержанного;
- обыск места жительства задержанного.

К типичным следственным действиям на данной стадии можно отнести осмотр и фиксацию состояния ЭВМ, сетей ЭВМ и машинных носителей, допросы очевидцев, а также лиц, обеспечивающих работу информационной системы, включая должностных. Важнейшим элементом работы является выемка (предпочтительно с участием специалиста) документов, в том числе на машинных носителях, фиксировавших состояние информационной системы или ее программ в момент вторжения злоумышленника и отражающих последствия вторжения.

Одновременно следует принять меры по фиксации состояния рабочего места заподозренного, откуда он мог осуществить вторжение в информационную систему и где могут сохраняться следы его действий. Полученные доказательства могут дать основания для принятия решения о привлечении лица к делу в качестве подозреваемого или обвиняемого.

При отсутствии заподозренного виновного лица первоначальная задача следствия заключается в сборе следующих доказательств:

- нарушения целостности/конфиденциальности информации в системе;
- наличия ущерба и его размера;
- причинной связи между действиями и наступившими последствиями.

Одновременно следует начать поиск рабочего места заподозренного, откуда он осуществил вторжение в информационную систему. Для этого необходимо определить:

- место входа в информационную систему и способ входа (с помощью должностных лиц);

- «пути следования» злоумышленника или его программы к «атакованной» системе (с помощью должностных лиц).

Место входа в систему может находиться как у него на службе, так и дома, а также в иных местах, где установлена соответствующая аппаратура.

Круг типичных общих версий сравнительно невелик:

- преступление действительно имело место при тех обстоятельствах, которые вытекают из первичных материалов;

- ложное заявление о преступлении.

Типичными частными версиями являются:

- версии о личности преступника (ов);

- версии о местах совершения внедрения в компьютерную систему;

- версии об обстоятельствах, при которых было совершено преступление;

- версии о размерах ущерба, причиненного преступлением.

Практические особенности отдельных следственных действий. Осмотр, обыск и выемка при совершении компьютерных преступлений являются важнейшими инструментами установления обстоятельств расследуемого события, а также главными процессуальными способами изъятия вещественных доказательств.

Следует напомнить, что осмотр – это непосредственное обнаружение, восприятие и исследование следователем материальных объектов, имеющих отношение к расследуемому событию. Обыск – следственное действие, в процессе которого производится поиск и принудительное изъятие объектов, имеющих значение для правильного решения задач уголовного судопроизводства. Выемка – следственное действие, в процессе которого производится изъятие объектов, имеющих значение для правильного решения задач уголовного судопроизводства, в тех случаях, когда их местонахождение точно известно следователю и изъятие прямо или косвенно не нарушает прав личности.

Носители информации, имеющей отношение к расследуемому событию, могут быть изъяты и приобщены к уголовному делу в качестве вещественного доказательства только с соблюдением установленного порядка. Для участия в обыске и выемке целесообразно приглашать специалиста в области компьютерной техники. При осмотрах, обысках, выемках, сопряженных с изъятием ЭВМ, машинных носителей и информации, возникает ряд общих проблем, связанных со спецификой изымаемых технических средств. Так, необходимо предвидеть меры безопасности, предпринимаемые преступниками с целью уничтожения вещественных доказательств. Например, они могут использовать специальное оборудование, в критических случаях создающее сильное магнитное поле, стирающее магнитные записи. Известна легенда о хакере, который создал в дверном проеме магнитное поле такой силы, что оно уничтожало магнитные носители информации при выносе их из его комнаты. Преступник имеет возможность включить в состав программного обеспечения

своей машины программу, которая заставит компьютер периодически требовать пароль, и если несколько секунд правильный пароль не введен, данные в компьютере автоматически уничтожаются. Желательно иметь с собой и использовать при обыске и осмотре устройство для определения и измерения магнитных полей.

Вещественные доказательства в виде ЭВМ, машинных носителей требуют особой аккуратности при транспортировке и хранении. Им противопоказаны резкие броски, удары, повышенные температуры, влажность. Все эти внешние факторы могут повлечь потерю данных, информации и свойств аппаратуры.

Не следует забывать при осмотрах и обысках о возможностях сбора традиционных доказательств (скрытых отпечатков пальцев на клавиатуре, выключателях и др., шифрованных рукописных записей и пр.). Осмотру подлежат все устройства конкретной ЭВМ.

Фактически оптимальный вариант изъятия ЭВМ и машинных носителей информации – это фиксация их и их конфигурации на месте обнаружения и упаковка таким образом, чтобы аппаратуру можно было бы успешно, правильно и точно так же, как на месте обнаружения, подключить в лабораторных условиях или месте проведения следствия с участием специалистов.

Указанные следственные действия могут производиться в целях:

- осмотра и изъятия ЭВМ и ее устройств;
- поиска и изъятия информации и следов воздействия на нее в ЭВМ и ее устройствах;
- поиска и изъятия информации и следов воздействия на нее вне ЭВМ.

По прибытии на место осмотра или обыска следует принять меры по обеспечению сохранности информации на находящихся здесь компьютерах и магнитных носителях. Для этого необходимо:

- запретить лицам, работающим на объекте обыска, прикасаться к работающим компьютерам, магнитным носителям, а также включать и выключать компьютеры;
- не производить самостоятельно никаких манипуляций с компьютерной техникой, если результат этих манипуляций заранее неизвестен;
- при наличии в помещении, где находятся средства компьютерной техники (СКТ) и магнитные носители информации, взрывчатых, легковоспламеняющихся, токсичных и едких веществ или материалов, как можно скорее удалить эти вещества в другое помещение.

Особенности производства осмотров и обысков. Если компьютер работает, ситуация для следователя, производящего следственное действие без помощи специалиста, существенно осложняется, однако и в этом случае не следует отказываться от оперативного изъятия необходимых данных. В данной ситуации необходимо определить, какая программа выполняется. Для этого требуется изучить изображение на экране дисплея и по возможности детально описать его. После остановки программы и выхода в операционную систему

(иногда при нажатии функциональной клавиши F3) можно восстановить наименование вызывавшейся последний раз программы. Можно произвести следующие действия:

- сфотографировать или сделать видеозапись изображения;
- остановить исполнение программы (остановка может осуществляться одновременным нажатием клавиш Ctrl-C либо Ctrl-Break);
- зафиксировать (отразить в протоколе) результаты своих действий и реакции компьютера на них;
- определить наличие у компьютера внешних устройств – накопителей информации на жестких магнитных дисках и виртуального диска;
- определить наличие у компьютера внешних устройств удаленного доступа к системе и определить их состояние (отразить в протоколе), после чего разъединить сетевые кабели так, чтобы никто не мог изменить или стереть информацию в ходе обыска (например, отключить телефонный шнур из модема);
- скопировать программы и файлы данных (копирование осуществляется стандартными средствами ЭВМ или командой DOS COPY);
- выключить подачу энергии в компьютер и далее действовать по схеме «компьютер не работает».

Если компьютер не работает, следует:

- точно отразить в протоколе и на прилагаемой к нему схеме местонахождение ПК и его периферийных устройств;
- точно описать порядок соединения между собой этих устройств с указанием особенностей (цвет, количество соединительных разъемов, их спецификация) соединительных проводов и кабелей; перед разъединением полезно осуществить видеозапись или фотографирование мест соединения;
- с соблюдением всех мер предосторожности разъединить устройства компьютера, предварительно обесточив его;
- упаковать раздельно носители на дискетах и магнитных лентах и поместить их в оболочки, не несущие заряда статического электричества;
- упаковать каждое устройство и соединительные кабели, провода;
- защитить дисководы гибких дисков согласно рекомендации изготовителя (вставить новую дискету или часть картона в щель дисковода);
- осторожно транспортировать все устройства ЭВМ, особенно винчестер.

Поиск и изъятие информации и следов воздействия на нее из ЭВМ и ее устройств. В компьютере информация может находиться непосредственно в оперативном запоминающем устройстве (ОЗУ) при выполнении программы, в ОЗУ периферийных устройств и во внешних запоминающих устройствах (ВЗУ).

Наиболее эффективным и простым способом фиксации данных из ОЗУ является распечатка на бумагу информации, появляющейся на дисплее.

Если компьютер не работает, информация может находиться в ВЗУ и других компьютерах информационной системы или в «почтовых ящиках» электронной почты или сети ЭВМ. Необходимо произвести детальный осмотр

файлов и изучить структуру их расположения; лучше это осуществить с участием специалиста в лабораторных условиях или на рабочем месте следователя. Следует обращать внимание на поиск так называемых «скрытых» файлов и архивов, где может храниться важная информация.

Периферийные устройства ввода-вывода могут также некоторое время сохранять фрагменты программного обеспечения и информации, однако для вывода этой информации необходимы глубокие специальные познания. Осмотр компьютеров и изъятие информации производится в присутствии понятых, которые расписываются в протоколе, составленном в ходе осмотра.

Поиск и изъятие информации и следов воздействия на нее, находящихся вне ЭВМ. В ходе осмотров, производимых в связи с наличием компьютерного преступления, могут быть обнаружены и изъяты следующие виды важных документов, которые могут стать вещественными доказательствами по делу:

- документы, носящие следы совершенного преступления, – телефонные счета, пароли и коды доступа, дневники связи и пр.;
- документы со следами действия аппаратуры: всегда следует искать в устройствах вывода (например в принтерах) бумажные носители информации, которые могли остаться внутри их в результате сбоя в работе устройства;
- документы, описывающие аппаратуру и программное обеспечение;
- документы и нормативные акты, регламентирующие правила работы с данной ЭВМ, системой, сетью, которые могут доказать, что преступник их знал и умышленно нарушал;
- личные документы подозреваемого или обвиняемого.

Использование специальных познаний и назначение экспертиз. Юрист-следователь не в состоянии отслеживать все технологические изменения в данной области компьютерных технологий. Поэтому для участия в обысках, осмотрах, выемках крайне необходимы специалисты в данной области. Поиск таких специалистов следует проводить на предприятиях и в учреждениях, осуществляющих обслуживание и эксплуатацию компьютерной и коммуникационной техники, в учебных и научно-исследовательских организациях.

Специалисты, привлекаемые в качестве экспертов, могут оказать действенную помощь при решении следующих вопросов (примерный список):

1. Какова конфигурация и состав компьютерных средств и можно ли с помощью этих средств осуществить действия, инкриминируемые обвиняемому?
2. Какие информационные ресурсы находятся в данной ЭВМ?
3. Не являются ли обнаруженные файлы копиями информации, находившейся на конкретной ЭВМ?
4. Заражены ли представленные файлы с программами вирусом, и если да, то каким именно?
5. Не являются ли представленные тексты на бумажном носителе записями исходного кода программы, и каково назначение этой программы?

6. Подвергалась ли данная компьютерная информация уничтожению, копированию, модификации?

7. Какие правила эксплуатации ЭВМ существуют в данной информационной системе, и были ли нарушены эти правила?

8. Находится ли нарушение правил эксплуатации в причинной связи с уничтожением, копированием, модификацией?

Следует иметь в виду, что в системе МВД начато производство так называемых программно-технических экспертиз (ПТЭ), в рамках которых решаются следующие задачи:

- распечатка всей или части информации, содержащейся на жестких дисках компьютеров и на внешних магнитных носителях, в том числе из нетекстовых документов;
- распечатка информации по определенным темам;
- восстановление стертых файлов и стертых записей в базах данных, уточнение времени стирания и внесения изменений;
- установление времени ввода в компьютер определенных файлов и записей в базы данных;
- расшифровка закодированных файлов и другой информации, преодоление рубежей защиты, подбор паролей;
- выяснение каналов утечки информации из ЛВС, глобальных сетей и распределенных баз данных;
- установление авторства, места подготовки и способа изготовления некоторых документов;
- выяснение технического состояния и исправности СКТ.

Наряду с этими основными задачами при проведении ПТЭ могут быть решены и некоторые вспомогательные задачи:

- оценка стоимости компьютерной техники, периферийных устройств, магнитных носителей, программных продуктов, а также проверка контрактов на их поставку;
- установление уровня профессиональной подготовки отдельных лиц в области программирования и работы с СКТ;
- перевод документов технического содержания.

В связи с тем, что при осмотре ЭВМ и носителей информации производится изъятие различных документов, в ходе расследования возникает необходимость в назначении криминалистической экспертизы для исследования документов. Например, дактилоскопическая экспертиза позволит выявить на документах, частях ЭВМ и машинных носителях следы пальцев рук причастных к делу лиц.

Парадоксальность компьютерных преступлений состоит в том, что трудно найти другой вид преступления, после совершения которого его жертва не выказывает особой заинтересованности в поимке преступника, а сам преступник, будучи пойман, всячески рекламирует свою деятельность на поприще компьютерного взлома, мало что утаивая от представителей правоохранительных органов. Психологически этот парадокс вполне объясним.

Во-первых, жертва компьютерного преступления совершенно убеждена, что затраты на его раскрытие (включая потери, понесенные в результате утраты банком своей репутации) существенно превосходят уже причиненный ущерб. А во-вторых, преступник, даже заработав максимальный срок тюремного наказания (не очень большой, а если повезет, то условный или сокращенный), приобретет широкую известность в деловых и криминальных кругах, что в дальнейшем позволит ему с выгодой использовать свои знания и умения.

Оценивая современное состояние уголовной и криминалистической теории и учитывая потребности оперативно-следственной практики, надо признать, что в целом проблемы уголовно-правовой характеристики, совершенствования практики раскрытия, расследования и предупреждения компьютерных преступлений изучены явно недостаточно. Необходимость всестороннего исследования обозначенных проблем диктуется как потребностью следственной практики, так и задачами дальнейшего совершенствования уголовно-правовой и криминалистической теории, усиления их влияния на результативность борьбы с компьютерной преступностью.

Мы еще не можем в полной мере оценить опасность, которую несут с собой наши «электронные братья по разуму», а потому стоит прислушаться к человеку с опытом. Директор ЦРУ Джон Дейч недавно сравнил электронную угрозу с ядерной, химической и бактериологической опасностью. Соединенные в единую сеть компьютеры становятся уязвимыми для разного рода хулиганов, террористов, преступников, а кроме того, дают возможность проведения электронных диверсий и войн.

8.2. Вопросы для самоконтроля

1. Какова криминалистическая характеристика преступлений в сфере компьютерной информации?
2. Назовите типовые ситуации первоначального этапа расследования преступлений в сфере компьютерной информации.
3. Какие следственные и розыскные мероприятия специфичны для начального этапа расследования компьютерных преступлений?
4. Каков круг обстоятельств, подлежащих установлению по делам о неправомерном доступе к компьютерной информации?
5. Каков круг обстоятельств, подлежащих установлению по делам о создании, использовании и распространении вредоносных программ для ЭВМ?
6. Каков круг обстоятельств, подлежащих установлению по делам о нарушении правил эксплуатации ЭВМ?
7. Опишите оптимальную последовательность действий следователя при осмотре компьютера.
8. Опишите оптимальную последовательность действий следователя при осмотре локальной компьютерной сети.

9. Каковы особенности проведения обыска ЭВМ подозреваемого и изъятия следов криминальной деятельности по делам, связанным с неправомерным доступом к компьютерной информации?

10. Каковы особенности проведения обыска ЭВМ подозреваемого и изъятия следов криминальной деятельности по делам, связанным с созданием, использованием и распространением вредоносных программ?

11. Опишите особенности транспортировки с места проведения осмотра (обыска) программных и аппаратных средств.

12. Назовите виды экспертных исследований, обычно проводящихся при расследовании преступлений в сфере компьютерной информации.

13. Сформулируйте вопросы для компьютерно-технической экспертизы.

14. Укажите известные вам типы субъектов преступлений в сфере компьютерной информации.

15. Какие международные акты по борьбе с преступностью могут быть применены для расследования преступлений в сфере компьютерной информации?

16. Из каких устройств состоит ЭВМ?

17. Что такое компьютерная информация?

18. Где и в каком виде находится компьютерная информация?

19. Какие действия с компьютерной информацией являются наказуемыми?

20. Какие устройства составляют сеть ЭВМ?

21. Как с помощью стандартных средств Windows установить, включена ли данная ЭВМ в сеть ЭВМ?

22. Каковы основные свойства файла и какие из них могут быть изменены при неправомерном доступе к компьютерной информации?

23. Какие правила работы с ЭВМ, сетью ЭВМ вам известны?

24. Каковы признаки нарушения правил эксплуатации ЭВМ и сети ЭВМ?

25. Что такое конфигурация ЭВМ и каковы признаки ее изменения?

8.3. Практическая часть

1. Определите конфигурацию вашей ЭВМ: какое именно программное обеспечение (в том числе операционная система) установлено на данной ЭВМ, какие устройства включены в данную ЭВМ, имеет ли данная ЭВМ соединение с сетью ЭВМ (с помощью каких устройств). Сделайте описание данной ЭВМ в виде фрагмента протокола ее осмотра.

2. Установите, какие именно программы и данные находятся на вашей ЭВМ (и где). Составьте описание местонахождения компьютерной информации на этой ЭВМ. Выдвиньте предположение об основном назначении данной конфигурации ЭВМ и проверьте его с помощью обычных средств операционной системы. Выявите стандартными средствами операционной системы все файлы с текстовой и графической информацией на этой ЭВМ и сделайте описание местонахождения этих файлов.

3. При наличии сети ЭВМ установите возможность передачи информации с одной ЭВМ на другую:

а) с помощью копирования специально созданного текстового файла с одного машинного носителя на другой;

б) с помощью стандартных средств электронной почты.

С помощью обычной утилиты поиска найдите перенесенную информацию с одной ЭВМ на другую и опишите результаты эксперимента, обращая особого внимание на изменение (или неизменность) свойств перенесенного файла.

4. Попросите другое лицо в ваше отсутствие изменить конфигурацию вашей ЭВМ стандартными средствами и выявите произведенные изменения путем контроля за состоянием устройств ЭВМ, изменением файловой системы, изменением настроек оборудования или программного обеспечения ЭВМ. Составьте протокол осмотра ЭВМ с отражением ее изменившихся свойств, свидетельствующих о доступе к ЭВМ постороннего лица.

Задача 1

Вредоносной программой-вирусом «Selver» были выведены из строя 1562 компьютера пользователей Интернета на территории России. Сумма средств, затраченных на анализ атаки, нахождение, удаление, исправление и восстановление работоспособности всех компьютеров, составила примерно 400 000 дол. США. По признакам состава преступления, предусмотренного ст. 273 УК РФ, следователь возбудил уголовное дело. Анализ маршрута заражения компьютеров в сети позволил установить, что начальной точкой распространения вредоносной программы был домен[1] www.maltus.ru. Провайдер[2] – владелец данного домена – согласился сотрудничать со следствием и представить следователю любую информацию, необходимую для проведения расследования.

1. Составьте план первоначального этапа расследования.

2. Определите, какую информацию должен запросить следователь у провайдера.

3. Сформулируйте возможные пути расследования и соответствующие следственные версии.

4. Решите, как следовало бы поступить следователю, если бы провайдер не согласился сотрудничать со следствием.

[1] Домен, доменное имя – совокупность символьных наименований, характеризующих адрес конкретной ЭВМ или их сети.

[2] Провайдер – физическое или юридическое лицо, предоставляющее услуги по хранению и распространению в сети информации заказчика.

Задача 2

В правоохранительные органы обратился гражданин В. с заявлением, что не может подключиться к Интернету, используя свои идентификаторы. От провайдера, к которому он обратился в связи с указанной проблемой, он узнал, что с использованием его имени пользователя и пароля к сети кто-то подключается с другого телефонного номера.

1. Оцените сложившуюся ситуацию.
2. Составьте план первоначального этапа расследования.
3. Определите, какие обстоятельства подлежат выяснению.
4. Укажите, какие версии, по вашему мнению, следует отработать в первую очередь.

Задача 3

По делу о нарушении работы компьютеров, обеспечивающих автоматизированную систему полетов аэропорта «В», было возбуждено уголовное дело. В ходе следствия было установлено, что гражданин Р. – сотрудник администрации аэропорта запустил на своем рабочем компьютере вирус WerewolF, чем вызвал сбой в работе компьютеров, обслуживающих полеты авиалайнеров. При допросе Р. пояснил, что он занимается коллекционированием вирусных программ. В июне он познакомился в чате с неким «PoiSon», который тоже интересуется вирусами и сам их пишет, после чего их общение по Интернету приобрело постоянный характер, в ходе которого они стали обмениваться вирусными программами и описаниями их работы.

Позже, в марте «PoiSon» сообщил, что сам создал «лучший в мире вирус» и переслал его в подарок Р. в пакете с описанием его работы. Р., изучив описание действия вируса и полагая, что полностью контролирует ситуацию, запустил вирус на своем рабочем компьютере, подключенном к сети аэропорта, однако вирусная программа стала работать несколько иным образом, чем было указано в описании, что и повлекло выведение из строя системы компьютеров аэропорта.

Р. уточнил, что лично с «PoiSon» он никогда не встречался. Общался с ним при помощи ICQ и электронной почты.

1. Решите, какие действия следует произвести следователю.
2. Определите, какие версии, по вашему мнению, следует отработать.
3. Опишите порядок проведения осмотра компьютерной сети, подвергшейся воздействию вирусной программы.
4. В целях установления личности «PoiSon» сформулируйте задание органу дознания с рекомендациями по тактике его выявления, задержания и осмотра его компьютера.
5. Установите, какие вопросы должны быть поставлены перед экспертами при расследовании данного уголовного дела.

Задача 4

В правоохранительные органы обратился председатель совета директоров банка «N» Ч. с заявлением о том, что неизвестный вымогает у банка 50 000 дол. США за нераспространение информации о лицевых счетах абонентов банка. Ч. уточнил, что две недели назад в его адрес по электронной почте пришло сообщение, в котором указывалось, что некто, называющий себя «SjOsRt?», заявил, что проник в компьютерную систему банка и скопировал информацию о лицевых счетах наиболее известных общественных деятелей, являющихся клиентами банка. За возврат этой информации он просит вышеуказанную сумму. Если требование не будет выполнено, то информация будет широко распространена в Интернете. О способе передаче денег будет сообщено дополнительно. В качестве подтверждения нахождения у «SjOsRt?» указанной информации в приложении к электронному письму содержались данные о движении средств по лицевому счету самого Ч.

1. Определите, имеются ли основания для немедленного возбуждения уголовного дела или сначала целесообразно провести розыскные мероприятия, и какие именно.

2. Решите, какие розыскные и следственные версии могут быть выдвинуты на данном этапе.

3. Определите, какие следственные и розыскные мероприятия надо провести для проверки версий преступления и доказательства фактов совершения преступления.

4. Составьте план осмотра компьютерной сети банка для поиска следов преступления.

5. При установлении лиц, причастных к совершению указанного преступления, опишите тактические приемы их задержания, обыска их служебных и домашних компьютеров.

Задача 5

В марте в результате вирусной атаки была выведена из строя корпоративная компьютерная сеть акционерного общества «МВ». В ходе атаки была уничтожена вся информация, содержащаяся на сервере общества, в связи с чем была приостановлена нормальная работа двенадцати его отделений. Общий ущерб, нанесенный обществу, составил 20 000 дол. США. Предположительно, атака была совершена путем запуска на сервере программы-вируса. В ходе следствия было установлено, что к преступлению может быть причастен бывший сотрудник этого общества Н., уволенный три месяца назад. Н. характеризовался как знающий специалист, но был уволен в связи с сокращением штата компании.

Следователь принимает решение провести обыск по месту проживания Н.

1. Опишите приемы подготовки к обыску.

2. Решите, как надлежит провести обыск (осмотр) компьютера гражданина Н. для поиска следов криминальной деятельности.

3. Приведите последовательность действий следователя в случае, если на момент обыска компьютер включен и если он выключен.

4. Определите, что именно следует искать в компьютере Н.

5. Укажите известные вам способы изъятия следов преступления, характерные для подобных ситуаций.

Задача 6

В ходе расследования убийства предпринимателя А. была выдвинута версия о причастности к совершению данного преступления партнера убитого – предпринимателя В. Однако ни наблюдение за В., ни контроль его телефонных переговоров не дали дополнительной информации. Из оперативных источников стало известно, что для «особо важных разговоров» В. использует возможности компьютерной сети.

1. Оцените сложившуюся ситуацию.

2. Сформулируйте версию, вытекающую из приведенной информации.

3. Определите, какие розыскные и следственные мероприятия необходимо провести для подтверждения или опровержения версии преступления.

Задача 7

В ночном клубе «Голубая устрица» были задержаны Г. и О., осуществлявшие сбыт наркотических веществ. После возбуждения дела в ходе допроса О. сообщила, что наркотические вещества для сбыта они с Г. получают от лица по кличке «Воздух». Ни она, ни Г. никогда его не видели. Встречи для передачи им наркотических веществ и получения денег он назначает при помощи электронной почты, указывая место, где будет находиться контейнер с товаром. После прочтения сообщения оно всегда сразу удаляется Г. На связь «Воздух» выходит с ними сам. Однако для экстренной связи в исключительных случаях он разрешает использовать свой электронный адрес: air@hotmail.ru. Компьютер, который Г. и О. используют для связи, находится дома у Г.

Составьте план розыскных и следственных мероприятий для получения доказательств, установления личности неизвестного преступника и его изобличения.

ПРАКТИЧЕСКАЯ РАБОТА №9
АНАЛИЗ БЕЗОПАСНОСТИ МОБИЛЬНЫХ ТЕХНОЛОГИЙ

Цель работы: изучить помехоустойчивость и помехозащищенность GSM-канала; принципы организации систем безопасности, использующих GSM-каналы.

9.1. Теоретическая часть

GSM-системы получили широкое распространение в начале XXI в. после бурного развития мобильной связи. Вначале в качестве каналообразующего оборудования использовались мобильные телефоны, которые подключались к охранным панелям через интерфейс RS-232 и управлялись AT-командами. Данное решение было очень ненадежным, т. к. телефоны могли зависнуть или просто отключиться, кроме того, условия эксплуатации мобильных телефонов не предусматривали работу в сырых и неотапливаемых помещениях, что существенно ограничивало область их применения.

Сегодня производители оборудования мобильной связи выпускают специализированные GSM-модемы (M2M-решения) для построения на их основе беспроводных систем безопасности. Данное решение существенно повысило надежность работы системы, а также предоставило разработчикам систем безопасности дополнительные возможности по работе с сервисами GSM. В качестве способа передачи информации в GSM-системах используются SMS-сообщения, модемное соединение (CSD), передача тоновых посылок (режим DTMF) и режим пакетной передачи сообщений GPRS. Появление режима GPRS позволило существенно снизить затраты на эксплуатацию систем радиоохраны.

В настоящее время беспроводные охранные системы на базе GSM получили широкое распространение благодаря их относительно невысокой стоимости и простоте установки и эксплуатации. Однако существенным недостатком подобных систем является низкая помехозащищенность. Не секрет, что GSM-канал легко подавить: «GSM-глушилки» находятся сегодня в свободной продаже, да и работа сети GSM не всегда отличается высокой стабильностью и может отказать в самый неподходящий момент. Указанные недостатки ограничивают применение оборудования подобного класса при построении систем безопасности. Данные системы в большей степени применяются в качестве резервных (дополнительных) каналов связи или для построения систем мониторинга удаленных объектов с целью сбора телеметрической информации.

Системы видеонаблюдения. Первыми в данной области появились электронные устройства, способные отдавать лишь текстовые SMS-сообщения с охраняемого объекта. Такое устройство состояло из электрического блока, к которому можно было подключить 1–4 внешних датчика или шлейф охранной

сигнализации и обычного мобильного телефона. Устройство можно было установить на любом объекте, имеющем устойчивый прием GSM-сети. Принцип работы устройства был основан на оповещении пользователя с помощью текстового SMS-сообщения, которое передавалось на мобильный телефон пользователя через GSM-канал в случае срабатывания охранного датчика или нарушения целостности шлейфа охранной сигнализации. Подобные устройства спешно завоевали популярность среди хозяев небольших загородных домов и коттеджей своей невысокой ценой и простотой установки. В качестве ответной меры владелец подобного устройства при получении SMS-сообщения просто перезванивал на мобильный телефон соседа или местного сторожа, тот в свою очередь шел к дому и выяснял причины срабатывания. Подобные устройства имели и существенные недостатки: невозможно было отличить неправильное срабатывание от тревожного сигнала без участия человека, в случае знака тревоги часто невозможно было предотвратить преступление. Причем при сильной загрузке сотовой сети SMS-извещение могло быть доставлено с опозданием от нескольких минут до нескольких часов, что делало данную систему ненужной.

Современные системы видеонаблюдения по GSM, как правило, выполняют следующие функции: взаимодействие пользователя с устройством для получения видеоизображения в любое время суток; передачу видеоизображения на 1–4 телекамерах в режиме реального времени (задержка от начала события до отображения на приемном мониторе не более 1–2 с); автоматический дозвон до пользователя по срабатыванию встроенного детектора движения и/или внешнего датчика; автоматическую запись фото- и видеоинформации во встроенную память устройства; запись принимаемой фото- и видеоинформации на жесткий диск компьютера; подключение внешнего охранного датчика или шлейфа к тревожному входу устройства; подключение исполнительного устройства к релейному выходу устройства и прямое управление им по каналу связи.

Применение систем удаленного видеонаблюдения по GSM целесообразно на удаленных объектах, где отсутствуют проводные каналы связи: загородные дома, дачи, склады, автостоянки, гаражи, автозаправочные станции, железнодорожные переезды. Также данные системы используются с целью удаленного видеоконтроля за коммуникациями: водо-, газо- и нефтепроводы, электростанции, раздельно стоящие подстанции, вышки и т. п.

Несмотря на кажущуюся сложность устройств видеонаблюдения по GSM, они остаются просты в подключении и комфортны в эксплуатации. Уже не требуется использование передающей стороной мобильного телефона, т. к. GSM-модуль встроен прямо в остов прибора. Электропитание осуществляется от источника постоянного тока с широким диапазоном напряжений 8–15 В или от электросети напряжением 220 В.

Альтернативой GSM-каналу являются беспроводные сети WLAN (Wireless Local Area Network – беспроводная локальная сеть). Сеть WLAN – вид локальной вычислительной сети (LAN), использующий для связи и передачи

данных между узлами высокочастотные радиоволны, а не кабельные соединения. Пользовательские устройства можно интегрировать в сеть, установив на них беспроводные сетевые адаптеры. Для обеспечения беспроводным пользователям доступа к уже существующей сети Ethernet нужно установить беспроводную точку доступа (англ. Wireless Access Point).

Точки доступа призваны выполнять самые разнообразные функции как для подключения группы компьютеров (каждый с беспроводным сетевым адаптером) в самостоятельные сети, так и для выполнения функции моста между беспроводными и кабельными участками сети. Такие совмещенные сети называются инфраструктурой (Infrastructure) и используются для доступа к центральным базам данных или беспроводного подключения мобильных пользователей.

Стандарт Wi-Fi (англ. Wireless Fidelity – «беспроводная точность», по аналогии с Hi-Fi – стандарт на оборудование Wireless LAN). При использовании современных потоковых алгоритмов сжатия скорости 0,5 Мбит/с этого вполне достаточно для передачи одного канала видео хорошего качества. Также это расстояние можно увеличивать с помощью направленных антенн и промежуточных точек доступа.

Защита видеоинформации в беспроводных IP-системах видеонаблюдения достигается несколькими способами. Ключевыми среди них являются: применение брандмауэров, использование паролей и шифрование. Брандмауэр работает как «электронные ворота», пропускающие зарегистрированных пользователей и запрещающие доступ неавторизованным лицам. Применение паролей позволяет не только ограничить доступ к системе видеонаблюдения, но и распределить права доступа персонала к определенным видеокамерам. А при шифровании попытки перехвата зашифрованных данных в IP-системе охранного видеонаблюдения становятся бессмысленными, если злоумышленник не знает уникального кода для расшифровки потока данных. Код, в свою очередь, устанавливается системным администратором.

GPS-мониторинг транспорта. Спутниковый мониторинг транспорта – система спутникового мониторинга и управления подвижными объектами, построенная на основе использования современных систем спутниковой навигации (GPS/ГЛОНАСС), оборудования и технологий связи (GSM/УКВ), вычислительной техники и цифровых карт. GPS-мониторинг транспорта – технология, применяемая в диспетчерских службах, а также в системах управления перевозками (англ. TMS – Transportation Management System) и автоматизированных системах управления автопарком (англ. FMS – Fleet Management System) для решения задач транспортной логистики и контроля фактических маршрутов транспортных средств при помощи системы GPS.

Автотрекер – прибор, устанавливаемый на автомобиль с целью отслеживания его дальнейшего перемещения и контроля его местоположения. Обычно автотрекер определяет свое местоположение, принимая сигналы ГЛОНАСС/GPS и отправляя их посредством мобильного интернет-канала

GPRS на сервер провайдера, на котором владелец прибора наблюдает перемещение автомобиля.

Для решения задач мониторинга используются следующие компоненты системы:

- спутниковые системы навигации (GPS – США, ГЛОНАСС – РФ),
- приемники GPS и/или ГЛОНАСС,
- системы связи с центральным пунктом (космическая/GSM/УКВ) и/или система локального накопления данных.

Иногда используются дополнительные датчики, установленные на самом техническом средстве и указывающие текущий запас топлива, факт открывания двери или капота, факт наличия пассажира (такси), температуру в рефрижераторе, факт работы или простоя спецмеханизмов (поворот стрелы крана, работы бетоносмесителя), факт нажатия тревожной кнопки и т. п. Полученные данные могут либо накапливаться в локальном устройстве и затем переноситься в центральную базу по возвращении в парк, либо передаваться на центральный сервер в режиме реального времени.

Типичная система GPS-мониторинга состоит из трех звеньев: терминалов, устанавливаемых на автомобили, сервера и клиентских рабочих мест. Терминалы представляют собой специализированные GPS-трекеры, содержащие модуль собственно GPS и модуль сотовой связи (GSM или CDMA). Функции сервера может выполнять обычный ПК с установленным серверным ПО. В отличие от рабочих мест сервер должен быть всегда включен, т. к. именно на нем накапливаются данные о маршрутах. Клиентское ПО в редких случаях может быть объединено в одну программу с серверной частью, но, как правило, допускается одновременное подключение нескольких рабочих мест к одному серверу.

На данный момент представлено порядка 20 различных систем GPS-мониторинга, как импортных, так и отечественных. Импортные решения, как правило, отличаются расширенной функциональностью, зато в отечественных лучше реализованы функции контроля за несанкционированным использованием автомобиля, лучше решен вопрос карт, а формы отчетов соответствуют российскому законодательству. Немаловажным в российских условиях фактором является также защита терминалов от противодействия водителей: наличие резервного аккумулятора, пломбирование устройств и пр.

В качестве основного канала связи в профессиональных системах контроля и управления доступом (СКУД) могут использоваться только те беспроводные технологии, которые эквивалентны по функционалу, назначению и стоимости стандартной проводной компьютерной сети предприятия, – это Wi-Fi, Wi-Max и аналогичные беспроводные сети.

Технологии сенсорных сетей типа ZigBee, Z-Wawe и многие аналогичные должны использоваться по своему прямому назначению – для получения информации от различных датчиков без прокладки проводов на ограниченной (локальной) территории. Такая привлекательная сеть, как GSM, может использоваться либо в домашних системах, либо как дополнительный канал

удаленного доступа к серверу СКУД для получения отчетов и аналогичных действий.

Стандарт GSM был разработан Европейским институтом телекоммуникационных стандартов (ETSI) и признан наиболее надежным и массовым по использованию в средствах телекоммуникации и связи. По очень приблизительным подсчетам число абонентов данного вида связи в Евразии составляет 100 млн.

Центр коммутации подвижной связи (MSC) обслуживает группу сот и обеспечивает все виды соединений, в которых нуждается в процессе работы мобильной связи, аналогичен коммутационной станции ISDN и представляет собой интерфейс между фиксированными сетями (PSTN, PDN, ISDN и т. д.) и сетью подвижной связи. Он обеспечивает маршрутизацию вызовов и выполняет функции управления вызовами. Кроме выполнения функций обычной коммутационной станции ISDN, на MSC возлагаются функции коммутации радиоканалов: «эстафетная передача», в процессе которой достигается непрерывность связи при перемещении подвижной станции из соты в соту, и переключение рабочих каналов в соте при появлении помех или неисправностях.

Использование пароля (или кода PIN – персонального идентификационного цифрового кода) – один из простых методов аутентификации. Он дает очень низкий уровень защиты в условиях использования радиосвязи. Достаточно услышать этот персональный код всего лишь один раз, чтобы обойти средства защиты. В действительности GSM использует PIN-код в сочетании с SIM (Subscriber Identify Module): данный PIN-код проверяется на месте самим SIM без передачи в эфир.

9.2. Практическая часть

Произвести анализ модели GSM-канала по уровню обеспечения требуемой зоны покрытия согласно заданию преподавателя.

Данные для расчета

На дальность радиосвязи влияют следующие факторы:

1. Местоположение BS и MS и рельеф местности.
2. Мощность и чувствительность MS.
3. Мощность и чувствительность BS.
4. Используемые на MS и BS антенны.

Обычно базовые станции имеют мощность 20–30 Вт. Антенны применяются либо штыревые, либо направленные. Чувствительность базовых станций составляет –100…115 дБ. Изменить или повлиять на все эти параметры пользователь, конечно, не может. Большинство операторов используют ограничение дальности работы мобильного телефона от базовой станции: 35 км для GSM-900, для GSM-1800 – порядка 10 км, что обусловлено особенностями стандарта). Однако в GSM предусмотрена также нестандартная конфигурация соты, при которой дальность связи увеличивается на 70–100 км

(конфигурация Extended Cell). К сожалению, при такой конфигурации количество разговорных каналов уменьшается до 2–3, что уменьшает емкость сети. Использовать такой режим в городе и около него оператору невыгодно. Иногда этот режим используется на морском побережье для создания прибрежной зоны покрытия.

Железобетонные строения способны ослаблять сигналы, проходящие через них (при внутреннем покрытии), в 100–1000 раз (т. е. на 20–30 дБ). К числу препятствий можно также отнести кузова автомобилей, кроны деревьев и т. д. Влияние могут оказать и атмосферные осадки.

При расчете зоны покрытия применяется модель Хата, т. к. она рекомендована Международным консультативным комитетом по радиосвязи (МККР) и довольно проста в применении. Эта модель позволяет вычислить потери на радиотрассе для конкретной местности и параметров базовой станции.

Средний уровень потерь на радиотрассе, следуя эмпирической модели Хата, определяется следующим образом:

$$L = 69.55 + 26.16\lg(f) - 13.82\lg(H_{bs}) + [44.9 - 6.55\lg(H_{bs})]\lg(r) + \alpha(h_{as}) +$$

$$+\alpha(U_r) + \alpha(b) + \alpha(H_{bs}, f),\ \text{дБ}.$$

где $f = [100;3000]$ – частота, МГц;

$H_{bs} = [30;300]$ – высота базовой станции, м;

$r = [1;100]$ – расстояние между базовой станцией и абонентской станцией, км;

$h_{as} = [1;3]$ – высота абонентской станции, м;

$\alpha(h_{as}) = (1-U)\beta_1 + U(\beta_2 F_1 + \beta_3 F_2)$ – коэффициент, учитывающий высоту антенны абонентской станции ($U = 0$ для небольшого или среднего города, $U = 1$ для большого города);

$$\beta_1 = (0.7 - 1.1\lg(f))h_{as} + 1.56\lg(f) - 0.8,\ \beta_2 = 1.1 - 8.29\lg^2(1.54h_{as}),$$

$$\beta_3 = 4.97 - 3.2\lg^2(11.75h_{as}),\ F_1 = \frac{300^4}{f^4 + 300^4},\ F_2 = \frac{f^4}{f^4 + 300^4};$$

$\alpha(U_r) = (1-U_r)\left(\left[1 - 2U_r\right]\gamma_1 + 4U_r\gamma_2\right)$ – коэффициент, учитывающий характер местности ($U_r = 0$ для сельской местности, $U_r = 0.5$ для пригорода, $U_r = 1$ для города), $\gamma_1 = 4.78\lg^2(f) - 18.33\lg(f) + 40.94,\ \gamma_2 = 2\lg^2\left(\frac{f}{28}\right) + 5.4;$

$\alpha(b) = 25\lg(b) - 30$ – коэффициент, отражающий влияние плотности застройки, $b = [3;50]$, (%) – плотность застройки;

$$\alpha(H_{bs}, f) = \left(27 + \frac{f}{230}\right)\lg\frac{17(H_{bs} + 20)}{17(H_{bs} + 20) + r^2} + 1.3 - \frac{f - 55}{750} -$$

коэффициент, учитывающий сферичность Земли (вводится, если $0.2R_0 < r \leq \leq 0.8R_0$, где R_0 – расстояние прямой видимости).

Задание

Необходимо рассчитать зону покрытия БС стандарта GSM-900 в большом городе с плотностью застройки 35 %, исходя из требования обеспечения надлежащего качества сигнала, при $f = 900$ МГц; $H_{bs} = 32$ м; $h_{as} = 1.7$ м.

Решение

$$\beta_1 = (0.7 - 1.1\lg 900)\cdot 1.7 + 1.56\lg 900 - 0.8 = -0.526;$$

$$\beta_2 = 1.1 - 8.29\lg^2(1.54\cdot 1.7) = -0.348;$$

$$\beta_3 = 4.97 - 3.2\lg^2(11.75\cdot 1.7) = -0.442;$$

$$F_1 = \frac{300^4}{900^4 + 300^4} = 0.012;\ F_2 = \frac{900^4}{900^4 + 300^4} = 0.988;$$

$$\alpha(h_{as}) = (1-1)\beta_1 + 1\cdot(\beta_2 F_1 + \beta_3 F_2) = -0.348\cdot 0.012 - 0.442\cdot 0.988 = -0.441.$$

$\alpha(U_r) = 0$ для города ($U_r = 1$).

$$\alpha(b) = 25\lg(35) - 30 = 8.6.$$

$$\alpha(H_{bs}, f) = \left(27 + \frac{900}{230}\right)\lg\frac{17(32+20)}{17(32+20)+r^2} + 1.3 - \frac{900-55}{750} = 30.9\lg\left(1 + \frac{r^2}{884}\right)^{-1} + 0.17.$$

Средний уровень потерь на радиотрассе:

$$L = 69{,}55 + 26{,}16\lg 900 - 13{,}82\lg 32 + [44{,}9 - 6{,}55\lg 32]\lg r - 0.441 + 8.6 +$$

$$+30.9\lg\left(1 + \frac{r^2}{884}\right)^{-1} + 0.17,\ \text{дБ};$$

$$L = 134.65 + 35\lg r + 30.9\lg\left(1 + \frac{r^2}{884}\right)^{-1},\ \text{дБ}.$$

Теперь, исходя из выходной мощности передатчика P(дБ), запаса по замираниям S(дБ) и требуемого уровня сигнала на входе приемника Q(дБ) (), запишем уравнение для нахождения R – максимального расстояния от БС, на котором достигается требуемое качество связи:

$$P - L - S = Q;$$

$$P - \left(134.65 + 35\lg R + 30.9\lg\left(1 + \frac{R^2}{884}\right)^{-1}\right) - S = Q.$$

Задавая соответствующие параметры P (дБ), S (дБ) (обычно берется равным 20 дБ), Q (дБ) (для МС берется –110 дБ), можно вычислить расстояние уверенной связи R; на основании этих данных строится зона покрытия БС с точки зрения качества сигнала (без учета нагрузки на соту и возможностей БС по пропускной способности).

На рис. 10 показан характерный вид функции уровня сигнала в зависимости от расстояния между БС и абонентом. Пересечение этой функции с прямой Q дает значение максимального значения радиуса зоны обслуживания, при котором еще предоставляются услуги требуемого качества. Для стандарта GSM-900 R~3–10 км (в отдельных случаях до 30 км).

Рис. 10. Зависимость уровня сигнала от расстояния между БС и абонентом

Таким образом, приходится сужать зону покрытия и увеличивать количество БС, исходя из прогнозов абонентской нагрузки на соту.

При расчете абонентской нагрузки и, следовательно, емкости соты часто пользуются моделью Эрланга для систем с отказом (модель Эрланга В). В этом случае вероятность отказа в обслуживании (вероятность поступления вызова в момент занятости всех каналов) вычисляется как

$$p_n = \frac{\frac{A^n}{n!}}{\sum_{i=0}^{n} \frac{A^i}{i!}},$$

где $A=\lambda T$ – нагрузка (в данной формуле);

n – общее число каналов.

Рассчитаем нагрузку на БС, обслуживающую поселок на 50 коттеджей, оборудованных охранной системой, использующих Voice-канал передачи сообщений.

Нагрузка на БС складывается из системных звонков (1 раз в 5 мин продолжительностью 5 с, т. к. первые 5 с бесплатные) и звонков, осуществляемых гражданскими абонентами. Такая нагрузка будет приблизительно равна 1. Вероятность отказа в обслуживании (вероятность поступления вызова в момент занятости всех каналов) вычисляется как

$$p_n = \frac{\frac{A^n}{n!}}{\sum_{i=0}^{n} \frac{A^i}{i!}}.$$

Тогда зависимость вероятности отказа от количества каналов будет представлена на рис. 11.

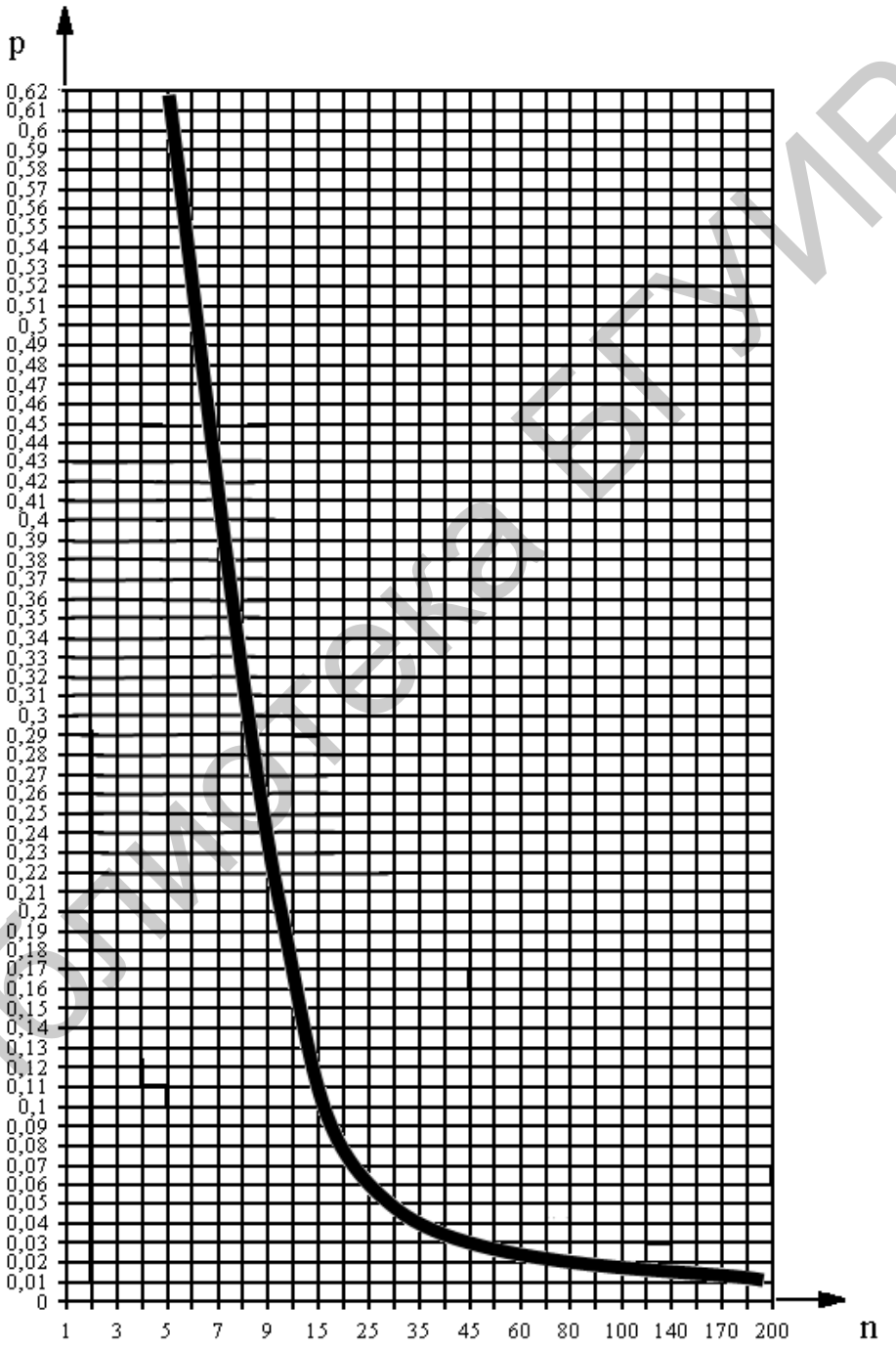

Рис. 11. Зависимость вероятности отказа в обслуживании от количества каналов

Варианты

1	2	3	4	5
f=900 МГц H_{bs}=75 м r=1 м h_{as}=1,5 м U=0 U_r=0 b=3	f=1800 МГц H_{bs}=32 м r=25 м h_{as}=3 м U=0 U_r=1 b=14	f=900 МГц H_{bs}=64 м r=70 м h_{as}=2 м U=1 U_r=1 b=2	f=1800 МГц H_{bs}=120 м r=5 м h_{as}=1,7 м U=0 U_r=0,5 b=35	f=900 МГц H_{bs}=32 м r=93 м h_{as}=1,6 м U=1 U_r=1 b=15м
6	**7**	**8**	**9**	**10**
f=1800 МГц H_{bs}=75 м r =56 м h_{as}=2 м U =0 U_r =0 b =10	f=900 МГц H_{bs}=48 м r =56 м h_{as}=2 м U =0 U_r =0 b =10	f=1800 МГц H_{bs}=94 м r =1,5 м h_{as}=1,4 м U =0 U_r =0,5 b =5	f=900 МГц H_{bs}=35 м r =45 м h_{as}=2,1 м U =1 U_r =1 b =28	f=1800 МГц H_{bs}=87 м r =25 м h_{as}=3 м U =0 U_r =1 b =2
11	**12**	**13**	**14**	**15**
f=900 МГц H_{bs}=169 м r=95 м h_{as}=2,2 м U=1 U_r=1 b=18	f=1800 МГц H_{bs}=65 м r=3 м h_{as}=2 м U=0 U_r=0,5 b=12	f=900 МГц H_{bs}=250 м r =15 м h_{as}=2,05 м U=1 U_r=1 b=10	f=1800 МГц H_{bs}=137 м r=69 м h_{as}=1,9 м U=0 U_r=0 b=5	f=900 МГц H_{bs}=190 м r =80 м h_{as}=1,6 м U=1 U_r=0,5 b=50

9.3. Содержание отчета

1. Цель работы.
2. Результаты выполнения практического задания.

ЛИТЕРАТУРА

1. Белов, Е. Б. Основы информационной безопасности / Е. Б. Белов. – М. : Горячая линия – Телеком, 2006. – 544 с.

2. Герасименко, В. А. Основы защиты информации / В. А. Герасименко. – М. : Инкомбук, 1997. – 540 с.

3. Дадалко, В. А. Реформирование экономики Республики Беларусь. В 5 ч. Ч. 3 : Национальная, экономическая, продовольственная, энергетическая и экологическая безопасность / В. А. Дадалко. – Минск : Армита. – 1997. – 280 с.

4. Доронин, А. Экономическая и информационная безопасность / А. Доронин. – Тула, 1997. – 142 с.

5. Об информации, информатизации и защите информации : Закон Респ. Беларусь от 10 нояб. 2008 г. №455-З.

6. О государственных секретах : Закон Респ. Беларусь от 19 июля 2010 г. №170-З.

7. Концепция национальной безопасности Республики Беларусь : Указ Президента Респ. Беларусь, 17 июля 2001 г., №390.

8. Основные направления обеспечения национальной безопасности Республики Беларусь. Современное состояние и перспективы / М. В. Мясникович [и др.]. – Минск : Экономика и право, 2003. – 451 с.

9. Национально-государственные интересы Республики Беларусь; под ред. Л. Ф. Заико. – Минск : Изд-во В. М. Скакун, 1999. – 268 с.

10. Национальная и региональная безопасность / Л. Ф. Заико [и др.]. – Минск : Несси, 2001. – 436 с.

11. Общая теория национальной безопасности : учебник / под общ. ред. А. А. Прохожева. – М. : Изд-во РАГС, 2002. – 320 с.

12. Основы информационной безопасности: учеб. пособие для вузов / Е. Б. Белов [и др.]. – М. : Горячая линия – Телеком, 2006. – 544 с.

13. Технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) : Постановление Совета Министров Респ. Беларусь, 15 мая 2013 г., №375.

14. Расторгуев, С. П. Введение в формальную теорию информационной войны / С. П. Расторгуев. – М. : Вузовская кн., 2002. – 120 с.

15. Романец, Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец. – М. : Радио и связь, 2001. – 376 с.

16. Семкин, С. Н. Основы информационной безопасности объектов обработки информации : науч.-практ. пособие / С. Н. Семкин, А. Н. Семкин. – Орел : Гелиос АРВ, 2005. – 300 с.

17. Соколов, А. В. Защита от компьютерного терроризма : справ. пособие. – СПб. : БХВ-Петербург : Арлит, 2002. – 496 с.

18. Об утверждении Концепции национальной безопасности Республики Беларусь: Указ Президента Респ. Беларусь, 9 нояб. 2010 г., №575.

19. О мерах по совершенствованию использования национального сегмента сети Интернет : Указ Президента Респ. Беларусь, 1 февр. 2010 г., №60.

20. Теоретические основы компьютерной безопасности : учеб. пособие для вузов / П. Н. Девянин [и др.]. – М. : Радио и связь, 2000. – 192 с.

21. Трахименок, С. А. Безопасность государства: методолого-правовые аспекты / С. А. Трахименок. – Минск : Бел. изд. товарищество «Хата», 1997. – 250 с.