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

Факультет инфокоммуникаций

Кафедра защиты информации

Т. А. Пулко

ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

*Допущено Министерством образования Республики Беларусь
в качестве учебного пособия
для студентов учреждений высшего образования по специальности
1-98 01 02 «Защита информации в телекоммуникациях»*

Минск БГУИР 2018

УДК 004.056(076)
ББК 32.973.26-018.2я7
П88

Р е ц е н з е н т ы:

кафедра технологий программирования
Белорусского государственного университета
(протокол №10 от 19.03.2015);

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. пособие / Т. А. Пулко. – Минск : БГУИР, 2018. – 164 с. : ил.

ISBN 978-985-543-250-1.

В учебном пособии рассмотрены основные уровни обеспечения информационной безопасности (административный, организационный, законодательный, программно-технический), вопросы технического нормирования и стандартизации в области информационной безопасности. Приводится описание основных угроз информационной безопасности и их источников, рассмотрены способы и средства обеспечения информационной безопасности. Проанализированы вопросы защиты информации в компьютерных системах. Представленное учебное пособие будет полезным для студентов технических высших учебных заведений и специалистов в области защиты информации.

УДК 004.056(076)
ББК 32.973.26-018.2я7

ISBN 978-985-543-250-1

СОДЕРЖАНИЕ

СПИСОК УСЛОВНЫХ СОКРАЩЕНИЙ

АБ	–	администратор безопасности антивирусные
АПС	–	программные средства автоматизированное
АРМ	–	рабочее место автоматизированная система
АС	–	автоматизированная система обработки данных
АСОД	–	Белорусский государственный институт стандартизации
БелГИСС	–	и сертификации
		Государственный центр безопасности информации
ГЦБИ	–	информационная безопасность
ИБ		информационные технологии
ИТ	–	критически важные объекты информатизации
КВОИ	–	компьютерная система
КС	–	локальная вычислительная сеть
ЛВС	–	машинные носители информации
МНИ	–	Международная организация по стандартизации
МОС	–	Межпарламентская ассамблея «Евразийское
МПА ЕврАзЭС	–	экономическое сообщество»
		Международный союз электросвязи
МСЭ-Т	–	Национальная книжная палата Беларуси
НКП	–	несанкционированный доступ
НСД	–	Национальный центр интеллектуальной собственности
НЦИС	–	Национальный центр правовой информации
НЦПИ	–	Оперативно-аналитический центр при Президенте
ОАЦ	–	Республики Беларусь
	–	оперативное запоминающее устройство
ОЗУ		объект информатизации
ОИ	–	программное обеспечение
ПО	–	программные средства защиты от воздействия
ПСЗВВП	–	вредоносных программ
ПЭВМ	–	побочные электромагнитные излучения и наводки
ПЭМИН	–	рабочее место администратора безопасности
РМ АБ	–	Республиканский центр трансфера технологий
РЦТТ	–	средства вычислительной техники
СВТ	–	средства защиты информации
СЗИ	–	служба информационной безопасности
СИБ	–	средства криптографической защиты информации
СКЗИ	–	система контроля доступа
СКУД	–	средства массовой инфомации
СМИ	–	система менеджмента информационной безопасности
СМИБ	–	системы речевого оповещения и управления эвакуацией
СОУЭ	–	система управления базой данных
СУБД	–	система электронного документооборота
СЭД	–	

ТСПН	TeXHWieCKIIe cpe,n:c1Ba rrepe,n:a"!IIIIH<j;JopMau:nn
ЗПЛ	3JieKTPOHHa5! I(II<j;JpoBa5! IIO,[(IIIICh
DNS	CIICTeMa !J:OMeHHbiX IIMeH
DoS	aTaKIIOTKa3a B o6CJIY)KIIBaHIIII
ERP	rrrraHIIpoBaHIIe pecypcoB rrpe,n:rrpii5!TII5!

ВВЕДЕНИЕ

Целью данного пособия является анализ существующих подходов, методов и средств обеспечения безопасности информации определенных нормативно-правовой базой Республики Беларусь.

Пособие состоит из четырех разделов, охватывающих основные направления комплексного обеспечения информационной безопасности (ИБ) на информационном объекте.

Первый раздел посвящен рассмотрению национальных информационных ресурсов, определенных Законом Республики Беларусь «Об информации, информатизации и защите информации», анализу понятия «информационная безопасность», определенного рамками Концепции национальной безопасности Республики Беларусь, Постановлением Правления Национального Банка Республики Беларусь, Соглашением о сотрудничестве государств – участников СНГ, Межпарламентской Ассамблеи Евразийского экономического сообщества. Проведен обзор законодательной базы Республики Беларусь в области информационной безопасности на базе конституции, Гражданского кодекса, Уголовного кодекса, кодекса РБ об административных правонарушений, трудового и налогового кодексов, международных договоров РБ. Рассмотрены основные законы Республики Беларусь, указы Президента РБ, постановления Совета Министров РБ в области информационной безопасности. Представлены выдержки документов по техническому нормированию и стандартизации в области информационной безопасности РБ. Определены основные понятия политики информационной безопасности организаций и предприятий.

Во втором разделе учебного пособия проанализированы известные подходы к классификации угроз информационной безопасности и их источников по различной природе возникновения. Отдельное внимание уделено внутренним и внешним источникам угроз национальной безопасности РБ, которые носят взаимосвязанный характер с различными сферами жизнедеятельности. Отмечается отсутствие единого подхода к идентификации и классификации уязвимостей для информационных систем, порождающих угрозы информационной безопасности и предлагается вариант классификации уязвимостей по основным критериям, связанным с местом и причинами их возникновения.

Третий раздел посвящен исследованию методов и средств обеспечения безопасности информации, которое начинается с определения уровней и характеристики защитных действий в данной области. Рассмотрены этапы процесса обеспечения безопасности информации, включающие в себя аудит ИБ, выбор методов и средств защиты (формальные и неформальные), проектирование и реализацию системы защиты. Представлен анализ отечественного рынка программно-технических средств защиты информации Республики Беларусь в соответствии с перечнем сертифицированных продуктов информационных технологий, прошедших сертификацию в Оперативно-аналитическом центре при Президенте Республике Беларусь, что является существенной отличительной особенностью данного пособия.

С учетом обширности темы, связанной с безопасностью информации в компьютерных системах, она была выделена в отдельный четвертый раздел. Рассмотрена модель политики безопасности компьютерной сети согласно особенностям внутренних и внешних потенциальных угроз. Предложены методы и способы обеспечения безопасности информации в компьютерных сетях по трем отдельным компонентам, оказывающим взаимное влияние друг на друга: информации, технических и программных средств, обслуживающего персонала и пользователей.

Учебное пособие может быть полезным для студентов технических высших учебных заведений и широкого круга читателей, интересующихся вопросами информационной безопасности.

1. СИСТЕМНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

1.1. Понятие безопасности в информационной сфере

Уровень развития информационного пространства общества определенным образом влияет на процесс функционирования государственных институтов, экономику, обороноспособность, во многом определяет вопросы внешней и внутренней политики.

Основными составляющими информационного пространства являются:

- система информационного законодательства;
- инфокоммуникационная инфраструктура;
- информационные ресурсы;
- рынок информационных технологий, услуг и продуктов;
- сопряженность с мировыми открытыми сетями;
- средства массовой информации;

Информационная среда современного общества базируется на достижениях в сфере информационных технологий и развитии инфраструктуры, а также на доступности информационных ресурсов. Данными факторами определяется организация системы общественной жизни и основа современной политики государств во всех ее областях.

По оценкам российских экспертов, в информационном обществе первичной становится не стоимость труда, а стоимость знаний. Наряду с традиционными формами богатства все большее значение приобретает накопление богатства информационного. Так, свыше 60 % всех ресурсов США приходится сегодня на информационные ресурсы. Обработка информации превратилась в новую индустрию, в структуре экономики сложился мощный информационный сектор. Быстро увеличивается доля трудоспособного населения, занятого в информационной сфере (в США, например, она составляет до 80 %) [1].

Национальные информационные ресурсы предоставляются потребителям:

1) государственными и общественными организациями (в соответствии с Законом Республики Беларусь от 10 ноября 2008 г. №455-З «Об информации, информатизации и защите информации» [2] государственные информационные ресурсы формируются или приобретаются за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц):

- библиотечная сеть РБ;
- архивный фонд РБ;
- государственная система статистики;
- государственная система научно-технической информации;

2) информационными центрами:

- Национальная книжная палата Беларуси (НКП);

- Национальный центр интеллектуальной собственности (НЦИС);

- Национальный центр правовой информации (НЦПИ);

- Белорусский государственный институт стандартизации и сертификации (БелГИСС);

- РУП «Стройтехнорм» – орган по сертификации строительных материалов, изделий и конструкций;

- ОДО «Экспертцентр», предоставляющий деловую информацию в электронном виде;

- Информационный центр посольства США в Беларуси, предоставляющий справочно-информационные услуги по удовлетворению тематических, профессиональных и научных интересов и обучению практическим основам информационной грамотности;

- Республиканский центр трансфера технологий (РЦТТ) [3];

3) коммерческими и некоммерческими структурами (например, Белорусская цифровая библиотека – частная некоммерческая электронная библиотека).

Информационное преимущество является важной социальной силой, способствующей перераспределению экономических, социальных и политических ресурсов. Вместе с тем, как отмечают эксперты, информационное неравенство ведет и к социальному неравенству, что составляет основную угрозу национальной безопасности любого государства. Опыт показывает, что деятельность, которая приводит к господству в информационной среде, в области культуры (так называемой «сфере смыслов») и, как следствие, в политике, всегда начинается с экономических акций, с проникновения иностранного капитала в сферу СМИ и информатизации [4].

Компьютерно-телевизионный компонент индустрии досуга усиливает непосредственное воздействие СМИ на психику человека, его образовательный потенциал, жизненные интересы и поведение. Расширение возможностей средств массовой коммуникации, возрастание роли информационных технологий в повышении эффективности воздействия на психику людей и общественное сознание стимулируют развитие такого междисциплинарного направления как информационно-психологическая безопасность [5].

Несмотря на то, что в настоящее время уделяется много внимания информационной безопасности вследствие использования технических средств обработки и передачи данных практически во всех сферах человеческой деятельности, единого подхода для определения термина «информационная безопасность» ни в науке, ни в законодательстве нет.

Что же понимается под безопасностью в информационной сфере?

В соответствии с Концепцией национальной безопасности Республики Беларусь, утвержденной Указом Президента Республики Беларусь от 9 ноября 2010 г. №575, **информационная безопасность** – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере [6].

Следует отметить, что интересы личности, общества и государства должны быть уравновешены и дополнять друг друга. ***Интересы личности*** в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, использование информации, а также в защите информации, обеспечивающей личную безопасность. ***Интересы общества*** в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства. ***Интересы государства*** – это создание условий для гармоничного развития информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности страны, политической, экономической и социальной стабильности, в обеспечении законности и правопорядка, развития равноправного и взаимовыгодного международного сотрудничества [7].

Согласно Инструкции об организации системы внутреннего контроля в банках, небанковских кредитно-финансовых организациях, банковских группах и банковских холдингах, утвержденной Постановлением Правления Национального Банка Республики Беларусь от 30 ноября 2012 г. №625, **информационная безопасность** – многоуровневый комплекс организационных мер, аппаратно-программных и технических средств, обеспечивающих защиту от случайных и преднамеренных угроз, в результате реализации которых возможно нарушение свойств доступности, целостности, подлинности или конфиденциальности обрабатываемой, хранящейся или передаваемой информации [8].

В Соглашении о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 г. **информационная безопасность** определяется как состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве [9].

Постановление Межпарламентской Ассамблеи Евразийского экономического сообщества от 28 мая 2004 г. №5-20 «О типовых проектах законодательных актов МПА ЕврАзЭС в сфере информационных технологий («Об информатизации», «Об информационной безопасности», «Основные принципы электронной торговли»)» содержит следующую норму: **информационная безопасность** – состояние защищенности прав, свобод, охраняемых законом интересов физических, юридических лиц и государства в информационной сфере от внутренних и внешних угроз [10].

В соответствии с Концепцией информационной безопасности государств – участников Содружества Независимых Государств в военной сфере, утвержденной Решением Совета глав правительств Содружества Независимых Государств от 4 июня 1999 г., **информационная безопасность** – состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства [11].

При определении понятия «информационная безопасность» его зачастую отождествляют с понятием «защита информации». В других случаях этот термин определяется более узко, как набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных в компьютерных сетях. Также под безопасностью в информационной сфере понимают защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры [12].

Таким образом, информационная безопасность является понятием многогранным и комплексным. Оно имеет два основных аспекта: содержательный (духовная сфера) и технический (материальная сфера). К *содержательному аспекту* можно отнести содержание и направленность всей циркулирующей информации; *технический аспект* – совокупность информационно-телекоммуникационных средств, технологий, систем, ресурсов, предназначенных для создания, хранения, распространения, передачи и обработки информации [13].

Вместе с тем, исходя из всех приведенных ранее определений, можно констатировать, что к основным **объектам** информационной безопасности следует отнести:

- *личность* – ее права и свободы;
- *общество* – его материальные и духовные ценности;
- *государство* – его конституционный строй, суверенитет и территориальная целостность.

Субъектами обеспечения безопасности могут выступать:

- государство, осуществляющее функции в этой области через органы законодательной, исполнительной и судебной власти;
- юридические лица;
- граждане, обладающие в соответствии с законодательством правами и обязанностями по участию в обеспечении безопасности государства.

Главную роль при этом играет государство, которое в соответствии с действующим законодательством должно обеспечивать безопасность каждого гражданина и юридического лица, их социальную и правовую защиту [14].

Происходящие в настоящее время процессы преобразования в политической жизни и экономике Республики Беларусь оказывают непосредственное влияние на состояние информационной безопасности и, как следствие, на состояние национальной безопасности государства. Возникают принципиально новые факторы, которые необходимо учитывать при оценке реального состояния информационной безопасности и определения ключевых проблем в этой области. Их условно можно разделить на *социально-политические*, *экономические* и *организационно-технические* [15].

Социально-политическими факторами являются:

- изменение геополитической обстановки вследствие фундаментальных перемен в различных регионах мира, сведение к минимуму вероятности войн;

- информационная экспансия стран с развитыми экономическими системами, осуществляющими глобальный мониторинг политических, экономических, военных, экологических процессов, распространяющих информацию в целях получения односторонних преимуществ;

- активизация деятельности спецслужб иностранных государств по добыванию сведений, составляющих государственные секреты Республики Беларусь;

- реализация конституционной реформы на основе принципов демократии, законности, информационной открытости;

- преодоление децентрализации системы государственного управления, преобразование в системе обеспечения безопасности страны;

- нарушение информационных связей между государствами – участниками СНГ;

- низкая общая правовая и информационная культура населения республики;

- обострение криминогенной обстановки, рост числа преступлений в информационной сфере, в том числе в отношении кредитно-финансовых учреждений [15].

Среди **экономических** факторов наиболее существенными являются:

- включение информационной продукции в систему товарных отношений;

- переход экономики Республики Беларусь на недостаточно регулируемые рыночные отношения, появление множества коммерческих структур – производителей и потребителей информации, средств информатизации и защиты информации;

- критическое состояние отечественных отраслей промышленности и науки, разрабатывающих и производящих средства информатизации и защиты информации;

- неконтролируемое расширение сотрудничества с зарубежными странами в развитии информационной инфраструктуры Республики Беларусь [15].

Из **организационно-технических** факторов можно выделить:

- бессистемность, непоследовательность развития и недостаточную разработанность нормативно-правовой базы в сфере информационных правоотношений, в том числе в области обеспечения информационной безопасности;

- слабое регулирование государством процессов функционирования и развития рынка средств информатизации, информационных продуктов и услуг;

- широкое использование в сфере государственного управления и кредитно-финансовой сфере незащищенных от утечки информации импортных технических и программных средств, предназначенных для хранения, обработки и передачи информации;

- возрастание объемов передачи информации, циркулирующей по открытым каналам связи, в том числе по сетям передачи данных и межмашинного обмена [15].

В настоящее время определяющим фактором для информационной безопасности РБ является активное внедрение информационно-телекоммуникационных технологий на основе компьютерной техники во все сферы жиз-

недеятельности общества, в первую очередь в республиканские органы государственного управления и кредитно-финансовую сферу. Такие технологии представляют собой совокупность программных, технических и организационно-экономических средств, объединенных структурно и функционально для решения задач передачи и обработки информации.

1.2. Комплексный подход по обеспечению информационной безопасности

Обеспечение информационной безопасности – это непрерывный процесс, заключающийся в обосновании и реализации наиболее рациональных методов, способов и путей совершенствования системы защиты, непрерывном контроле ее состояния, выявлении ее узких и слабых мест и противоправных действий [16.].

Комплекс мероприятий, направленных на обеспечение информационной безопасности по различным направлениям, представляет собой **защиту информации**. Комплексный характер информационной безопасности проистекает из того, что защита – это сложная система неразрывно взаимосвязанных и взаимозависимых процессов, каждый из которых в свою очередь имеет множество различных взаимообусловливающих друг друга сторон, свойств, тенденций [17].

Наибольший эффект достигается, когда все используемые средства, методы и меры объединяются в единый целостный механизм – **систему защиты информации** (СЗИ) [18]. При этом функционирование системы должно контролироваться, обновляться и дополняться в зависимости от изменения внешних и внутренних условий. Однако ни одна СЗИ не может обеспечить требуемого уровня безопасности информации без надлежащей подготовки пользователей и соблюдения ими всех установленных правил, направленных на ее защиту.

Для того чтобы обеспечить выполнение всех требований, предъявляемых к системе защиты информации (табл. 1), должны быть соблюдены условия организации информационной деятельности: необходимо разнообразить используемые средства доступа и защиты информации, обеспечить доступность к системе для внесения изменений и дополнений, простоту и удобство технического обслуживания и эксплуатации пользователями, надежность системы, ее комплексность и целостность (ни одна часть не может быть изъята без ущерба для всей системы) [19].

Таблица 1

Требования к системе защиты информации

Требование к СЗИ	*Примечание*
Непрерывность	Злоумышленники непрерывно ищут возможность обойти защиту интересующей их информации
Планирование	Осуществляется путем разработки каждой службой детальных планов защиты информации в сфере ее компетенции с учетом общей цели предприятия (организации)
Целенаправленность	Защите подлежит информация, которая должна защищаться в интересах конкретной цели
Конкретность	Защите подлежат конкретные данные, объективно нуждающиеся в охране, утрата которых может причинить организации определенный ущерб
Активность	Мероприятия по защите информации необходимо проводить регулярно
Надежность	Методы и формы защиты должны надежно перекрывать возможные пути неправомерного доступа к охраняемой информации, независимо от формы ее представления, языка выражения и вида физического носителя, на котором она закреплена
Универсальность	Где бы ни проявился канала утечки или способ несанкционированного доступа, его необходимо перекрывать эффективными средствами, независимо от характера, формы и вида информации
Комплексность	Для защиты информации должны применяться все виды и формы защиты в полном объеме. Недопустимо применять лишь отдельные формы или технические средства

Выполнение системой возложенных на нее функций возможно при соблюдении определенных видов собственного обеспечения (табл. 2).

Таблица 2

Вид обеспечения системы защиты информации

Вид обеспечения системы защиты информации	*Состав обеспечения системы защиты информации*
1	2
Правовое обеспечение	Нормативные документы, положения, инструкции, руководства, требования которых являются обязательными в рамках сферы их действий
Организационное обеспечение	Служба защиты документов, службы режима, допуска, охраны, служба защиты информации техническими средствами, информационно-аналитическая деятельность и др.
Аппаратное обеспечение	Технические средства как для защиты информации, так и для обеспечения деятельности собственно СЗИ
Информационное обеспечение	Сведения, данные, показатели, параметры, лежащие в основе решения задач, обеспечивающих функционирование системы; показатели доступа, учета, хранения; системы информационного обеспечения расчетных задач различного характера, связанных с деятельностью службы обеспечения безопасности

1	2
Программное обеспечение	Информационные, учетные, статистические и расчетные программы, обеспечивающие оценку наличия и опасности различных каналов утечки и путей несанкционированного проникновения к источникам конфиденциальной информации
Математическое обеспечение	Использование математических методов для различных расчетов, связанных с оценкой опасности технических средств злоумышленников, зон и норм необходимой защиты
Лингвистическое обеспечение	Нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации; различного рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований защиты информации

Система информационной безопасности представляет собой организованную совокупность специальных органов, служб, средств, методов и мероприятий, обеспечивающих защиту жизненно важных интересов личности, предприятия и государства от внутренних и внешних угроз (рис. 1) [20].

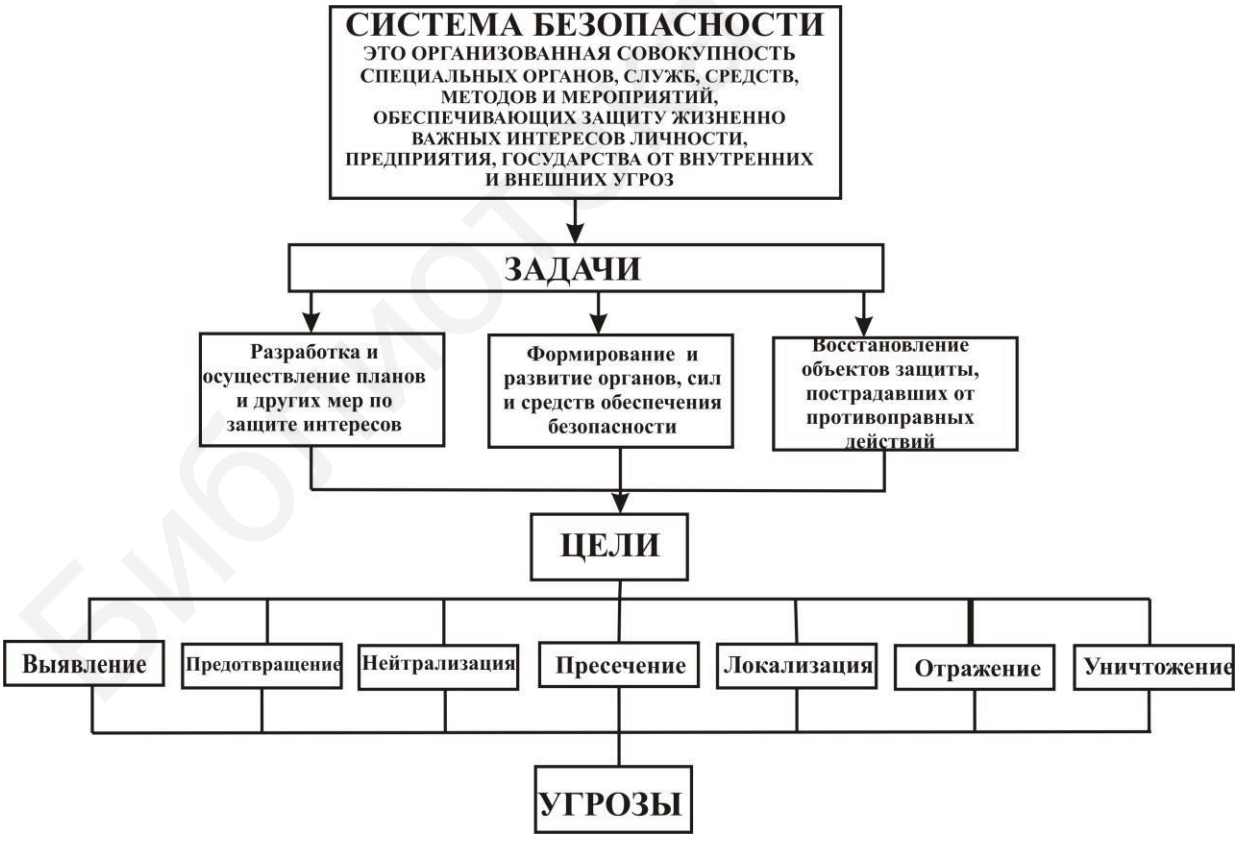

Рис. 1. Цели и задачи системы информационной безопасности

К системе информационной безопасности предъявляются определенные требования [21]:

- четкость определения полномочий и прав пользователей на доступ к определенным видам информации;
- предоставление пользователю минимальных полномочий, необходимых для выполнения порученной работы;
- сведение к минимуму числа общих для нескольких пользователей средств защиты;
- учет случаев и попыток несанкционированного доступа к конфиденциальной информации;
- обеспечение оценки степени конфиденциальности информации;
- обеспечение контроля целостности средств защиты и немедленное реагирование на их выход из строя.

Выполнение приведенных требований к системе информационной безопасности возможно при определении субъектов, объектов и средств защиты, источников угроз и направленности опасных информационных потоков, принципов обеспечения информационной безопасности.

Основными аспектами системы информационной безопасности являются (рис. 2):

- доступность (возможность за короткое время получить требуемую информационную услугу);
- целостность (защищенность информации от разрушения и несанкционированного изменения);
- конфиденциальность (защита от несанкционированного прочтения);
- достоверность.

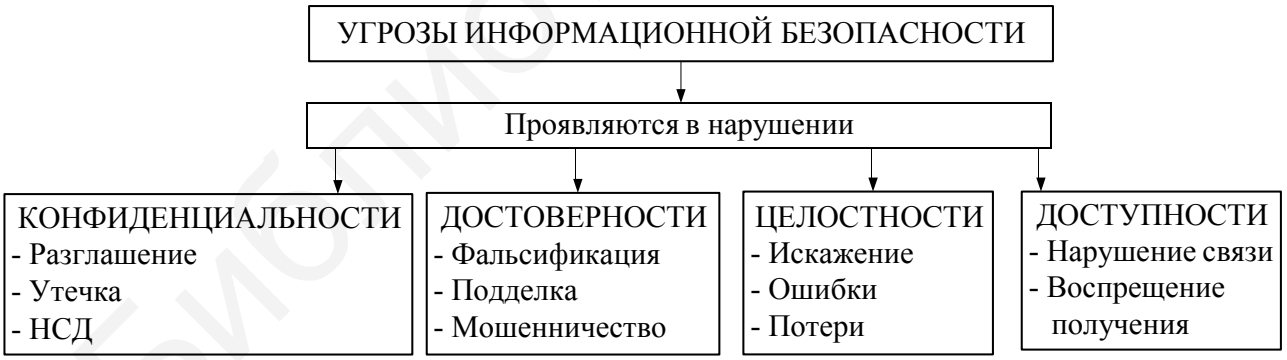

Рис. 2. Возможные проявления угроз информационной безопасности

Формирование режима информационной безопасности – проблема комплексная, решаемая как минимум на четырех уровнях:

- нормативно-правовой (законы, нормативные акты, стандарты и т. п.);
- административный (действия общего характера, предпринимаемые руководством организации);
- процедурный (конкретные меры безопасности, связанные с людьми);
- программно-технический (конкретные технические меры).

Примечание. **Информационная система** – это совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств [2].

Рассмотрим основные задачи, решение которых обеспечивает информационную безопасность [22].

Конфиденциальность информации. У каждого человека или организации есть документы, которые не должны стать всеобщим достоянием, будь то личные медицинские данные, информация о финансовых операциях или государственная тайна. Пока для хранения используются неэлектронные средства (бумага, фотопленка), секретность обеспечивается административными методами (хранение в сейфах, транспортировка в сопровождении охраны и т. д.), но когда информация обрабатывается на компьютерах и передается по открытым каналам связи, административные методы дополняются другими методами информационной безопасности. Задача обеспечения секретности заключается в хранении и передаче данных в таком виде, чтобы злоумышленник, даже получив доступ к носителю или среде передачи, не смог получить сами защищенные данные.

Целостность информации. Информация может быть изменена прямо на носителе в процессе обработки и передачи по каналам связи. Также данные могут быть искажены как случайно, так и преднамеренно. Проверка целостности необходима в ситуациях, когда интерпретация неправильных данных может привести к серьезным последствиям (например, при возникновении ошибки в сумме банковского перевода или значении скорости самолета, заходящего на посадку).

Идентификация. Необходима для того, чтобы отождествить пользователя с некоторым уникальным идентификатором, после чего ответственность за выполненные действия возлагается на пользователя, за которым этот идентификатор закреплен.

Аутентификация. Необходимое дополнение к идентификации, предназначенное для подтверждения истинности (аутентичности) пользователя, предъявившего идентификатор.

Уполномочивание. Ни один пользователь не должен получить доступ к системе без успешного выполнения идентификации и последующей аутентификации, а также без уполномочивания на такие действия специальным разрешением.

Контроль доступа. Комплексное понятие, обозначающее совокупность методов и средств, предназначенных для ограничения доступа к ресурсам, который имеют только уполномоченные пользователи. Попытки доступа к ресурсам должны протоколироваться. Право собственности предоставляет пользователю законное право на использование некоторого ресурса и возможность передачи этого ресурса в собственность другому пользователю. Право собственности обычно является составной частью системы контроля доступа.

Сертификация. Процесс подтверждения некоторого факта стороной, которой пользователь доверяет. Чаще всего сертификация используется для удостоверения принадлежности открытого ключа конкретному пользователю или

компании, т. к. эффективное использование инфраструктуры открытых ключей возможно лишь при наличии системы сертификации. Организации, занимающиеся выдачей сертификатов, называются удостоверяющими центрами. Подпись позволяет получателю документа доказать, что данный документ был подписан именно отправителем. При этом подпись не может быть перенесена на другой документ, отправитель не может отказаться от своей подписи, любое изменение документа приведет к нарушению подписи, и любой пользователь при желании может самостоятельно убедиться в подлинности подписи.

Неотказуемость. Существует доказательство, которое получатель сообщения способен предъявить третьей стороне, чтобы та смогла независимо проверить, кто является отправителем сообщения, следовательно, отправитель сообщения не имеет возможности отказаться от авторства, т. к. существуют математические доказательства того, что никто кроме него не способен создать такое сообщение. Расписка в получении передается от получателя к отправителю и может впоследствии быть использована отправителем для доказательства того, что переданная информация была доставлена получателю не позже определенного момента, указанного в расписке.

Датирование. Позволяет зафиксировать момент подписания документа и часто применяется совместно с подписью. Может быть использовано, например, для доказательства первенства, если один документ был подписан несколькими пользователями, каждый из которых утверждает, что именно он является автором документа. Кроме этого, датирование широко используется в сертификатах, которые имеют ограниченный срок действия. Если же отметка времени отсутствует, то после истечения срока действия сертификата подпись не может быть признана корректной.

Аннулирование. Используется для отмены действия сертификатов, полномочий или подписей. Если какой-либо участник информационного обмена или принадлежащие ему ключи и сертификаты оказались скомпрометированы, необходимо предотвратить доступ этого пользователя к ресурсам и отказать в доверии соответствующим сертификатам, т. к. ими могли воспользоваться злоумышленники. Также процедура аннулирования может быть использована в отношении удостоверяющего центра.

Свидетельствование. Удостоверение (подтверждение) факта создания или существования информации некоторой стороной, не являющейся создателем.

Анонимность. Задача осуществляется довольно редко. Как правило, правительствам и корпорациям невыгодно, чтобы пользователь мог остаться анонимным при совершении каких-либо действий в информационном пространстве. Кроме того, большинство средств коммуникаций позволяют определить маршрут передачи того или иного сообщения, а значит, вычислить отправителя. Возможно, по этим причинам проекты по обеспечению анонимности носят временный характер.

1.3. Нормативно-правовое обеспечение информационной безопасности Республики Беларусь

Опыт эксплуатации информационных систем и ресурсов в различных сферах жизнедеятельности показывает, что существуют различные и весьма вероятные угрозы потери информации, приводящие к материальным и иным ущербам. Развитие информационных технологий создает качественно новые угрозы, способные приводить порой к катастрофическим по своим масштабам последствиям. Разработка и совершенствование законодательной базы информационной безопасности является необходимой мерой, удовлетворяющей важнейшую потребность в защите информации при развитии социально-экономических, политических, военных направлений деятельности каждого государства.

К **международным договорам** РБ в области информационной безопасности можно отнести:

- Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 г. [23];
- Постановление Межпарламентской Ассамблеи государств – участников Содружества Независимых Государств от 18 ноября 2005 г. №26-7 «О гармонизации законодательства государств – участников СНГ в области информатизации и связи» [24];
- Соглашение между Правительством Республики Беларусь и Правительством Республики Казахстан о сотрудничестве в области защиты информации [25];
- Соглашение между Правительством Республики Беларусь и Правительством Российской Федерации о сотрудничестве в области защиты информации [26];
- Постановление Межпарламентского комитета Республики Беларусь, Республики Казахстан, Кыргызской Республики, Российской Федерации и Республики Таджикистан от 15 октября 1999 г. №9-9 «О модельном законе «О безопасности» [27].

В основном законе государства – **Конституции Республики Беларусь** от 15 марта 1994 г. – 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; указывается, что пользование информацией может быть ограничено законодательством в целях защиты чести, достоинства, личной и семейной жизни граждан и полного осуществления ими своих прав [28].

В **Гражданском кодексе Республики Беларусь** содержатся нормы, касающиеся служебной и коммерческой тайны, закрепляется такая форма отношений, как информационные услуги, электронная подпись признается как

средство, подтверждающее подлинность сторон в сделках, предусматривается ответственность за незаконное использование информации [29].

В **Уголовном кодексе Республики Беларусь** закрепляется ответственность за преступления против информационной безопасности, а также иные составы преступлений в информационной сфере: хищение путем использования компьютерной техники, умышленное разглашение государственной тайны, разглашение государственной тайны по неосторожности, умышленное разглашение служебной тайны и т. д. [30].

Кодексом Республики Беларусь об административных правонарушениях определяются административно-правовые санкции за правонарушения в информационной сфере. К таким правонарушениям относятся: отказ в предоставлении гражданину информации, несанкционированный доступ к компьютерной информации, нарушение правил защиты информации и т. д. [31].

Трудовым кодексом Республики Беларусь для работников устанавливается обязанность хранить государственную и служебную тайну, не разглашать коммерческую тайну нанимателя, коммерческую тайну третьих лиц, к которой наниматель получил доступ [32].

Налоговый кодекс Республики Беларусь (общая часть) включает нормы, определяющие порядок защиты различных видов конфиденциальной информации [33].

Рассмотрим основные законы Республики Беларусь в области информационной безопасности.

1. Закон РБ **«Об информации, информатизации и защите информации»** от 10 ноября 2008 г. №455-З, изменения и дополнения от 4 января 2014 г. №102-З. 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 [34].

В тексте закона сообщается, что 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 этого закона не распространяется на общественные отношения, связанные с деятельностью СМИ и охраной информации, являющейся объектом интеллектуальной собственности.

Среди внесенных в Закон Республики Беларусь «Об информации, информатизации и защите информации» изменений и дополнений от 4 января 2014 г. выделим следующие:

- введено определение термина «персональные данные» – это основные и дополнительные персональные данные физического лица, подлежащие в соответствии с законодательными актами Республики Беларусь внесению в регистр населения, а также иные данные, позволяющие идентифицировать такое лицо;

- уточнены полномочия Оперативно-аналитического центра при Президенте Республики Беларусь в области информатизации и защиты информации;

- закон дополнен статьей 181 «Служебная информация ограниченного распространения»;

- внесены изменения и дополнения в ряд статей закона, регламентирующих вопросы распространения и (или) предоставления общедоступной информации.

2. Закон РБ **«О государственных секретах»** от 19 июля 2010 г. №170-З 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 [35].

3. Закон РБ **«О коммерческой тайне»** от 5 января 2013 г. №16-З регулирует отношения, возникающие в связи с установлением, изменением и отменой режима коммерческой тайны, а также в связи с правовой охраной коммерческой тайны. Действие этого закона не распространяется на отношения, связанные с государственными секретами. Законодательство о коммерческой тайне основывается на Конституции Республики Беларусь и состоит из Гражданского кодекса Республики Беларусь, рассматриваемого закона и иных актов законодательства, а также международных договоров Республики Беларусь. Если международным договором Республики Беларусь установлены иные правила, чем те, которые содержатся в Законе РБ «О коммерческой тайне», то применяются правила международного договора [36].

4. Закон РБ **«Об электронном документе и электронной цифровой подписи»** от 28 декабря 2009 г. №113-З направлен на установление правовых основ применения электронных документов, определение основных требований, предъявляемых к электронным документам, а также правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе является равнозначной собственноручной подписи в документе на бумажном носителе [37].

5. Закон РБ **«Об органах государственной безопасности Республики Беларусь»** от 10 июля 2012 г. №390-З определяет правовые и организационные основы деятельности органов государственной безопасности Республики Беларусь, устанавливает обязанности и права органов государственной безопасности и их сотрудников, гарантии правовой и социальной защиты сотрудников органов государственной безопасности и членов их семей [38]. Основными задачами органов государственной безопасности являются:

- защита независимости и территориальной целостности Республики Беларусь, обеспечение национальной безопасности Республики Беларусь в политической, экономической, военной, научно-технологической, информационной, социальной, демографической и экологической сферах;

- оценка текущего состояния национальной безопасности Республики Беларусь, прогнозирование его развития, а также разработка и осуществление

комплекса мер по предупреждению и выявлению угроз национальной безопасности Республики Беларусь, внесение в соответствии с законодательством Республики Беларусь предложений Президенту Республики Беларусь по обеспечению национальной безопасности Республики Беларусь;

- информирование Президента Республики Беларусь и по его поручению соответствующих государственных органов и иных организаций по вопросам состояния национальной безопасности Республики Беларусь;

- разработка и проведение мероприятий по оказанию содействия государственным органам и иным организациям в осуществлении мер в области политического, социально-экономического развития и научно-технического прогресса Республики Беларусь;

- организация и осуществление в пределах своей компетенции контрразведывательной деятельности и внешней разведки;

- предупреждение, выявление и пресечение террористической и иной экстремистской деятельности, организованной преступности и коррупции, незаконной миграции, незаконного оборота наркотических средств, психотропных веществ, их прекурсоров и аналогов, оружия, боеприпасов, ядерных материалов и их компонентов, а также иных объектов экспортного контроля, контрабанды, других преступлений, дознание и предварительное следствие по которым законодательными актами Республики Беларусь отнесены к ведению органов государственной безопасности;

- осуществление предусмотренных законодательством Республики Беларусь полномочий в сфере государственных секретов;

- обеспечение государственных органов и иных организаций правительственной и оперативной связью, организация и обеспечение в пределах своей компетенции криптографической и инженерно-технической безопасности шифрованной и других видов специальной связи в Республике Беларусь и организациях Республики Беларусь, находящихся за ее пределами, и осуществление государственного контроля за этой деятельностью.

Особое место в правовом регулировании в области обеспечения информационной безопасности занимают **указы Президента Республики Беларусь** и **постановления Совета Министров Республики Беларусь**. Среди данных правовых актов можно выделить основные блоки нормативных правовых актов:

- о защите информации (в том числе технической защиты);

- о доступе граждан к информации;

- о компетенции органов государственной власти в сфере защиты информации;

- о международном сотрудничестве в данной сфере, включая государства – члены Содружества Независимых Государств [39].

1. Указ Президента РБ **«Об утверждении Концепции национальной безопасности Республики Беларусь»** от 9 ноября 2010 г. №575 закрепляет совокупность официальных взглядов на сущность и содержание деятельности Республики Беларусь по обеспечению баланса интересов личности, общества, государства и их защите от внутренних и внешних угроз. Являясь базисом для

консолидации усилий личности, общества и государства в целях реализации национальных интересов, Концепция призвана обеспечить единство подходов к формированию и реализации государственной политики обеспечения национальной безопасности, а также методологическую основу совершенствования актов законодательства в различных сферах национальной безопасности, разработки документов стратегического планирования [40].

В Концепции используются следующие основные понятия:

- *национальная безопасность* – состояние защищенности национальных интересов Республики Беларусь от внутренних и внешних угроз;

- *национальные интересы* – совокупность потребностей государства по реализации сбалансированных интересов личности, общества и государства, позволяющих обеспечивать конституционные права, свободы, высокое качество жизни граждан, независимость, территориальную целостность, суверенитет и устойчивое развитие Республики Беларусь;

- *источник угрозы национальной безопасности* – фактор или совокупность факторов, способных при определенных условиях привести к возникновению угрозы национальной безопасности;

- *угроза национальной безопасности* – потенциальная или реально существующая возможность нанесения ущерба национальным интересам Республики Беларусь;

- *научно-технологическая безопасность* – состояние отечественного научно-технологического и образовательного потенциала, обеспечивающее возможность реализации национальных интересов Республики Беларусь в научно-технологической сфере;

- *социальная безопасность* – состояние защищенности жизни, здоровья и благосостояния граждан, духовно-нравственных ценностей общества от внутренних и внешних угроз;

- *демографическая безопасность* – состояние защищенности общества и государства от демографических явлений и тенденций, социально-экономические последствия которых оказывают негативное воздействие на устойчивое развитие Республики Беларусь;

- *информационная безопасность* – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере;

- *военная безопасность* – состояние защищенности национальных интересов Республики Беларусь от военных угроз.

2. Указ Президента РБ **«О некоторых вопросах развития информационного общества в Республике Беларусь»** от 8 ноября 2011 г. №515 (с изменениями и дополнениями от 11 января 2014 г. № 17) утверждает Положение о Совете по развитию информационного общества при Президенте Республики Беларусь и состав указанного Совета, а также Положение о независимом регуляторе в сфере информационно-коммуникационных технологий и состав Совета независимого регулятора в сфере информационно-коммуникационных технологий. Устанавливает сферы деятельности Оперативно-аналитического цен-

тра при Президенте Республики Беларусь. Постановляет Оперативно-аналитическому центру создание республиканского унитарного предприятия «Национальный центр электронных услуг», осуществляющего функции оператора межведомственных информационных систем, корневого и иных удостоверяющих центров Государственной системы управления открытыми ключами поставщика электронных услуг организациям и гражданам с использованием межведомственных информационных систем [41].

3. Указ Президента РБ **«О некоторых мерах по обеспечению безопасности критически важных объектов информатизации»** от 25 октября 2011 г. №486 (изменения и дополнения от 16 апреля 2013 г. №196) утверждает Положение об отнесении объектов информатизации к критически важным и обеспечении безопасности критически важных объектов информатизации. Положение определяет понятие *критически важный объект информатизации* как объект информатизации, который:

- обеспечивает функционирование экологически опасных и (или) социально значимых производств и (или) технологических процессов, нарушение штатного режима которых может привести к чрезвычайной ситуации техногенного характера;

- осуществляет функции информационной системы, нарушение штатного режима которой может привести к значительным негативным последствиям для национальной безопасности в политической, экономической, социальной, информационной, экологической, иных сферах;

- обеспечивает предоставление значительного объема информационных услуг, частичное или полное прекращение оказания которых может привести к значительным негативным последствиям для национальной безопасности в политической, экономической, социальной, информационной, экологической, иных сферах» [42].

4. Указ Президента РБ **«О мерах по совершенствованию использования национального сегмента сети Интернет»** от 01 февраля 2010 г. №60 описывает меры по обеспечению защиты интересов личности, общества и государства в информационной сфере, создания условий для дальнейшего развития национального сегмента глобальной компьютерной сети Интернет, повышения качества и доступности предоставляемой гражданам и юридическим лицам информации о деятельности государственных органов, иных организаций и интернет-услуг [43].

5. Указ Президента РБ **«Об использовании государственными органами и иными государственными организациями телекоммуникационных технологий»** (27.01.2014 №1/14787) от 23 января 2014 г. №46 подписан в целях дальнейшего развития в Республике Беларусь информационного общества, совершенствования инфраструктуры сети передачи данных, а также повышения уровня обслуживания и качества предоставляемых информационных услуг [44].

Согласно Указу в Беларуси будет создана республиканская платформа, действующая на основе технологий облачных вычислений (далее – республиканская платформа), для размещения программно-технических средств, инфор-

мационных ресурсов и информационных систем государственных органов, иных государственных организаций.

Республиканская платформа представляет собой программно-технический комплекс для распределенной обработки данных, реализующий технологии облачных вычислений и обеспечивающий взаимодействие с внешней средой. Она создается и размещается на базе республиканского центра обработки данных и единой республиканской сети передачи данных.

На республиканской платформе обеспечиваются:

- размещение программно-технических средств, информационных ресурсов и информационных систем;

- доступность государственных информационных систем для пользователей;

- хранение информации и мониторинг работоспособности информационных систем;

- защита информации от неправомерного доступа, уничтожения, модификации (изменения), копирования, распространения и (или) предоставления информации, блокирования правомерного доступа к ней, а также от иных неправомерных действий с момента ее поступления на республиканскую платформу и до момента ее передачи в соответствующую информационную систему или информационный ресурс.

Обеспечение создания данной платформы, ее функционирование осуществляет СООО «Белорусские облачные технологии», которому на правах собственности принадлежит республиканский центр обработки данных.

В соответствии с Указом, государственным органам и организациям до 31 декабря 2018 г. необходимо осуществить поэтапный переход на использование ресурсов республиканской платформы.

В структуре республиканского унитарного предприятия «Национальный центр электронных услуг» создается республиканский удостоверяющий центр Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь для выполнения основных функций корневого удостоверяющего центра, в том числе издания, распространения, предоставления информации о статусе, приостановления и возобновления действия, отзыва, хранения сертификатов открытых ключей регистрационных центров, государственных органов, иных организаций и физических лиц.

Для обеспечения его функционирования до 1 июля 2014 г. была осуществлена безвозмездная передача необходимого оборудования, нематериальных активов, иного имущества республиканского унитарного предприятия «Информационно-издательский центр по налогам и сборам» и республиканского унитарного предприятия электросвязи «Белтелеком» в хозяйственное ведение республиканского унитарного предприятия «Национальный центр электронных услуг».

Указом также внесены изменения и дополнения в Указы Президента Республики Беларусь «О мерах по совершенствованию использования национального сегмента сети Интернет» от 1 февраля 2010 г. №60 и

«О некоторых мерах по развитию сети передачи данных в Республике Беларусь» от 30 сентября 2010 г. №515.

6. Постановление Совета Министров РБ **«Об утверждении технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность»** (ТР 2013/027/BY)» от 15 мая 2013 г. №375 [45].

Технический регламент 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.

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.

7. Постановление Совета Министров РБ «**О некоторых вопросах защиты информации»** от 26 мая 2009 г. №675 разработано в соответствии с Законом Республики Беларусь «Об информации, информатизации и защите информации» и определяет порядок защиты информации в государственных информационных системах, а также информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено; включает положения о мероприятиях по созданию системы защиты информации в информационных системах, порядке аттестации систем защиты информации, порядке проведения государственной экспертизы средств защиты информации [46].

Таким образом, анализируя проблемы систематизации законодательства в сфере обеспечения информационной безопасности, ученые делают вывод, что система законодательства в данной области включает нормы конституционного, административного, гражданского, уголовного, трудового и ряда других отраслей права.

Вся деятельность по правовому обеспечению информационной безопасности основывается на трех фундаментальных положениях права:

- соблюдении законности;
- обеспечении баланса интересов отдельных субъектов и государства;
- неотвратимости наказания.

В развитие положений, закрепленных в Концепции национальной безопасности Республики Беларусь в части правового регулирования обеспечения информационной безопасности, а также в соответствии с поручением Премьер-министра Республики Беларусь от 22.01.2010 г. №35/105-38 в рамках выполнения Государственной программы научных исследований на 2011–2015 гг. «Научное обеспечение повышения эффективности работы государственных органов по укреплению обороноспособности и безопасности Республики Беларусь, уровня национальной безопасности и защищенности населения и терри-

торий от чрезвычайных ситуаций природного и техногенного характера» на основе данных сентября–декабря 2012 г. аналитической группой Института Национальной безопасности Республики Беларусь было проведено комплексное исследование «Информационная безопасность Республики Беларусь». В ходе исследования проведено анкетирование среди сотрудников и экспертов 22 министерств и ведомств Республики Беларусь. Анкетный опрос сотрудников государственных органов (411 человек) и экспертов (12 человек) показал следующие результаты:

1) 77,5 % респондентов на вопрос «По Вашему мнению, требуют ли совершенствования существующие в Республике Беларусь нормативные правовые акты в сфере информационной безопасности?» ответили «Требуют совершенствования»;

2) 59,5 % респондентов на вопрос «По Вашему мнению, существует ли необходимость принятия нормативных правовых актов, регулирующих отношение в сфере обеспечения информационной безопасности Республики Беларусь?» ответили «Существует необходимость принятия» [47].

В Республике Беларусь имеется огромный комплекс нормативных правовых актов, в том числе и международных договоров, регулирующих отношения в сфере информационной безопасности. Многими учеными предлагаются различные меры по совершенствованию данного законодательства, в том числе выдвигаются идеи о выделении информационной безопасности в качестве подотрасли информационного права.

Реализация и совершенствование национальной безопасности РБ осуществляется **под руководством Президента Республики Беларусь** на основе консолидации усилий и ресурсов государства, институтов гражданского общества и граждан по защите и реализации национальных интересов Республики Беларусь. Контроль за ходом реализации осуществляется **Государственным секретариатом Совета Безопасности Республики Беларусь**, в том числе в рамках подготовки ежегодного доклада Государственного секретаря Совета Безопасности Республики Беларусь Президенту Республики Беларусь о состоянии национальной безопасности и мерах по ее укреплению [48].

12 января 1993 г. решением правительства РБ на базе бывшего Минского специального центра Гостехкомиссии СССР был создан **Государственный центр безопасности информации** (ГЦБИ) при Министерстве обороны Республики Беларусь. Задача ГЦБИ заключалась в обеспечении защиты охраняемых сведений инженерно-техническими методами в органах государственного управления, на предприятиях, в учреждениях и организациях в ходе исследований, разработок, производства и эксплуатации вооружения, военной техники, автоматизированных систем управления, электронных вычислительных машин, используемых в интересах обороны и безопасности страны. В октябре 1994 г. Указом Президента Республики Беларусь ГЦБИ при Министерстве обороны Республики Беларусь был преобразован в ГЦБИ при Совете Безопасности Республики Беларусь, а в ноябре 2000 г. – в ГЦБИ при Президенте Республики Беларусь [49].

21 апреля 2008 г. Указом Президента Республики Беларусь на базе ГЦБИ при Президенте Республики Беларусь создан **Оперативно-аналитический центр при Президенте Республики Беларусь** (ОАЦ). ОАЦ является государственным органом, осуществляющим регулирование деятельности по обеспечению защиты информации, содержащей сведения, составляющие государственные секреты Республики Беларусь или иные сведения, охраняемые в соответствии с законодательством, от утечки по техническим каналам, несанкционированных и непреднамеренных воздействий. ОАЦ осуществляет свою деятельность на основе положений Конституции Республики Беларусь и других законодательных актов Республики Беларусь [49].

Техническое нормирование и стандартизация в области информационной безопасности регулируется следующими документами

Технический регламент «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY), утвержденный Советом Министров Республики Беларусь 15.05.2013 г., 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 [50]. 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. До введения в действие технического регламента в отношении средств защиты информации, подлежащих согласно законодательству обязательному подтверждению соответствия, применяются правила, установленные Национальной системой подтверждения соответствия Республики Беларусь.

СТБ 34.101.1-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель» устанавливает основные понятия и принципы оценки безопасности информационных технологий, а также определяет общую модель оценки. Данный стандарт, СТБ 34.101.2 и СТБ 34.101.3 в целом предназначены для использования в качестве основы при оценке характеристик безопасности продуктов информационных технологий. В стандарте установлено основное понятие объекта оценки, контекста оценки, описана целевая аудитория, которой адресованы критерии оценки, представлен краткий обзор СТБ 34.101.2 и СТБ 34.101.3. В стандарте определяются отдельные операции, посредством которых функциональные компоненты и гарантийные компоненты, приведенные в СТБ 34.101.2 и СТБ 34.101.3, могут быть доработаны для конкретного применения путем использования разрешенных операций. В стандарте определяются ключевые понятия профилей защиты, пакетов требований безопасности, а также рассматриваются вопросы, связанные с утверждениями о соответствии; описываются выводы и результаты оценки, даются инструкции по спецификации заданий по безопасности, описываются структуры компонентов в рамках всей

модели. Также дается общая информация о методологии оценки, приведенной в ISO/IEC 18045, и области действия системы оценки [51].

СТБ 34.101.2-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 2. Функциональные требования безопасности» определяет требуемую структуру и содержание функциональных компонентов безопасности с целью оценки безопасности. Стандарт включает в себя каталог функциональных компонентов, который будет соответствовать общим требованиям функциональных возможностей безопасности множества продуктов информационных технологий [51].

СТБ 34.101.3-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Ч. 3. Гарантийные требования безопасности» устанавливает гарантийные требования безопасности. Стандарт включает: уровни гарантии оценки, которые определяют шкалу оценки гарантии простого (однокомпонентного) ОО; составные пакеты гарантии, которые определяют шкалу оценки гарантии для составного ОО; отдельные компоненты гарантии, из которых формируются УГО и пакеты гарантии; критерии оценки профилей защиты и заданий по безопасности [51].

СТБ 34.101.8-2006 «Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования» распространяется на программные средства защиты от воздействия вредоносных программ (ПСЗВВП) и антивирусные программные средства (АПС) отечественного и импортного производства. Стандарт устанавливает классификацию ПСЗВВП и АПС и общие требования к ним при обработке информации, представляющей ценность для собственника, и информации ограниченного распространения, не отнесенной к государственным секретам Республики Беларусь. Может применяться для разработки дополнительных требований при обработке информации, отнесенной к государственным секретам Республики Беларусь. Стандарт не распространяется на программно-аппаратные средства защиты от воздействия вредоносных программ и программно-аппаратные антивирусные средства [51].

СТБ 34.101.9-2004 «Информационные технологии. Требования к защите информации от несанкционированного доступа, устанавливаемые в техническом задании на создание автоматизированной системы» распространяется на автоматизированные системы всех видов и типов, обрабатывающих защищаемую информацию. Стандарт устанавливает порядок изложения требований к защите информации от несанкционированного доступа в техническом задании на создание автоматизированных систем [51].

СТБ 34.101.23-2012 «Информационные технологии и безопасность. Синтаксис криптографических сообщений» устанавливает синтаксис криптографических сообщений, которые используются для обеспечения конфиденциальности, контроля целостности и подлинности данных при их передаче и хранении. Стандарт определяет форматы криптографических сообщений, пра-

вила создания и обработки сообщений. Применяется при разработке, испытаниях и эксплуатации средств криптографической защиты информации [51].

СТБ 34.101.31-2011 «Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности» определяет семейство криптографических алгоритмов шифрования и контроля целостности, которые используются для защиты информации при ее хранении, передаче и обработке. Применяется при разработке средств криптографической защиты информации [51].

СТБ П 34.101.54-2012 «Информационные технологии. Методы и средства безопасности. Профиль защиты критически важных объектов информатизации класса А2-у» распространяется на критически важные объекты информатизации (КВОИ) класса А2-у, размещенные в одной контролируемой зоне, на которой в пределах области действия комплекса безопасности объекта используются критичные активы и обрабатывается общедоступная информация; при этом обеспечивается доступность и целостность критичных активов путем реализации мер, направленных на предотвращение умеренного ущерба. Предстандарт устанавливает необходимый перечень функциональных и гарантийных требований безопасности, предъявляемых к КВОИ класса А2-у. Предназначен для применения: организациями и учреждениями Республики Беларусь при выработке требований безопасности для собственных КВОИ; разработчиками при разработке задания по безопасности и при создании систем защиты информации КВОИ, отвечающих требованиям предстандарта; экспертами (испытателями) при проведении ими оценки соответствия задания по безопасности на КВОИ класса А2-у требованиям предстандарта [51].

СТБ П 34.101.57-2012 «Информационные технологии. Методы и средства безопасности. Профиль защиты критически важных объектов информатизации класса В1-у» распространяется на КВОИ класса В1-у (совокупность КВОИ), размещенный в одной или нескольких объединенных защищенными каналами передачи данных контролируемых зонах, на которых в пределах области действия комплекса безопасности объекта используются критичные активы и обрабатывается информация, распространение и (или) предоставление которой ограничено, и (или) иная информация, охраняемая в соответствии с законодательством Республики Беларусь, за исключением сведений, отнесенных в установленном порядке к государственным секретам. При этом одно или несколько средств вычислительной техники из совокупности имеют защищенные каналы обмена информацией за пределами контролируемой зоны с другими объектами информатизации; обеспечивается доступность, целостность и конфиденциальность критичных активов путем реализации мер, направленных на предотвращение умеренного ущерба. Предстандарт устанавливает необходимый перечень функциональных и гарантийных требований безопасности, предъявляемых к КВОИ класса В1-у. Предназначен для применения: организациями и учреждениями Республики Беларусь при выработке требований безопасности для собственных КВОИ; разработчиками при разработке задания по безопасности и при создании систем защиты информации

КВОИ, отвечающих требованиям предстандарта; экспертами (испытателями) при проведении ими оценки соответствия задания по безопасности на КВОИ класса В1-у требованиям предстандарта [51].

В **СТБ ISO/IEC 27000-2012 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и словарь»** представлены: общий обзор серии стандартов СМИБ; введение в систему менеджмента информационной безопасности (СМИБ); краткое описание процесса «Планируй – Делай – Проверяй – Действуй» (PDCA); термины и определения, используемые в серии стандартов СМИБ. Стандарт применим для всех типов организаций [51].

СТБ ISO/IEC 27001-2011 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» содержит требования к разработке, внедрению, обеспечению функционирования, мониторингу, анализу, поддержке и улучшению документально оформленной СМИБ в контексте общих бизнес-рисков организации. Стандарт устанавливает требования к внедрению средств управления безопасностью с учетом потребностей конкретных организаций и их подразделений [51].

СТБ ISO/IEC 27002-2012 «Информационные технологии. Методы обеспечения безопасности. Кодекс практики для менеджмента информационной безопасности» устанавливает общие правила планирования, реализации, сопровождения и улучшения информационной безопасности в организации. Стандарт может служить в качестве практического руководства по разработке стандартов организаций по информационной безопасности и реализации эффективного менеджмента безопасности, а также для обеспечения конфиденциальности при межорганизационном взаимодействии [51].

СТБ ГОСТ Р 50922-2000 «Защита информации. Основные термины и определения» представляет собой полный аутентичный текст государственного стандарта Российской Федерации ГОСТ Р 50922-96 «Защита информации. Основные термины и определения». Стандарт устанавливает основные термины и определения в области защиты информации [51].

ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» устанавливает единые функциональные требования к защите средств вычислительной техники (СВТ) от несанкционированного доступа (НСД) к информации, к составу документации на эти средства, а также номенклатуру показателей защищенности СВТ, описываемых совокупностью требований к защите и определяющих классификацию СВТ по уровню защищенности от НСД к информации [51].

1.4. Основные понятия политики информационной безопасности организаций и предприятий

Политика безопасности определяет стратегию управления в области информационной безопасности, а также меру внимания и количество ресурсов, которые считает целесообразным выделить руководство.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для ИС организации. Когда проведен анализ рисков и определена стратегия защиты, составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т. п.

Политика безопасности организации должна иметь структуру краткого, легко понимаемого документа высокоуровневой политики, поддерживаемого конкретными документами специализированных политик и процедур безопасности.

Высокоуровневая политика безопасности должна периодически пересматриваться, гарантируя тем самым учет текущих потребностей организации. Документ политики составляют таким образом, чтобы политика была относительно независимой от конкретных технологий, в этом случае документ не потребуется изменять слишком часто. Для того чтобы ознакомиться с основными понятиями политики безопасности, рассмотрим в качестве конкретного примера гипотетическую локальную сеть, принадлежащую некоторой организации, и ассоциированную с ней политику безопасности [52].

Политика безопасности обычно оформляется в виде документа, включающего такие разделы, как описание проблемы, область применения, позиция организации, распределение ролей и обязанностей, санкции и др. [54].

Описание проблемы. Информация, циркулирующая в рамках локальной сети, является критически важной. Локальная сеть позволяет пользователям совместно использовать программы и данные, что увеличивает угрозу безопасности, поэтому каждый из компьютеров, входящих в сеть, нуждается в усиленной защите. Эти повышенные меры безопасности и являются темой данного документа, который нацелен проинформировать сотрудников организации о важности защиты сетевой среды, описать их роль в обеспечении безопасности, а также распределить конкретные обязанности по защите информации, циркулирующей в сети.

Область применения. В сферу действия данной политики попадают все аппаратные, программные и информационные ресурсы, входящие в локальную сеть предприятия. Политика ориентирована также на людей, работающих с сетью, в том числе на пользователей, субподрядчиков и поставщиков.

Позиция организации. Основные цели – обеспечение целостности, доступности и конфиденциальности данных, а также их полноты и актуальности. К частным целям относятся:

- обеспечение уровня безопасности, соответствующего нормативным документам;

- следование экономической целесообразности в выборе защитных мер (расходы на защиту не должны превосходить предполагаемый ущерб от нарушения информационной безопасности);

- обеспечение безопасности в каждой функциональной области локальной сети;

- обеспечение подотчетности всех действий пользователей с информацией и ресурсами;

- обеспечение анализа регистрационной информации;

- предоставление пользователям достаточной информации для сознательного поддержания режима безопасности;

- выработка планов восстановления после аварий и иных критических ситуаций для всех функциональных областей с целью обеспечения непрерывности работы сети;

- обеспечение соответствия с имеющимися законами и общеорганизационной политикой безопасности [53].

Распределение ролей и обязанностей. За реализацию сформулированных выше целей отвечают соответствующие должностные лица и пользователи сети.

Руководители подразделений отвечают за доведение положений политики безопасности до пользователей и за контакты с ними.

Администраторы локальной сети обеспечивают непрерывное функционирование сети и отвечают за реализацию технических мер, необходимых для осуществления политики безопасности, они обязаны:

- обеспечивать защиту оборудования локальной сети, в том числе интерфейсов с другими сетями;

- оперативно и эффективно реагировать на события, содержащие угрозу, информировать администраторов сервисов о попытках нарушения защиты;

- использовать проверенные средства аудита и обнаружения подозрительных ситуаций, ежедневно анализировать регистрационную информацию, относящуюся к сети в целом и к файловым серверам в особенности;

- не злоупотреблять своими полномочиями, т. к. пользователи имеют право на тайну;

- разрабатывать процедуры и подготавливать инструкции для защиты локальной сети от вредоносного программного обеспечения, оказывать помощь в обнаружении и ликвидации вредоносного кода;

- регулярно выполнять резервное копирование информации, хранящейся на файловых серверах;

- выполнять все изменения сетевой аппаратно-программной конфигурации;

- гарантировать обязательность процедуры идентификации и аутентификации для доступа к сетевым ресурсам, выделять пользователям входные имена и начальные пароли только после заполнения регистрационных форм;

- периодически производить проверку надежности защиты локальной сети, не допускать получения привилегий неавторизованными пользователями.

Администраторы сервисов отвечают за конкретные сервисы и, в частности, за построение защиты в соответствии с общей политикой безопасности, они обязаны:

- управлять правами доступа пользователей к обслуживаемым объектам;
- оперативно и эффективно реагировать на события, содержащие угрозу, оказывать помощь в отражении угрозы, выявлении нарушителей и предоставлении информации для их наказания;
- регулярно выполнять резервное копирование информации, обрабатываемой сервисом;
- выделять пользователям входные имена и начальные пароли только после заполнения регистрационных форм;
- ежедневно анализировать регистрационную информацию, относящуюся к сервису;
- регулярно контролировать сервис на предмет вредоносного программного обеспечения;
- периодически производить проверку надежности защиты сервиса;
- не допускать получения привилегий неавторизованными пользователями [53].

Пользователи работают с локальной сетью в соответствии с политикой безопасности, подчиняются распоряжениям лиц, отвечающих за отдельные аспекты безопасности, ставят в известность руководство обо всех подозрительных ситуациях. Они обязаны:

- знать и соблюдать законы, правила, принятые в данной организации, политику безопасности, процедуры безопасности, использовать доступные защитные механизмы для обеспечения конфиденциальности и целостности своей информации;
- использовать механизм защиты файлов и должным образом задавать права доступа;
- выбирать качественные пароли, регулярно менять их, не записывать пароли на бумаге, не сообщать их другим лицам;
- информировать администраторов или руководство о нарушениях безопасности и иных подозрительных ситуациях;
- не использовать слабости в защите сервисов и локальной сети в целом, не совершать неавторизованной работы с данными, не создавать помех другим пользователям;
- всегда сообщать корректную идентификационную и аутентификационную информацию, не пытаться работать от имени других пользователей;
- обеспечивать резервное копирование информации с жесткого диска своего компьютера;
- знать принципы работы вредоносного программного обеспечения, пути его проникновения и распространения, знать и соблюдать процедуры для

предупреждения проникновения вредоносного кода, его обнаружения и уничтожения;

- знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий [53].

Санкции. Нарушение политики безопасности может подвергнуть локальную сеть и циркулирующую в ней информацию недопустимому риску. Случаи нарушения безопасности со стороны персонала должны оперативно рассматриваться руководством для принятия дисциплинарных мер вплоть до увольнения.

Дополнительная информация. Конкретным группам исполнителей могут потребоваться для ознакомления дополнительные документы, в частности, документы специализированных политик и процедур безопасности, а также другие руководящие указания. Необходимость в дополнительных документах политик безопасности в значительной степени зависит от размеров и сложности организации. Для большой организации могут потребоваться в дополнение к базовой политике специализированные политики безопасности. Организации меньшего размера нуждаются только в некотором подмножестве специализированных политик. Многие из этих документов поддержки могут быть краткими, объемом в одну-две страницы.

Управленческие меры обеспечения информационной безопасности. Главной целью мер, предпринимаемых на управленческом уровне, является формирование программы работ в области информационной безопасности и обеспечение ее выполнения путем выделения необходимых ресурсов и осуществления регулярного контроля состояния дел. Основой этой программы является многоуровневая политика безопасности, отражающая комплексный подход организации к защите своих ресурсов и информационных активов [53].

С практической точки зрения политику безопасности можно разделить на три уровня: *верхний*, *средний* и *нижний* [54].

Верхний уровень политики безопасности определяет решения, затрагивающие организацию в целом, они носят общий характер и исходят, как правило, от руководства организации.

Такие решения могут включать в себя следующие элементы:

- формулировку целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;

- формирование или пересмотр комплексной программы обеспечения информационной безопасности, определение ответственных лиц за продвижение программы;

- обеспечение материальной базы для соблюдения законов и правил;

- формулировку управленческих решений по вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

Политика безопасности верхнего уровня формулирует цели организации в области информационной безопасности в терминах целостности, доступности

и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане должна стоять целостность данных. Например, для организации, занимающейся продажами, важна актуальность информации о предоставляемых услугах и ценах, а также ее доступность максимальному числу потенциальных покупателей, а режимная организация в первую очередь будет заботиться о конфиденциальности информации, т. е. о ее защите от НСД.

На верхний уровень выносится управление ресурсами безопасности и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем, поддержание контактов с другими организациями, обеспечивающими или контролирующими режим безопасности. Политика верхнего уровня должна четко определять сферу своего влияния. В нее могут быть включены не только все компьютерные системы организации, но и домашние компьютеры сотрудников, если политика регламентирует некоторые аспекты их использования. Возможна и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы.

В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и по ее реализации, т. е. политика может служить основой подотчетности персонала. Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины. Во-первых, организация должна соблюдать существующие законы. Во-вторых, следует контролировать действия лиц, ответственных за выработку программы безопасности. В-третьих, необходимо обеспечить исполнительскую дисциплину персонала с помощью системы поощрений и наказаний.

Средний уровень политики безопасности определяет решение вопросов, касающихся отдельных аспектов информационной безопасности, но важных для различных систем, эксплуатируемых организацией. Примеры таких вопросов – доступ к сети Интернет (проблема сочетания свободы получения информации с защитой от внешних угроз), использование домашних компьютеров и т. д.

Политика безопасности среднего уровня должна определять для каждого аспекта информационной безопасности следующие моменты:

- описание аспекта (позиция организации может быть сформулирована в достаточно общем виде, а именно как набор целей, которые преследует организация в данном аспекте);
- область применения (следует специфицировать, при каких обстоятельствах и по отношению к кому и чему применяется данная политика безопасности);
- роли и обязанности (документ должен содержать информацию о должностных лицах, отвечающих за реализацию политики безопасности);
- санкции (политика должна содержать общее описание запрещенных действий и наказаний за них);
- точки контакта (должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией; обычно «точкой контакта» служит должностное лицо).

Нижний уровень политики безопасности относится к конкретным сервисам. Он включает два аспекта – цели и правила их достижения, поэтому ее порой трудно отделить от вопросов реализации. В отличие от двух верхних уровней, рассматриваемая политика должна быть более детальной, т. е. при следовании политике безопасности нижнего уровня необходимо дать ответ, например, на такие вопросы:

- кто имеет право доступа к объектам, поддерживаемым сервисом;
- при каких условиях можно читать и модифицировать данные;
- как организован удаленный доступ к сервису.

Политика безопасности нижнего уровня может исходить из соображений целостности, доступности и конфиденциальности, но она не должна на них останавливаться. Из целей выводятся правила безопасности, описывающие, кто и при каких условиях имеет право на определенные действия. Чем более детально, четко и формально изложены правила, тем проще поддерживать их выполнение программно-техническими мерами. Обычно наиболее соответствуют этим требованиям права доступа к объектам [54].

2. АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Угрозы информационной безопасности

Угроза информационной безопасности – это потенциально возможные события, действия, явления, которые создают опасность нарушения информационной безопасности, что может привести к нанесению материального, морального и иного ущерба защищаемому объекту системы.

2.1.1. Классификация угроз информационной безопасности

Исследователи В. Ю. Гайкович и Д. В. Ершов все множество потенциальных угроз **по природе их возникновения** разделяют на два класса [55]:

- *естественные* угрозы, вызванные воздействиями на КИС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека;
- *искусственные* угрозы, вызванные деятельностью человека.

В свою очередь, среди искусственных угроз **исходя из мотивации действий** выделяют:

- *непреднамеренные (случайные)* угрозы, вызванные ошибками в проектировании системы и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала;
- *преднамеренные (умышленные)* угрозы, связанные с корыстными устремлениями людей.

По целям, преследуемым злоумышленником, угрозы информационной безопасности делят на [56] :

- угрозы конфиденциальности данных и программ;
- угрозы целостности данных, программ, аппаратуры;
- угрозы доступности данных;
- угрозы отказа от выполнения транзакций (действий).

Относительно объекта защиты угрозы делят на [57]:

- внешние;
- внутренние.

По размерам наносимого ущерба различают угрозы:

- *общие* – нанесение ущерба объекту безопасности в целом, причинение значительного ущерба;
- *локальные* – причинение вреда отдельным частям объекта безопасности;
- *частные* – причинение вреда отдельным свойствам элементов объекта безопасности [58].

По степени воздействия на информационную систему угрозы делят на:

- *пассивные* – структура и содержание системы не изменяются;
- *активные* – структура и содержание системы подвергается изменениям.

Рассмотрим классификацию угроз, на основе **объектов сетей инфокоммуникаций**, на которые они направлены [59]:

1) угрозы **компьютерам или серверам**:

- заражение вредоносными программами (вирусы);
- несанкционированное внедрение в систему;

2) угрозы **пользователям**:

- подмена персоналий;
- нарушение приватности;

3) угрозы **электронным документам**:

- нарушение целостности документа;
- искажение аутентичности отправителя документа – незаконное присвоение идентификатора, повторная передача сообщения, искажение реквизитов документа;
- непризнание участия – отказ от факта формирования документа, от получения информации или заявление ложных сведений о времени ее получения, утверждение, что получателю в определенное время была выслана информация, которая по факту не высылалась или высылалась в другое время.

Примечание. **Инфокоммуникационная сеть** – это технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

По отношению к сети Интернет различают следующие угрозы [60]:

- *вредоносное программное обеспечение* – вирусные и «троянские» программы, сетевые пакеты, используемые в хакерских атаках;
- *спам* – массовая неперсонифицированная рассылка с использованием специальных программ коммерческой, политической и иной рекламы или иного вида сообщений людям, не выразившим желания их получать;
- *глобальные сетевые атаки* – результат запланированных действий хакеров или неконтролируемого распространения сетевых «вирусов-червей».

2.1.2. Основные угрозы национальной безопасности

Угрозы национальной безопасности Республики Беларусь носят комплексный и взаимосвязанный характер. Отдельные источники способны порождать спектр угроз, проявляющихся в различных сферах жизнедеятельности. Некоторые угрозы могут воздействовать на состояние национальной безопасности одновременно по нескольким направлениям. Формами угроз в стадии их зарождения и насыщения являются риски и вызовы национальной безопасности [61].

Основными потенциальными либо реально существующими **угрозами национальной безопасности** являются [61]:

- посягательства на независимость, территориальную целостность, суверенитет и конституционный строй Республики Беларусь;
- навязывание Республике Беларусь политического курса, не отвечающего ее национальным интересам, вмешательство извне во внутриполитические процессы;
- недостаточная конкурентоспособность экономики Республики Беларусь;
- снижение уровня благосостояния и качества жизни населения;

- дестабилизация национальной финансовой и денежно-кредитной систем, потеря стабильности национальной денежной единицы;

- неспособность возвращать и обслуживать внешний и внутренний долг;

- невозможность гарантированного обеспечения сырьевыми и энергетическими ресурсами в объемах, обеспечивающих намеченный рост ВВП;

- потеря внешних рынков, в том числе в результате дискриминации белорусских производителей;

- отставание в темпах перехода экономики к передовым технологическим укладам от других государств, деградация технологической структуры реального сектора экономики;

- депопуляция – общее старение нации, снижение темпов рождаемости, ухудшение других основных показателей демографии и здоровья нации;

- рост преступных и иных противоправных посягательств на личность и собственность, коррупционные проявления;

- подготовка или осуществление террористических актов на территории либо в воздушном пространстве Республики Беларусь, использование ее территории либо воздушного пространства террористическими организациями и группами против иных государств;

- проявления социально-политического, религиозного, этнического экстремизма и расовой вражды на территории Республики Беларусь;

- возникновение в Республике Беларусь беспорядков, сопровождающихся насилием либо угрозой насилия со стороны группы лиц и организаций, в результате которых возникает опасность для жизни и здоровья людей, независимости, территориальной целостности, суверенитета и существования государства;

- дезорганизация системы государственного управления, создание препятствий функционированию государственных институтов;

- активизация эмиграционных процессов, рост нерегулируемой иммиграции в страну;

- нарушение устойчивости системы социальной защиты;

- рост безработицы, в том числе нерегистрируемой и скрытой;

- деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам;

- нарушение функционирования критически важных объектов информатизации;

- возникновение на территории Республики Беларусь либо вблизи ее границ крупномасштабных чрезвычайных ситуаций природного и техногенного характера, эпидемий и эпизоотии;

- недостаточные объемы и низкое качество иностранных инвестиций;

- снижение научно-технологического и образовательного потенциала до уровня, не способного обеспечить инновационное развитие;

- незаконное распространение в Беларуси или перемещение через ее территорию оружия массового уничтожения, его компонентов и средств доставки,

технологий и оборудования двойного назначения, боеприпасов, радиоактивных, химических, биологических и других опасных веществ и материалов;

- утрата значительной частью граждан традиционных нравственных ценностей и ориентиров, попытки разрушения национальных духовно-нравственных традиций и необъективного пересмотра истории, затрагивающие данные ценности и традиции;

- резкое либо масштабное снижение доверия граждан к основным государственным институтам;

- целенаправленные посягательства на жизнь, здоровье и свободу белорусских граждан, пребывающих за рубежом;

- недостаточные масштабы и уровень внедрения передовых информационно-коммуникационных технологий;

- снижение или потеря конкурентоспособности отечественных информационно-коммуникационных технологий, информационных ресурсов и национального контента;

- деградация земель, лесов и природных комплексов, истощение минерально-сырьевых, водных и биологических ресурсов;

- радиоактивное, химическое и биологическое загрязнение почв, недр, вод, растительности и атмосферы;

- утрата либо разглашение сведений, составляющих охраняемую законодательством тайну и способных причинить ущерб национальной безопасности.

В информационной сфере **внутренними** источниками угроз национальной безопасности являются [61]:

- распространение недостоверной или умышленно искаженной информации, способной причинить ущерб национальным интересам Республики Беларусь;

- зависимость Республики Беларусь от импорта информационных технологий, средств информатизации и защиты информации, неконтролируемое их использование в системах, отказ или разрушение которых может причинить ущерб национальной безопасности;

- несоответствие качества национального контента мировому уровню;

- недостаточное развитие государственной системы регулирования процесса внедрения и использования информационных технологий;

- рост преступности с использованием информационно-коммуникационных технологий;

- недостаточная эффективность информационного обеспечения государственной политики;

- несовершенство системы обеспечения безопасности критически важных объектов информатизации.

Внешними источниками угроз национальной безопасности в информационной сфере являются [61]:

- открытость и уязвимость информационного пространства Республики Беларусь для внешнего воздействия;

- доминирование ведущих зарубежных государств в мировом информационном пространстве, монополизация ключевых сегментов информационных рынков зарубежными информационными структурами;

- информационная деятельность зарубежных государств, международных и иных организаций, отдельных лиц, наносящая ущерб национальным интересам Республики Беларусь, целенаправленное формирование информационных поводов для ее дискредитации;

- нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве;

- развитие технологий манипулирования информацией;

- препятствование распространению национального контента Республики Беларусь за рубежом;

- широкое распространение в мировом информационном пространстве образцов массовой культуры, противоречащих общечеловеческим и национальным духовно-нравственным ценностям;

- попытки несанкционированного доступа извне к информационным ресурсам Республики Беларусь, приводящие к причинению ущерба ее национальным интересам.

2.1.3. Источники угроз информационной безопасности

Все источники угроз информационной безопасности можно разделить на три основные группы [62]:

1. Источники, обусловленные **действиями субъекта (антропогенные источники)**; данные действия, которые могут привести к нарушению безопасности информации; данные действия могут быть квалифицированы как случайные (непреднамеренные) или умышленные (преднамеренные) преступления.

К **непреднамеренным** источникам угрозам относятся:

- неумышленные действия, приводящие к частичному или полному отказу или разрушению технических, программных, информационных ресурсов объекта информатизации (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 компонентов (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 не-

обоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

- заражение ПЭВМ компьютерными вирусами;
- неосторожные действия, приводящие к разглашению защищаемой информации или открытия доступа к ней;
- 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 возможностями, представляющими опасность для работоспособности ОИ и средств защиты информации (СЗИ) от несанкционированного доступа (НСД);
- игнорирование организационных ограничений (установленных правил) при работе на ОИ;
- вход в 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.

К **преднамеренным** источникам угроз относятся:

- физическое разрушение ОИ (путем взрыва, поджога и т. п.) или вывод из строя отдельных наиболее важных компонентов (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 через недостатки многозадачных операционных систем и систем программирования;

- незаконное получение паролей и других реквизитов разграничения доступа (используя халатность 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, позволяющего 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» посредством использования 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 адресности и своевременности информационного обмена в ЛВС.

Источники, действия которых могут привести к нарушению безопасности информации, могут быть как *внешними*, так и *внутренними*. Данные источники можно спрогнозировать и принять адекватные меры по их устранению.

2. **Источники, обусловленные техническими средствами (техногенные источники)** – эти источники угроз затруднительно прогнозировать, они напрямую зависят от свойств техники и поэтому требуют особого внимания. Данные источники угроз информационной безопасности, также как и антропогенные, могут быть *внутренними* или *внешними* [62].

3. **Стихийные источники** – данная группа объединяет обстоятельства, которые составляют непреодолимую силу (стихийные бедствия и другие обстоятельства, которые невозможно предусмотреть, предотвратить или возможно предусмотреть, но невозможно предотвратить) и носят объективный и абсолютный характер. Поскольку такие источники угроз редко поддаются прогнозированию, меры против них должны применяться постоянно. Стихийные источники, как правило, являются внешними по отношению к защищаемому объекту, под ними чаще всего понимаются природные катаклизмы.

Классификация источников угроз представлена на рис. 3 [67].

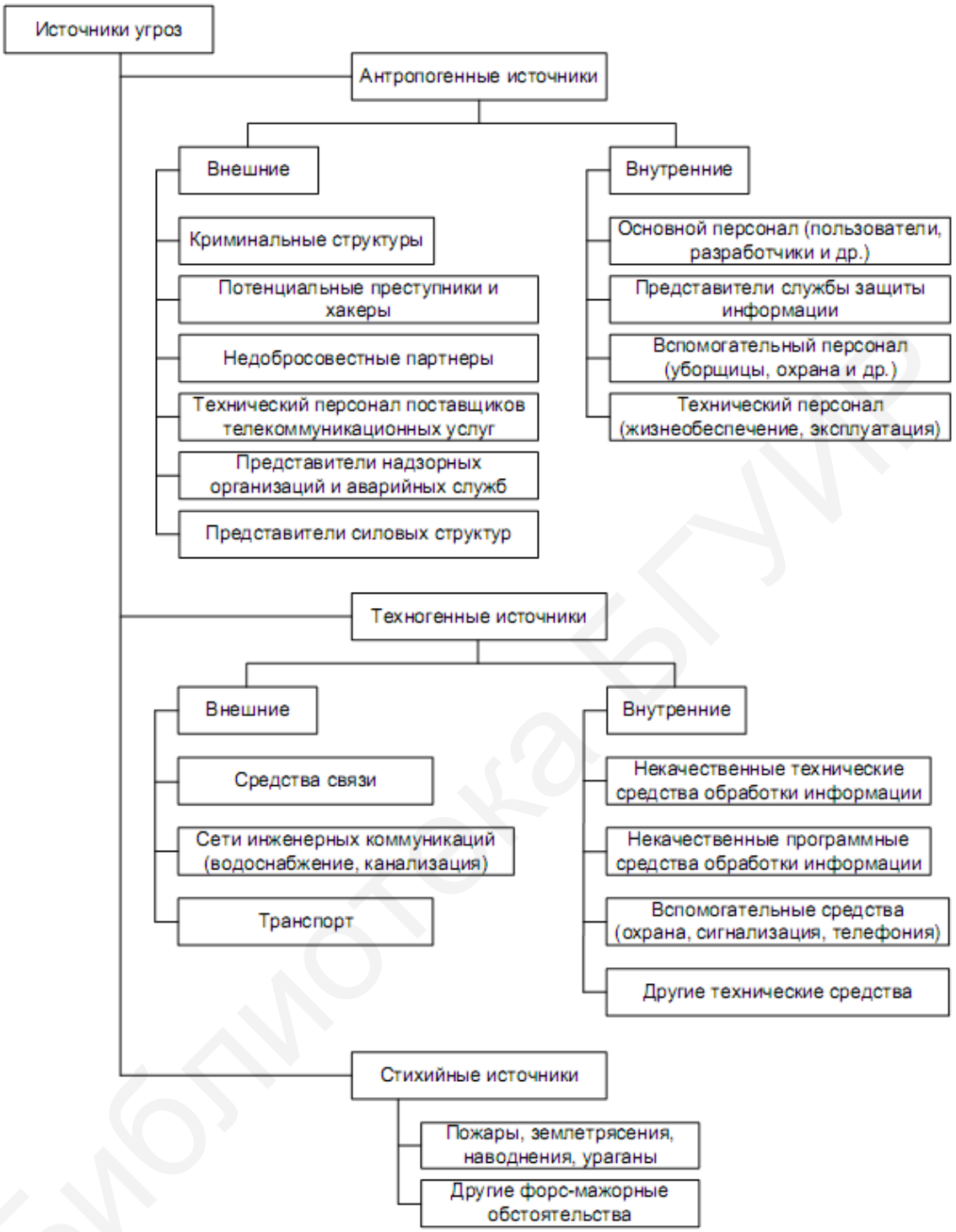

Рис. 3. Классификация источников угроз

2.2. Уязвимости информационных систем

Угрозы, как правило, возникают через уязвимости, приводящие к нарушению безопасности в информационных системах.

Уязвимость – это присущие объекту информационной системы причины, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные недостатками процесса функционирования объекта информа-

ционной системы, свойствами архитектуры информационной системы, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации и расположения, невнимательностью сотрудников.

Уязвимость может быть результатом ошибок в организации системы информационной безопасности, в программировании, недостатков, допущенных при проектировании информационной системы, ненадежных паролей, вирусов и др. Некоторые уязвимости известны только теоретически, другие же активно используются и имеют известные эксплойты.

Источники угроз могут использовать уязвимости для нарушения безопасности информации, получения незаконной выгоды (нанесения ущерба собственнику, владельцу, пользователю информации). Устранение или существенное ослабление уязвимостей влияет на возможности реализации угроз безопасности информации.

На данный момент существует проблема, связанная с отсутствием единого подхода к идентификации и классификации уязвимостей для информационных систем, который бы учитывал все составляющие комплексного обеспечения информационной безопасности. Степень актуальности программных уязвимостей в современных условиях постоянно изменяется ввиду появления новых уязвимостей или модификации старых.

В данном пособии предлагается следующая классификация уязвимостей для информационных систем.

1. Объективные уязвимости.

Зависят от особенностей построения и технических характеристик оборудования, применяемого в информационных системах. Полное устранение этих уязвимостей представляется весьма сложным процессом, однако они могут существенно ослабляться техническими и инженерно-техническими методами. К таким типам уязвимостей можно отнести [63]:

а) сопутствующие техническим средствам **излучения**:

- *электромагнитные* (побочные излучения элементов технических средств, кабельных линий технических средств, излучения на частотах работы генераторов, на частотах самовозбуждения усилителей);

- *электрические* (наводки электромагнитных излучений на линии и проводке, просачивание сигналов в сети электропитания, в цепи заземления, неравномерность потребления тока электропитания);

- *звуковые* (акустические, виброакустические);

б) **активизируемые**:

- *аппаратные закладки*, устанавливаемые в телефонные линии, сети электропитания, а также в помещениях и технических средствах;

- *программные закладки* (вредоносные программы, технологические выходы из программ, нелегальные копии программного обеспечения);

в) уязвимости, **определяемые особенностями элементов**:

- элементы, обладающие *эффектом электроакустического преобразования* (телефонные аппараты, громкоговорители, микрофоны);

- элементы, *подверженные воздействию электромагнитного поля* (магнитные носители, микросхемы);

г) уязвимости, **определяемые особенностями защищаемого объекта**:

- *местоположением объекта* (отсутствие контролируемой зоны, наличие прямой видимости объектов, удаленных и мобильных элементов объекта);

- *организацией каналов обмена информацией* (использование радиоканалов, глобальных информационных сетей, арендуемых каналов).

2. Субъективные уязвимости.

Зависят от действий сотрудников, в основном устраняются организационными и программно-аппаратными методами. Среди таких уязвимостей выделяют:

а) **ошибки**:

- *при подготовке и использовании программного* обеспечения (при разработке алгоритмов и программного обеспечения, инсталляции и загрузке программного обеспечения, эксплуатации программного обеспечения, вводе данных);

- *при управлении сложными системами* (при использовании возможностей самообучения систем, организация управления потоками обмена информации);

- *при эксплуатации технических средств* (при включении/выключении технических средств, использовании технических средств охраны, использовании средств обмена информацией);

б) **нарушения**:

- *режима охраны и защиты* (доступа на объект, доступа к техническим средствам);

- *режима эксплуатации технических средст*в (энергообеспечения, жизнеобеспечения);

- *режима использования информации* (обработки и обмена информацией, хранения и уничтожения носителей информации, уничтожения производственных отходов и брака);

- *режима конфиденциальности* (действия сотрудников в нерабочее время, уволенных и имеющих личные мотивы сотрудников).

3. Случайные уязвимости.

Зависят от особенностей окружающей информационную систему среды и непредвиденных обстоятельств, их составляют:

а) **сбои** и **отказы**:

- *отказы и неисправности технических средств*, обрабатывающих информацию, обеспечивающих работоспособность средств обработки информации, обеспечивающих охрану и контроль доступа;

- *старение и размагничивание носителей информации* (дискет и съемных носителей, жестких дисков, микросхем, кабелей и соединительных линий);

- *сбои программного обеспечения* (операционных систем и СУБД, прикладных программ, сервисных программ, антивирусных программ);

- *сбои электроснабжения* оборудования, обрабатывающего информацию, а также обеспечивающего и вспомогательного оборудования).

б) **повреждения**:

- *жизнеобеспечивающих коммуникаций* (электро-, водо-, газо-, теплоснабжения, канализации, кондиционирования и вентиляции);

- *ограждающих конструкций* (внешних ограждений территорий, стен и перекрытий зданий, корпусов технологического оборудования).

Рассмотрим основные *признаки наличия уязвимых мест* в безопасности информационной системы.

- Не разработаны или не соблюдаются положения о защите информации. Не назначен ответственный за информационную безопасность.

- Пароли пишутся на компьютерных терминалах, помещаются в общедоступные места, появляются на компьютерном экране при их вводе, ими делятся с другими людьми.

- Удаленные терминалы и микрокомпьютеры оставляются без присмотра в рабочие и нерабочие часы. Данные отображаются на компьютерных экранах, оставленных без присмотра.

- Не существует ограничений на доступ к информации или на характер ее использования. Все пользователи имеют доступ к любой информации и могут использовать все функции системы.

- Не ведутся системные журналы и не хранится информация о том, кто и какой целью использует компьютер. Документация отсутствует или не позволяет совершать следующие действия: понимать получаемые отчеты и формулы, по которым выводятся результаты, модифицировать программы, готовить данные для ввода, исправлять ошибки, производить оценку мер защиты, понимать сами данные (их источники, формат хранения, взаимосвязи между ними). Не производится анализ информации, обрабатываемой в компьютере, с целью определения необходимого для нее уровня безопасности.

- Изменения в программы могут вноситься без предварительного утверждения руководством.

- Совершаются многочисленные попытки войти в систему с неправильными паролями. Вводимые данные не проверяются на корректность и точность или при проверке отвергаются из-за ошибок в них; требуется сделать много исправлений в данных; не вносятся записи в журналы об отвергнутых транзакциях.

- Имеют место выходы из строя системы, приносящие большие убытки.

- Мало внимания уделяется информационной безопасности, несмотря на существование политики безопасности [64].

Рассмотрим более подробно **программные уязвимости**.

Термин «уязвимость» часто упоминается именно в связи с компьютерной безопасностью. В общем случае уязвимость ассоциируется с нарушением политики безопасности, вызванным неправильно заданным набором правил или ошибкой в программе, обеспечивающей безопасность компьютера. Стоит отметить, что теоретически все компьютерные системы имеют уязвимости. В зави-

симости от степени потенциального ущерба от вирусной атаки уязвимости подразделяются на активно используемые и неиспользуемые [65].

MITRE (исследовательская группа, финансируемая федеральным правительством США, занимающаяся анализом и разрешением критических проблем с безопасностью) разработала следующее определение термина «уязвимость».

Уязвимость – это состояние вычислительной системы (или нескольких систем), которое позволяет:

- исполнять команды от имени другого пользователя;
- получать доступ к информации, закрытой от доступа для данного пользователя;
- показывать себя как иного пользователя или ресурс;
- производить атаку типа «отказ в обслуживании».

Большинство современных классификаций угроз и уязвимостей допускают их разделение по этапу жизненного цикла ПО: проектирование (архитектура), кодирование (реализация), эксплуатация (администрирование). При определении контроля безопасности ПО используют два подхода: анализ кода и сканирование ресурсов. Для реализации уязвимости необходимо наличие субъекта, воздействующего на информационную систему и способного эксплуатировать уязвимость.

В настоящее время можно встретить ряд как простых, так и сложных иерархических классификаций (таксономий) в области программной безопасности [66]:

- классификации угроз и атак;
- классификации вредоносных программ;
- классификации и реестры уязвимостей;
- классификации дефектов.

Примечание. **Таксономия** – абстрактная структура категорированных экземпляров, включает комплексное исследование предметной области и создание теоретической модели полного множества изучаемых объектов, что позволяет определить признаки, которые могут быть положены в основу той или иной классификации. Таксономия позволяет построить полное множество категорий исследуемых объектов для любой выбранной классификации.

Классификации угроз и атак. Данные классификации являются самыми методически проработанными и систематизируют различные виды искусственных и естественных, случайных и злонамеренных, внутренних и внешних угроз по многим параметрам [67, 68, 69].

Как правило, классификации выделяют класс угроз, связанный с возможностью реализации нарушителем программных уязвимостей, однако классы уязвимостей описываются только в общем плане. При этом данные классификации являются основой для построения моделей угроз безопасности информации.

Классификации вредоносных программ. Разработчики средств антивирусной защиты придерживаются классификаций «вредоносного» программного обеспечения по модели распространения, по способу активации, по действию и другим параметрам, что позволяет разрабатывать эффективные тесты и базы сигнатур антивирусов. Данные классификации полезны при описании подклас-

са уязвимостей эксплуатационного типа, напрямую не касаясь уязвимостей этапа проектирования и кодирования.

Классификации и реестры уязвимостей. Исторически реестры уязвимостей были обусловлены потребностью в регулярном распространении бюллетеней и сводок о найденных уязвимостях для каждого типа и версии программных продуктов и сред. Такие реестры поддерживаются как крупными разработчиками ПО (например, Adobe, Microsoft, RedHat), так и различными ассоциациями (US-CERT, Secunia, Open Security Foundation). Последние создали ряд реестров, группирующих в единой системе идентификаторов (например, CVE-ID) уязвимости ПО различных разработчиков.

Классификации дефектов. Данный вид таксономий касается систематизации дефектов безопасности ПО при исследовании исходного кода ПО. В отличие от известных описанных уязвимостей (внесенных в реестры) дефекты представляют собой внутреннее свойство каждой реализации ПО или системы. Большая часть дефектов возникает в процессе создания ПО. Это могут быть ошибки проектирования, ошибки кодирования программистов, ошибки, допущенные при сборке дистрибутива и интеграции различных версий компонентов ПО. Некоторые таксономии включают понятие дефектов информационной системы, которые связаны с конфигурацией системы и вызваны либо ошибками администраторов (например, неверными настройками схемы аутентификации, несвоевременной установкой обновлений операционной системы или сетевых сервисов), либо ошибками операторов информационных систем (например, слабыми паролями в учетной записи, некорректным выключением компьютера).

В табл. 3 представлены популярные классификации в области безопасности программ.

Как видно, в настоящее время известно достаточно большое количество таксономий в области ИБ, но в основном они ориентированы на конкретные задачи, будь то сетевые атаки, уязвимости операционных систем или некорректности программирования.

Таблица 3

Классификация в области безопасности программ

Вид	**Примеры**	**Особенности**
1	2	3
Классификация вредоносного программного обеспечения	Mitre MAEC (Malware Attrribute Enumeratoin and Characterization) – перечень и характеристики признаков вредоносного ПО	Язык описания вредоносного ПО, учитывающий признаки поведения, тип атаки и т. п.
	Kaspersky Classification – классификация Лаборатории Касперского	Классификация вредоносного ПО по способам воздействия
	Symantec Classification – классификация фирмы Symantec	Классификация обнаруженного вредоносного ПО

Продолжение таблицы 3

Реестры и классификации уязвимостей программных систем	Mitre CVE (Common Vulnerabilities and Exposures) – общие уязвимости и «незащищенности»	База данных известных уязвимостей
	NVD (National Vulnerability Database) – национальная база уязвимостей США	База данных, использующая идентификаторы CVE
	OSVDB (Open Security Vulnerability Database) – база уязвимостей открытого доступа	База данных известных уязвимостей
	US-CERT Vulnerability Notes Database – база уязвимостей	Описание уязвимостей и способов их обнаружения
	Бюллетени разработчиков: - Microsoft Bulletin ID; - Secunia ID; - VUPEN ID	Сводки найденных уязвимостей
	Таксономия Бишопа и Бейли	Устаревшая классификация уязвимостей Unix-систем
Классификация угроз безопасности и компьютерных атак на ресурсы системы	OWASP Top Ten – 10 самых распространенных угроз для веб-приложений	Десять наиболее актуальных классов угроз, связанных с уязвимостями web-приложений за последний год
	MITRE CAPEC (Common Attack Pattern Enumeration and Classification) – перечень и классификация распространенных типов атак	Всесторонняя классификация типов атак
	Microsoft STRIDE Threat Model – модель угроз Microsoft	Описание пяти основных категорий уязвимостей
	WASC Threat Classification 2.0 – классификация угроз Консорциума безопасности web-приложений	Классификация изъянов, угроз web-безопасности, нацеленная на практическое применение
Классификации дефектов, внесенных в процессе разработки	MITRE CWE (Common Weaknesses Enumeration) – общая классификация дефектов ПО	Система классификации «изъянов» ПО
	Fortify Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors	Классификация ошибок безопасности программного обеспечения
	CWE/SANS Top 25 Mast Dangerous Software Errors – 25 наиболее опасных ошибок в разработке ПО	25 наиболее распространенных и опасных ошибок, которые могут стать причиной уязвимости
	OWASP CLASP (OWASP Comprehensive, Lightweight, Application Security Process) – описание процесса безопасной разработки приложений	Принципы безопасности организации процесса разработки приложений

Окончание таблицы 3

	DoD Software Fault Patterns – образцы программных ошибок Минобороны США	Система типов дефектов ПО, ассоциированная с CWE и разработанная с целью автоматизации их выявления
	Устаревшие классификации: - перечни RISOS/PA; - таксономия Ландвера; - таксономия Аслама; - таксономия Макгоу; - таксономия Вебера; - перечень PLOVER	Первые проекты по частичной каталогизации известных дефектов безопасности и их классификации
	MITRE Common Configuration Enumeration (CCE) – общий реестр конфигураций	Идентификация проблемных конфигураций системы, устанавливающая соответствие между различными источниками
Классификации дефектов, внесенных в процессе внедрения и эксплуатации	DPE (Security-Database Default Password Enumeration) – реестр паролей по умолчанию	Основное назначение – повышение эффективности аудита безопасности паролей сетевых устройств

Среди рассмотренных таксономий лучшим, с точки зрения разработчика, является реестр CWE (по показателям полноты, всесторонности классификации, наличия подробных описаний с примерами кода), а с точки зрения администратора, самой эффективной представляется таксономия CVE (по показателям объема записей, оперативности обновления). С другой стороны, классификация CWE в общем случае неоднозначна и достаточно сложна, к тому же не отражает в полной мере вопросы безопасности конфигураций. Что касается практического статического анализа программного обеспечения, по оценкам большинства экспертов, более удобна простая таксономия Fortify Seven Pernicious Kingdoms. Следует отметить, что в академической литературе можно встретить иерархические (включающие группы, виды, типы и т. д.) классификации уязвимостей, заимствованные из области технических систем, в частности, ориентированные на всевозможные классы и виды ПО информационно-вычислительных систем (ОС, ППП, ПЗУ, SCADA-системы и т. д.) и далее типы ошибок соответствующих классов и подклассов ПО.

Рассмотрим систематику дефектов и уязвимостей.

Учитывая опыт существующих классификаций и таксономий, можно сформулировать требования к перспективным таксономиям дефектов и уязвимостей в области безопасности ПО:

- в классификации или свойствах отдельного таксона должна содержаться информация об этапе жизненного цикла, на котором возникает дефект ПО и его области (общая архитектура, код, внутренняя конфигурация, внешнее окружение);

- в классификации уязвимостей или свойствах их отдельных таксонов необходимо указать ссылку на виды угроз или механизмы атак, при которых

возможна эксплуатация этой уязвимости (например, атаки внедрения данных, атаки подмены идентификатора, атаки физического доступа и т. п.);

- если первопричиной появления уязвимости является связь с конкретными внешними компонентами (СУБД, web-сервер), то в свойствах отдельного таксона должна быть указана ссылка на наименование соответствующей уязвимости внешнего компонента.

Схема возможного разделения таксонов представлена на рис. 4.

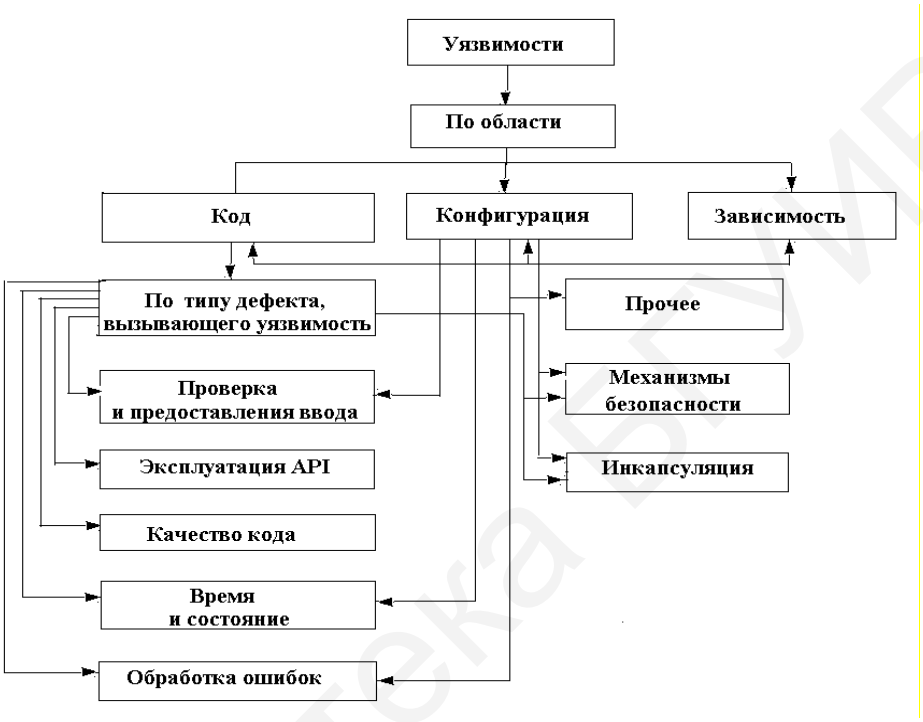

Рис. 4 Классификация уязвимостей по области их определения

Классификация уязвимостей на основе **причин их возникновения** (дефектов) в общем виде включает два *типа* и восемь *классов* [66].

Типы представляют собой:

- уязвимости, вызванные дефектами проектирования и программирования;
- уязвимости, вызванные дефектами конфигурирования и управления.

Восемь **классов** соответствуют наиболее применимым с точки зрения практики анализа кода международным таксономиям, а именно включают уязвимости, связанные:

- с обработкой и представлением данных;
- внутренней структурой и зависимостями компонентов;
- обработкой событий и состояний;
- внутренними механизмами и ресурсами;
- преднамеренным внедрением;
- качеством проектирования и документированием;
- конфигурациями;
- окружением.

3. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

3.1. Уровни и направления обеспечения безопасности информации

На рынке информационных технологий (ИТ) растет спектр предложений по обеспечению информационной безопасности (ИБ). Мероприятия по обеспечению ИБ не приносят доходов, с их помощью можно лишь уменьшить ущерб от возможных инцидентов (рис. 5) [70].

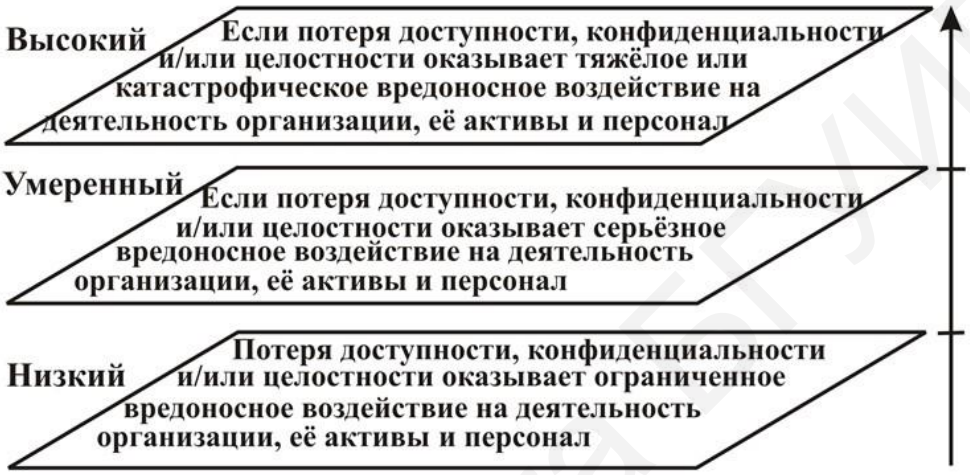

Рис. 5. Уровни оценки ущерба при нарушении информационной безопасности

Очень важно, чтобы затраты на создание и поддержание ИБ на должном уровне были соразмерны ценности активов организации, связанных с ее информационной системой (ИС).

Базовые требования к безопасности информации включают в себя: планирование; реагирование на нарушения ИБ; физическую защиту; защиту систем и телекоммуникаций; сертификацию, аккредитацию и оценку ИБ; кадровую безопасность; протоколирование и аудит; защиту носителей; обеспечение целостности данных; аутентификацию и авторизацию данных; мониторинг регуляторов ИБ; управление конфигурацией системы; формирование политики безопасности; оценку рисков.

Требования делятся на три уровня: административный, процедурный и программно-технический.

Защитные действия, ориентированные на обеспечение информационной безопасности, могут быть охарактеризованы целым рядом параметров, отражающих направления, ориентацию на объекты защиты, характер угроз, способы действий, их распространенность, охват и масштабность (рис. 6) [71].

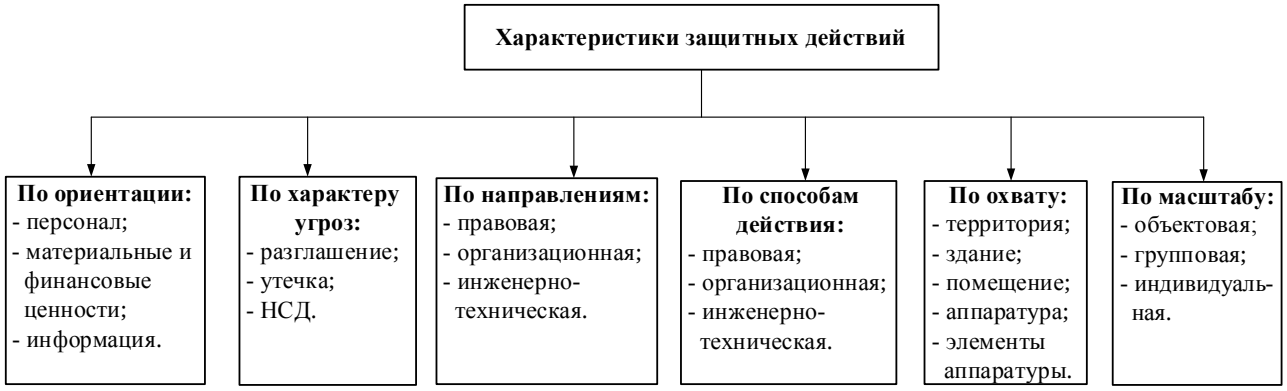

Рис. 6. Характеристики защитных действий [74]

Обеспечение безопасности информации представляет собой сложную задачу, включающую следующие уровни.

1. Программно-технический уровень.

С современной точки зрения, информационным системам должны быть доступны следующие механизмы безопасности:

- управление доступом;
- экранирование;
- проверка подлинности пользователей и их идентификация;
- протоколирование и аудит;
- обеспечение высокой доступности;
- криптография.

2. Организационный уровень.

К нему относятся меры, реализуемые персоналом информационного объекта. Существуют следующие группы организационных мер:

- управление персоналом;
- поддержание работоспособности;
- планирование восстановительных работ;
- физическая защита;
- реагирование на нарушение безопасного режима.

Для каждой группы должны существовать правила, определяющие действия персонала. Они должны быть учреждены в каждой конкретной организации и отработаны на практике.

3. Административный уровень.

Политика безопасности, предпринимаемая руководством организации, является основой мер административного уровня. Это совокупность документированных решений руководства, которые направлены на защиту информации, а также ресурсов, ассоциированных с ней. Политика безопасности основывается на анализе реальных рисков, угрожающих информационной системе той или иной организации. После анализа разрабатывается стратегия защиты – программа, на которую выделяются деньги, назначаются ответственные, устанавливается порядок контроля ее выполнения и т. д. Поскольку каждая организация имеет свою специфику, бессмысленно переносить практику государственных режимных предприятий на коммерческие структуры, персональные ком-

пьютерные системы или учебные заведения. Целесообразно использовать основные принципы разработки политики безопасности или готовые шаблоны для основных разновидностей организаций.

4. Законодательный уровень.

Это важнейший уровень обеспечения информационной безопасности. В него входит комплекс мер, направленных на создание и поддержание в обществе негативного отношения к нарушителям и нарушениям в этой области. Необходимо создать механизм, который позволил бы согласовывать разработку законов с постоянным совершенствованием информационных технологий. Государство должно выполнять координирующую и направляющую роль в этом вопросе. Стандарты информационных технологий и информационной безопасности, принятые в РБ, должны соответствовать международному уровню.

Взаимодействие всех уровней обеспечения информационной безопасности делают ее максимально эффективной.

Обеспечение информационной безопасности – это деятельность, направленная на достижение состояния защищенности информационной среды, а именно обеспечения целостности, конфиденциальности и доступности.

Доступность информации – свойство системы (среды, средств и технологии обработки), в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов в любой момент обращения к ним.

Нарушение доступности представляет собой создание таких условий, при которых доступ к услуге или информации будет либо заблокирован, либо возможен за время, которое не обеспечит выполнение тех или иных бизнес-целей. Например, в случае выхода из строя сервера, на котором расположена требуемая для принятия стратегического решения информация, нарушается свойство доступности информации. Аналогично в случае изоляции по какой-либо причине (выход из строя сервера, отказ каналов связи) почтового сервера можно говорить о нарушении доступности услуги «электронная почта». Особо следует отметить тот факт, что причина нарушения доступности информации или информационной услуги не обязательно должна находиться в зоне ответственности владельца услуги или информации. Например, в рассмотренном выше примере с нарушением доступности почтового сервера причина может лежать вне зоны ответственности администраторов сервера (например, отказ магистральных каналов связи). Также следует отметить, что понятие «доступность» субъективно в каждый момент времени для каждого из субъектов, потребляющих услугу или информацию в данный момент времени. В частности, нарушение доступности почтового сервера для одного сотрудника может означать срыв индивидуальных планов и потерю контракта, а для другого сотрудника той же организации – невозможность получить выпуск свежих новостей.

Целостность информации – существование информации в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состо-

янию). Чаще субъектов интересует обеспечение более широкого свойства – достоверности информации, которое складывается из адекватности (полноты и точности) отображения состояния предметной области и непосредственно целостности информации, т. е. ее неискаженности.

Угрозы нарушения целостности – это угрозы, связанные с вероятностью модификации той или иной информации, хранящейся в ИС. Нарушение целостности может быть вызвано различными факторами – от умышленных действий персонала до выхода из строя оборудования (рис. 7).

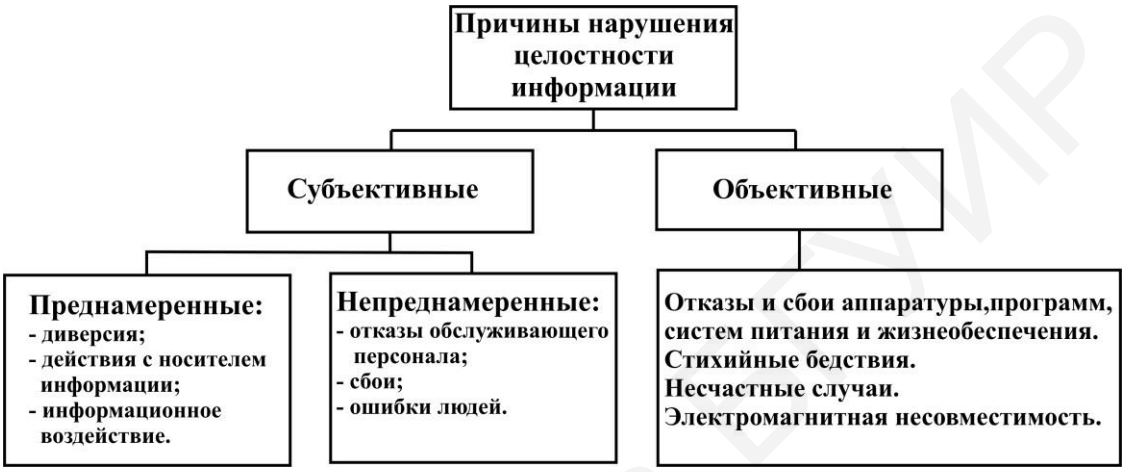

Рис. 7. Причины нарушения целостности информации

Конфиденциальность информации – способность системы обеспечивать целостность и сохранность информации ее законных пользователей.

Угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Она имеет место всякий раз, когда получен доступ к некоторой секретной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Иногда в связи с угрозой нарушения конфиденциальности используется термин «утечка».

Подобные угрозы могут возникать вследствие антропогенных факторов (например, случайное делегировании тому или иному пользователю привилегий другого пользователя) или сбоев в работе программных и аппаратных средств.

Реализация каждой из указанных угроз в отдельности или их совокупности приводит к нарушению информационной безопасности предприятия, а именно [72]:

1) к нарушению конфиденциальности защищаемых сведений (разглашение, утрата, хищение, утечка, перехват и т. п.);

2) к нарушению целостности защищаемой информации (уничтожение, искажение, подделка и т. п.);

3) к нарушению регламентируемой доступности к защищаемой информации и работоспособности программно-технических комплексов информационных систем.

Все мероприятия по обеспечению информационной безопасности должны строиться по принципу минимизации указанных угроз, и условно их можно рассматривать на двух основных уровнях: на уровне *физического доступа* к данным и на уровне *логического доступа* к данным, которые являются следствием административных решений (политик).

На уровне **физического доступа** к данным рассматриваются механизмы защиты данных от несанкционированного доступа и от повреждения физических носителей данных. Защита от несанкционированного доступа предполагает размещение серверного оборудования с данными в отдельном помещении, доступ к которому имеет лишь персонал с соответствующими полномочиями. На этом же уровне в качестве средств защиты возможно создание географически распределенной системы серверов. Уровень защиты от физического повреждения предполагает организацию различного рода специализированных систем, предотвращающих подобные процессы, к их числу относят серверные кластеры и серверы резервного копирования. При работе в кластере (например, двух серверов) в случае физического отказа одного из них второй будет продолжать работу, таким образом, работоспособность вычислительной системы и данных не будет нарушена. При дополнительной организации резервного копирования сервера возможно быстрое восстановление вычислительной системы и данных даже в случае выхода из строя второго сервера в кластере.

Примечание. **Резервное копирование** – это сохранение очередного текущего состояния информации (системы) без обязательного сохранения предыдущего [73].

Уровень защиты от **логического доступа** к данным предполагает защиту от несанкционированного доступа в систему (предназначенную для порождения, хранения и обработки, данных любого класса – от простых учетных систем до решений класса ERP) как на уровне баз данных, так и на уровне ядра системы и пользовательских форм. Защита на этом уровне предполагает принятие мер по предотвращению доступа к базе данных как из сети Интернет, так и из локальной сети организации (на последний аспект обеспечения безопасности традиционно обращается мало внимания, хотя он напрямую связан с таким явлением, как промышленный шпионаж). Защита ядра системы предполагает, наряду с обозначенными выше мерами, вычисление контрольных сумм критических частей исполнимого кода и периодический контроль этих контрольных сумм.

Примечание. **ERP (англ. Enterprise Resource Planning – планирование ресурсов предприятия)** – организационная стратегия интеграции производства и операций, управления трудовыми ресурсами, финансового менеджмента и управления активами, ориентированная на непрерывную балансировку и оптимизацию ресурсов предприятия посредством специализированного интегрированного пакета прикладного программного обеспечения, обеспечивающего общую модель данных и процессов для всех сфер деятельности.

Подобный подход позволяет повысить общую степень защищенности системы. Обеспечение безопасности на уровне пользовательских форм декларирует обязательное шифрование трафика, передающегося по локальной сети (или через сеть Интернет) между клиентом (пользовательской формой) и приложением (ядром системы). Также безопасность на этом уровне может обеспечиваться вычислением контрольных сумм этих форм с последующей их про-

веркой, принятием идеологии «разделения данных и кода». Например, система, построенная по технологии «тонкого клиента», с позиций обеспечения безопасности на данном уровне имеет преимущество перед системой, построенной по технологии «толстого клиента», поскольку на уровне пользовательских форм не предоставляет доступа к коду бизнес-логики (например, путем дизассемблирования исполняемого файла) [74].

К этому же уровню защиты относится механизм аутентификации с использованием сертификатов. Сертификат представляет собой набор атрибутов, идентифицирующих владельца, подписанный центром сертификации (доверенной третьей стороной), который выступает в роли посредника и гарантирует подлинность сертификатов.

Для компьютерных сетей на этапе эксплуатации целостность и доступность информации в системе обеспечивается путем:

- дублирования информации;
- повышения отказоустойчивости компьютерной сети;
- противодействия перегрузкам и зависаниям системы;
- использования строго определенного множества программ;
- контроля целостности информации в компьютерной сети;
- особой регламентации процессов технического обслуживания и проведения доработок;
- выполнения комплекса антивирусных мероприятий.

Одним из главных условий обеспечения целостности и доступности информации в компьютерной сети является ее дублирование. Стратегия дублирования выбирается с учетом важности информации, требований к непрерывности работы компьютерной сети, трудоемкости восстановления данных. Дублирование информации обеспечивается дежурным администратором компьютерной сети.

Целостность и доступность информации поддерживается также путем резервирования аппаратных средств, блокировок ошибочных действий людей, использования надежных элементов КС и отказоустойчивых систем. Устраняются преднамеренные угрозы перегрузки элементов систем, для чего используются механизмы измерения интенсивности поступления заявок на выполнение (передачу) и механизмы ограничения или полного блокирования передачи таких заявок. Должна быть предусмотрена также возможность определения причин резкого увеличения потока заявок на выполнение программ или передачу информации. В сложных системах практически невозможно избежать ситуаций, приводящих к зависаниям систем или их фрагментов. В результате сбоев аппаратных или программных средств, алгоритмических ошибок, допущенных на этапе разработки, ошибок операторов в системе происходят зацикливания программ, непредусмотренные остановки и другие ситуации, выход из которых возможен лишь путем прерывания вычислительного процесса и последующего его восстановления. На этапе эксплуатации ведется статистика и осуществляется анализ таких ситуаций. Зависания своевременно обнаруживаются, и вычислительный процесс восстанавливается. При восстановлении, как прави-

ло, необходимо повторить выполнение прерванной программы с начала или с контрольной точки, если используется механизм контрольных точек (механизм используется при выполнении сложных вычислительных программ, требующих значительного времени для их реализации).

Рекомендациями МОС и МСЭ-Т предусматриваются следующие основные *механизмы защиты* [75]:

- шифрование данных;
- обеспечение аутентификации;
- обеспечение целостности данных;
- цифровая подпись;
- контроль доступа.

Механизм шифрования может обеспечивать конфиденциальность либо передаваемых данных, либо информации о параметрах трафика и может быть использован в некоторых других механизмах безопасности или дополнять их. Существование механизма шифрования подразумевает использование, как правило, механизма управления ключами.

При рассмотрении *механизмов аутентификации* основное внимание уделяется методам передачи в сети информации специального характера (паролей, аутентификаторов, контрольных сумм и т. п.). В случае односторонней или взаимной аутентификации обеспечивается процесс проверки подлинности пользователей (передатчика и приемника сообщений), что гарантирует предотвращение соединения с логическим объектом, образованным злоумышленником.

Механизм обеспечения целостности данных предполагает введение в каждое сообщение некоторой дополнительной информации, являющейся функцией от содержания сообщения. Эти методы применяются как при передаче данных по виртуальному соединению, так и при использовании датаграммной передачи. В первом случае гарантируется устранение неупорядоченности, потерь, повторов, вставок или модификации данных при помощи специальной нумерации блоков либо путем введением меток времени. В датаграммном режиме метки времени могут обеспечить только ограниченную защиту целостности последовательности блоков данных и предотвратить переадресацию отдельных блоков.

Механизм электронной цифровой подписи, реализующий один из процессов аутентификации пользователей и сообщения, применяется для подтверждения подлинности содержания сообщения и удостоверения того факта, что оно отправлено абонентом, указанным в заголовке в качестве источника данных. Электронная цифровая подпись также необходима для предотвращения возможности отказа передатчика от факта выдачи какого-либо сообщения, а приемника – от его приема.

Механизмом электронной цифровой подписи определяются две процедуры:

- формирование блока данных, добавляемого к передаваемому сообщению;
- подписание блока данных.

Процесс формирования блока данных содержит общедоступные процедуры и в отдельных случаях специальные (секретные) ключи преобразования, известные на приеме. Процесс подписания блока данных использует информацию, которая является информацией частного использования (т. е. уникальной и конфиденциальной). Этот процесс подразумевает либо шифрование блока данных, либо получение криптографического контрольного значения блока данных с использованием частной информации подписавшего пользователя в качестве ключа шифрования частного пользования. Таким образом, после проверки подписи в последующем третьему лицу (например, арбитру) в любое время может быть доказано, что подпись может выполнить только единственный держатель секретной (частной) информации.

Механизмы контроля доступа могут использовать аутентифицированную идентификацию объекта (отождествление анализируемого объекта с одним из известных объектов), информацию объекта (например, принадлежность к известному множеству объектов) либо возможности этого объекта для установления и применения прав доступа к нему. Если объект делает попытку использовать несанкционированный или санкционированный с неправильным типом доступа ресурс, то функция контроля доступа будет отвергать эту попытку и может сообщить о ней для инициирования аварийного сигнала и (или) регистрации его как части данных проверки безопасности. Механизмы контроля доступа могут использоваться на любом конце соединения и (или) в любом промежуточном узле.

3.2. Способы и средства обеспечения безопасности информации

Применение современных технических систем безопасности может не только существенно улучшить защищенность объекта, усовершенствовать систему охраны в целом, но и оптимизировать работу службы безопасности, а на некоторых участках и полностью заменить ее. Совершенные цифровые охранные системы и комплексы, обладающие элементами искусственного интеллекта, не только гарантированно обеспечивают защиту объекта от несанкционированных проникновений, хищений и пожаров, но и дают возможность для полного ежеминутного контроля функционирования любого предприятия и его служб, соблюдения трудового распорядка и дисциплины, обеспечения безопасности и сохранности материальных ценностей.

Сегодня все чаще используются автоматизированные комплексные системы безопасности, состоящие из нескольких подсистем, конструктивно объединенных в единое целое: системы видеонаблюдения, контроля и управления доступом и оповещения, а также охранной, периметровой и пожарной сигнализации

Процесс обеспечения безопасности информации на объекте состоит из нескольких этапов [76]:

1) проведение аудита информационной безопасности системы электронного документооборота (СЭД);

2) выбор методов и средств защиты;

3) проектирование системы защиты, ее реализация и сопровождение системы.

Аудит информационной безопасности является первым этапом конструирования системы защиты информации. Его сущность заключается в поэтапном проведении анализа существующего информационного, программно-аппаратного и кадрового компонентов организации, выявлении уязвимостей, оценке рисков и прогнозировании их последствий, что позволяет оперативно получать систематизированную и достоверную информацию для оценки системы, принятия решения, управления ею.

При проведении аудита должны быть учтены и рассмотрены все составляющие: состав информационного массива, способы хранения документированной информации, ее передача, обработка, ценность, степень доступа к ней и др.

В процессе проведения аудита устанавливается степень важности информации для организации и выделяется комплекс документов (производственных, технологических, финансовых), при нежелательном воздействии на который организация может понести серьезные убытки. Проводится обследование программно-технической составляющей системы и персонала, тестирование конкретных программных продуктов на выявление слабых мест, определяется степень изношенности, соответствие нынешнему развитию программных продуктов на рынке. Определяются функциональные права групп пользователей, распределение доступа к документам путем включения принятых положений в локальные нормативные акты организации (должностные инструкции, договоры о неразглашении конфиденциальной информации, положения о структурном подразделении и т. д.).

На заключительном этапе аудита проводится оценка рисков реализации угроз. В настоящий момент основой большинства ошибок при принятии решений по вопросам безопасности является неправильная оценка рисков. При проведении оценки рисков определяется [77]:

- перечень сил и средств защиты, необходимый для гарантии безопасности объекта;
- адекватность задействованных сил и средств защиты, расстановка приоритетов в реализации алгоритмов противодействия;
- реальная оценка возможного экономического ущерба.

Работы по проведению оценки рисков заключаются в следующем [78]:

- идентификация ключевых ресурсов;
- определение важности ресурсов;
- идентификация существующих угроз и уязвимостей;
- создание неформальной модели нарушителя;
- вычисление рисков, связанных с осуществлением угроз безопасности.

По результатам аудита формируют запросы и цели дальнейших этапов построения системы защиты информации.

Проведенный аудит позволит обоснованно создать следующие документы:

- долгосрочный план развития информационной системы;

- политику безопасности организации;
- методологию работы информационной системы организации;
- план восстановления информационной системы в чрезвычайной ситуации.

Результаты аудита влияют на принятие решений во многих сферах повседневной деятельности организации, таких как долгосрочные планы развития информационной инфраструктуры, политика в области управления службой безопасности, отделом документального обеспечения управления, кадрами в целом, а также выявляют степень необходимости защиты, и в результате составляется экономически обоснованный план, который предопределяет дальнейший ход действий руководства в этой области [83]

На втором этапе построения системы защиты информации осуществляется выбор **способов и средств защиты информации**.

Согласно [2] различают правовые, организационные и технические способы защиты информации.

К *правовым* способам защиты информации относятся заключаемые обладателем информации с пользователем информации договоры, в которых устанавливаются условия пользования информацией, а также ответственность сторон по договору за нарушение указанных условий [2].

К *организационным* способам защиты 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 [2].

К *техническим* способам защиты информации относятся меры по использованию средств защиты информации, в том числе криптографических, а также систем контроля доступа и регистрации фактов доступа к информации [2].

Средства защиты информации – технические, программные, программно-аппаратные средства, предназначенные для защиты информации, а также средства контроля эффективности ее защищенности [79].

Примечание. **Дестабилизирующий фактор** – это явление или событие, следствием наступления которого может быть нарушение конфиденциальности, целостности и/или доступности информационных ресурсов, нарушение работоспособности сети или ее элементов.

Количество и разнообразие возможных средств защиты определяется прежде всего способами воздействия на дестабилизирующие факторы или порождающие их причины (табл. 4).

Таблица 4

Способы обеспечения безопасности информации посредством воздействия на дестабилизирующие факторы

Способы воздействия на дестабилизирующие факторы	Способ защиты системы
Препятствие	Возникновение или распространение дестабилизирующего фактора (блокировка, физические препятствия, экранирование)
Управление	Определение управляющих воздействий для каждого этапа функционирования систем обработки информации, чтобы способствовать решению одной или нескольких задач защиты информации
Маскировка	Преобразование информации, вследствие чего она становится недоступной / труднодоступной для злоумышленников или обладает низкой степенью распознавания (криптографические методы, дезинформация, легендирование, зашумление)
Регламентация	Разработка и реализация в процессе функционирования правил обращения с конфиденциальной информацией и средствами ее обработки, которые позволили бы максимально затруднить получение этой информации злоумышленником
Принуждение	Пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защиты информации
Побуждение	Пользователи и персонал системы внутренними факторами (материальными, моральными, этическими, психологическими и др.) побуждаются к соблюдению всех правил обработки информации
Нападение	Применение информационного оружия при информационной войне, непосредственное физическое уничтожение противника (при ведении боевых действий) или его средств разведки

Рассмотренные способы воздействий на дестабилизирующие факторы реализуются **формальными** и **неформальными** средствами защиты информации (рис. 8) [80].

Основу **неформальных средств** составляет целенаправленная деятельность людей, которая может включать в себя *организационные, законодательные* и *морально-этические* средства. **Формальные средства** выполняют свои функции не требуя непосредственного участия человека и делятся на *технические* (*физические* и *аппаратные*), *программные* и *криптографические*.

Рис. 8. Способы и средства обеспечения безопасности информации

3.2.1. Неформальные средства обеспечения безопасности информации

Организационные средства защиты информации определяют и вырабатывают порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации.

Организационные мероприятия, направленные на обеспечение безопасности информации, охватывают все структурные элементы системы защиты на всех этапах их жизненного цикла любой ИС: строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и проверка в эксплуатации аппаратуры, оргтехники, средств обработки и передачи данных. В их основе находится политика безопасности, отражающая подход организации к защите своих информационных активов. Руководство каждой организации должно осознавать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов. В организациях, использующих в своей деятельности сведения с ограниченным доступом, для проведения мероприятий по защите информации могут создаваться соответствующие службы безопасности.

Основные **принципы** организационной защиты информации [81]:

- *принцип комплексного подхода* – эффективное использование сил, средств, способов и методов защиты информации для решения поставленных

задач в зависимости от конкретной складывающейся ситуации и наличия факторов, ослабляющих или усиливающих угрозу защищаемой информации;

- *принцип оперативности принятия управленческих решений* существенно влияет на эффективность функционирования и гибкость системы защиты информации и отражает нацеленность руководства и персонала предприятия на решение задач защиты информации;

- *принцип персональной ответственности* – наиболее эффективное распределение задач по защите информации между руководством и персоналом предприятия и определение ответственности за полноту и качество их выполнения.

Среди основных **условий** организационной защиты информации можно выделить [82]:

- непрерывность всестороннего анализа функционирования системы защиты информации в целях принятия своевременных мер по повышению ее эффективности;

- неукоснительное соблюдение руководством и персоналом предприятия установленных норм и правил защиты конфиденциальной информации.

К организационным **мерам** защиты информации относятся следующие:

- организация разработки, внедрения и использования средств и систем защиты;

- управление доступом персонала на территорию, в здания и помещения объекта путем проверки пропусков;

- контроль состояния и использования технических средств, документов, машинных носителей информации;

- контроль соблюдения правил защиты информации пользователями и персоналом автоматизированных систем обработки данных (АСОД);

- планирование и организация обработки защищаемой информации;

- подбор, расстановка и подготовка кадров, участвующих в обработке защищаемой информации;

- организация уничтожения бумажных документов, содержащих защищаемую информацию, но утративших свою актуальность;

- организация ведения архивных массивов данных и документов;

- ведение журналов регистрации сбоев и отказов средств и систем защиты;

- организация учета и обработки сведений об обнаруженных удачных и неудачных попытках несанкционированных действий в АСОД;

- организация и проведение профилактических осмотров и ремонта средств и систем защиты информации;

- анализ функционирования средств и систем защиты информации в целях их совершенствования;

- разработка и внедрение в практику инструкций и других документов, регламентирующих правила обращения с защищаемой информацией.

Законодательные средства защиты информации определяются существующими в стране нормативно-правовыми актами, с помощью которых регламентируются права и обязанности, связанные с обеспечением защиты информации, всех лиц и подразделений, имеющих отношение к функционированию системы защиты, а также устанавливается ответственность за нарушение правил обработки информации, следствием чего может быть нарушение защищенности информации.

Законы Республики Беларусь по вопросам защиты информации в основном освещают ключевые термины и понятия, относящиеся к данной сфере, цели, объекты, субъекты защиты, их права и обязанности. Также они регламентируют правонарушения в этой области и меры ответственности за них. Эти и иные аспекты законодательных средств защиты информации рассмотрены в подразделе 1.3 данного пособия.

Морально-этические средства защиты информации представляют собой сложившиеся в обществе или в данном коллективе моральные нормы и этические правила, соблюдение которых способствует защите информации, а нарушение приравнивается к несоблюдению правил поведения в обществе или коллективе [79].

Морально-этические средства предполагают прежде всего «воспитание» сотрудника, т. е. проведение специальной работы, направленной на формирование у него системы определенных качеств, взглядов и убеждений, и обучение сотрудника правилам и методам защиты информации, привитие ему навыков работы с носителями секретной и конфиденциальной информации.

Одним из основных компонентов неформальных средств обеспечения ИБ является **служба информационной безопасности** (СИБ) – орган управления системы защиты информации.

Эффективность мер по защите информации зависит от:

- качества построения службы информационной безопасности;
- профессиональной подготовленности ее сотрудников;
- наличия в арсенале сотрудников современных средств управления безопасностью.

Основная **цель** функционирования СИБ – используя организационные меры и программно-аппаратные средства, избежать или свести к минимуму возможность нарушения политики безопасности либо в крайнем случае вовремя заметить и устранить последствия нарушения. Рациональная структура службы информационной безопасности на предприятии, как правило, занимается анализом избранной политики безопасности, соотношением вероятных угроз и потерь в случае их реализации с эффективностью системы защиты информации и финансовыми затратами на их реализацию. Главное требование к службе информационной безопасности – высокая профессиональная подготовленность.

Существует несколько вариантов штатного расписания СИБ, например:

- заместитель директора по безопасности и защите информации;

- администратор безопасности АС – штатный сотрудник отдела защиты информации;

- администратор системы – штатный сотрудник отдела автоматизации;

- администраторы групп – штатные сотрудники подразделений, эксплуатирующих АС;

- менеджеры безопасности;

- операторы.

К **задачам** службы безопасности предприятия относятся:

- определение перечня сведений, составляющих коммерческую тайну, а также круга лиц, которые в силу занимаемого служебного положения на предприятии имеют к ним доступ;

- определение участков сосредоточения сведений, составляющих коммерческую тайну, а также технологического оборудования, выход из строя которого может привести к большим экономическим потерям;

- формирование требований к системе защиты в процессе создания и участие в проектировании системы защиты, ее испытаниях и приемке в эксплуатацию;

- планирование, организация и обеспечение функционирования системы защиты информации;

- распределение между пользователями необходимых реквизитов защиты, паролей, управление средствами защиты коммуникаций и криптозащиты данных;

- координация действий с аудиторской службой, контроль функционирования системы защиты и ее элементов, тестирование системы защиты;

- организация обучения сотрудников службы информационной безопасности;

- расследование произошедших нарушений защиты, принятие мер реагирования на попытки НСД к информации и нарушения правил функционирования системы защиты;

- выполнение восстановительных процедур после фактов нарушения безопасности;

- изучение, анализ, оценка состояния и разработка предложений по совершенствованию системы обеспечения информационной безопасности предприятия;

- совместная работа с представителями других организаций по вопросам безопасности – непосредственный контакт и консультации с партнерами или клиентами;

- регулярная проверка соответствия принятых в организации правил безопасной обработки информации существующим правовым нормам, контроль над соблюдением этого соответствия.

Организационно-правовой статус службы информационной безопасности определяется следующим образом:

- численность службы должна быть достаточной для выполнения всех перечисленных выше функций;

- служба должна подчиняться лицу, несущему персональную ответственность за соблюдение правил обращения с защищаемой информацией в данном учреждении;

- штатный состав службы не должен иметь других обязанностей, связанных с функционированием автоматизированной системы (АС);

- сотрудники службы должны иметь право доступа во все помещения, где установлена аппаратура АС, и право прекращать автоматизированную обработку информации при наличии непосредственной угрозы для защищаемой информации;

- руководителю службы должно быть предоставлено право запрещать включение в число действующих новые элементы АС, если они не отвечают требованиям защиты информации;

- службе информационной безопасности должны быть обеспечены все условия, необходимые для выполнения своих функций.

Ключевой (иногда единственной) фигурой в службе информационной безопасности является *администратор безопасности* (АБ), который должен взаимодействовать с любыми подразделениями и должностными лицами организации для более эффективного выполнения своих обязанностей. Деятельность администратора непосредственно связана с выполнением правил эксплуатации средств защиты информации, обеспечением непрерывности процесса обработки информации, реагированием на нарушения в компьютерной системе и восстановлением работоспособности компьютерной системы.

Установка и снятие средств защиты производится силами СИБ в соответствии с планом защиты. После установки администратору безопасности передается полная документация на средства защиты, ключевые дискеты и электронные идентификаторы. В случае выявления конфликтов в работе средств защиты, приводящих к серьезным нарушениям и затрудняющим обработку информации, администратор должен немедленно сообщить об этом в службу информационной безопасности.

Администратор безопасности принимает участие в обеспечении непрерывности процесса обработки информации. В пределах своей зоны ответственности он поддерживает:

- аварийный архив – копии используемого в компьютерной системе программного обеспечения;

- текущий архив – данные компьютерной системы по состоянию на конец предыдущего рабочего дня;

- долговременный архив – данные компьютерной системы за предварительно установленный период.

Рабочее место администратора безопасности (РМ АБ) предназначено для реализации функций настройки, контроля и поддержания в актуальном состоянии программных средств защиты на АРМ пользователей и выполнения мероприятий по обеспечению безопасности технических средств и обрабатываемой в сети информации.

РМ АБ обеспечивает выполнение следующих функций:

- сигнализация на РМ АБ о нарушениях на АРМ пользователей и серверах компьютерной сети;
- мониторинг состояния АРМ пользователей;
- администрирование программных средств защиты;
- обеспечение сервиса деятельности АБ.

На РМ АБ производится сигнализация:

- о нарушении целостности ПО (без детализации о виде нарушения);
- событиях, подлежащих регистрации в системных журналах Windows (по определенному АБ списку);
- запуске и/или завершении процессов на АРМ пользователей и серверах компьютерной сети (по определенному АБ списку).

При срабатывании сигнализации на экран компьютера АБ выдаются следующие сведения о нарушениях: вид и описание нарушения; адрес компьютера, на котором оно произошло; дата и время его совершения.

Мониторинг состояния АРМ пользователей заключается в отображении текущего состояния АРМ пользователей и включает в себя следующие сведения: сетевое имя ПЭВМ, IP-адрес ПЭВМ, имя пользователя, состояние сети (подключен ли пользователь к компьютерной сети), категории выполняемых на ПЭВМ процессов (настраиваются АБ), состояние целостности ПО на ПЭВМ (блокировка, формирование эталонов, проверка целостности, ожидание);

Администрирование программных средств защиты включает следующие функции управления:

- *управление контролем целостности* заключается в обеспечении АБ возможностью добавления наименований расширений в установленный по умолчанию перечень типов проверяемых файлов, а также исключения из проверки конкретных файлов и выдачи команд на АРМ пользователей на проведение контроля целостности или формирование эталонных значений;
- *управление опознанием* заключается в обеспечении АБ возможностью генерации паролей, их назначения пользователям, создания новых учетных записей, сохранения списка действующих идентификаторов и паролей (пароли сохраняются в зашифрованном виде) на магнитном носителе, загрузки списка идентификаторов и паролей с магнитного носителя, распечатки установленных идентификаторов и паролей для доведения их до пользователей, распечатки списка пользователей, предназначенного для отметки об ознакомлении их с действующим идентификатором и паролем, использования средств MS Windows 2000 Server, предназначенных для работы со службой каталогов Active Directory;
- *управление контролем доступа* обеспечивает выдачу команд на блокировку и разблокировку ПЭВМ пользователей;
- *управление аудитом* заключается в обеспечении возможности настройки перечня событий аудита, регистрируемых в системных журналах на АРМ пользователей, в рабочем журнале на РМ АБ, а также изменения размеров журналов и их архивирования на магнитных носителях.

Обеспечение сервиса деятельности АБ включает следующие функции:

- получение быстрого доступа к журналам аудита, средствам управления службы каталогов Active Directory;
- настройка панели вызова документов АБ;
- настройка панели вызова программных средств АБ.

В случае возникновения нарушения в компьютерной системе администратор безопасности классифицирует его (нарушение конфиденциальности, целостности, подлинности информации; нарушение работоспособности компьютерной системы), сообщает о нарушении руководителю подразделения и в службу информационной безопасности, определяет причину возникновения нарушения (НСД, вирусное воздействие, сбой, отключение электропитания, кража носителей, выход оборудования из строя и т. д.), локализует нарушение, т. е. определяет нарушителя и его настоящие и дальнейшие действия.

Конкретные **действия оператора и/или администратора безопасности** в каждом случае определяются особенностями АС и системы защиты:

- исключение из компьютерной системы скомпрометированных идентификаторов и ключей;
- принятие мер по ликвидации последствий нарушения (восстанавление разрушенных данных и программ с использованием аварийных, текущих и долговременных архивов);
- остановка процесса обработки информации до прибытия специалистов отдела автоматизации и СИБ, если в результате нарушения дальнейшая работа может повлечь за собой увеличение размеров ущерба;
- определение размера ущерба, вызванного нарушением; размер выражается во временных потерях или денежных затратах;
- составление служебной записки о факте нарушения в компьютерной системе; в случае необходимости инициирование проведения служебного расследования.

Организация работы службы безопасности компании с персоналом. Мировая статистика свидетельствует о том, что около 80 % ущерба материальным активам организаций наносит их собственный персонал. Так, например, за последние 20 лет около 100 банков США потерпели крах из-за мошенничества сотрудников.

СИБ позволяет лучше изучить сотрудников и предусмотреть их действия. Сотрудники СИБ в своей работе с персоналом используют различные методы предупредительно-профилактического характера, такие как обучение, инструктажи, санкции. СИБ тесно сотрудничает со службой по управлению персоналом (отделом кадров) и руководителями структурных подразделений. Взаимодействие со структурными подразделениями регламентируется в соответствующем разделе Положения о службе безопасности, где определяются функции, зоны ответственности и права СИБ.

Работа с персоналом проводится по следующим направлениям:

- проверка кандидатов при приеме на работу, выявление возможных рисков и угроз для компании;

- обеспечение безопасности в процессе исполнения персоналом служебных обязанностей;

- предотвращение нанесения экономического ущерба и утечки информации, составляющей коммерческую тайну, в случае увольнения сотрудника.

Рассмотрим более подробно этап **проверки кандидатов при приеме на работу**.

При отборе кандидатов на вакантные должности необходимо руководствоваться тем, что потенциальный сотрудник должен:

- иметь надлежащую квалификацию или возможность быстро ее приобрести;

- быть лояльным к компании;

- обладать высокими моральными качествами.

СИБ подключается к работе с кадрами уже на этапе подготовки объявлений о вакантных рабочих местах. При подборе кандидатов используются различные способы поиска потенциальных сотрудников:

- изучаются предложения служб занятости, рекрутинговых агентств;

- размещаются объявления о вакансиях в периодических изданиях;

- рассматриваются рекомендации лояльных сотрудников, уже работающих в компании;

- просматриваются базы анкет и резюме, собранные ранее;

- изучаются предложения кандидатов в интернете, в специализированных периодических изданиях и т. д.

СИБ участвует в подготовке психологических тестов, а также профессиональных вопросов (вместе со специалистами тех подразделений, где открыты вакансии). Содержание всех предоставленных кандидатами документов анализируется совместно сотрудниками отдела кадров и СИБ. При этом оценивается уровень образования кандидата, опыт работы, умение грамотно оформлять документы и пр.

Цель сотрудника СИБ – собрать максимум дополнительной информации о кандидате, что исключительно важно для предотвращения потенциальной угрозы безопасности компании. Необходимо выяснить:

- привлекался ли кандидат к уголовной ответственности за правонарушения, связанные с финансовой или иной деятельностью на предыдущих местах работы;

- был ли кандидат уволен с прежних мест работы по причинам, связанным с финансовыми и иными нарушениями, которые официально не получили огласки;

- есть ли в числе мест прежней работы организации, которые практикуют «теневые» схемы бизнеса.

При решении о приеме кандидата на работу сотрудник СИБ проводит с ним инструктаж по такому кругу вопросов:

- предотвращение нанесения экономического ущерба фирме;

- правила работы с коммерческой информацией компании.

Затем новый сотрудник подписывает обязательства в связи с допуском к конфиденциальной информации, подлежащей защите, где указаны требования по выполнению обязательств и ответственность за их нарушения.

Специалисты аналитического отдела компании Falcongaze подвели итоги ежегодного исследования, посвященного причинам, по которым руководство чаще всего увольняло своих подчиненных в 2016 году. Данное исследование базировалось на данных, собранных при помощи системы SecureTower, предназначенной для защиты информации от утечек и детального контроля деятельности персонала на рабочих местах. В ходе исследования специалисты компании не только обратились к цифрам и фактам, свидетельствующим о нарушениях со стороны персонала, но и выяснили, какие из причин увольнений преобладали в различных сферах бизнеса (рис. 9).

Наиболее частой причиной для увольнений названа добровольная смена работы. Собственная инициатива работника стала причиной увольнения в 29 % случаев. В 27 % случаях увольнений причиной стали нарушения рабочего процесса (некорректное поведение в коллективе, несоблюдение рабочего графика, прогулы). В 2016 году 23 % из всех уволенных работников попали под сокращения. В связи со случаями коррупции, растрат и прямого хищения были уволены с работы около 11 % сотрудников. Нарушение соглашения о неразглашении служебной, коммерческой или иной охраняемой законом тайны явилось причиной увольнения в 10 % от общего числа [83].

.

Рис. 9. Основные причины увольнений в 2016 году

3.2.2. Формальные средства обеспечения безопасности информации

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

Реализуется следующими средствами:

- охранная и охранно-пожарная сигнализация;
- охранное телевидение и наблюдение;
- инженерно-технические средства защиты объектов;

- средствами управления доступом к информации;

- охрана периметра;

- система оповещения и т. д.

Физические средства защиты информации выполняют следующие **функции**:

- *внешняя защита* – защита от воздействия дестабилизирующих факторов, проявляющихся за пределами основных средств объекта;

- *внутренняя защита* – защита от дестабилизирующих факторов, проявляющихся непосредственно в средствах обработки информации;

- *опознавание* – специфическая группа средств, предназначенных для опознавания людей и идентификации технических средств по различным индивидуальным характеристикам;

- организация режима *охраны объектов*;

- организация *пропускного режима*;

- организация *противопожарной защиты*.

Системывидеонаблюдения(CCTV), илиохранноетелевидение

Система видеонаблюдения – это интегрированный комплекс специальных технических средств безопасности, обеспечивающих непрерывный визуальный контроль за конкретным объектом (всей территории или отдельных ее частей) с целью фиксации и своевременного реагирования на нештатные события и противоправные действия.

Установка комплексной системы видеонаблюдения на объекте позволяет эффективно выполнять целый ряд важнейших функций:

- постоянный визуальный мониторинг территории, прилегающей области, помещений, стратегически важных зон объекта;

- оперативный контроль обстановки и всех событий на объекте: технологического процесса, действий персонала и посетителей, перемещений материальных ценностей, транспорта и механизмов и т. д.;

- выявление и фиксация противоправных посягательств, хищений, попыток несанкционированного проникновения, а также в комплексе с другими структурными средствами безопасности пресечение таких попыток;

- осуществление контроля въезда/выезда автотранспорта, ввоза/вывоза материальных ценностей (с распознаванием и фиксацией номерных знаков автомобилей);

- оказание психологического воздействия на потенциальных нарушителей и преступников, предупреждающее противоправные поступки;

- возможность осуществления не только визуального контроля, но и фиксации, архивирования и хранения информации для последующего использования.

Стремительный переход от аналоговых схем передачи информации к цифровым изменил архитектуру построения видеосистем безопасности. На смену аналоговым системам пришли цифровые распределенные, децентрализованные системы. Передача видеоинформации в цифровом формате позволяет избежать искажения и потери качества сигнала, независимо от расстояния и способа транспортировки его по каналам связи [84].

Видеосигналы от телевизионных камер, установленных в локальных зонах наблюдения, поступают на локальные видеосерверы. Локальный видеосервер осуществляет сбор, обработку и накопление видеоинформации, оцифровку аналогового сигнала, видеодетекцию движения, компрессию видеоизображения, запись по тревоге от других систем безопасности или от детектора движения. Далее по высокоскоростному магистральному интерфейсу (Fast Ethernet или Gigabit Ethernet) поток видеоинформации поступает на пульт видеоконтроля (рабочее место оператора). Оператор, в зависимости от конкретной задачи, может наблюдать за каждой локальной зоной на компьютерном мониторе. Причем наблюдение ведется в разных режимах: полный экран либо полиэкран со свободно настраиваемым размером окна для любого количества видеокамер. Каждое окно может сопровождаться текстовым заголовком с указанием времени, даты и состоянии видеокамеры. Оператор может осуществлять сохранение необходимой информации на различного рода носителях информации (рис. 10). При необходимости оператор может распечатать интересующую его информацию на лазерном или видеопринтере.

Рис. 10. Цифровые системы видеонаблюдения

Система видеонаблюдения может иметь ряд вспомогательных функций, например, дистанционный контроль объекта с применением беспроводных систем, использующих для передачи информации сети Wi-Fi, 3G и GPRS. Это существенно упрощает монтаж системы, позволяет располагать видеокамеры в нестандартных местах, обеспечивая большую полноту обзора местности. При этом оператор, имеющий соответствующие полномочия, может наблюдать за происходящим на объекте с помощью обычного мобильного телефона или ноутбука из любой точки мира.

Профессиональная система мониторинга автоматически реагирует на малейшее движение, подавая сигнал тревоги и записывая изображение в архив. Некоторые системы настраиваются на заданные характеристики движущихся

объектов, например, система может не реагировать на проходящих через ворота предприятия людей, но подает сигнал тревоги при приближении автомобиля. Современные видеокамеры воспринимают окружающее пространство не только в том спектре, что и человеческий глаз, но также в инфракрасных лучах, что делает возможным использование систем при слабом освещении и его отсутствии.

Монтаж систем безопасности, как правило, не ограничивается только видеонаблюдением, нередко осуществляется интеграция с системами контроля доступа (СКУД).

IP-видеонаблюдение

IP-видеонаблюдение – относительно новое перспективное направление развития рынка безопасности, основанное на высокоэффективных алгоритмах сжатия и передачи информации по сетям TCP/IP, что позволяет вести эффективное круглосуточное наблюдение удаленного объекта или группы территориально распределенных объектов. Одновременно могут контролироваться в реальном масштабе времени десятки, сотни и даже тысячи камер видеонаблюдения, также может обеспечиваться непрерывная запись происходящих событий на цифровые носители. IP-камеры могут быть установлены в любом месте, где есть сеть LAN, или подключены напрямую, через модем или сотовый телефон [85].

При устройстве IP-видеонаблюдения работа осуществляется только с цифровыми данными, которые передаются и обрабатываются в общей сети. Аналоговый видеосигнал оцифровывается IP-камерой или IP-видеосервером, и в дальнейшем данные могут быть записаны на любой (даже удаленный) видеорегистратор. Просмотр получаемого изображения в режиме «онлайн» осуществляется через web-браузер, подключенный к сети персональный компьютер или на экране охранных мониторов через IP-сервер.

Охранно-пожарнаясигнализация

Системы охранной и пожарной сигнализации могут быть установлены на объектах как совместно, так и по отдельности. Основной задачей охранной сигнализации является выявление факта вторжения на подконтрольную территорию и активизация сигнальных устройств на пульте сигнализации на посту охраны или предупредительных устройств на местах (светового сигнала, звуковой сирены). Основной задачей системы пожарной сигнализации является обнаружение места возникновения очага возгорания на ранней стадии, оповещение о пожаре находящихся на объекте людей, формирование управляющих сигналов для систем автоматического пожаротушения, для инженерных систем здания (отключения вентиляции, включения систем дымоудаления, опускания лифтов и т. д.).

Приемные устройства сигнализации, расположенные на пульте управления, служат для приема тревожного сигнала от охранных и пожарных извещателей и определения конкретного места происшествия (номера охраняемой зоны, с которой был принят сигнал) [86].

Современная охранно-пожарная сигнализация имеет собственную развитую функцию оповещения. Благодаря возможности гибкой интеграции с различными системами безопасности и жизнеобеспечения здания, охранно-пожарная сигнализация может быть настроена на выполнение самых разнообразных задач в случае обнаружения пожара, несанкционированного проникновения или неисправности в одной из зон. Например, при возникновении пожарной тревоги панель пожарной сигнализации может автоматически осуществлять отключение электропитания в зоне пожара, включение системы пожаротушения, дымоудаления, разблокировку выходов на путях эвакуации и одновременное включение системы оповещения с информацией для мест возгорания и смежных с ней зон.

Все охранные и пожарные сигнальные системы построены по схожей схеме (рис. 11).

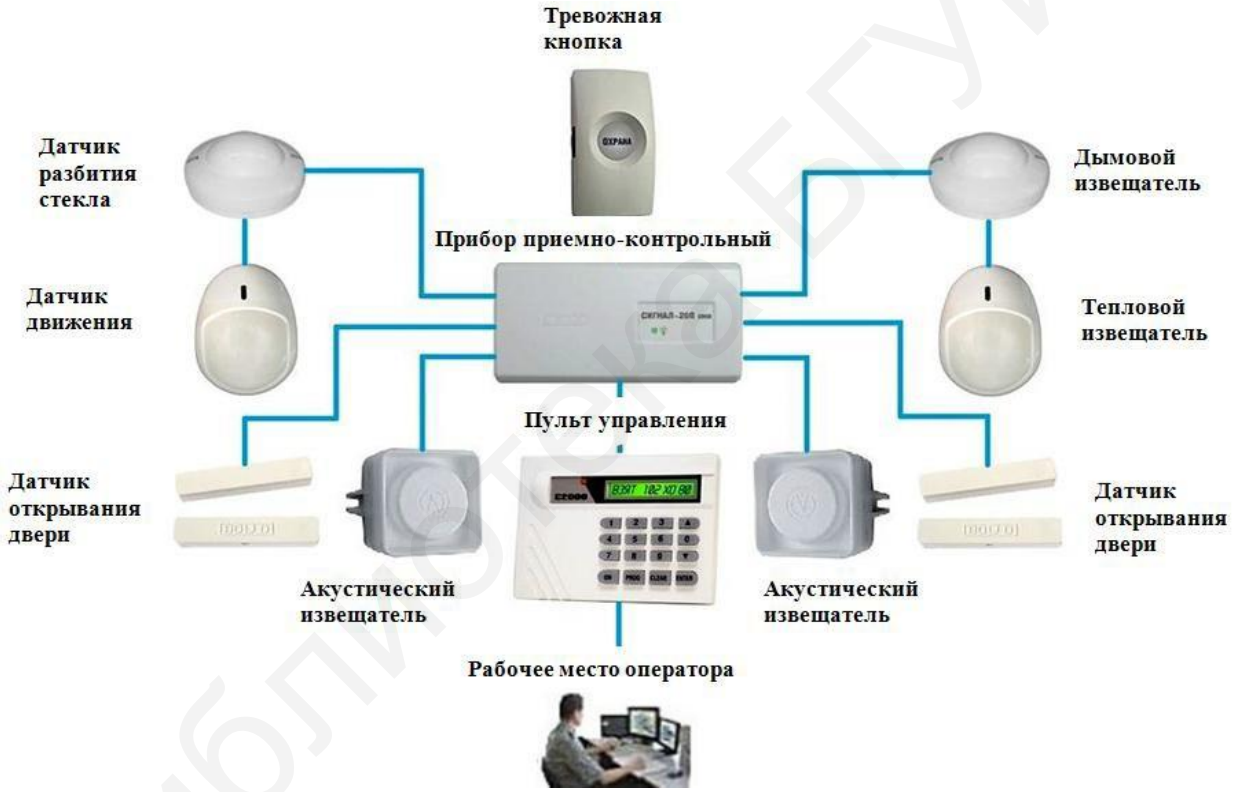

Рис. 11. Охранно-пожарная сигнализация

Набор датчиков распределен по помещениям в соответствии с определенным планом разбивки его на охраняемые зоны, за каждую из которых отвечает один или несколько датчиков. Все датчики связаны сигнальными шлейфами с центральным устройством – контрольной панелью (пультом управления) сигнализации. Системы охранной и пожарной сигнализации снабжаются резервными источниками питания, обеспечивающими бесперебойное функционирование систем при отключении напряжения основного источника питания.

Система сигнализации может программироваться непосредственно с пульта управления при помощи встроенной клавиатуры или через управляющее программное обеспечение, установленное на компьютере. Назначение кон-

трольной панели сигнализации – распознать тревожный сигнал, поступивший от сработавших датчиков, идентифицировать опасную зону.

Все элементы системы сигнализации могут быть подключены по беспроводной технологии, что позволяет в любой момент изменить конфигурацию расположения датчиков, не прибегая к прокладке кабеля.

К *техническим средствам* охранно-пожарной сигнализации относятся:

- охранно-пожарные извещатели (датчики);
- охранно-пожарные приемно-контрольные приборы и пульты (панели), исполняющие устройства (пожарные и охранные сигнально-пусковые устройства, GSM- и коммуникационные модули оповещения, приборы управления);
- охранно-пожарные оповещатели (световые и звуковые сирены, указатели эвакуации);
- тревожная кнопка;
- специальные источники бесперебойного питания.

Типы датчиков для систем *пожарной* сигнализации: дымовые, тепловые, комбинированные, ручные, а также специальные извещатели пламени, линейные инфракрасные и аспирационные системы.

Типы датчиков для системы *охранной* сигнализации:

- магнитно-контактные датчики (герконы) открытия двери, окна, форточки и т. д.;
- пассивные инфракрасные датчики движения;
- активные инфракрасные датчики движения;
- акустические датчики разбития стекла;
- вибрационные извещатели для определения разрушения или пролома поверхности;
- емкостные извещатели для определения прикосновения к охраняемому объекту;
- радиоволновые датчики для контроля внутреннего объема помещения;
- датчики утечки воды;
- датчики утечки газа;
- датчики температуры;
- датчик отключения электричества.

Системы сигнализации могут быть автономными или заведены на пульт сигнализации на посту охраны. Автономные системы сигнализации могут иметь различные каналы передачи тревожного сигнала: по телефонной линии, по радиоканалу, по GSM-каналу.

Охрана периметра объекта

Технические средства системы охраны периметра – датчики – основываются на различных методах обнаружения нарушителя, например, на определении пересечения лучей, изменении температуры среды охраны, вибрации забора или проволоки, изменении плотности контролируемой среды, подкопе, пролазе и пр. [87].

Принцип работы систем охраны периметра достаточно прост и учитывает изменение параметров электрического поля при приближении или прикосновении нарушителя. Технически система представляет собой электрический контур, подключенный к контрольному устройству. При изменении параметров безопасности, например, при касании проводника или при приближении к нему человека, система охраны периметра посылает сигнал о нарушении границы периметра на центральный пост охраны либо на пульт управления вневедомственной охраны. В настоящий момент техника охраны периметра настолько разнообразна, что позволяет организовать эффективную защиту любого периметра без полосы отчуждения и предварительной очистки рубежей, а также не только зафиксировать факт проникновения на территорию, но и определить место нарушения границы, т. е. конкретный участок периметра, что немаловажно при защите периметра большой протяженности (рис. 12).

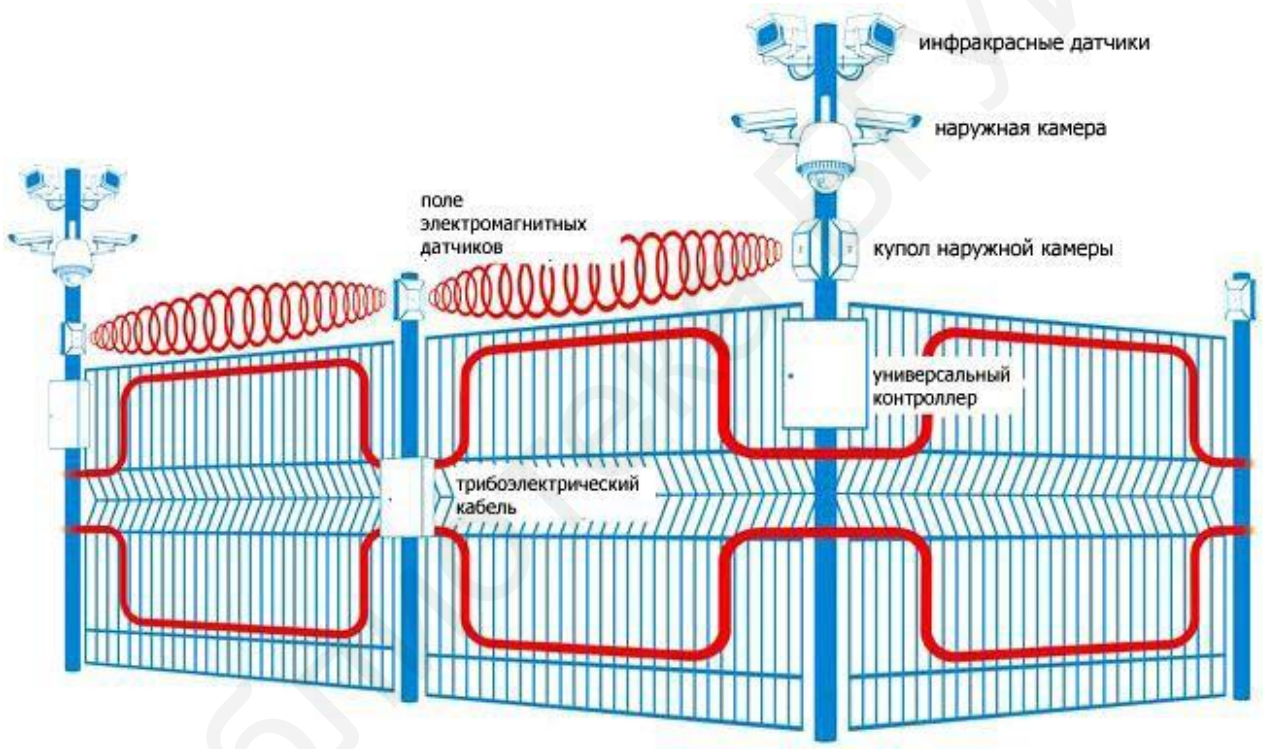

Рис. 12. Система охраны периметра

Для надежной и эффективной охраны периметра система должна устойчиво функционировать в условиях сложной помеховой обстановки. Помехи могут быть природного (метеофакторы, мелкие животные) и промышленного происхождения (высоковольтные линии, близкопролегающие автомобольные трассы или железнодорожные пути). Система охраны периметра должна обеспечивать защиту от попыток преодоления заградительных препятствий методами подкопа, перелаза или его разрушения, а также обнаруживать перемещение металлических предметов (режущих инструментов, оружия). Поэтому еще на стадии предпроектного обследования инженер должен учесть множество факторов: рельеф местности, климатическую зону, наличие заграждения, конструкцию заграждения, наличие растительности и построек вдоль периметра и др.

Системы охраны периметра относятся к средствам раннего обнаружения, которые позволяют выявить нарушителя еще до его проникновения на охраняемую территорию. Если использовать системы охраны периметра одновременно с интеллектуальными системами видеонаблюдения, можно не только вести непрерывный визуальный контроль за обстановкой, но и фиксировать нештатные события и противоправные действия, а также сохранять и передавать видеоинформацию удаленным пользователям.

Системаконтролядоступа(СКУД)

Системы контроля и управления доступом как часть охранной и учетной системы эффективны и многофункциональны. Такие системы используются как для ограничения пропускного режима в закрытые для посторонних зоны, контроля за передвижением персонала, поиска требуемого сотрудника в любой момент времени, так и в качестве учета времени прихода/ухода сотрудника и количества отработанного времени в целом. При попытке несанкционированного прохода происходит мгновенное извещение службы охраны объекта. Для массового прохода на общую территорию объекта используют автоматические турникеты и шлагбаумы, оснащенные различными системами контроля доступа. Системы просты в использовании, что позволяет легко и быстро обучить персонал работе с охранным комплексом.

В систему контроля доступа входят [88]:

- средства управления доступом (автономные или сетевые контроллеры, кодовые панели, считыватели, картоприемники);
- исполняющие устройства (электронные замки и доводчики на двери, турникеты, шлагбаумы, ворота, контрольно-пропускные шлюзы и т. д.);
- персональные индификаторы (магнитная карточка, ключи Touch Memory, бесконтактные карты Proximiti);
- программное компьютерное обеспечение с базой данных и статистикой проходов.

На платформе систем контроля и управления доступом часто создаются интегрированные системы, объединяющие в единый комплекс системы охранно-пожарной сигнализации, видеонаблюдения, ограничения доступа, жизнеобеспечения зданий. Простейшие системы контроля доступа можно построить с помощью домофонов, электрозамков и кодовых панелей на входных дверях.

Новые технологии для систем контроля доступа в настоящее время развиваются по направлениям: биометрические системы идентификации СКУД и бесконтактные смарт-карты [89].

Схема типовой системы контроля доступа приведена на рис. 13.

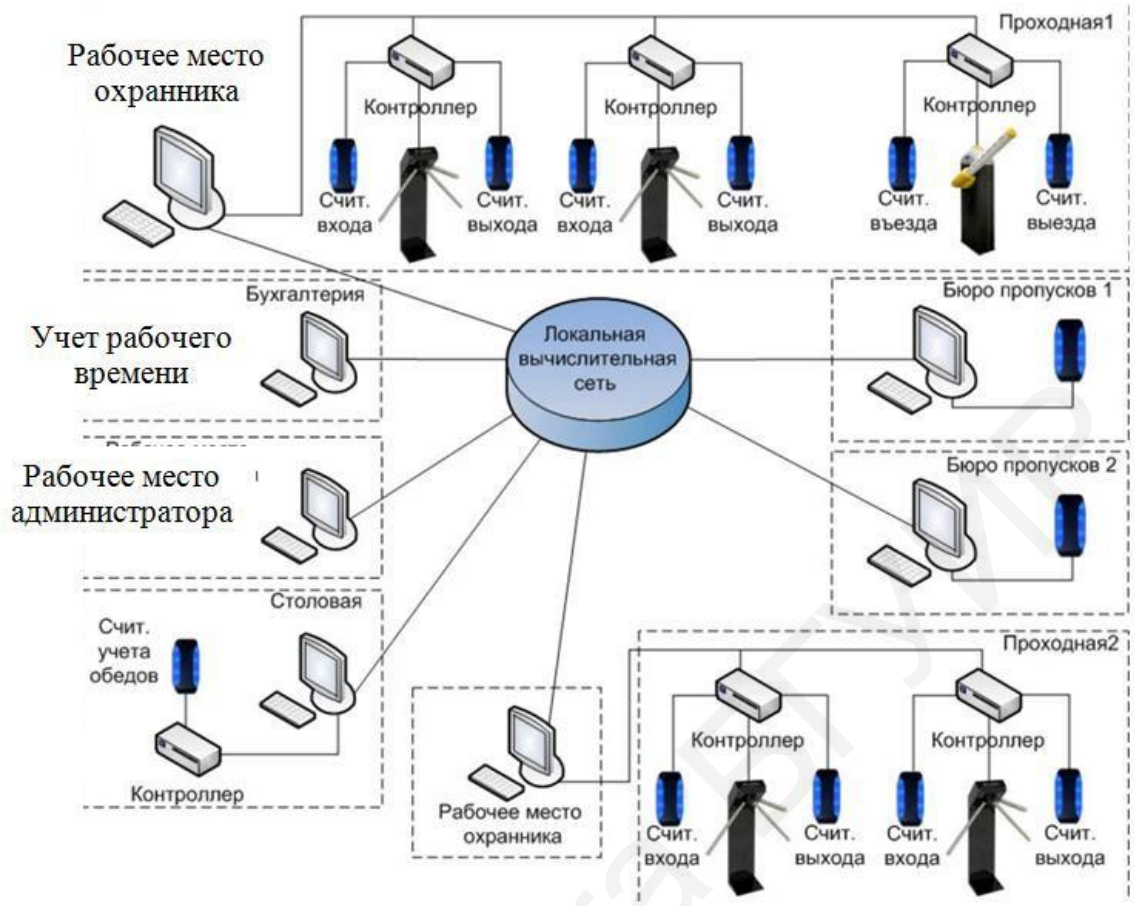

Рис. 13 Система контроля доступа

Домофоны

Домофоны являются наиболее простыми устройствами контроля доступа и обеспечения безопасности квартиры, подъезда жилого дома, небольшого офиса или частного дома и состоят из видеомонитора и наружной видеопанели. Основным назначением домофона является обеспечение возможности увидеть по монитору посетителей и переговорить с ними перед тем, как открыть дверь. Домофон оборудуется дополнительными исполняющими устройствами: электронными дистанционно управляемыми замками и доводчиками на двери.

Системыоповещения

Системы речевого оповещения и управления эвакуацией (СОУЭ) предназначены для голосового предупреждения людей при пожаре, стихийных бедствиях и других чрезвычайных и аварийных ситуациях, что приводит к сокращению времени их эвакуации.

Большинство систем оповещения строится по модульному принципу. В зависимости от архитектурных особенностей здания и его назначения система оповещения может включать в себя устройства, предназначенные для экстренной трансляции, или дополняться модулями, служащими для повышения качества звука.

Существуют системы музыкального, информационного озвучивания помещений и системы оповещения сотрудников и посетителей о чрезвычайной ситуации; некоторые системы объединяют в себе все перечисленные функции. В случае поступления сигнала тревоги трансляция общего назначения прерывается, и система воспроизводит оповещение об экстренном случае.

Технические средства защиты информации включают в себя различные электронные, электронно-механические и тому подобные устройства, встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач по защите информации.

Технические средства предназначены для нейтрализации **технических каналов утечки информации** (радиоканал, ПЭМИН, акустические каналы, оптические каналы и др.), защиты информации от утечки, поиска закладных устройств съема информации, маскировки сигнала, содержащего конфиденциальную информацию.

Примечание. **Технические каналы утечки информации** представляют собой совокупность источника информации, физической среды распространения информационного сигнала, шумов, препятствующих передаче сигнала в физической среде, и технических средств перехвата информации.

С точки зрения утечки информации, электромагнитные, оптические, тепловые и акустические каналы утечки информации представляют наибольшую угрозу, что связано с возможностью скрытого получения информации о защищаемых объектах на значительном расстоянии.

Электромагнитныйканалутечкиинформации

К электромагнитным относятся каналы утечки информации, возникающие за счет появления в окружающем пространстве побочных электромагнитных излучений и наводок (ПЭМИН) при функционировании технических средств приема, обработки, хранения и передачи информации.

При возникновении электромагнитных излучений технических устройств либо при передаче информации по функциональному каналу связи (например, радиоканалу) возможна утечка информации посредством перехвата опасных сигналов (рис. 14) [90].

Рис. 14. Структурная схема электромагнитного канала утечки информации

За счет ПЭМИН на соединительных линиях вспомогательных технических средств и посторонних проводниках, выходящих за пределы контролируемой зоны, возникает электрический канал утечки информации технических средств передачи информации (ТСПИ)

В индукционном канале используется эффект возникновения вокруг кабеля связи электромагнитного поля при прохождении по нему информационных электрических сигналов, которые перехватываются специальными индук-

ционными датчиками в основном для съема информации с симметричных высокочастотных кабелей.

Для бесконтактного съема информации с незащищенных телефонных линий связи могут использоваться специальные высокочувствительные низкочастотные усилители, снабженные магнитными антеннами.

Параметрический электромагнитный канал может возникать в процессе облучения технических средств передачи информации побочными электромагнитными излучениями, вследствие чего может возникнуть переизлучение электромагнитного излучения, которое будет содержать информацию, обрабатываемую в технических средствах передачи информации.

Оптическийканалутечкиинформации

Отражательная способность объектов наблюдения, зависящая от длины волны падающего света, является источником информации в оптическом канале. Структура оптического канала утечки информации представлена на рис. 15.

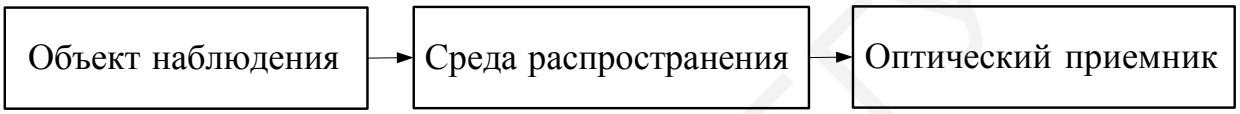

Рис. 15. Структурная схема оптического канала утечки информации

В оптических каналах утечка информации осуществляется посредством электромагнитного поля (фотонов) в диапазоне 0,46…0,76 мкм (видимый свет) и 0,76…3 мкм (инфракрасные излучения) посредством использования различных оптических приборов, позволяющих уменьшить величину порогового контраста объекта на окружающем фоне.

Источники информации в видимом и ИК-диапазонах оптических каналов утечки информации характеризуются следующими показателями:

- диапазоном длин волн 0,38…0,76 мкм в видимом диапазоне, 0,76…3 мкм – в ближнем ИК-диапазоне, 3…6 мкм – в среднем ИК-диапазоне, 8…14 мкм – в дальнем ИК-диапазоне;
- освещенностью объектов наблюдения внешним (солнечным) светом 10^{-5}…10^{5} лк [91, 92].

Распространение оптического излучения в атмосфере сопровождается линейными и нелинейными взаимодействиями света со средой, которые можно разделить на три основные группы:

- поглощение и рассеяние молекулами газов воздуха;
- ослабление на аэрозолях (пыль, дождь, снег, туман);
- флуктуации излучения на турбулентностях атмосферы [93, 94, 95].

Защита объектов в видимом диапазоне длин волн на фоне подстилающей поверхности во многом определяется цветом грунта и пигментами растительности. В частности, содержащийся в зеленых растениях хлорофилл определяет величину отражения солнечных лучей в выделенной части спектра. Спектральная яркость растительных объектов (травяных покровов, леса) и почв в оптическом диапазоне длин волн во многом определяются составом пигментов, струк-

турой клеток и листьев, содержанием воды и наличием плесневых микроорганизмов. Так, спектральные характеристики растительности содержат несколько характерных полос поглощения электромагнитного излучения, в соответствии с перечисленными факторами.

Отражательная способность влагосодержащих поверхностей в 2,7 раза меньше по сравнению с безводными поверхностями в видимой части спектра [96].

Тепловойканалутечкиинформации

Тепловые каналы утечки информации позволяют получить информацию об объектах путем приема и анализа электромагнитных волн ИК-диапазона, излученных и отраженных объектами и предметами на общем фоне.

Различают *видовое* и *параметрическое* ИК-обнаружение. *Видовое* ИК-обнаружение обеспечивает получение информации в виде изображений различных объектов и местности, а *параметрическое* ИК-обнаружение обеспечивает получение информации, содержащейся в пространственных и излучательных характеристиках различных объектов и местности. Пассивные средства теплового обнаружения обеспечивают получение визуального изображения земной поверхности и наземных объектов, имеющих различную температуру или излучательную способность, а также позволяют определить направление на источник ИК-излучения и определить его температурный контраст по отношению к окружающему фону. Получение информации об объектах посредством теплового обнаружения актуально в ночное время суток, когда наземные объекты не отражают солнечного света.

Дальность обнаружения объектов тепловыми средствами обнаружения определяется температурой нагрева их поверхностей. Большинство средств теплового обнаружения работают в спектральных диапазонах 3…5,5 мкм и 8…14 мкм, соответствующих окнам прозрачности атмосферы и максимальной излучательной способности наблюдаемых объектов в наиболее часто используемом температурном диапазоне от –50 до +500 °С [97].

Проходя через земную атмосферу, ИК-излучение ослабляется в результате рассеяния и поглощения. В приземных слоях атмосферы в средней инфракрасной области имеется лишь небольшое число «окон», прозрачных для ИК-излучения (рисунок 16).

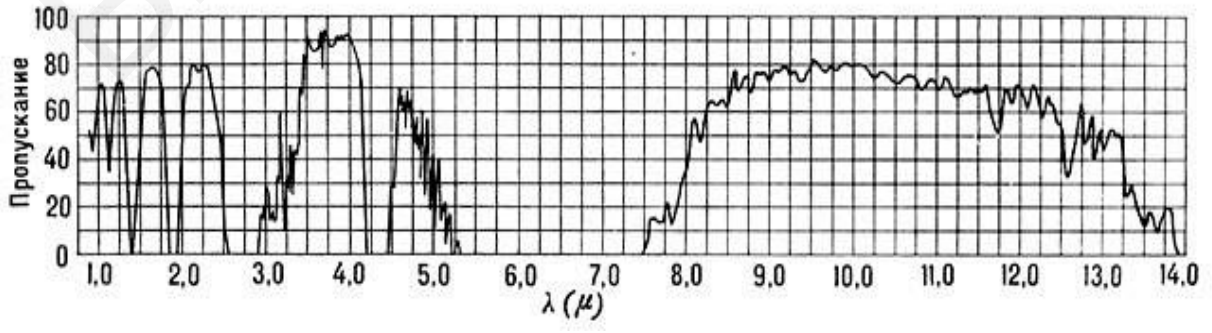

Рис. 16. Кривая пропускания атмосферы в области 0,6…14 мкм

Полосы «окна» прозрачности составляют: 2,0…2,5 мкм, 3,2…4,2 мкм, 4,5…5,2 мкм, 8,0…13,5 мкм. Полосы поглощения с максимумами при L = 0,93; 1,13; 1,4; 1,87; 2,74 мкм принадлежат парам воды; при L = 2,7; 4,26 мкм – углекислому газу; при L = 9,5 мкм – озону.

Тепловизоры регистрируют ИК-излучение всех объектов с температурой выше абсолютного нуля. Длины волн излучения среднего и дальнего ИК-диапазонов, на которых работают современные тепловизоры, находятся в пределах 3…5 мкм и 8…12 мкм. Обнаружение происходит за счет сравнения температуры объекта с температурой окружающей среды. Основные характеристики ИК-сигналов любого объекта: абсолютная температура, коэффициент излучения поверхностей объекта и количество тепла, выделяемого объектом.

Акустическиеканалыутечкиинформации

Прямойакустическийканал

Наиболее простым способом перехвата речевой информации является подслушивание (прямой перехват). Разведываемые акустические сигналы могут приниматься непосредственно ухом человека, реагирующим на изменение звукового давления, возникающего при распространении звуковой волны в окружающем пространстве. Диапазон частот акустических колебаний, слышимых человеком составляет от 16…25 Гц до 16…18 кГц в зависимости от индивидуальных особенностей слушателя. Человек воспринимает звук в очень широком диапазоне звуковых давлений, одной из базовых величин этого диапазона является стандартный порог слышимости. Под ним условились понимать эффективное значение звукового давления, создаваемого гармоническим звуковым колебанием частотой F = 1000 Гц, едва слышимым человеком со средней чувствительностью слуха. Порогу слышимости соответствует звуковое давление $P = 2 \cdot 10^{-5}$ Па. Верхний предел определяется значением P = 20 Па, при котором наступает болевое ощущение (стандартный порог болевого ощущения) [98].

В случаях, когда уровни звукового давления, создаваемого звуковой волной, ниже порога слышимости (отсутствие возможности непосредственно прослушивать речевые сообщения или требуется их зафиксировать), используют микрофон.

Микрофон является преобразователем акустических колебаний в электрические сигналы. В зависимости от физического явления, приводящего к такому преобразованию, различают основные типы микрофонов:

- электродинамические;
- электромагнитные;
- электростатические;
- пьезоэлектрические;
- магнитострикционные;
- контактные и т. д.

К микрофонам, используемым в технике акустической разведки, предъявляют высокие требования. Преобразование звука в электрический сигнал должно осуществляться с высокой информационной точностью, необходимо обеспечить высокую разборчивость и узнаваемость речевого сигнала, избежать

появления различных искажений в пределах динамического диапазона в заданной полосе частот. Кроме того, микрофоны должны обладать направленными свойствами, высокой чувствительностью и приемлемыми массогабаритными характеристиками.

При необходимости передать перехваченное речевое сообщение на расстояние используют проводные, радио- и другие каналы, по которым сообщение, преобразованное в электрический, оптический, радио- или другого вида сигнал, передается на пункт прослушивания. В этих случаях используемые устройства называются закладными устройствами для перехвата акустической информации. В состав радиозакладки может быть включено запоминающее устройство, в которое предварительно записывается перехваченная речевая информация. Ее передача в пункт прослушивания в этом случае осуществляется не в реальном масштабе времени, а с определенной временной задержкой, что повышает скрытность радиозакладных устройств.

Структурная схема, иллюстрирующая прямой перехват акустической информации, представлена на рис. 17.

К настоящему времени разработано достаточно большое количество типов направленных микрофонов и закладных подслушивающих устройств.

Рис. 17. Структурная схема процесса перехвата акустической информации

Виброакустическийканал

Воздействие акустических волн на поверхность твердого тела приводит к возникновению в нем вибрационных колебаний в результате виброакустиче-

ского преобразования. Эти колебания, распространяющиеся в твердой среде, могут быть перехвачены специальными средствами разведки, а речевая информация, содержащаяся в акустическом поле, при определенных условиях может быть восстановлена. С этой целью используют устройства, преобразующие вибрационные колебания в электрические сигналы, соответствующие звуковым частотам, – вибродатчики. Сигнал, снимаемый с выхода вибродатчика, после усиления может быть прослушан, зарегистрирован на магнитном или другом носителе или передан в пункт приема, находящийся на удалении от места прослушивания, по проводному, радио- или иному каналу передачи информации. Обобщенная структурная схема виброакустического канала утечки информации представлена на рис. 18.

В целях ведения разведки с использованием виброакустического канала широко применяются стетоскопы, т. е. устройства, содержащие вибродатчик (стетоскопный микрофон), блок обработки сигнала, осуществляющий его усиление и ослабление помех, и головные телефоны. В ряде таких устройств предусмотрена возможность записи сигнала на магнитный носитель [99].

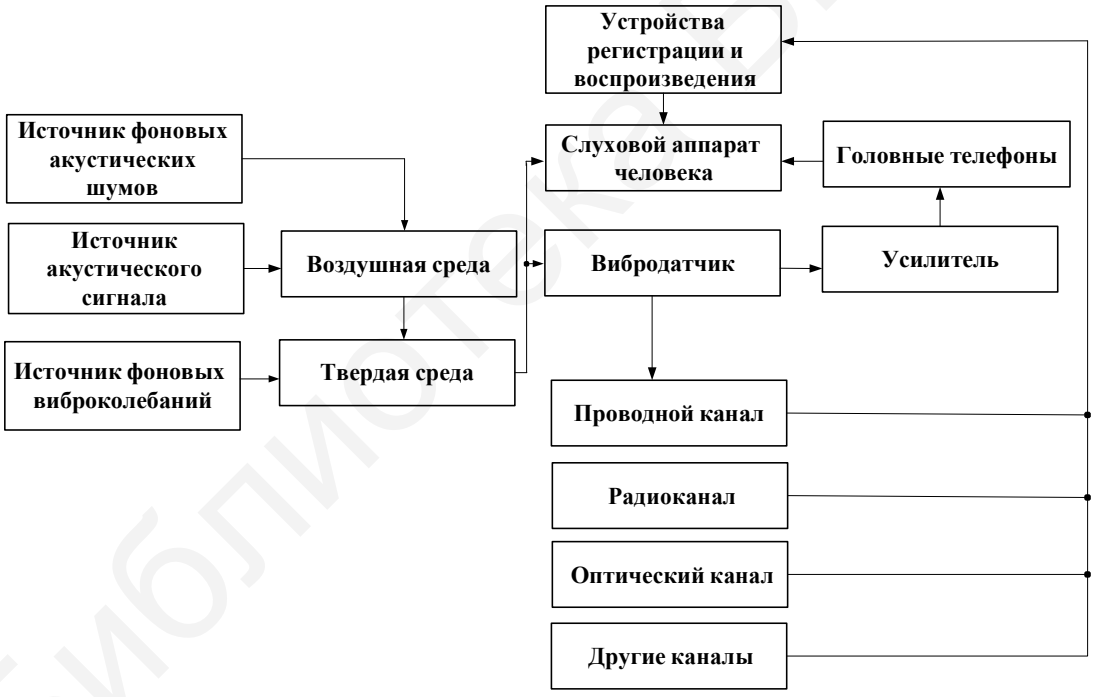

Рис. 18. Структурная схема виброакустического канала

Необходимо отметить, что чем тверже материал преграды на пути распространения акустических колебаний, тем лучше он передает вибрации, вызываемые ими. Вибродатчик обычно крепится к металлическому предмету, вмонтированному в стену. В качестве звукопровода могут использоваться трубы водоснабжения, канализации, батареи отопления и т. д. На качество приема вибросигналов, кроме свойств вибродатчика и материала твердой среды, влияют

ее толщина, а также уровни фоновых акустических шумов в помещении и вибраций в твердой среде.

В ряде случаев, когда нет возможности разместить пункт прослушивания в непосредственной близости от места установки вибродатчика (стетоскопа), в состав аппаратуры прослушивания включают проводные, радио- и другие каналы передачи информации, аналогичные каналам, используемым в закладных устройствах.

Оптико-акустическийканал

Перехват речевой информации из помещений может осуществляться с помощью лазерных средств акустической разведки. В этом случае применяется дистанционное лазерно-локационное зондирование объектов, обладающих определенными свойствами и являющихся потенциальными источниками конфиденциальной речевой информации. В качестве таких объектов могут выступать оконные стекла и другие виброотражающие поверхности.

Генерируемое лазерным передатчиком колебание наводится на оконное стекло помещения. Возникающие при разговоре акустические волны, распространяясь в воздушной среде, воздействуют на оконное стекло и вызывают его колебания в диапазоне частот, соответствующих речевому сообщению. Таким образом, происходит виброакустическое преобразование речевого сообщения в мембране, роль которой играет оконное стекло. Лазерное излучение, падающее на внешнюю поверхность оконного стекла (мембраны), в результате виброоптического преобразования оказывается промодулированным сигналом, вызывающим колебания мембраны. Отраженный оптический сигнал принимается оптическим приемником, в котором осуществляется восстановление сообщения.

На рис. 19 приведена обобщенная структурная схема оптико-акустического канала перехвата речевой информации. К настоящему времени созданы различные системы лазерных средств акустической разведки, имеющие дальность действия от десятков метров до единиц километров. Наведение лазерного излучения на оконное стекло нужного помещения осуществляется с помощью телескопического визира. Использование специальной оптической насадки позволяет регулировать угол расходимости выходящего светового пучка.

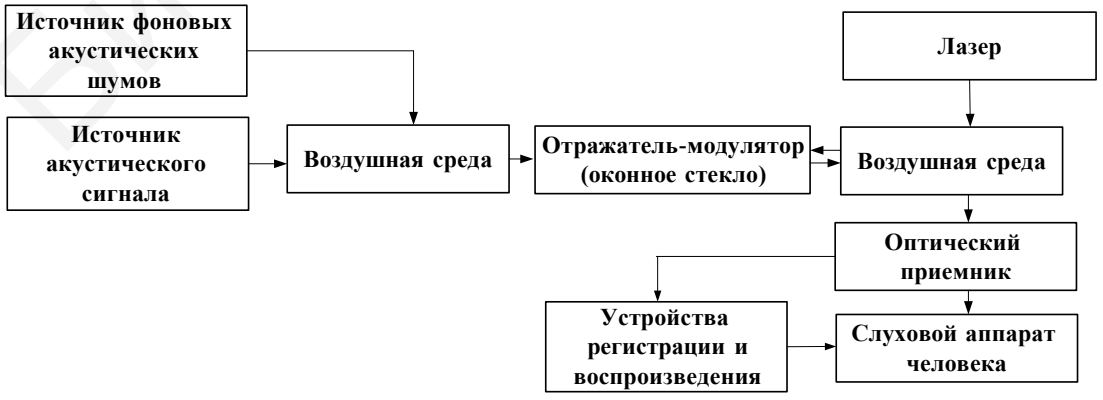

Рис. 19. Структурная схема оптико-акустического канала

К устройствам лазерной акустической разведки предъявляются высокие требования с точки зрения их помехоустойчивости, поскольку качество перехватываемой информации существенно зависит от наличия и уровней фоновых акустических шумов, помеховых вибраций отражателя-модулятора, а также ослабления лазерного излучения в атмосфере и фоновой оптической засветки при приеме отраженного от объекта сигнала.

От каждого источника защищаемая информация по техническим каналам утечки может попасть к нарушителю. Нарушители, совершая действия с преднамеренными или непреднамеренными угрозами и используя соответствующие способы реализации угроз, осуществляют несанкционированный доступ по техническим каналам утечки к защищаемой информации.

Для защиты информации от угроз информационной безопасности, осуществления несанкционированного доступа (НСД) по техническим каналам утечки на каждом объекте информатизации разрабатывается и применяется комплексная система защиты информации от несанкционированного доступа – КСЗИ НСД, объединяемая в подсистему информационной безопасности (табл. 5).

Утечку информации в общем плане можно рассматривать как бесконтрольный и неправомерный выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация была доверена. Показательно, что наиболее опасными являются электромагнитные каналы утечки информации, охватываемые шестью способами НСД. Более того, в обиход уверенно вошло такое понятие, как «магнитный терроризм» – воздействие на объект электромагнитным полем.

Таблица 5

Взаимосвязь способов НСД и каналов утечки информации

Способы несанкционированного доступа	Типы технических каналов утечки информации			
	Визуально-оптические	Акустические	Электромагнитные	Материально-вещественные
Подслушивание	–	+	+	–
Визуальное наблюдение	+	–	–	–
Хищение	–	–	+	+
Копирование	–	–	+	+
Подделка	–	–	+	+
Незаконное подключение	–	+	+	–
Перехват	–	+	+	–
Фотографирование	+	–	–	–
Всего	2	3	6	3

Любые технические средства потенциально могут создавать технические каналы утечки информации, что расширяет возможности не только использования этих средств, но и несанкционированного съема информации.

Рассмотрим относительно полное множество каналов несанкционированного получения информации, сформированного на основе такого показателя, как степень взаимодействия злоумышленника с элементами объекта обработки информации и самой информацией [100].

К **первому классу** относятся каналы от источника информации при НСД к нему:

- хищение носителей информации;
- копирование информации с носителей (материально-вещественных, магнитных и т. д.);
- подслушивание разговоров (в том числе аудиозапись);
- установка закладных устройств в помещение и съем информации с их помощью;
- выведывание информации у обслуживающего персонала на объекте;
- фотографирование или видеосъемка носителей информации внутри помещения.

Ко **второму классу** относятся каналы со средств обработки информации при НСД к ним:

- снятие информации с устройств электронной памяти;
- установка закладных устройств в системах обработки информации;
- ввод программных продуктов, позволяющих злоумышленнику получать информацию;
- копирование информации с технических устройств отображения (фотографирование с мониторов и др.).

К **третьему классу** относятся каналы от источника информации без НСД к ним:

- получение информации по акустическим каналам (в системах вентиляции, теплоснабжения, а также с помощью направленных микрофонов);
- получение информации по виброакустическим каналам (с использованием акустических датчиков, лазерных устройств);
- использование технических средств оптической разведки (биноклей, подзорных труб и т. д.);
- использование технических средств оптико-электронной разведки (внешних телекамер, приборов ночного видения и т. д.);
- осмотр отходов и мусора;
- выведывание информации у обслуживающего персонала за пределами объекта;
- изучение выходящей за пределы объекта открытой информации (публикаций, рекламных проспектов и т. д.).

К **четвертому классу** относятся каналы со средств обработки информации без НСД к ним:

- электромагнитные излучения систем обработки информации (паразитные ЭМИ, паразитная генерация усилительных каскадов, паразитная модуляция высокочастотных генераторов низкочастотным сигналом, содержащим конфиденциальную информацию);

- ЭМИ линий связи;
- подключения к линиям связи;
- снятие наводок электрических сигналов с линий связи;
- снятие наводок с системы питания;
- снятие наводок с системы заземления;
- снятие наводок с системы теплоснабжения;
- использование высокочастотного навязывания;
- снятие с линий, выходящих за пределы объекта, сигналов, образованных на технических средствах за счет акустоэлектрических преобразований;
- снятие излучений оптоволоконных линий связи;
- подключение к базам данных и ПЭВМ.

Таким образом, защита информации от утечки по **каналам связи** может быть обеспечена следующими средствами и мероприятиями:

- использование экранированного кабеля и прокладка проводов и кабелей в экранированных конструкциях;
- установка на линиях связи высокочастотных фильтров;
- построение экранированных помещений («капсул»);
- использование экранированного оборудования;
- установка активных систем зашумления;
- создание контролируемых зон.

Защита информации в **каналах компьютерной сети** (рис. 20) может быть улучшена за счет использования специальных генераторов шума, маскирующих побочные электромагнитные излучения и наводки, помехоподавляющих сетевых фильтров, устройств зашумления сети питания, скремблеров (шифраторов телефонных переговоров), подавителей работы сотовых телефонов и т. д.

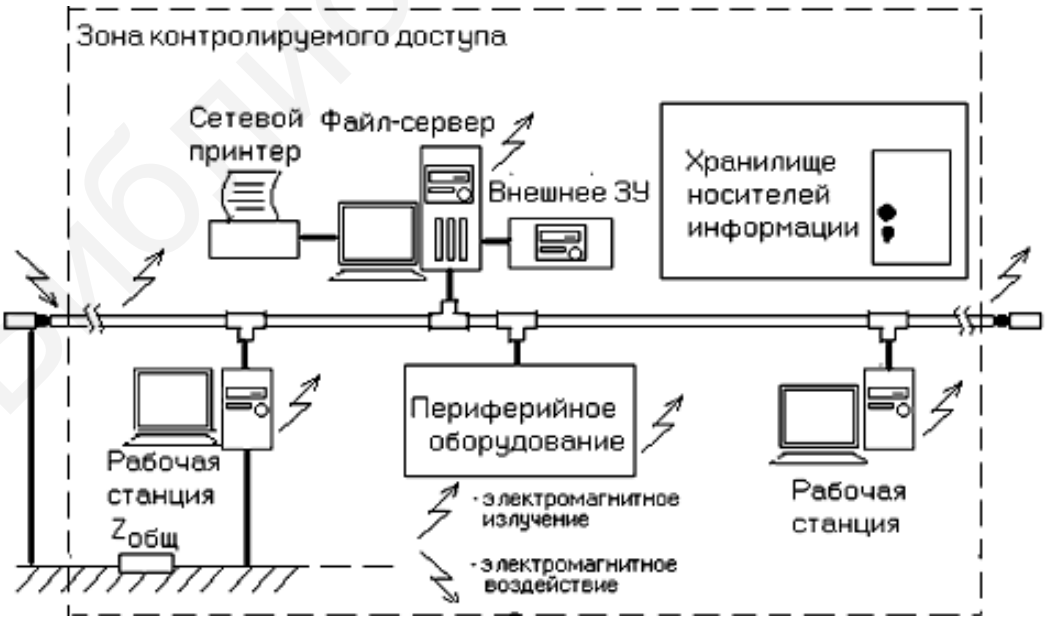

Рис. 20. Места и каналы возможного несанкционированного доступа к информации в компьютерной сети

Кардинальным решением является переход к соединениям на основе оптоволокна, свободным от влияния электромагнитных полей и позволяющим обнаружить факт несанкционированного подключения.

Для защиты информации от утечки по **техническим каналам** могут использоваться системы активной защиты (рис. 21), предназначенные для создания шумовых сигналов, маскирующих информативные сигналы, а также средства, создающие большое затухание для наведенных информативных токов в сети электропитания и системе заземления [101]:

- двигатели-генераторы;
- разделительные трансформаторы;
- силовые помехоподавляющие фильтры;
- диэлектрические вставки, прокладки в трубопроводах и воздухопроводах;
- помехоподавляющие фильтры в линиях связи;
- системы активной защиты, вырабатывающие шумовые сигналы и служащие для маскирования информативных наведенных сигналов.

Защитить объект от возникновения **акустических каналов утечки** информации частично можно путем: качественной звукоизоляции стен, дверей, потолков, пола; звуковой защиты вентиляционных каналов, отверстий и труб, проходящих через эти помещения (оклеивание стекол материалом, обеспечивающим рассеяние лазерного луча); устранения возможности визуального дистанционного доступа на объект (занавешивание окон).

Рис. 21. Средства защиты информации от утечки по техническим каналам

Если звукоизоляция и звуковая защита, связанные с капитальным строительством, не могут быть обеспечены указанными методами, целесообразно использовать системы акустической и виброакустической защиты, например, специальную криптографическую аппаратуру засекречивания (телефонные скремблеры – средства телефонных переговоров, обеспечивающие достаточно стойкие алгоритмы шифрования речевых сообщений).

Выпускаются также аппаратные средства, позволяющие криптографически защищать системы передачи данных, использующие в качестве элемента канала связи телефонные линии.

Защиту от активных способов перехвата осуществляют применением:

- пороговых устройств, сигнализирующих о появлении нештатных сигналов;
- различных фильтров, прозрачных для рабочих сигналов, но ослабляющих сигналы за пределами рабочего диапазона частот;
- шунтирования нелинейных элементов и других пассивных способов.

При применении активных способов защиты осуществляют модуляцию шумовым сигналом высокочастотных колебаний.

Большинство каналов утечки информации в отдельных случаях могут быть выявлены путем осмотра объекта и его окрестностей (физический поиск), а также с помощью специальных поисковых приборов. Для поиска подслушивающих устройств (радиозакладок) применяют приборы, работающие на одном из следующих принципов:

- обнаружение рабочего сигнала, излучаемого радиозакладкой;
- обнаружение излученного закладкой отклика на специально генерируемый зондирующий сигнал (нелинейная локация);
- с помощью рентгеновской аппаратуры.

Программные средства защиты подразумевают специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения информационных систем с целью решения задач защиты информации (рис. 22, 23, 24).

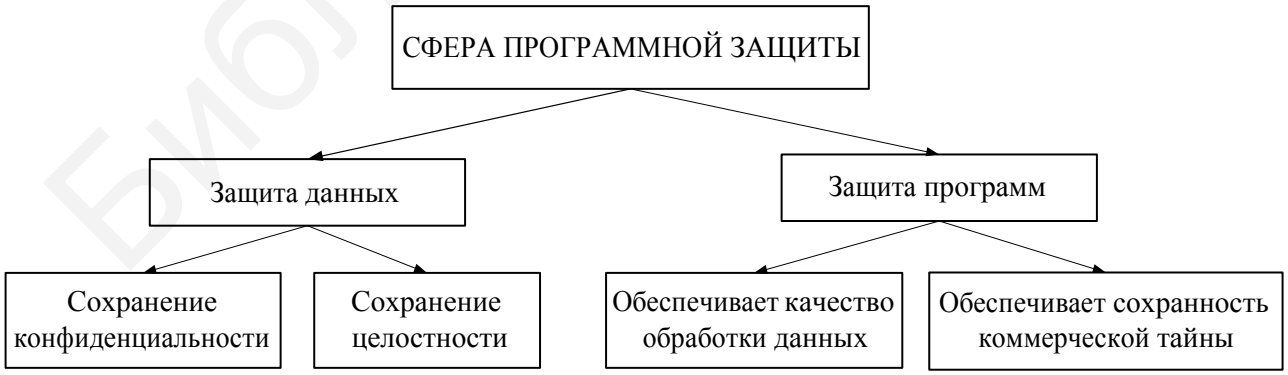

Рис. 22. Сферы программной защиты

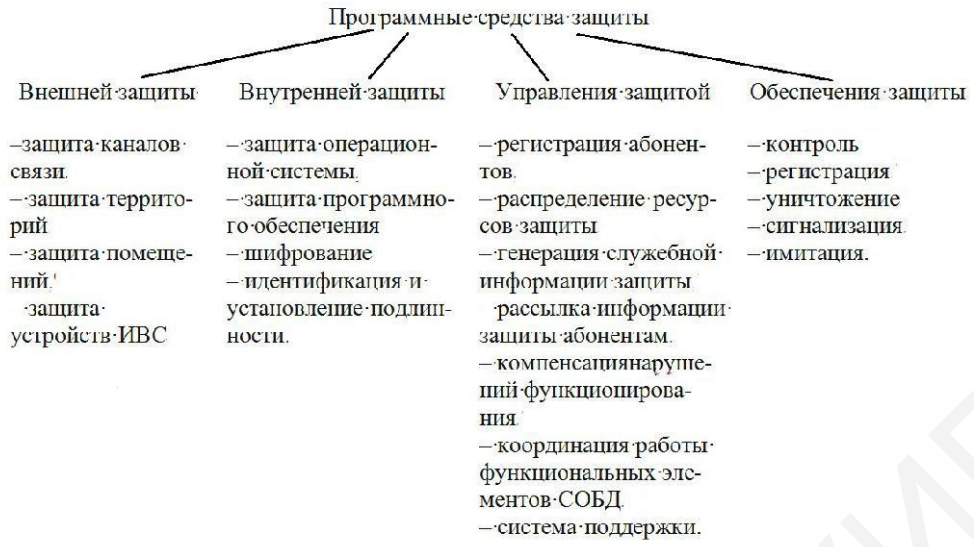

Рис. 23. Средства программной защиты

Рис. 24. Направления программной защиты информации

К основным **программным** средствам защиты информации относятся [102]:

- проверка прав доступа (по простому паролю, по сложному паролю, по разовым паролям);
- опознавание пользователей по различным идентификаторам;
- опознавание компонентов программного обеспечения;
- опознавание элементов баз данных;
- разграничение доступа к защищаемым данным по матрице полномочий, уровню секретности и другим признакам;
- управление доступом к задачам, программам и элементам баз данных по специальным мандатам;

- регистрация обращений к системе, задачам, программам и элементам защищаемых данных;

- подготовка к выдаче конфиденциальных документов (формирование и нумерация страниц, определение и присвоение грифа конфиденциальности, регистрация выданных документов);

- проверка адресата перед выдачей защищаемых данных в каналы связи;

- управление выдачей данных в каналы связи;

- криптографическое преобразование данных;

- контроль процессов обработки и выдачи защищаемых данных;

- уничтожение остаточной информации в ОЗУ после выполнения запросов пользователей;

- сигнализация при попытках несанкционированных действий;

- блокировка работы пользователей, нарушающих правила защиты информации;

- организация псевдоработы с нарушителем в целях отвлечения его внимания;

- программное обеспечение комплексных средств и систем защиты.

Для организационного построения программных средств в настоящее время наиболее характерной является тенденция разработки комплексных программ, выполняющих целый ряд защитных функций. Чаще всего в число этих функций входит опознавание пользователей, разграничение доступа к массивам данных, запрещение доступа к некоторым областям памяти и т. п.

Различают три принципиально важных требования к формированию программных средств: функциональная полнота, гибкость и унифицированность использования.

Более подробно вопросы, связанные с обеспечением безопасности информации путем использования программных средств защиты, будут рассмотрены в следующем подразделе.

3.3. Криптографические средства защиты информации

Средство криптографической защиты информации (СКЗИ) – совокупность аппаратных и (или) программных компонентов, обеспечивающих возможность шифрования информации с использованием одного или нескольких криптографических методов защиты. Средствами криптографической защиты информации решается множество задач, непосредственно связанных с обеспечением информационной безопасности любой системы, базы данных или сети передачи информации.

Существует ряд направлений, в которых применению средств криптографической защиты информации практически нет альтернативы. Согласно [103], такими направлениями в настоящий момент являются:

- защищенная электронная почта;

- обеспечение безопасности электронных платежей (электронный документооборот);

- виртуальные частные сети;

- создание и использование носителей ключевой информации;

- шифрование данных, хранимых в базе данных или в электронном виде на различных носителях информации;

- электронная цифровая подпись и связанные с ней виды шифрования, в частности, проверка авторства;

- криптографические интерфейсы;

- задачи идентификации и аутентификации и т. п.

Существует ряд возможных *реализаций* методов криптографической защиты информации:

- *программные*, представляющие собой реализацию одного или нескольких криптоалгоритмов на языке программирования высокого или низкого уровня в виде модулей, отдельных библиотек или выделенных программ с функцией криптографической защиты;

- *аппаратные*, реализующие криптоалгоритмы или их отдельные участки в микросхемах, процессорах и специализированных блоках (системы встроенной защиты) и аппаратных модулях (системы наложенной защиты), совмещенные со средствами вычислительной техники или встраиваемые в автоматизированные системы;

- *программно-аппаратные*, представляющие собой комплексы, состоящие из взаимосвязанных программной и аппаратной частей с функциями криптографической защиты.

Можно выделить несколько узловых точек (рис. 25), в которых возможно внедрить информационно-телекоммуникационную систему средств криптографической защиты информации.

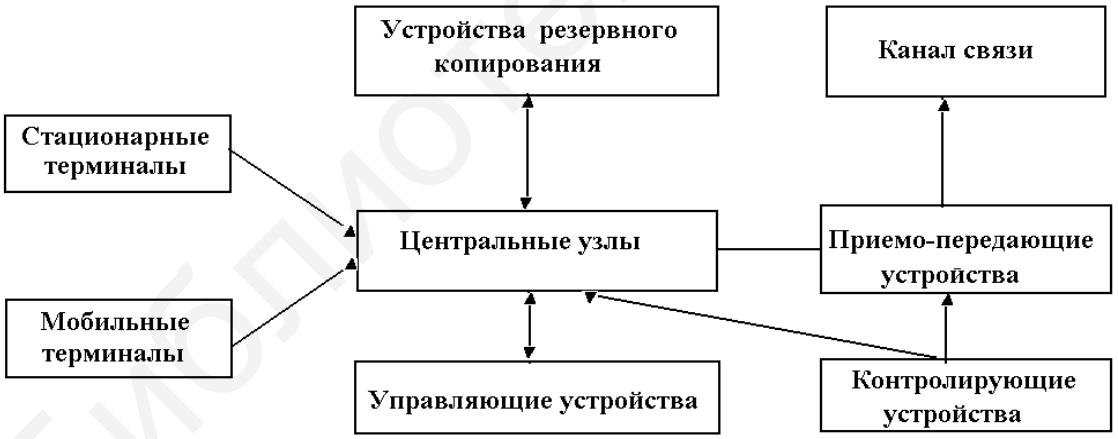

Рис. 25. Места внедрения средств криптографической защиты информации в инфокоммуникационной системе

Системы встроенной защиты, сопрягаемые с программными и аппаратными устройствами автоматизированных систем, могут использоваться в следующих случаях:

- защита стационарных или мобильных терминалов, а также устройств ввода/вывода информации и периферийных устройств;

- защита центральных узлов, а также соединений с внешними терминалами;

- защита управляющих и контролирующих устройств с обязательной гарантией высокого уровня надежности;

- обеспечение безопасности хранения информации, в том числе и резервных копий.

Системы наложенной защиты, реализуемые в виде отдельных блоков, используются:

- для организации независимого защищенного канала передачи информации;
- обеспечения «прозрачного» шифрования передаваемой по каналу связи информации;
- применения их в качестве устройств защиты приемо-передающих компонентов информационно-телекоммуникационных систем.

Особенностью использования СКЗИ в информационно-телекоммуникационных системах является наличие нескольких (обычно трех-четырех) выделенных режимов работы. Такими режимами обычно являются:

- абонентское шифрование;
- сквозное шифрование;
- канальное шифрование;
- цифровая подпись;
- идентификация/аутентификация.

3.3.1. Аппаратная технология реализации криптографической защиты информации

Аппаратное средство криптографической защиты информации – специализированный блок, компонент средства вычислительной техники или отдельное устройство, выполняющее шифрование информации. Собственно шифрование, согласно [108], представляет собой криптографическое преобразование данных для получения шифртекста (закрытого текста). Шифрование в аппаратных средствах криптографической защиты требует взаимодействия различных специализированных компонентов автоматизированной системы или средства вычислительной техники для реализации криптоалгоритмов.

Устройство криптографической защиты данных (УКЗД) – аппаратное СКЗИ, выполняющее также дополнительные функции по защите информации, например, защиту от НСД [2]. Кроме того, аппаратное средство криптографической защиты содержит ряд дополнительных блоков, которые не требуются в программной реализации:

- блок управления криптографическими ключами;
- генератор случайных чисел;
- постоянная и оперативная память;
- блок синхронизации времени;
- устройство хранения и проверки контрольных сумм и хэш-значений.

Также возможно использование специализированных шифропроцессоров для вычислений и отдельных блоков идентификации, аутентификации и авторизации (проверки и генерации электронной цифровой подписи). Полнофункциональное (с реализацией всех перечисленных функций) аппаратное СКЗИ

может являться даже специализированным компьютером, реализованным в виде внешнего или внутреннего аппаратного блока, связанного с центральным процессором собственными каналами передачи данных (например, системной шиной).

В [105] выделены несколько функций, которые также могут быть реализованы аппаратно:

- контроль доступа;
- выдача идентификационных ключей;
- проверка целостности данных.

Именно такое СКЗИ с дополнительными функциями в дальнейшем будем называть устройством криптографической защиты данных.

Рассмотрим **структуру аппаратного СКЗИ**.

Поскольку аппаратные реализации требуют физического исполнения на плате, при проектировании таких средств соблюдаются определенные требования и ограничения, в целом соответствующие следующей базовой схеме (рис. 26).

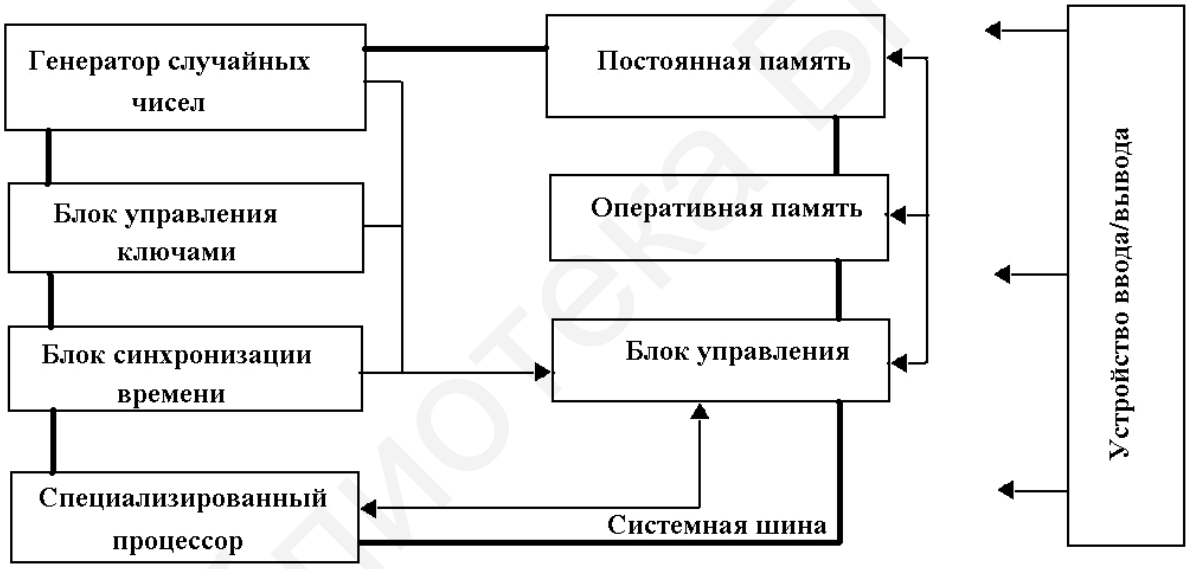

Рис. 26. Базовая схема аппаратных средств криптографической защиты информации

Блок управления выполняет координацию функций различных компонентов СКЗИ, коммутацию устройств и внешних потоков, управление данными, передаваемыми по системной шине.

Память аппаратного средства подразделяется на два блока:

- *оперативная*, хранящая программное обеспечение СКЗИ, а также все программируемые компоненты, изменяемые значения и пр.;
- *постоянная*, содержащая набор команд, реализующих защитные функции и загрузку программного обеспечения СКЗИ.

Кроме того, выделяются два дополнительных блока памяти:

- память журнала;
- память хранения ключей.

Специализированные процессоры применяются в аппаратных СКЗИ для увеличения скорости вычислений и исполнения большинства криптографических операций. Они представляют собой программируемые блоки или блоки с жестко установленным набором команд.

Генератор случайных чисел используется для получения псевдослучайных последовательностей, отвечающих требованиям криптоалгоритма, используемого СКЗИ. Использование таких генераторов в аппаратной реализации криптографической защиты основано на различных физических процессах.

Блок управления ключами выполняет прием, обработку и выдачу ключевой информации, а также при необходимости выполняет функции идентификации и аутентификации.

Блок синхронизации времени требуется в операциях контроля функционирования самого СКЗИ, при синхронизации потока данных, для расчета и согласования операций.

Устройство ввода/вывода информации обеспечивает обработку сигналов, поступающих от внешних устройств. Для таких устройств в аппаратных СКЗИ является принципиально важным обеспечение возможности взаимодействия со следующими устройствами:

- *системная шина* компьютерной системы, либо приемно-передающее устройство линии передачи информации, что актуально для организации сквозного («прозрачного») шифрования;
- *устройства хранения ключевой информации*, применяемые в задачах идентификации/аутентификации, а также контроля функционирования аппаратного СКЗИ;
- *контроллеры жестких дисков* и *устройства резервного копирования* информации позволяют организовать безопасное хранение данных и их резервных копий.

Достоинства аппаратных СКЗИ:

- гарантия неизменности алгоритма шифрования;
- наличие аппаратного датчика случайных чисел, используемого при создании криптографических ключей;
- возможность прямой (минуя системную шину компьютера) загрузки ключей шифрования в специализированный процессор аппаратного СКЗИ с персональных идентификаторов – носителей типа смарт-карт и «таблеток» Touch Memory (TM);
- хранение ключей шифрования не в ОЗУ компьютера (как в случае с программной реализацией), а в памяти шифропроцессора;
- идентификация и аутентификация пользователя до загрузки операционной системы;
- высокая скорость шифрования данных;
- надежность, позволяющая использовать средство криптографической защиты в критичных по надежности узлах автоматизированных систем;
- возможность реализации отдельным блоком, что зачастую позволяет более гибко строить топологию защищенной автоматизированной системы;

- исключение возможности программного повреждения ключей шифрования, что дает гарантию стабильности системы в целом.

3.3.2. Программная реализация криптографической защиты информации

Программные средства шифрования представляют собой реализацию криптографического алгоритма на высокоуровневом или низкоуровневом языке программирования. Обычно функционирование таких средств криптографической защиты требует выполнения ряда вычислительных операций стандартными аппаратными средствами компьютерной системы. При использовании программного СКЗИ применение аппаратного расширения не является обязательным условием.

Технология реализации криптоалгоритмов программными средствами имеет ряд особенностей и отличий:

- необходимость дополнительного контроля за качеством функционирования, поскольку в общем случае работу программного СКЗИ нарушить легче, чем его аппаратного аналога;
- возможность контроля ошибок в закрытом тексте при шифровании путем внедрения избыточности;
- необходимость обеспечения надежного хранения ключей, что решается путем создания мастер-ключа (ключа для шифрования файла, содержащего базу данных ключей) и других технологий, не требующихся при использовании аппаратного СКЗИ;
- возможность масштабирования и дополнения СКЗИ новыми программными блоками и модификациями используемых;
- принципиальная возможность использования программного СКЗИ с открытым кодом, что допускается при шифровании информации в частных целях и облегчает общую схему защиты.

Таким образом, программное СКЗИ отличает способность использования в распределенных и глобальных информационно-телекоммуникационных системах, более гибкая реализация, способность масштабирования и высокая мобильность.

Можно выделить следующие *функции* программных средств криптографической защиты:

- идентификация/аутентификация пользователей;
- обеспечение встроенной производителем криптографической защиты программных и операционных систем;
- генерация псевдослучайных последовательностей;
- шифрование данных на диске;
- «прозрачное» шифрование данных;
- абонентское шифрование данных;
- формирование и проверка ключей, цифровых подписей, защита от копирования программного кода;

- обеспечение безопасной передачи секретного ключа при инициализации СКЗИ, в том числе и аппаратных.

Базовые функции аппаратного СКЗИ дополняются возможностями встраивания программных средств в программное обеспечение, используемое для хранения, обработки и передачи данных в информационно-телекоммуникационных системах.

Рассмотрим **структуру программного СКЗИ**.

Программные технологии реализации криптоалгоритмов имеют в целом схожие базовые элементы, соответствующие следующей схеме (рис. 27).

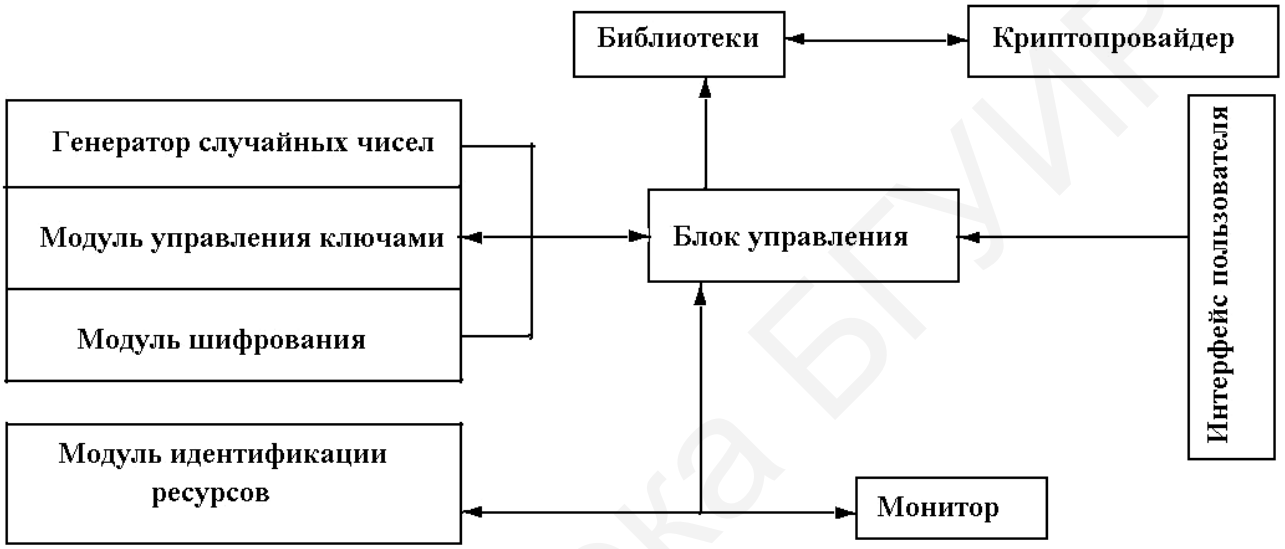

Рис. 27. Схема программных средств криптографической защиты информации

Блок управления выполняет координацию функций различных компонентов СКЗИ, коммутацию модулей и внешних потоков информации, а также внешних команд.

Модуль управления ключами выполняет задачи обработки ключевой информации, идентификации/аутентификации пользователей. Дополнительно используется идентификация устройств, которая может использоваться как элемент защитной подсистемы.

Генератор случайных чисел, используемый в программных СКЗИ, также реализуется программно, в нем применяются различные алгоритмы генерации псевдослучайных битовых последовательностей.

Библиотеки программных средств криптографической защиты применяются при решении прикладных задач и настройке СКЗИ в зависимости от условий эксплуатации.

Компонентом взаимодействия с пользователем является *интерфейс*, который предоставляет возможности управления программной реализацией алгоритма, контроля функционирования.

Программное средство криптографической защиты информации вне зависимости от реализованного криптоалгоритма имеет ряд особенностей шифрования [106]:

- файлы, зашифрованные программной СКЗИ, могут храниться на других носителях автоматизированной системы;

- размер блока в блочном алгоритме может превышать размер сегмента файла, в результате размер файла увеличивается;

- скорость шифрования программными средствами может быть ниже, чем в аппаратной реализации, за счет загрузки центрального процессора криптографическими вычислениями;

- работа с ключами усложняется отсутствием аппаратной идентификации пользователей.

Программные средства предназначены для решения прикладных задач криптографической защиты информации, в которых требуется гибкость и масштабируемость системы. Реализация криптографических алгоритмов такого типа не позволяет гарантированно обеспечивать защиту от атак на программный код, но другие аспекты, в частности, экономический и эксплуатационный, могут обосновать их использование в системах защиты информации любой сложности.

Рассмотрим, к примеру, **криптографический комплекс «Игла-П»** [110].

Данное программное средство построено по модульному принципу и представляет собой сетевой драйвер для ОС Windows NT, который заменяет типовой программный драйвер NDIS, с комплектом установочных и конфигурационных программ. Скорость шифрования – до 10 Мбит/с. На практике такая скорость работы достигается редко, поскольку характерным недостатком любого программного СКЗИ, как уже было отмечено выше, является зависимость от ресурсов центрального процессора. Рекомендуется использовать данное программное СКЗИ для защиты вновь подключаемых к локальной вычислительной сети и предназначенных для передачи защищаемой информации рабочих станций. Можно отметить, что использование СКЗИ «Игла-П» представляет собой достаточно практичный способ защиты трафика в локальной сети, а также возможность взаимодействия с многофункциональным программно-аппаратным комплексом «Шип».

Следующий пример – **программный эмулятор «Криптон»** – является частью широкой линейки продуктов фирмы «Анкад», позволяющей подбирать звенья системы криптографической защиты по необходимым функциям. Целью разработки именно этого звена, по утверждению производителя, стало обеспечение гибкости использования криптографических средств. Таким образом, программный эмулятор решает задачу обеспечения криптографической защиты абонентских терминалов, а также подключаемых мобильных устройств. Схема функционирования программного эмулятора позволяет использовать ключевые носители различных типов, что частично устраняет недостаток систем идентификации. Уязвимость возникает в процессе передачи ключа по системной шине, но перехват в этой зоне маловероятен. Отметим, что использование программного «Криптона» может дополняться его аппаратным аналогом. Все специальное программное обеспечение, используемое программными СКЗИ, в данном случае поддерживается и другими продуктами, в состав которых могут

входить и аппаратные, и программные модули. Производитель рекомендует использовать данное программное обеспечение в прикладных задачах криптографии, в которых требуется совместимость разных средств криптографической защиты. Среди них можно выделить наиболее важные: межсетевое экранирование; шифрование трафика в гетерогенных сетях; шифрование информации на диске.

Таким образом, программные средства криптографической защиты используются обычно в качестве дополнения к аппаратным, защищающим наиболее критичные узлы информационной системы (в данном пособии рассматриваются только сертифицированные средства).

3.3.3. Программно-аппаратные комплексы криптографической защиты информации

Наиболее сложную и эффективной разновидностью средств обеспечения информационной безопасности с использованием криптоалгоритмов являются *программно-аппаратные средства криптографической защиты информации*, под которыми будем понимать специальным образом организованные комплексы, содержащие взаимосвязанные программные и аппаратные блоки и реализующие следующий набор функций:

- идентификацию и аутентификацию пользователей;
- криптографическое преобразование данных;
- обеспечение целостности информации.

Основной *целью* применения программно-аппаратных средств обеспечения информационной безопасности является усиление или замещение существующих функций защиты компьютерных систем для обеспечения требуемого уровня защищенности.

Важное свойство программно-аппаратных средств заключается в возможности реализации комплексного метода криптографической защиты информации – метода как целостности, так и конфиденциальности информации. При его использовании основную роль играют шифрование, электронная цифровая подпись и криптографические ключи. Следовательно, программно-аппаратное СКЗИ являются одним из важнейших компонентов комплексного обеспечения информационной безопасности в компьютерных системах [111].

В состав программно-аппаратного СКЗИ (как системы, состоящей из программных и аппаратных компонентов) должны входить следующие *базовые модули*:

- блок шифрования (для программного шифрования используются ассиметричные криптосистемы, для аппаратного – симметричные) – программный, аппаратный или комбинированный;
- блок электронной цифровой подписи;
- блок управления ключами;
- модуль идентификации/аутентификации;
- модуль управления с внешним интерфейсом;
- модуль контроля функционирования.

Структура программно-аппаратного СКЗИ соответствует приведенной на рис. 28 базовой схеме. Однако нужно учитывать, что при проектировании программно-аппаратных средств постоянно происходит поиск новых решений, повышающих эффективность и надежность защиты.

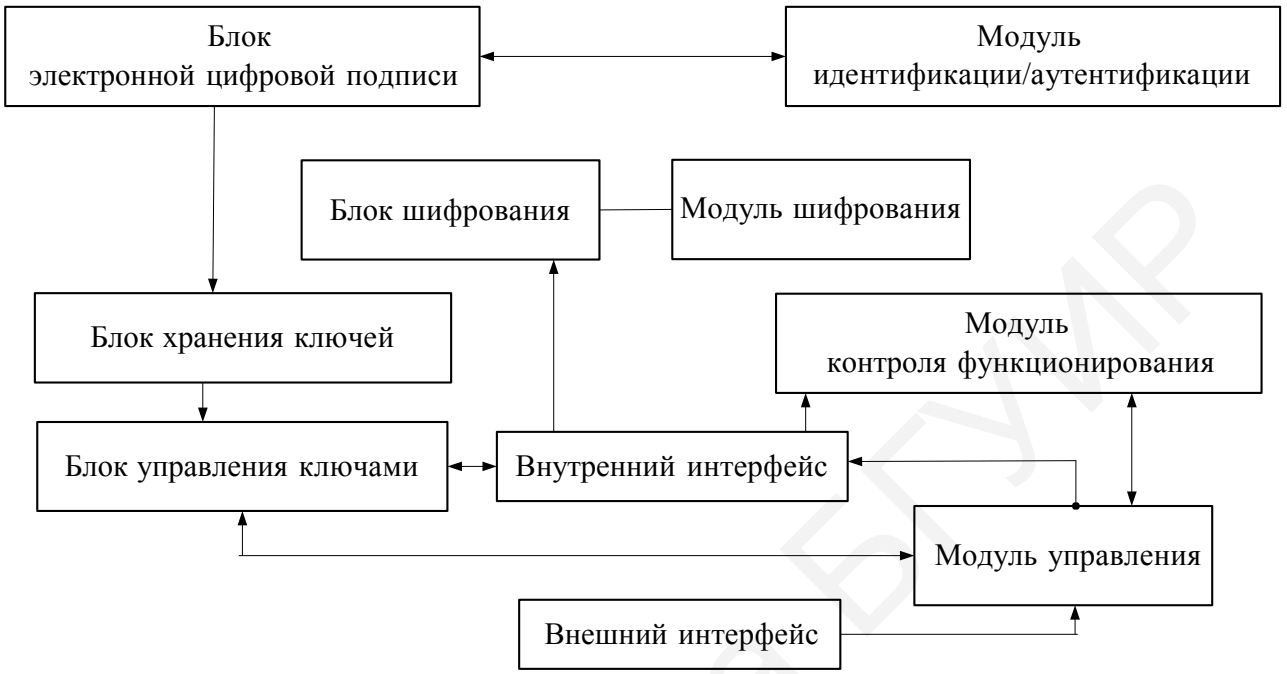

Рис. 28. Базовая схема программно-аппаратного комплекса СКЗИ

Модули программной защиты в данном случае связывает с программной частью специализированный внутренний интерфейс, т. е. взаимодействие происходит по собственным каналам СКЗИ (без использования системной шины) и с соблюдением внутренней (встроенной по умолчанию) политики безопасности.

Рассмотрим в качестве примера **СКЗИ «Шип»** – программно-аппаратный комплекс криптографической защиты информации, основной функцией которого является комплексная защита компьютерной сети.

Наиболее важными функциями СКЗИ являются:

- возможность создания защищенной виртуальной частной сети;
- шифрование IP-пакетов;
- организация фильтрации и маршрутизации;
- шифрование и проверка целостности данных с использованием имитовставки;
- односторонняя аутентификация узлов защищенной сети на основе имитовставки;
- управление ключевой системой защищенной сети.

Основными компонентами СКЗИ «Шип» являются программно- аппаратный комплекс «Шип» и центр управления ключевой системой [115]. Программно-аппаратный комплекс «Шип» используется при создании защищенной виртуальной частной сети. Его основными достоинствами являются реализация

режимов прозрачного и сквозного шифрования, скрытие трафика в защищенной сети, а также проверка целостности данных при их получении. Центр управления ключевой системой является реализацией блока управления ключами (см. рис. 28) в виде отдельного компонента комплекса и выполняет следующие функции:

- генерация и управление списком абонентов, имеющих право доступа (справочников соответствия по терминологии разработчика);
- журналирование внештатных ситуаций;
- периодическая (плановая) смена ключей шифрования, используемых в системе;
- оповещение о компрометации ключей.

Программно-аппаратный комплекс «Шип» поставляется в двух вариантах по производительности и по оснащению портами. Вариант №1 – «Шип-1», его производительность составляет до 15 Мбит/с (3000 пакетов/с); оснащен двумя асинхронными портами V.24, двумя портами Ethernet (FastEthernet/FDDI) для сетей пакетной коммутации с возможностью модемного подключения. Вариант №2 – «Шип-2», его производительность составляет около 8 Мбит/с (3000 пакетов/с) при обмене информацией по схеме «Ethernet (вход) – Ethernet (выход)» и около 2 Мбит/с (750 пакетов/с) при обмене по интерфейсу V.35 и протоколу Frame Relay; оснащают двумя асинхронными V.24, двумя портами Ethernet (Fast-Ethernet/FDDI), одним синхронным портом V.24/V35 (X.25/Frame Relay/PPP/Cisco HDLC) для сетей канальной коммутации либо подключения по модему с использованием дополнительных аппаратных устройств защиты информации.

Таким образом, использование программно-аппаратных СКЗИ целесообразно при организации комплексной защиты информации. Являясь мощным инструментом обеспечения информационной безопасности, особенно в аспекте защиты компьютерной информации, СКЗИ такого типа могут резко повышать надежность и эффективность системы защиты информации.

3.3.4. Анализ рынка программно-технических средств защиты информации Республики Беларусь

В соответствии с законодательством Республики Беларусь в области защиты информации государственным организациям и предприятиям предписывается использование криптографических средств защиты информации, сертифицированных Оперативно-аналитическим центром при Президенте Республики Беларусь. В настоящее время на рынке средств защиты информации РБ активно работают: ЗАО «БелХард Групп», ИП «С-Терра Бел», ЗАО «Авест», ЗАО «НТЦ Контакт», Производственно-внедренческое частное унитарное предприятие «СОФТМАРКЕТ», ООО «Энигма», ООО «БАЙТИС», Частное торгово-производственное унитарное предприятие «Авест-Системс», Научно-производственное республиканское унитарное предприятие «НИИ ТЗИ», ЗАО «БЕЛТИМ СБ» СП ООО «Солидекс ПИ», ЗАО «НПП БЕЛСОФТ», ОАО «АГАТ – системы управления» и др. Спектр выпускаемой продукции широк:

аппаратные, аппаратно-программные средства защиты документальной и речевой информации, комплексы для реализации инфраструктуры открытых ключей, средства защиты электронной почты и пр. За основу анализа средств защиты информации был взят перечень сертифицированных продуктов информационных технологий, прошедших сертификацию в Оперативно-аналитическом центре при Президенте Республике Беларусь [108].

ЗАО «БелХард Групп»

BELCrypt – аппаратно-программное средство криптографической защиты информации. BELCrypt выполнено на основе многофункциональной микропроцессорной карты (ММК) и имеет несколько исполнений:

- в виде смарт-карты с контактным интерфейсом;
- в виде смарт-карты с бесконтактным (радио) интерфейсом;
- в виде USB-ключа с SIM-модулем.

BHMCrypt32v2 – программное средство криптографической защиты информации, используемое банковскими организациями.

BelIPSEC – средство криптографической защиты сетевого протокола IP. Автоматически обеспечивает защиту всех протоколов лежащих на более высоком уровне: TCP, FTP, TFTP, X.400, HTPP, Telnet, SMTP, SNMP, NFS, FTAM и др.

Перечисленные средства защиты реализуют следующие функции криптографической защиты информации в соответствии со стандартами Республики Беларусь:

- шифрование данных IP-пакетов по алгоритму ГОСТ 28147-89;
- ЭЦП в соответствии с СТБ 1176.2-99;
- функция хэширования в соответствии с СТБ 1176.1-99;
- процедура выработки псевдослучайных данных в соответствии с РД РБ 07040.1202-2003 «Банковские технологии. Процедуры выработки псевдослучайных данных с использованием секретного параметра»;
- протокол формирования общего ключа шифрования в соответствии с алгоритмом, определенным в проекте руководящего документа Республики Беларусь РД РБ «Банковские технологии. Протоколы формирования общего ключа».

Многофункциональная микропроцессорная карта (ММК) с реализацией средств цифровой подписи и шифрования соответствует стандартам Республики Беларусь и международным стандартам. Система безопасности ММК обеспечивает защиту от несанкционированного доступа, достоверность данных и безопасную передачу сообщений.

Основные функции, выполняемые системой безопасности:

- разграничение прав доступа к данным карты;
- обеспечение конфиденциальности данных;
- обеспечение целостности и достоверности данных;
- подтверждение подлинности данных;
- гибкая система управления ключами.

ОАО «АГАТ – системы управления»

Программа контроля целостности «ПКЦЛ» предназначена для реализации контроля целостности файлов программного обеспечения и данных, хранящихся на ПЭВМ, и доведения до администратора защиты сообщений о результатах работы программы. Контроль осуществляется путем сравнения актуального состояния файлов ПО с контрольными данными (эталонами), которые формируются при установке программы, а также по команде администратора.

Программа «ПКЦЛ» работает совместно с программой расчета значения хэш-функции файла «ХЭШ».

Программа «ХЭШ» предназначена для расчета значения хэш-функции файла, который производится по СТБ 1176.1-99, результат расчета выводится в командную строку.

Среди разработок компании есть ряд комплексных решений по обеспечению защиты информации.

Комплекс программ защиты информации автоматизированного рабочего места администратора защиты (КП ЗИ АРМ АЗ) предназначен для реализации функций администрирования программных средств защиты на АРМ пользователей и серверах автоматизированной системы, а также настройки, контроля и поддержания в актуальном состоянии программных средств защиты и параметров групповых политик безопасности.

КП ЗИ АРМ АЗ обеспечивает выполнение следующих функций:

- управление контролем целостности программного обеспечения, установленного на ПЭВМ;
- управление опознанием;
- управление доступом;
- управление контролем доступа;
- управление аудитом.

КП ЗИ АРМ АЗ состоит из следующих программ:

- программа «Администратор ЗИ» ЕИРВ.50644-01;
- программа «ПКЦ» ЕИРВ.50607-01;
- программа «ПГН» ЕИРВ.50643-01;
- программа «Сбор НСД».

Кроме разработки программного обеспечения, ОАО «Агат – системы управления» оказывает следующие услуги в области защиты информации:

- разработка концепций защиты информации корпоративных локальных и распределенных систем обработки информации;
- разработка технических заданий на создание систем защиты информации по СТБ 34.101.9-2004;
- разработка программных средств защиты информации, в т. ч. средств контроля и управления доступом, аудита безопасности, генерации, оценки качества и назначения паролей, проверки целостности данных и ПО;
- разработка протоколов защищенного информационного взаимодействия объектов автоматизированных информационных систем;

- интеграция в информационные системы типовых проектных решений в области защиты информации.

ЗАО «АВЕСТ»

Криптопровайдер AVEST CSP – расширение криптографического ядра системы Microsoft Windows (разработанное в соответствии со спецификацией Microsoft Crypto API), которое позволяет использовать криптографические алгоритмы, сертифицированные Государственным центром безопасности информации при Президенте Республики Беларусь (ГЦБИ), всем приложениям Microsoft Windows. В марте 2004 года завершена сертификация криптопровайдера AVEST CSP на соответствие национальному стандарту СТБ, что позволяет использовать его в соответствии с Законом РБ «Об электронном документе» для оформления любых юридических и хозяйственных действий в Республике Беларусь электронным способом. В настоящее время криптопровайдер AVEST CSP – единственный криптопровайдер в Республике Беларусь.

Набор программного обеспечения для организации инфраструктуры открытых ключей (PKI) включает в себя Центр цифровых сертификатов, Центр регистрации, Персональный менеджер сертификатов.

Основные разработки ЗАО «АВЕСТ», прошедшие сертификацию:

- программное обеспечение программно-аппаратной платформы республиканского удостоверяющего центра инфраструктуры открытых ключей «Программа автоматической обработки запросов к удостоверяющему центру. AvCAServer.exe»;
- программное средство криптографической защиты информации «Криптопровайдер Avest CSP for BelSSF»;
- программный комплекс «Автоматизированное рабочее место плательщика»;
- программный комплекс «Сервер TLS АВЕСТ»;
- программный комплекс «АВЕСТ TLS tunnel»;
- программный комплекс «Определение статуса цифровых сертификатов Avest Revocation Provider»;
- программное средство электронной цифровой подписи и шифрования «AvCrypt ver.5.0».

В настоящее время деятельность предприятия ведется по следующим основным направлениям:

1) усовершенствование и разработка новых программных решений для организации инфрастуктуры открытых ключей с целью защиты документооборота в крупных корпорациях, а также по другим направлениям криптографической защиты информации (защита сетевого трафика и др.);

2) сотрудничество с разработчиками офисного ПО (систем электронного документооборота, электронного архива, систем «Клиент-банк» и т. д.) на предмет тестирования работы этих приложений с криптоядром AVEST CSP;

3) сотрудничество с государственными органами в области разработки нормативно-правовой базы регулирующей защиту информации в электронном документообороте в Республике Беларусь.

ЗАО «НПП БЕЛСОФТ»

Системный интегратор осуществляет проектирование, построение современных сетевых и телекоммуникационных решений, поставку телекоммуникационного и сетевого оборудования от ведущих мировых производителей, а также обладает лицензией на осуществление работ по обеспечению информационной безопасности организаций на основании соответствующих лицензий ГЦБИ при Президенте Республики Беларусь [115].

Комплексные решения ЗАО «НПП БЕЛСОФТ» в области сетевой безопасности информационных систем включают:

- системы обнаружения и предотвращения вторжений;
- системы контроля защищенности;
- системы защиты от несанкционированного доступа;
- системы криптографической защиты;
- виртуальные частные сети;
- межсетевые экраны;
- системы мониторинга событий безопасности;
- системы централизованного управления средствами защиты информации.

ООО «Солидекс»

Консалтинговая компания «Солидекс» специализируется на трех направлениях:

- создание и развитие сетей передачи данных и центров обработки данных как для предприятий, так и для операторов связи;
- защита информационных ресурсов;
- создание и развитие коммуникационных систем (телефонных систем, базирующихся на принципах пакетной коммутации; систем видеоконференцсвязи; центров обработки вызовов).

ООО «С-Терра Бел»

Компания специализируется на разработке продукции в сфере сетевой информационной безопасности, содержащей встроенные средства криптографической защиты информации, сертифицированные в Республике Беларусь.

Продукция *Bel VPN* предназначена для защиты межсетевого взаимодействия и удаленного доступа в ведомственных (корпоративных) географически распределенных IP-сетях, банковских платежных системах, IP-телефонии, видеоконференциях. Продукты Bel VPN содержат встроенные средства криптографической защиты информации, сертифицированные в Республике Беларусь, и работают как под управлением Unix-систем (Solaris, Linux), так и под управлением ОС семейства Windows (Windows XP, Windows Vista).

Основной продукт компании – *«Шлюз безопасности Bel VPN Gate»* – полностью встроен в систему централизованного управления Cisco Security Manager 3.2 (CSM).

Преимущества продукта:

- технологичность и универсальность;
- многообразие используемых сетевых решений Cisco Systems и глубокая интеграция с ними продуктов Bel VPN;

- сертифицированная криптография;

- трафик защищен белорусскими криптоалгоритмами, в основе которых лежат следующие стандарты: СТБ 1176.1-99, СТБ 1176.2-99, СТБ П 34.101.31-2007, РД РБ 07040.1202-2003;

- уникальность.

ООО «Хедтекнолоджи Бел»

Компания успешно закрепилась на рынке как эксклюзивный поставщик продуктов по информационной безопасности от ведущих мировых разработчиков: Lumension, F5, Astaro, Aventail, Clavister, IronPort, Insightix и др. Специализируется на поставках решений по защите информации в сети Интернет и предлагает:

- фильтрацию электронной почты, анти-СПАМ;

- фильтрацию WEB-трафика;

- защиту WEB-приложений.

Наиболее популярным поставляемым продукт компании – программа *«Blue Coat»*.

Продукт обеспечивает высокую степень безопасность при защите пользователей Web и Web-ориентированных приложений (фильтр нежелательного Web-контента, сканирование и блокировка шпионского ПО и вирусов, а также распознавание вредоносного контента внутри зашифрованных SSL-туннелей). Более того, Blue Coat поддерживает все известные системы аутентификации, что помогает предотвратить какие-либо попытки неавторизованного доступа к важной корпоративной информации с использованием Web. В результате продукт минимизирует все внутренние и внешние угрозы, имеющее отношение к Web.

Несмотря на перечисленные достоинства, программа еще не адаптирована к использованию в Беларуси. Так, устройства Blue Coat работают под управлением операционной системы SGOS – облегченной специализированной операционной системы. При этом данное средство сертифицировано в Беларуси.

ОАО «ЭНИГМА»

Наиболее популярным решением компании является аппаратный продукт *CryptoKey 2001*, его назначение: генерация и хранение ключей криптозащиты, выполнение криптографических функций – ЭЦП, хеширование, шифрование, протоколы формирования общего ключа, защита от несанкционированного доступа к персональному компьютеру.

CryptoKey 2001 применяется в системах электронного документооборота, включая «Банк-Клиент».

Перечень криптофункций, выполняемых на процессоре устройства:

- хеширование по СТБ1176.1-99;

- выработка подписи по СТБ 1176.2-99;

- проверка подписи по СТБ1176.2-99;

- выработка общего ключа для зашифрования (односторонний протокол схемы ОРК);

- выработка общего ключа для расшифрования (односторонний протокол схемы ОРК).

ЗАО «БЕЛТИМ СБ»

Аналогичное аппаратное обеспечение предлагает компания «БЕЛТИМ», определяющая основным направлением деятельности создание комплексных систем безопасности и защиты информации. Так, компания предлагает *электронный ключ Guardant Sign* – скоростной USB-ключ с асимметричной криптографией, аппаратной реализацией AES и возможностью работы без драйверов.

Выбор модели ключа зависит от лицензионной политики разработчика и особенностей защищаемого программного продукта:

- для защиты тиражного программного обеспечения, лицензируемого по классическим схемам, рекомендуется использовать локальный ключ *Guardant Sign*, либо его сетевой аналог – *Guardant Sign Net;*

- для защиты программного обеспечения, лицензируемого по времени использования, применяется *Guardant Time*;

- для сетевого программного обеспечения следует использовать *Guardant Time Net*;

Для защиты особенно ценного программного обеспечения, распространяемого единичными копиями, эффективнее использовать технологию «Загружаемый код», реализованную в электронном ключе *Guardant Code* и его модификации с часами реального времени – *Guardant Code Time.*

Белорусский государственный университет информатики и радиоэлектроники. Подразделение-разработчик: НИЛ 5.3 «Материалы и элементы электронной и сверхпроводниковой техники»

Устройство защиты речевой информации «Прибой-Р» предназначено для защиты речевой информации от утечки по акустическим и вибрационным каналам из помещения за пределы охранной зоны. Представляет собой автоматически управляемый источник возбуждения акустических шумов и вибраций, маскирующих речь в элементах конструкции здания и в других возможных акустических каналах утечки речевой информации (в зависимости от уровня речевого сигнала в защищаемом помещении).

Таким образом, рынок средств защиты в области информационной безопасности в Беларуси находится на стадии формирования. Функционируют десятки начинающих организаций, еще не укрепившихся на рынке средств защиты, программно-аппаратные решения которых, как правило, носят идентичный характер.

Однако, среди компаний, которые были исследованы, вызывают интерес организации **ООО «Хедтекнолоджи Бел»**, **ЗАО «Авест»** и их решения:

- криптопровайдер AVEST CSP – аппаратно-программное средство выработки и проверки ЭЦП, а также криптографической защиты информации;

- программа «Blue Coat», которая обеспечивает фильтрацию электронной почты, анти-СПАМ, фильтрацию WEB-трафика, защиту WEB-приложений.

Выбор рассматриваемых средств защиты основан на следующих критериях и требованиях, которые можно предъявить к современной системе защиты.

1. Прочность. Выбранная система должна обеспечить выигрыш во времени, пока потенциальные нарушители не разработали способ вскрытия данного продукта.

2. Обоснованность. При расчете стоимости защиты следует учитывать стоимость защищаемого программного продукта.

3. Гибкость. Защита эффективна при постоянном развития (разработчики защиты отслеживают хакерские форумы с целью выявления недостатков собственных систем).

4. Защита не должна препятствовать свободному копированию защищенных данных (запрет только на несанкционированный запуск).

5. Защита должна быть подобрана с учетом традиций данного сегмента рынка ПО, а средства защиты обязательно сертифицированы.

6. Не следует использовать для защиты дорогие дополнительные аппаратные приспособления, повышающие стоимость конечного продукта

7. По возможности не следует привязываться к аппаратной конфигурации компьютера, поскольку отдельные компоненты персонального компьютера необходимо заменять по мере старения.

4. БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

4.1. Политика безопасности компьютерных сетей

Любая организация, использующая компьютерную сеть (КС) в своей деятельности, должна учитывать возможность реализации угроз несанкционированного доступа и предпринять ряд мер для их нейтрализации. Для этого необходимо провести анализ обрабатываемой информации и отнести ее к определенной категории (государственная тайна, персональные данные, данные, составляющие коммерческую тайну, или иные сведения, носящие конфиденциальный характер), разработать политики безопасности (ПБ) и, в соответствии с ними, внести необходимые корректировки в модель разрабатываемой КС. Следует отметить, что разрабатывать единую политику безопасности для всех узлов КС нецелесообразно, т. к. каждый узел имеет присущие ему уязвимости, следовательно, общая политика безопасности будет избыточной, что приведет к необоснованному ограничению функциональности данного узла.

Выделение нескольких узлов в группу делает возможным установить правила для взаимодействия внутри группы и с объектами вне группы. Соблюдение этих правил позволяет исключить внешнее несанкционированное воздействие. Полученный периметр можно считать защищенным. Защищенные периметры (ЗП) могут взаимодействовать на равных, как, например, несколько локальных групп пользователей, или входить один в состав другого, как локальная сеть, входящая в состав распределенной сети [110].

Персональный компьютер не включает в себя других узлов, и в связи с этим его ЗП носит характер базового уровня (рис. 29).

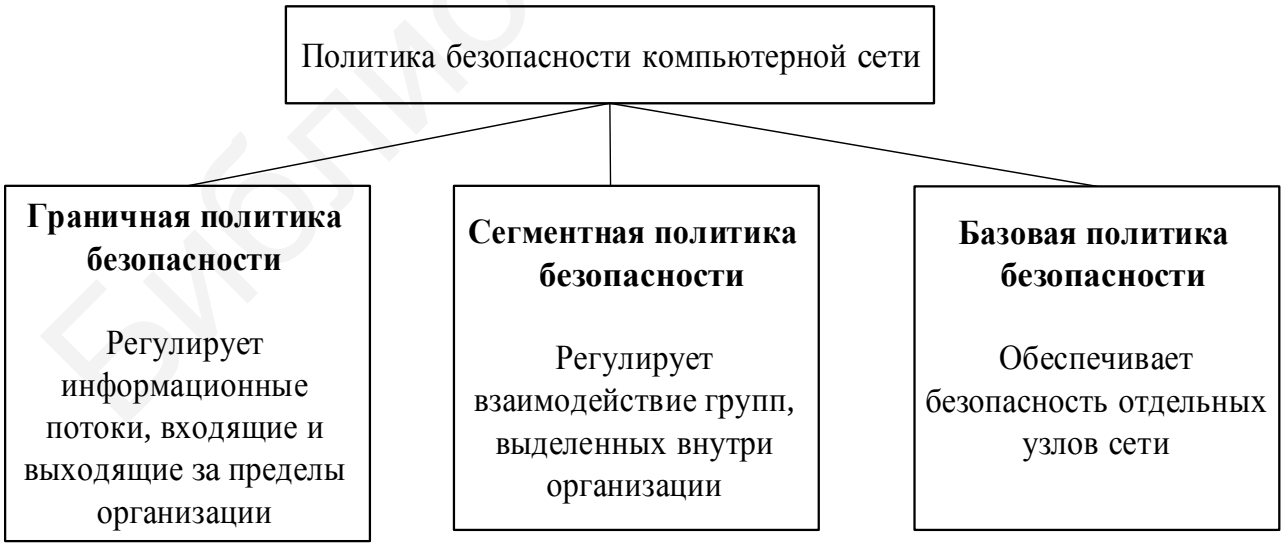

Рис. 29. Модель политики безопасности компьютерной сети

Для построения защиты периметра базового уровня необходимо определить набор характеристик, соответствующих данной структурной единице.

Название «персональный компьютер» подразумевает, что компьютер использует один человек, однако это не всегда так. Практически все современные операционные системы позволяют зарегистрировать на одном ПК несколько пользователей. Такая возможность очень важна для домашнего компьютера, который несколько человек используют в разное время и хотят хранить личные данные, использовать персональные настройки интерфейса и т. п. Такая возможность важна также для рабочего ПК в случаях, когда компьютеры используются в несколько рабочих смен разными пользователями или когда пользователь временно, например, на период отпуска, передает ПК другому сотруднику. Существует практика, при которой несколько человек используют одну учетную запись, что не целесообразно, поскольку теряется возможность объективного мониторинга: невозможно отследить, кто совершал конкретные действия в системе, назначить разные права или наложить ограничения на пользователя. Использование нескольких учетных записей на ПК необходимо также при разграничении прав доступа к системе – в большинстве случаев на администратора и пользователя. Администратор обладает правами настраивать систему, устанавливать программное обеспечение, а пользователь имеет доступ лишь к области прикладных задач [111].

Подключение рабочей станции к сети Интернет значительно повышает шансы злоумышленника на успешную атаку, поскольку появляется риск получения им несанкционированного удаленного доступа к ПК и риск инсайдерской атаки, направленной на хищение информации и передачу ее за пределы ЗП. Переносные накопители информации приобретают все меньшие габариты, но все большую емкость данных, появляется возможность незаметно внести или вынести большой объем информации. В связи с этим возникает необходимость аппаратными и программными средствами ограничивать любое несанкционированное подключение устройств, способствующих хищению конфиденциальной информации. Внутренняя угроза, исходящая от одного из сотрудников или группы лиц и направленная на хищение конфиденциальной информации, наиболее реальна и способна нанести огромный урон, т. к. может затронуть любую область информационных потоков организации. На этапе проектирования системы защиты невозможно определить, кто из членов организации решит воспользоваться служебным положением для получения личной выгоды. Кроме того, данный субъект, не имея прямого доступа к информации, может получить таковой, используя полученные обманным или иным способом идентификационные данные другого сотрудника (пароль, ключдоступа и т. п.) [112].

Одна из особенностей данной угрозы заключается в том, что выявить потерю данных в короткие сроки практически невозможно, а значит, у злоумышленника остается достаточно времени распоряжаться полученной информацией по своему усмотрению. Рынок индустрии информационных технологий предлагает в качестве решения данной проблемы установку так называемых *DLP (Data Loss Prevention)* систем, предотвращающих потери конфиденциальных данных. Такие системы включают в себя компоненты контекстного анализа на сетевых узлах и конечных хостах и компоненты,

направленные на устранение возможности несанкционированного подключения оборудования.

Выделение нескольких ПК в отдельную группу на основании схожих функциональных параметров (принадлежность к одному подразделению, обработка данных одного уровня конфиденциальности) позволяет назначить им ПБ, отличную от базовой. Такая ПБ отвечает за взаимодействие ПК внутри данного сегмента и нескольких сегментов сети между собой (рис. 30). Взаимодействие происходит посредством сетевых технологий.

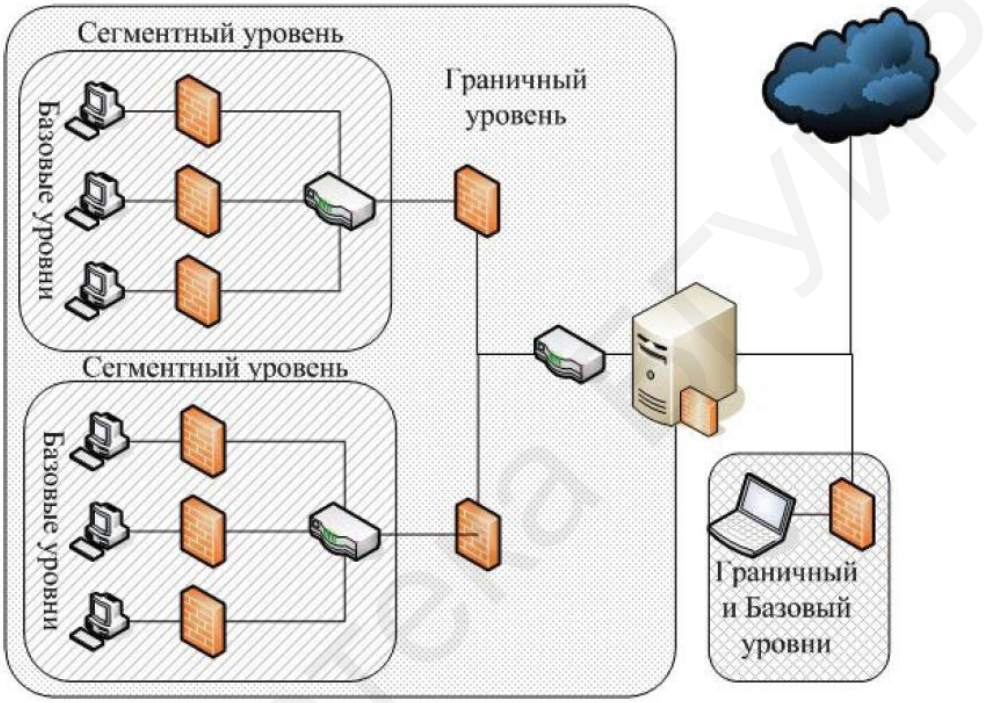

Рис. 30. Иерархия политик безопасности

Основной угрозой является захват злоумышленником одного из объектов либо внедрение ложного, и первоочередной целью системы защиты становится выявление таких объектов. Фактором, позволяющим распознать злоумышленника, является аномальное, нетипичное поведение объекта. Подозрение может вызвать резкое увеличение сетевой активности, изменение графика активности, попытки внедрения или анализа и т. п. В большинстве случаев злоумышленник будет активно действовать в отношении соседних либо вышестоящих узлов.

Создание ПБ на базовом и сегментном уровнях позволит контролировать информационные потоки внутри КС. Информационный обмен с внешней средой должен быть регламентирован отдельной ПБ. Исходящие или входящие данные пересекают границу КС. Граничный уровень защиты наиболее подвержен риску, т. к. именно этот уровень напрямую связан с внешней средой (см. рис. 30). Именно этот уровень может быть подвержен случайным атакам, не направленным против данной организации. Внешняя среда как таковая является агрессивной по причине полной открытости, поэтому необходимо

выявлять данные, не относящиеся к полезной информации, и блокировать им доступ в КС. Защита внешнего периметра носит двунаправленный характер: должны быть предусмотрены и отражение внешних атак, и контроль за информацией, покидающей пределы организации. Часть рассмотренной выше DLP-системы настроена на предотвращение попыток копирования конфиденциальной информации за границы защищенного периметра организации. Данные ПБ находятся в иерархической зависимости друг от друга. При перемещении данных через несколько уровней они будут подчинены ПБ более высокого уровня, например, передача данных от ПК одной группы на ПК другой будет в первую очередь ограничена ПБ сегментного уровня, а после этого – ПБ базового уровня.

Существуют ситуации, при которых ПБ граничного или сегментного уровня ограничивается одним узлом. ПК может входить в состав КС, но не быть членом группы, или это может быть удаленный ПК, отделенный сетью Интернет от основной КС. В этих случаях иерархия не должна нарушаться, а ПБ должны составляться отдельно для каждого уровня, т. к., например, изменение требований организации к информационному обмену между группами не должно приводить к изменению ПБ на базовом уровне.

Степень защищенности различных узлов системы не может быть одинаковой, следовательно, данные, обрабатываемые в этих узлах, будут подвержены разной степени риска несанкционированного воздействия. Разделив информацию по степени важности на несколько категорий, можно оптимизировать модель системы защиты любой организации. Цель оптимизации состоит в том, чтобы усилить защиту узлов, обрабатывающих более важную информацию, потеря которой нанесет большой урон предприятию. Наиболее действенным будет разделение данных на две группы: критические (данные, НСД к которым приведет к существенным потерям) и некритические. Дальнейшее дробление этих групп зависит от конкретных информационных потоков. Основной принцип при проектировании системы защиты критических данных заключается в избыточности применяемых мер по защите. С одной стороны, необходимо усилить защиту узлов, на которых обрабатывается информация такого рода, с другой – запретить ее обработку на узлах, подверженных риску НСД. Проектируя защиту наиболее важных данных, необходимо принять все возможные меры по предотвращению угроз: подбор персонала, проверку аппаратно-программных комплексов на наличие встроенных «закладок», пропускной режим в помещениях и т. п. Возможно, некоторые угрозы не удастся свести к минимуму, в таком случае их придется исключить, например, отключить некий сегмент сети от глобальной сети на граничном уровне защиты, от остальной сети предприятия на сегментном уровне и запретить использование переносных запоминающих устройств на нижнем уровне. При передаче информации между различными участками КС возникают ситуации, требующие определить, какая из политик безопасности должна быть применена. Формализованный подход к данному вопросу исключит возможность неоднозначного ответа и позволит программно

обрабатывать возникшие противоречия. ПБ исходящего и входящего узлов должны иметь удельный вес (УВ), позволяющий при сравнении установить, какая из политик имеет приоритетное значение. Факторами, определяющими удельный вес ПБ, являются уровень, на котором действует политика, и степень важности информации, которую обрабатывает узел, подпадающий под действие данной политики. Сумма УВ этих факторов определяет УВ ПБ (табл. 5).

Таблица 5

Определение удельного веса политики безопасности

Степень конфиденциальности информации (УВ)	Уровень ПБ (УВ)		
	Базовый (1)	Сегментный (2)	Граничный (3)
Не критичная (1)	2	3	4
Критичная (2)	3	4	5

Диапазон УВ степени конфиденциальности может быть расширен в зависимости от требования конкретной организации. При совпадении значений УВ должны быть соблюдены требования обеих ПБ.

4.2. Угрозы безопасности информации в компьютерных системах

Обеспечение безопасности информации в КС следует рассматривать в виде единства трех компонентов, оказывающих взаимное влияние друг на друга:

- информация;
- технические и программные средства;
- обслуживающий персонал и пользователи.

В отношении приведенных компонентов иногда используют и термин «информационные ресурсы», который в этом случае трактуется значительно шире, чем в Законе РБ «Об информации, информатизации и защите информации».

Целью создания любой КС является удовлетворение потребностей пользователей в своевременном получении достоверной информации и сохранении ее конфиденциальности (при необходимости). Информация является конечным «продуктом потребления» в КС и выступает в виде центрального компонента системы, безопасность информации на уровне КС обеспечивают остальные компоненты системы.

Под **угрозой безопасности информации** понимается потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации.

Все множество потенциальных угроз безопасности информации в КС может быть разделено на два класса (рис. 31) [113].

Рис. 31. Угрозы безопасности в компьютерных системах

Сбои и **отказы** сложных систем неизбежны. Нарушается работоспособность технических средств, уничтожаются и искажаются данные и программы, нарушается алгоритм работы устройств, что может также привести к нарушению конфиденциальности информации. Например, сбои и отказы средств выдачи информации приводят к несанкционированному доступу к информации путем несанкционированной ее выдачи в канал связи, на печатающее устройство и т. п.

Ошибки при разработке КС, **алгоритмические** и **программные ошибки** приводят к последствиям, аналогичным последствиям сбоев и отказов технических средств, и могут быть использованы злоумышленниками для воздействия на ресурсы КС. Особую опасность представляют ошибки в операционных системах (ОС) и программных средствах зашиты информации.

Согласно данным Национального института стандартов и технологий США (NIST), 65 % случаев нарушения безопасности информации происходит в результате **ошибок пользователей и обслуживающего персонала**. Некомпетентное, небрежное или невнимательное выполнение функциональных обязанностей сотрудниками приводит к уничтожению, нарушению целостности и конфиденциальности информации, а также компрометации механизмов защиты.

К методам **шпионажа** и **диверсий** относятся:

- подслушивание;
- визуальное наблюдение;
- хищение документов и машинных носителей информации;
- хищение программ и атрибутов системы защиты;

- подкуп и шантаж сотрудников;
- сбор и анализ отходов машинных носителей информации;
- поджоги;
- взрывы.

Термин **«несанкционированный доступ к информации» (НСД)** определен как доступ к информации, нарушающий правила разграничения доступа, с использованием штатных средств вычислительной техники или автоматизированных систем.

Примечание. Под **правилами разграничения доступа** понимается совокупность положений, регламентирующих права доступа лиц или процессов (субъектов доступа) к единицам информации (объектам доступа).

Несанкционированный доступ к информации возможен только с использованием штатных аппаратных и программных средств в следующих случаях:

- отсутствие системы разграничения доступа;
- сбой или отказ в КС;
- ошибочные действия пользователей или обслуживающего персонала компьютерных систем;
- ошибки в СРД;
- фальсификация полномочий.

Процесс обработки и передачи информации техническими средствами КС сопровождается электромагнитными излучениями в окружающее пространство и наведением электрических сигналов в линиях связи, сигнализации, заземлении и других проводниках, т. е. **побочными электромагнитными излучениями и наводками (ПЭМИН)**. С помощью специального оборудования сигналы принимаются, выделяются, усиливаются и могут либо просматриваться, либо записываться в запоминающих устройствах. Дальность удовлетворительного приема таких сигналов при использовании дипольной антенны составляет 50 м. Использование направленной антенны приемника позволяет увеличить зону уверенного приема сигналов до 1 км. Восстановление данных возможно также путем анализа сигналов излучения неэкранированного электрического кабеля на расстоянии до 300 м. Для получения информации злоумышленник может использовать также «просачивание» информационных сигналов в цепи электропитания технических средств КС.

Большую угрозу безопасности информации в КС представляет **несанкционированная модификация** алгоритмической, программной и технической **структур** системы, которая может осуществляться на любом жизненном цикле КС. Несанкционированное изменение структуры КС на этапах разработки и модернизации получило название *«закладка»*.

Одним из основных источников угроз безопасности информации в КС является использование специальных программ, получивших общее название **«вредительские программы»**. В зависимости от механизма действия вредительские программы делятся на четыре класса:

- *«логические бомбы»* – это программы или их части, постоянно находящиеся в ЭВМ или вычислительных системах (ВС) и выполняемые

только при соблюдении определенных условий (наступление заданной даты, переход в определенный режим работы, наступление некоторых событий установленное число раз и т. п.);

- *«черви»* – программы, которые выполняются каждый раз при загрузке системы, обладают способностью перемещаться в ВС или сети и самовоспроизводить копии; лавинообразное размножение программ приводит к перегрузке каналов связи, памяти и в конечном итоге к блокировке системы;

- *«троянские кони»* – это программы, полученные путем явного изменения или добавления команд в пользовательские программы; при последующем выполнении пользовательских программ наряду с заданными функциями выполняются несанкционированные, измененные или новые функции;

- *«компьютерные вирусы»* – это небольшие программы, которые после внедрения в ЭВМ самостоятельно распространяются путем создания своих копий, а при выполнении определенных условий оказывают негативное воздействие на КС; поскольку вирусам присущи свойства всех классов вредительских программ, то в последнее время любые вредительские программы часто называют вирусами.

Возможности осуществления вредительских воздействий в большой степени зависят от *статуса злоумышленника* по отношению к КС.

- *Разработчик КС*. Владеет наиболее полной информацией о программных и аппаратных средствах КС и имеет возможность внедрения «закладок» на этапах создания и модернизации систем. Но он, как правило, не получает непосредственного доступа на эксплуатируемые объекты КС.

- *Сотрудник из числа обслуживающего персонала*. Наибольший вред могут нанести работники службы безопасности информации, системные программисты, прикладные программисты и инженерно-технический персонал.

- *Пользователь*. Имеет общее представление о структурах КС, о работе механизмов защиты информации. Он может осуществлять сбор данных о системе защиты информации методами традиционного шпионажа, а также предпринимать попытки несанкционированного доступа к информации. Возможности внедрения «закладок» пользователями очень ограничены.

- *Постороннее лицо, не имеющее отношения к КС*. Как правило, в его распоряжении имеются дистанционные методы традиционного шпионажа и возможность диверсионной деятельности, или осуществляются вредительские воздействия с использованием электромагнитных излучений и наводок, а также каналов связи, если КС является распределенной.

На практике степень опасности злоумышленника зависит от финансовых, материально-технических возможностей и квалификации.

Угрозы безопасности информации в компьютерных системах, как правило, выражены следующими *типами атак* со стороны злоумышленника.

Атаки отказа в обслуживании (DoS)

Направлены на информационные серверы предприятия, функционирование которых является критически важным условием для

работоспособности всего предприятия. Чаще всего объектами DoS-атак становятся основные веб-серверы, файловые и почтовые серверы предприятия, а также корневые серверы системы DNS. Применяются для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене.

Примечание. **DNS** (англ. Domain Name System – система доменных имен) – компьютерная распределенная система для получения информации о доменах.

Для проведения DoS-атак злоумышленники часто координируют работу нескольких компьютеров (как правило, без участия их непосредственных пользователей). В таких случаях имеет место распределенная атака отказа в обслуживании (Distributed Denial of Service, DDoS). Злоумышленник, захватив управление над группой удаленных компьютеров, инициирует рассылку пакетов в адрес «узла-жертвы» (рис. 32) [114].

Рис. 32. Пример DDoS-атаки

Получившийся в результате мощный суммарный поток «затопляет» атакуемый компьютер, вызывая его перегрузку и в конечном счете делает его недоступным. Блокировка атакуемого узла происходит в результате исчерпания ресурсов либо процессора, либо операционной системы, либо канала связи (полосы пропускания).

Перехват и перенаправление трафика

Имеет целью направить трафик атакуемого компьютера по ложному адресу, в качестве которого может выступать адрес либо злоумышленника, либо третьей стороны. Потоком данных, который пользователь посылает, например, на свой корпоративный сервер или сервер банка, злоумышленник может распорядиться двумя способами:

- злоумышленник маскируется под сервер адресата, передавая клиенту «картинку» и сообщения, которые тот ожидает: имитирует для пользователя-

жертвы процедуру логического входа, получая при этом идентификатор и пароль пользователя для несанкционированного доступа к серверу предприятия или банка, которые и являются главной целью атаки;

- организация транзита трафика, при котором каждый перехваченный пакет запоминается и (или) анализируется на атакующем узле, после чего перенаправляется на «настоящий» сервер; таким образом весь трафик между клиентом и сервером пропускается через компьютер злоумышленника.

Использование протокола ICMP

В тех случаях, когда маршрутизатор обнаруживает, что для некоторого адреса-назначения хост использует нерациональный маршрут, или при отказе этого маршрута, в соответствии с ICMP-протоколом, сообщение о перенаправлении маршрута отсылается маршрутизатором хосту по умолчанию. Применяемый по умолчанию маршрутизатор R1, получив от хоста H1 пакет, адресованный хосту H2, определяет, что наилучший маршрут к хосту H2 пролегает через другой маршрутизатор данной локальной сети, а именно через маршрутизатор R2 (рис. 33).

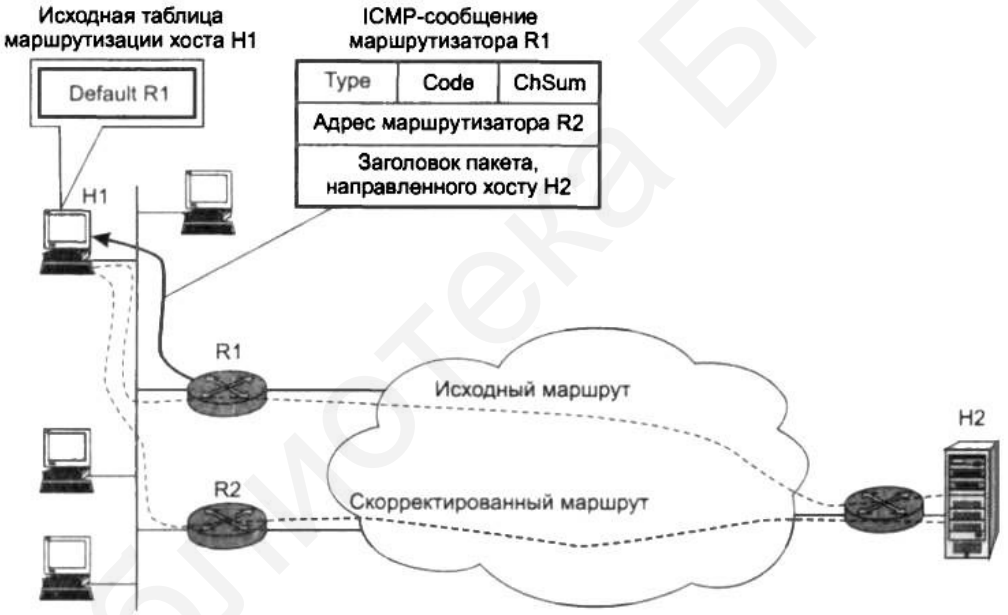

Рис. 33. Работа протокола ICMP

Маршрутизатор R1 отбрасывает полученный пакет и помещает в заголовок ICMP-сообщения для хоста H1 информацию о перенаправлении маршрута. В сообщении содержится IP-адрес альтернативного маршрутизатора R2, который хост теперь должен использовать, посылая данные хосту H2. Хост H1 вносит изменения в свою таблицу маршрутизации и с этого момента отправляет пакеты хосту H2 по новому скорректированному маршруту.

Для перехвата трафика, направляемого хостом H1 хосту H2, злоумышленник должен сформировать и послать хосту H1 пакет, маскирующийся под ICMP-сообщение о перенаправлении маршрута. В этом сообщении содержится запрос о корректировке таблицы маршрутизации хоста H1, так чтобы во всех пакетах с адресом IP-H2 адресом следующего

маршрутизатора стал IP-HA, являющийся адресом хоста-злоумышленника HA (рис. 34).

Для того чтобы хост «поверил» этому сообщению, в поле IP-адреса отправителя должен быть помещен адрес маршрутизатора R1, являющегося маршрутизатором по умолчанию.

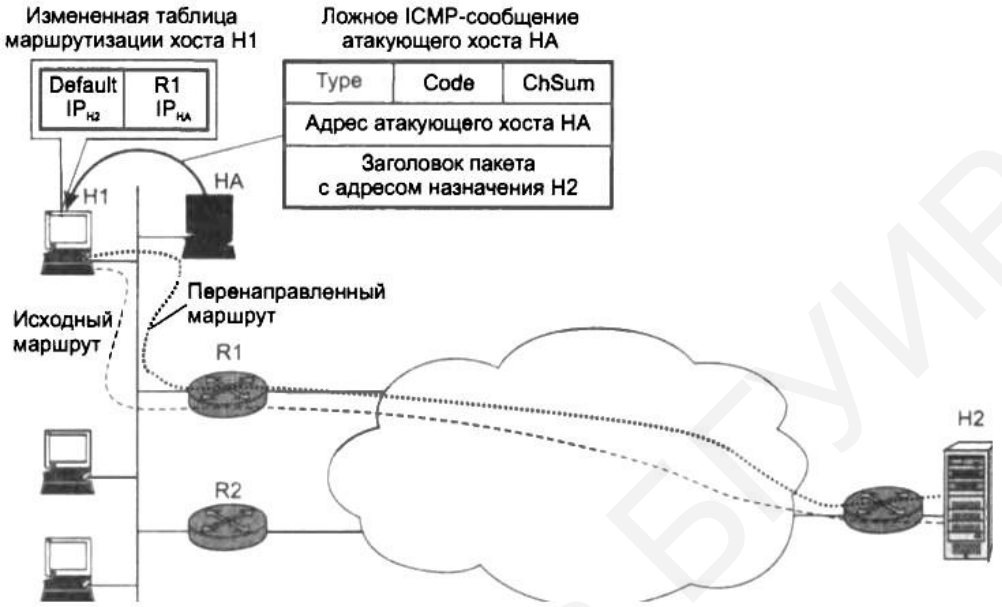

Рис. 34. Пример использования злоумышленником протокола ICMP

Когда пакеты, передаваемые «введенным в заблуждение» хостом, начнут поступать на узел злоумышленника, он может захватывать и не передавать эти пакеты дальше. При этом для поддержания «диалога» злоумышленник имитирует приложение, которому эти пакеты предназначались, или может организовать транзитную передачу данных по указанному адресу назначения. Читая весь трафик между узлами H1 и H2, злоумышленник получает всю необходимую информацию для несанкционированного доступа к серверу H2.

Использование ложных DNS-ответов

Задача злоумышленника состоит в получении доступа к корпоративному серверу, для чего ему нужно завладеть именем и паролем авторизованного пользователя корпоративной сети. Эту информацию он может получить путем ответвления потока данных, которые корпоративный клиент посылает корпоративному серверу (рис. 35).

Злоумышленник знает, что клиент обращается к серверу, указывая его символьное DNS-имя (например, www.example.com). Также ему известно, что перед тем, как отослать пакет серверу, программное обеспечение клиентской машины направляет запрос DNS-серверу, чтобы узнать, какой IP-адрес соответствует этому имени. Цель злоумышленника – опередить ответ DNS-сервера и навязать клиенту свой вариант ответа, в котором вместо IP-адреса корпоративного сервера (в примере 193.25.34.125) злоумышленник указывает IP-адрес атакующего хоста (203.13.1.123).

Рис. 35. Пример использования злоумышленником DNS-запроса корпоративного пользователя

На пути реализации этого плана существует несколько серьезных препятствий. Протокол DNS может использовать для передачи своих сообщений как протокол UDP, так и протокол TCP в зависимости от того, как он будет сконфигурирован администратором. Поскольку протокол TCP устанавливает логическое соединение с отслеживанием номеров посланных и принятых байтов, «вклиниться» в диалог клиента и сервера в этом случае гораздо сложнее, чем в случае, когда используется дейтаграммный протокол UDP.

4.3. Защита от несанкционированного изменения структур компьютерных систем

Типовая система автоматизированного документооборота состоит:
- из операционной среды;
- программных средств управления базами данных;
- телекоммуникационных программ;
- текстовых редакторов;
- антивирусных средств;
- средств для криптографической защиты данных;
- средств аутентификации и идентификации пользователей.

Главным условием правильного функционирования такой компьютерной системы является обеспечение защиты от вмешательства в процесс обработки информации таких программ, как:

- программные закладки;
- компьютерные вирусы.

4.3.1. Программные закладки

Программная закладка способна выполнять хотя бы одно из следующих действий:

- внесение произвольных искажений в коды программ, находящихся в оперативной памяти компьютера (1-й тип);
- перенос фрагментов информации из одних областей оперативной или внешней памяти компьютера в другие (2-й тип);
- искажение выводимой на внешние компьютерные устройства или в канал связи информации, полученной в результате работы других программ (3-й тип).

Закладка (программная закладка ПЗ) – скрытно внедренная в защищенную систему программа (либо намеренно измененный фрагмент программы), которая позволяет злоумышленнику осуществить НСД к ресурсам системы на основе изменения свойств системы защиты.

Закладка может быть внедрена самим разработчиком программного обеспечения. Несанкционированному изменению могут быть подвергнуты алгоритмическая, программная и техническая структуры КС на этапах ее разработки и эксплуатации. Часто программные закладки выполняют роль перехватчиков паролей, трафика, а также служат в качестве проводников для компьютерных вирусов.

По методу внедрения в КС различают следующие *типы* программных закладок:

- *программно-аппаратные* закладки (среда обитания BIOS – набор программ, записанных в виде машинного кода в ПЗУ);
- *загрузочные* закладки, ассоциированные с программами начальной загрузки, которые располагаются в загрузочных секторах (из этих секторов в процессе выполнения начальной загрузки РС считывает программу, берущую на себя управление для последующей загрузки самой ОС);
- *драйверные* закладки, ассоциированные с драйверами (файлами, в которых содержится информация, необходимая операционной системе для управления подключенными к компьютеру периферийными устройствами);
- *прикладные* закладки, ассоциированные с прикладным программным обеспечением общего назначения (текстовые редакторы, утилиты, антивирусные мониторы и программные оболочки);
- *исполняемые* закладки, ассоциированные с исполняемыми программными модулями, содержащими код этой закладки (чаше всего эти модули представляют собой пакетные файлы, состоящие из команд операционной системы, выполняемых одна за другой, как если бы их набирали на клавиатуре компьютера);
- *закладки-имитаторы*, интерфейс которых совпадает с интерфейсом некоторых служебных программ, требующих ввод конфиденциальной

информации (паролей, криптографических ключей, номеров кредитных карточек);

- *замаскированные* закладки, которые маскируются под программные средства оптимизации работы компьютера (файловые архиваторы, дисковые дефрагментаторы) или под программы игрового и развлекательного назначения.

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

- программная закладка должна попасть в оперативную память компьютера (если закладка относится к 1-му типу, то она должна быть загружена до начала работы другой программы, которая является целью воздействия закладки, или во время работы этой программы);

- работа закладки, находящейся в оперативной памяти, начинается при выполнении ряда условий, которые называются активизирующими.

С учетом замечания о том, что программная закладка должна быть обязательно загружена в оперативную память компьютера, можно выделить:

- *резидентные* закладки (находятся в оперативной памяти постоянно, начиная с некоторого момента и до окончания сеанса работы компьютера, т. е. до его перезагрузки или до выключения питания);

- *нерезидентные* закладки (попадают в оперативную память компьютера аналогично резидентным, однако, в отличие от последних, выгружаются по истечении некоторого времени или при выполнении особых условий).

Существуют три основные группы деструктивных действий, которые могут осуществляться программными закладками:

- копирование информации пользователя компьютерной системы (паролей, криптографических ключей, кодов доступа, конфиденциальных электронных документов), находящейся в оперативной или внешней памяти этой системы либо в памяти другой компьютерной системы, подключенной к ней через локальную или глобальную компьютерную сеть;

- изменение алгоритмов функционирования системных, прикладных и служебных программ (например, внесение изменений в программу разграничения доступа может привести к тому, что она разрешит вход в систему всем без исключения пользователям вне зависимости от правильности введенного пароля);

- навязывание определенных режимов работы (например, блокирование записи на диск при удалении информации, при этом информация, которую требуется удалить, не уничтожается и может быть впоследствии скопирована хакером).

У всех программных закладок независимо от метода их внедрения в компьютерную систему, срока их пребывания в оперативной памяти и назначения имеется важная общая черта: они обязательно выполняют операцию

записи в оперативную или внешнюю память системы. При отсутствии данной операции никакого негативного влияния программная закладка оказать не может. Для целенаправленного воздействия она должна выполнять и операцию чтения, иначе в ней может быть реализована только функция разрушения (например, удаление или замена информации в определенных секторах жесткого диска).

Существуют следующие основные модели воздействия программных закладок на компьютеры.

В модели **«перехват»** программная закладка внедряется в ПЗУ, системное или прикладное программное обеспечение и сохраняет всю или выбранную информацию, вводимую с внешних устройств компьютерной системы или выводимую на эти устройства, в скрытой области памяти локальной или удаленной компьютерной системы. Объектом сохранения, например, могут служить символы, введенные с клавиатуры (все повторяемые два раза последовательности символов), или электронные документы в процессе распечатывания на принтере. Данная модель может быть двухступенчатой. На первом этапе сохраняются только, например, имена или начальные части файлов. На втором накопленные данные анализируются злоумышленником с целью принятия решения о конкретных объектах дальнейшей атаки.

В модели **«искажение»** программная закладка изменяет информацию, которая записывается в память компьютерной системы в результате работы программ, либо подавляет/инициирует возникновение ошибочных ситуаций в компьютерной системе. Можно выделить статическое и динамическое искажение.

Статическое искажение происходит всего один раз. При этом модифицируются параметры программной среды компьютерной системы, чтобы впоследствии в ней выполнялись нужные злоумышленнику действия. Так, например, специалистам Федерального агентства правительственной связи и информации при Президенте РФ (ФАПСИ) удалось выявить при анализе одной из российских систем цифровой подписи интересное статистическое искажение. Злоумышленник (сотрудник отдела информатизации финансовой организации, в которой была внедрена данная система) исправил в исполняемом EXE-модуле программы проверки правильности цифровой подписи символьную строку «Подпись некорректна» на символьную строку «Подпись корректна». В результате перестали фиксироваться документы с неверными цифровыми подписями, и, следовательно, в электронные документы стало возможным вносить произвольные изменения уже после их подписания электронной цифровой подписью.

Динамическое искажение заключается в изменении каких-либо параметров системных или прикладных процессов при помощи заранее активизированных закладок. Динамическое искажение можно условно разделить так: искажение на входе (когда на обработку попадает уже искаженный документ) и искажение на выходе (когда искажается информация,

отображаемая для восприятия человеком или предназначенная для работы других программ).

Практика применения цифровой подписи в системах автоматизированного документооборота показала, что именно программная реализация цифровой подписи особенно подвержена влиянию программных закладок типа «динамическое искажение», которые позволяют осуществлять проводки фальшивых финансовых документов и вмешиваться в процесс разрешения споров по фактам неправомерного применения цифровой подписи. Например, в одной из программных реализаций широко известной криптосистемы PGP электронный документ, под которым требовалось поставить цифровую подпись, считывался блоками по 512 байт, причем процесс считывания считался завершенным, если в прочитанном блоке данные занимали меньше 512 байт. Работа одной программной закладки, выявленной специалистами, основывалась на навязывании размера файла. Эта закладка позволяла считывать только первые 512 байт документа, и в результате цифровая подпись определялась на основе только этих 512 байт. Такая же схема действовала и при проверке поставленной под документом цифровой подписи. Следовательно, оставшаяся часть этого документа могла быть произвольным образом искажена, и цифровая подпись под ним продолжала оставаться «корректной».

Модель **«уборка мусора»** заключается в следующем. Как известно, при хранении компьютерных данных на внешних носителях прямого доступа выделяется несколько уровней иерархии: секторы, кластеры и файлы. Секторы являются единицами хранения информации на аппаратном уровне. Кластеры состоят из одного или нескольких подряд идущих секторов. Файл – это множество кластеров, связанных по определенному закону.

Работа с конфиденциальными электронными документами обычно сводится к последовательности следующих манипуляций с файлами: создание, хранение, коррекция, уничтожение.

Для защиты конфиденциальной информации обычно используется шифрование. Основная угроза исходит не от использования нестойких алгоритмов шифрования и «плохих» криптографических ключей (как это может показаться на первый взгляд), а от текстовых редакторов и баз данных, применяемых для создания и коррекции конфиденциальных документов. Подобные программные средства, как правило, в процессе функционирования создают в оперативной или внешней памяти компьютерной системы временные копии документов, с которыми они работают. Все эти временные файлы выпадают из поля зрения любых программ шифрования и могут быть использованы злоумышленником для того, чтобы составить представление о содержании хранимых в зашифрованном виде конфиденциальных документов.

При записи отредактированной информации меньшего объема в тот же файл, где хранилась исходная информация до начала сеанса ее редактирования, образуются так называемые «хвостовые» кластеры, в которых эта исходная информация полностью сохраняется. И тогда «хвостовые» кластеры не только

не подвергаются воздействию программ шифрования, но и остаются незатронутыми даже средствами гарантированного стирания информации. В течение времени информация из «хвостовых» кластеров затирается данными из других файлов, однако, по оценкам специалистов ФАПСИ, из «хвостовых» кластеров через сутки можно извлечь до 85 %, а через десять суток – до 25–40 % исходной информации.

При использовании модели типа **«наблюдение»** программная закладка встраивается в сетевое или телекоммуникационное программное обеспечение. Подобное программное обеспечение всегда находится в состоянии активности, и внедренная в него программная закладка может следить за всеми процессами обработки информации в компьютерной системе, а также осуществлять установку и удаление других программных закладок.

Модель типа **«компрометация»** позволяет получать доступ к информации, перехваченной другими программными закладками. Например, инициируется постоянное обращение к такой информации, приводящее к росту соотношения сигнал/шум. Это значительно облегчает перехват побочных излучений данной компьютерной системы и позволяет эффективно выделять сигналы, сгенерированные закладкой типа «компрометация», из общего фона излучения, исходящего от оборудования.

Особыми разновидностями программных закладок являются **троянские программы** и **клавиатурные шпионы**.

Злоумышленник, решивший запустить в компьютер **троянскую программу**, обычно пытается сделать его частью системного файла. Такие файлы входят в дистрибутив операционной системы, и их присутствие на любом компьютере, где эта операционная система установлена, не вызывает никаких подозрений. Однако любой системный файл имеет определенный размер. Если данный атрибут будет каким-либо образом изменен, это встревожит пользователя. В борьбе с «троянцами» нельзя положиться на отметку о времени последней модификации файла и его размер, поскольку злоумышленник может легко подделать их.

Примечание. **Троянской программой (троянцем, троянским конем)** называется программа, которая, являясь частью другой программы с известными пользователю функциями, способна втайне от него выполнять некоторые дополнительные действия с целью причинения ему определенного ущерба, а также программа с известными ее пользователю функциями, в которую были внесены изменения, чтобы, помимо этих функций, она могла втайне от него выполнять некоторые другие (разрушительные) действия.

Более надежной в отношении троянских программ является контрольная сумма файла, для подсчета которой элементы файла суммируются. Однако более популярным решением для проверки целостности файловой системы компьютера является использование особой разновидности алгоритма вычисления контрольной суммы, называемым *односторонним хэшированием*. Функция хэширования называется односторонней, если задача отыскания двух аргументов, для которых ее значения совпадают, является труднорешаемой. Поэтому она может быть применена для того, чтобы отслеживать изменения, вносимые злоумышленником в файловую систему компьютера, поскольку

попытка злоумышленника изменить какой-либо файл так, чтобы значение, полученное путем одностороннего хэширования этого файла, осталось неизменным, обречена на неудачу.

Клавиатурные шпионы нацелены на перехват паролей пользователей операционной системы, а также на определение их легальных полномочий и прав доступа к компьютерным ресурсам.

Их поведение в общем случае является довольно традиционным: типовой клавиатурный шпион обманным путем завладевает пользовательскими паролями, а затем переписывает эти пароли туда, откуда их может извлечь злоумышленник.

Различия между клавиатурными шпионами определяются способами, которые применяются ими для перехвата пользовательских паролей. Соответственно, все клавиатурные шпионы делятся на три типа – *имитаторы*, *фильтры* и *заместители*.

Имитаторы работают по следующему алгоритму.

1. Злоумышленник внедряет в операционную систему программный модуль, который имитирует приглашение пользователю зарегистрироваться для того, чтобы войти в систему.
2. Внедренный модуль (в принятой терминологии – имитатор) переходит в режим ожидания ввода пользовательского идентификатора и пароля.
3. После того как пользователь идентифицирует себя и введет свой пароль, имитатор сохраняет эти данные там, где они доступны злоумышленнику.
4. Имитатор инициирует выход из системы (что в большинстве случаев можно сделать программным путем), и в результате на экране пользователя появляется множество уже настоящих приглашений для входа в систему.
5. Обманутый пользователь, видя, что ему предлагается еще раз внести пароль, приходит к выводу, что он допустил какую-то ошибку во время предыдущего ввода пароля, и повторяет всю процедуру входа в систему.

Некоторые имитаторы для убедительности выдают на экран монитора правдоподобное сообщение о якобы совершенной пользователем ошибке, например: «Неверный пароль. Попробуйте еще раз».

Злоумышленнику, умеющему программировать на одном из универсальных языков программирования, для внедрения понадобится несколько часов. Единственная трудность, с которой он может столкнуться, состоит в том, чтобы отыскать в документации соответствующую программную функцию, реализующую выход пользователя из системы.

Перехват пароля зачастую облегчают сами разработчики операционных систем, которые не предусматривают создание усложненных по форме приглашений пользователю зарегистрироваться для входа в систему. Подобное пренебрежительное отношение характерно для большинства версий операционной системы UNIX, в которых регистрационное приглашение состоит из двух текстовых строк, выдаваемых поочередно на экран терминала:

login:
password:

Фильтры отслеживают все данные, которые пользователь операционной системы вводит с клавиатуры компьютера. Элементарные фильтры просто сбрасывают перехваченный клавиатурный ввод на жесткий диск или в другое место, к которому имеет доступ злоумышленник. Более сложные программные закладки этого типа подвергают анализу перехваченные данные и отфильтровывают информацию, имеющую отношение к пользовательским паролям.

Фильтры являются резидентными программами, перехватывающими одно или несколько прерываний, которые связаны с обработкой сигналов от клавиатуры. Эти прерывания возвращают информацию о нажатой клавише и введенном символе, которая анализируется фильтрами на предмет выявления данных, имеющих отношение к паролю пользователя. В общем случае можно утверждать, что если в операционной системе разрешается переключать клавиатурную раскладку во время ввода пароля, то для этой операционной системы возможно создание фильтра. Поэтому, чтобы обезопасить ее от фильтров, необходимо обеспечить выполнение следующих трех условий:

1) запретить переключение раскладок клавиатуры во время ввода пароля;

2) разрешить конфигурирование цепочки программных модулей, участвующих в работе с паролем пользователя, только системному администратору;

3) позволить доступ к файлам этих модулей исключительно системному администратору.

Заместители полностью или частично подменяют собой программные модули операционной системы, отвечающие за аутентификацию пользователей.

Подобного рода клавиатурные шпионы могут быть созданы для работы в среде практически любой многопользовательской операционной системы. Трудоемкость написания заместителя определяется сложностью алгоритмов, реализуемых подсистемой аутентификации, и интерфейсов между ее отдельными модулями. Поскольку заместители берут на себя выполнение функций подсистемы аутентификации, перед тем как приступить к перехвату пользовательских паролей, они должны выполнить следующие действия:

1) подобно компьютерному вирусу, внедриться в один или несколько системных файлов;

2) использовать интерфейсные связи между программными модулями подсистемы аутентификации для встраивания себя в цепочку обработки введенного пользователем пароля.

Для того чтобы защитить систему от внедрения заместителя, ее администраторы должны строго соблюдать адекватную политику безопасности. Подсистема аутентификации должна быть одним из самых защищенных элементов операционной системы.

Таким образом, клавиатурные шпионы представляют собой реальную угрозу для безопасности современных компьютерных систем. Для того чтобы отвести эту угрозу, требуется реализовать целый комплекс административных мер и программно-аппаратных средств защиты. Надежная защита от клавиатурных шпионов может быть построена только при наличии у операционной системы затрудняющих их работу средств. Для защиты от клавиатурных шпионов администратор операционной системы должен соблюдать политику безопасности, при которой только администратор может:

- конфигурировать цепочки программных модулей, участвующих в процессе аутентификации пользователей;
- осуществлять доступ к файлам этих программных модулей;
- конфигурировать саму подсистему аутентификации.

4.3.2. Защита от программных закладок

Защита от программных закладок может рассматриваться в решении трех принципиально различных задач:

- недопущение внедрения программной закладки в компьютерную систему;
- своевременное обнаружение внедренной программной закладки;
- удаление внедренной программной закладки.

Решение этих задач возможно с помощью средств контроля за целостностью запускаемых системных и прикладных программ, информации, хранимой в компьютерной системе, а также за критическими для функционирования системы событиями [115].

Однако данные средства действенны только, когда сами не подвержены влиянию программных закладок, которые могут:

- навязывать конечные результаты контрольных проверок;
- влиять на процесс считывания информации и запуск программ, за которыми осуществляется контроль;
- изменять алгоритмы функционирования средств контроля.

При этом чрезвычайно важно, чтобы включение средств контроля выполнялось до начала воздействия программной закладки либо чтобы контроль осуществлялся только с использованием программ управления, находящихся в ПЗУ компьютерной системы.

Универсальным средством защиты от внедрения программных закладок является **создание изолированного компьютера**. Компьютер называется изолированным, если выполнены следующие условия:

- в нем установлена система BIOS, не содержащая программных закладок;
- операционная система проверена на наличие в ней закладок;
- достоверно установлена неизменность BIOS и операционной системы для данного сеанса;
- на компьютере не запускалось и не запускается никаких иных программ, кроме уже прошедших проверку на присутствие в них закладок;

- исключен запуск проверенных программ в каких-либо иных условиях, кроме перечисленных выше, т. е. вне изолированного компьютера.

Для определения степени изолированности компьютера может использоваться модель ступенчатого контроля:

1) проверка наличия изменений в BIOS;

2) при отсутствии изменений считываются загрузочный сектор диска и драйверы операционной системы, которые, в свою очередь, также анализируются на предмет внесения в них несанкционированных изменений;

3) с помощью операционной системы запускается драйвер контроля вызовов программ, который следит за тем, чтобы в компьютере запускались только проверенные программы.

Интересный метод борьбы с внедрением программных закладок может быть использован в информационной банковской системе, в которой циркулируют исключительно файлы-документы. Для того чтобы не допустить проникновения программной закладки через каналы связи, в этой системе не допускается прием никакого исполняемого кода. Для распознавания событий типа «Получен исполняемый код» и «Получен файл-документ» применяется контроль за наличием в файле запрещенных символов: файл признается содержащим исполняемый код, если в нем присутствуют символы, которые никогда не встречаются в файлах-документах.

Выявление внедренного кода программной закладки заключается в обнаружении *признаков* его присутствия в компьютерной системе.

Эти признаки можно разделить на следующие два класса.

1. *Качественные* и *визуальные* признаки – ощущения и наблюдения пользователя компьютерной системы, который отмечает определенные отклонения в ее работе (изменяется состав и размер файлов, старые файлы исчезают, вместо них появляются новые; программы начинают работать медленнее, или заканчивают свою работу слишком быстро, или перестают запускаться). Например, пользователи пакета шифрования и цифровой подписи «Криптоцентр» в течении некоторого времени замечали, что цифровая подпись под электронными документами ставится слишком быстро. Исследование, проведенное специалистами ФАПСИ, показало присутствие программной закладки, работа которой основывалась на навязывании размера файла. В другом случае тревогу забили пользователи пакета шифрования и цифровой подписи «Криптон», которые отметили, что скорость шифрования по криптографическому алгоритму ГОСТ 28147-89 резко возросла более, чем в 30 раз. А в третьем случае программная закладка обнаружила свое присутствие в программе клавиатурного ввода тем, что пораженная ею программа перестала работать в нормальном режиме.

2. Признаки, *обнаруживаемые средствами тестирования и диагностики*, характерны как для программных закладок, так и для компьютерных вирусов. Например, загрузочные закладки успешно обнаруживаются антивирусными программами, которые сигнализируют о наличии подозрительного кода в загрузочном секторе диска. С инициированием статической ошибки на дисках

хорошо справляется Disk Doctor, входящий в распространенный комплект утилит Norton Utilities. А средства проверки целостности данных на диске типа Adinf позволяют успешно выявлять изменения, вносимые в файлы программными закладками. Кроме того, эффективен поиск фрагментов кода программных закладок по характерным для них последовательностям нулей и единиц (сигнатурам), а также разрешение выполнения только программ с известными сигнатурами.

Способ **удаления внедренной программной закладки** зависит от метода ее внедрения в компьютерную систему. Если это программно-аппаратная закладка, то следует перепрограммировать ПЗУ компьютера. Если это загрузочная, драйверная, прикладная, замаскированная закладка или закладка-имитатор, то можно заменить ее на соответствующую загрузочную запись, драйвер, утилиту, прикладную или служебную программу, полученную от источника, заслуживающего доверия. Если это исполняемый программный модуль, то можно добыть его исходный текст, убрать из него имеющиеся закладки или подозрительные фрагменты, а затем заново откомпилировать.

4.4. Компьютерные вирусы и методы борьбы с ними

По среде обитания компьютерные вирусы делятся [116]:

- на *сетевые* (обитают в элементах компьютерных сетей);
- *файловые* (размещаются в исполняемых файлах);
- *загрузочные* (находятся в загрузочных секторах (областях) внешних запоминающих устройств (boot-секторах) – бутовые вирусы;
- *комбинированные* (размещаются в нескольких средах обитания).

По способу заражения среды обитания компьютерные вирусы делятся:

- на *резидентные* – после активизации полностью или частично перемещаются из среды обитания (сеть, загрузочный сектор, файл) в оперативную память ЭВМ; используя привилегированные режимы работы, разрешенные только операционной системе, заражают среду обитания и при выполнении определенных условий реализуют деструктивную функцию;
- *нерезидентные* – попадают в оперативную память ЭВМ только на время их активности, в течение которого выполняют деструктивную функцию и функцию заражения, после чего полностью покидают оперативную память, оставаясь в среде обитания; если вирус помещает в оперативную память программу, которая не заражает среду обитания, то такой вирус считается нерезидентным.

Рассмотрим основные категории, на которые делится **антивирусное ПО** (рис. 36).

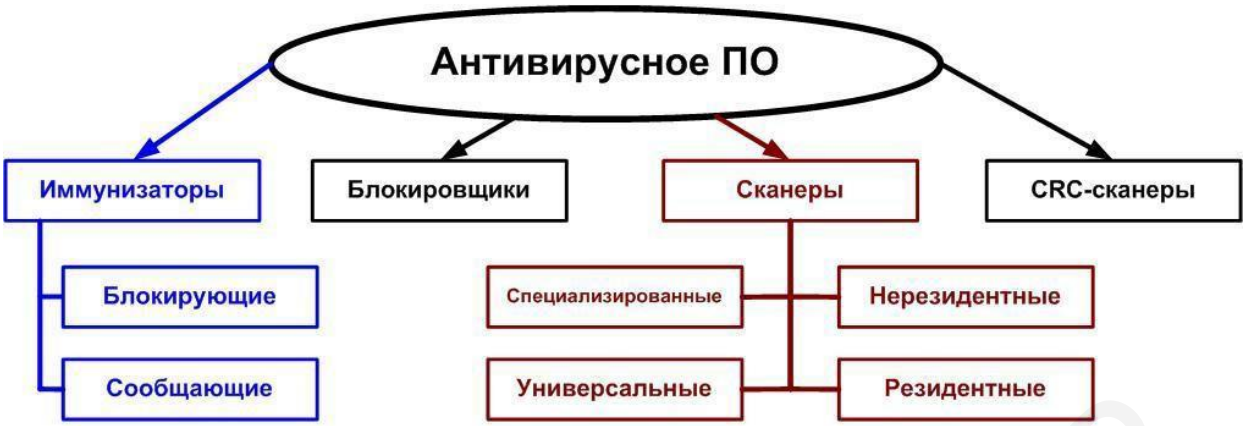

Рис. 36. Классификация антивирусного программного обеспечения

Сканеры

Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используется так называемая «маска» – некоторая постоянная последовательность кода, специфичная для этого конкретного вируса.

Если вирус не содержит постоянной маски или длина этой маски недостаточно велика, то используются другие методы, например алгоритмический язык, описывающий все возможные варианты кода, которые могут встретиться при заражении подобного типа вирусом. Во многих сканерах используются также алгоритмы «эвристического сканирования», т. е. анализ последовательности команд в проверяемом объекте, набор некоторой статистики и принятие решения («возможно заражен» или «не заражен») для каждого проверяемого объекта. Поскольку эвристическое сканирование является вероятностным методом поиска вирусов, на него распространяются многие законы теории вероятностей. Например, чем выше процент обнаруживаемых вирусов, тем больше количество ложных срабатываний.

Универсальные сканеры рассчитаны на поиск и обезвреживание всех типов вирусов вне зависимости от операционной системы, на работу в которой рассчитан сканер.

Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса. Например, сканеры, рассчитанные только на макро-вирусы, часто оказываются наиболее удобным и надежным решением для защиты систем документооборота в средах MS Word и MS Excel.

Сканеры также делятся на *резидентные* (мониторы), производящие сканирование «на лету», и *нерезидентные*, обеспечивающие проверку системы только по запросу. Как правило, «резидентные» сканеры обеспечивают более надежную защиту системы, поскольку они немедленно реагируют на появление вируса, в то время как нерезидентный сканер способен опознать вирус только во время своего очередного запуска.

CRC-сканеры

Принцип работы CRC-сканеров основан на подсчете CRC-сумм (контрольных сумм) для присутствующих на диске файлов / системных секторов. CRC-суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая другая информация: размеры файлов, даты их последней модификации и т. д. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом.

Антивирусные блокировщики

Это резидентные программы, перехватывающие «вирусо-опасные» ситуации и сообщающие о них пользователю.

Иммунизаторы

Сообщающие иммунизаторы обычно записываются в конец файлов (по принципу файлового вируса) и при запуске файла каждый раз проверяют его на наличие изменений. Недостаток таких иммунизаторов заключается в абсолютной неспособности сообщить о заражении стелс-вирусом. Поэтому такие иммунизаторы, как и блокировщики, практически не используются в настоящее время.

Блокирующий иммунизатор защищает систему от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные (пример – известная строка «MsDos», предохраняющая от вируса «Jerusalem»).

4.5. Межсетевое экранирование

При подключении корпоративной или локальной сети к глобальным сетям администратор сетевой безопасности должен решать следующие задачи [117]:

- защита корпоративной или локальной сети от несанкционированного удаленного доступа со стороны глобальной сети;
- скрытие информации о структуре сети и ее компонентов от пользователей глобальной сети;
- разграничение доступа в защищаемую сеть из глобальной и из защищаемой сети в глобальную.

Необходимость работы с удаленными пользователями требует установления жестких ограничений доступа к информационным ресурсам защищаемой сети. При этом в организации часто возникает потребность иметь в составе корпоративной сети несколько сегментов с разными уровнями защищенности:

- свободно доступные сегменты;
- сегменты с ограниченным доступом;
- закрытые сегменты.

Посредством использования открытости корпоративных компьютерных сетей нарушитель может:

- вторгнуться во внутреннюю сеть предприятия и получить несанкционированный доступ к конфиденциальной информации;
- незаконно скопировать важную и ценную для предприятия информацию;
- получить пароли, адреса серверов, а подчас и их содержимое;
- войти в информационную систему предприятия под именем зарегистрированного пользователя и т. д.

Для отражения наиболее вероятных угроз для внутренних сетей используются межсетевые экраны.

Межсетевой экран – это система межсетевой защиты, позволяющая разделить каждую сеть на две и более части и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Межсетевой экран представляет собой набор компонентов, настраиваемых для реализации выбранной политики безопасности.

Как правило, эта граница проводится между корпоративной (локальной) сетью предприятия и глобальной сетью Интернет, также ее можно провести и внутри корпоративной сети предприятия. Использование межсетевых экранов позволяет организовать внутреннюю политику безопасности сети предприятия, разделив всю сеть на сегменты. Это позволяет сформулировать основные *принципы* архитектуры безопасности корпоративной сети.

1. Введение N категорий секретности и создание соответственно N выделенных сетевых сегментов пользователей. При этом каждый пользователь внутри сетевого сегмента имеет одинаковый уровень секретности (допущен к информации одного уровня секретности). Эта структура объясняется тем, что ни в коем случае нельзя смешивать потоки информации разных уровней секретности. Не менее очевидным объяснением подобного разделения всех пользователей на N изолированных сегментов является легкость осуществления атаки внутри одного сегмента сети.

2. Выделение в отдельный сегмент всех внутренних серверов компании. Эта мера также позволяет изолировать потоки информации между пользователями, имеющими различные уровни доступа.

3. Выделение в отдельный сегмент всех серверов компании, к которым будет предоставлен доступ из сети Интернет (создание демилитаризованной зоны для внешних ресурсов).

4. Создание выделенного сегмента административного управления.

5. Создание выделенного сегмента управления безопасностью.

Межсетевой экран пропускает через себя весь трафик, принимая относительно каждого проходящего пакета решение насчет его пропуска. Для того чтобы межсетевой экран мог осуществить эту операцию, необходимо определить набор правил фильтрации, которые зависят от принятой в защищаемой сети политики безопасности.

Политика сетевой безопасности каждой организации должна включать две составляющие.

1. *Политика доступа к сетевым сервисам*.

Политика доступа к сетевым сервисам должна быть уточнением общей политики организации в отношении защиты информационных ресурсов в организации. Для того чтобы межсетевой экран успешно защищал ресурсы организации, политика доступа пользователей к сетевым сервисам должна быть реалистичной – таковой считается политика, при которой найден гармоничный баланс между защитой сети организации от известных рисков и необходимостью доступа пользователей к сетевым сервисам. В соответствии с принятой политикой доступа к сетевым сервисам определяется список сервисов сети Интернет, к которым пользователи должны иметь ограниченный доступ. Задаются также ограничения на методы доступа, необходимые для того, чтобы пользователи не могли обращаться к запрещенным сервисам сети Интернет обходными путями.

2. *Политика реализации межсетевых экранов.*

Межсетевой экран может реализовать ряд политик доступа к сервисам. Но, как правило, такая политика основана на одном из следующих принципов: запретить доступ из сети Интернет во внутреннюю сеть и разрешить доступ из внутренней сети в сеть Интернет, например, обеспечивая работу только отдельных авторизованных систем (информационных и почтовых серверов). В соответствии с политикой реализации межсетевых экранов определяются правила доступа к ресурсам внутренней сети. Прежде всего необходимо установить, насколько «доверительной» или «подозрительной» должна быть система защиты.

Правила доступа к внутренним ресурсам должны базироваться на одном из следующих принципов:

- запрещать все, что не разрешено в явной форме;
- разрешать все, что не запрещено в явной форме.

Эффективность защиты внутренней сети с помощью межсетевых экранов зависит не только от выбранной политики доступа к сетевым сервисам и ресурсам внутренней сети, но и от рациональности выбора и использования основных компонентов межсетевого экрана.

Функциональные требования к межсетевым экранам охватывают следующие сферы:

- фильтрация на сетевом уровне;
- фильтрация на прикладном уровне;
- настройка правил фильтрации и администрирование;
- средства сетевой аутентификации;
- внедрение журналов и учет.

В настоящее время не существует единой и общепризнанной **классификации межсетевых экранов**, однако можно выделить следующие их категории:

- коммутаторы, функционирующие на канальном уровне;

- фильтрующие маршрутизаторы (сетевые/пакетные фильтры);
- шлюзы сеансового уровня;
- шлюзы уровня приложений.
- инспекторы состояния.

Эти категории можно рассматривать как базовые компоненты реальных межсетевых экранов, поскольку немногие межсетевые экраны включают лишь одну из перечисленных категорий.

Коммутаторы

Данные устройства, функционирующие на канальном уровне, не принято причислять к классу межсетевых экранов, т. к. они разграничивают доступ в рамках локальной сети и не могут быть применены для ограничения трафика из сети Интернет. Однако, если учитывать, что межсетевой экран разделяет доступ между двумя сетями или узлами, такое причисление вполне закономерно.

Многие производители коммутаторов, например, Cisco, Nortel, 3Com, позволяют осуществлять фильтрацию трафика на основе MAC-адресов, которые содержатся во фреймах, пытающихся получить доступ к определенному порту коммутатора. Наиболее эффективно данная возможность реализована в решениях компании Cisco, в частности в семействе коммутаторов Catalyst, которые обладают механизмом Port Security.

Когда через коммутатор проходят Ethernet-фреймы, он заполняет таблицу MAC-адресов, используя адрес отправителя, который указан в этих фреймах. Злоумышленник посредством специального софта генерирует множество фреймов со случайными обратными адресами. Результатом этих действий является переполнение таблицы MAC-адресов, и коммутатор может начать действовать как концентратор. Злоумышленник запускает сниффер (программу для просмотра входящих пакетов), и все пакеты, проходящие через коммутатор, будут видны атакующему.

Для того чтобы избежать подобной ситуации, на всех коммутаторах настраивается Port Security. Для каждого порта ограничивается список (или количество)
MAC-адресов, которые на нем могут появляться; если на порте замечено слишком много адресов, то он «тушится» (идея с генерированием фреймов со случайными обратными адресами исключается).

Существует два способа введения ограничений на MAC-адреса:

- *статический* – администратор перечисляет, какие адреса разрешены;
- *динамический* – администратор указывает количество разрешенных адресов, а коммутатор обучается, запоминая, какие адреса в настоящий момент обращаются через указанный порт.

Если безопасность нарушена и к порту обращается адресов больше, чем настроено в Port Security, то за действия коммутатора в этом случае отвечает один из трех режимов:

- *Protect* – фреймы с новыми MAC-адресами игнорируются, остальные фреймы и порт продолжают работать;

- *Restrict* – идентичен режиму Protect за тем исключением, что коммутатор по SNMP уведомляет о происходящей ситуации и записывает информацию об этом в syslog;

- *Shutdown* – кроме передачи сообщений в syslog и по SNMP, порт закрывается, что отрицательно влияет на отказоустойчивость сети, но зато злоумышленник не может продолжить исследование сети до включения порта.

Фильтрующие маршрутизаторы

Основными функциями IP-маршрутизатора являются создание таблицы маршрутизации и продвижение IP-пакетов на основе данных этой таблицы. Для выполнения этих функций маршрутизатор должен поддерживать протокол IP и протоколы маршрутизации.

Фильтрующий маршрутизатор представляет собой маршрутизатор или работающую на сервере программу, сконфигурированную таким образом, чтобы фильтровать входящие и исходящие пакеты. Фильтрация пакетов осуществляется на основе информации, содержащейся в TCP- и IP-заголовках пакетов.

Под **фильтрацией** понимается нестандартная обработка IP-пакетов маршрутизаторами, приводящая к отбрасыванию некоторых пакетов или изменению их маршрута.

Многие маршрутизаторы поддерживают развитые средства фильтрации пользовательского трафика, а также фильтрации объявлений протоколов маршрутизации, что позволяет дифференцированно управлять достижимостью узлов [118].

Условия фильтрации маршрутизаторов обычно учитывают различные признаки, например:

- IP-адрес источника и приемника;
- MAC-адреса источника и приемника;
- идентификатор интерфейса, с которого поступил пакет;
- тип протокола, сообщение которого несет IP-пакет (т. е. TCP, UDP, ICMP или OSPF);
- номер порта TCP/UDP (т. е. тип протокола прикладного уровня).

При наличии фильтра маршрутизатор сначала проверяет совпадение условия, описанного этим фильтром, с признаками пакета и при положительной проверке выполняет ряд нестандартных действий. Пакет может быть:

- отброшен (drop);
- направлен к следующему маршрутизатору, отличающемуся от того, который указан в таблице маршрутизации;
- помечен как вероятный кандидат на отбрасывание при возникновении перегрузки;
- передан соответствии с записями таблицы маршрутизации.

Рассмотрим примеры фильтров, написанных на командном языке маршрутизаторов Cisco.

Фильтры, называемые **списками доступа**, сегодня в IP-маршрутизаторах являются очень распространенным средством ограничения пользовательского трафика.

Наиболее простым является **стандартный список доступа**, который учитывает в качестве условия фильтрации только IP-адрес источника. Общая форма такого условия выглядит следующим образом:

access-list номер_списка_доступа {deny | permit}
{адрес_источника [метасимволы_источника] | any}

Стандартный список доступа определяет два действия с пакетом, который удовлетворяет описанному в фильтре условию:

- **deny** – отбросить;
- **permit** – передать для стандартной обработки в соответствии с таблицей маршрутизации.

Условием выбора того или иного действия в стандартном списке доступа является совпадение IP-адреса источника пакета с адресом источника, заданным в списке.

Совпадение проверяется таким же образом, что и при проверке таблицы маршрутизации, при этом *метасимволы* являются аналогом маски, но в несколько модифицированном виде:

- «0» в поле метасимволов источника означает, что требуется совпадение значения этого разряда в адресе пришедшего пакета и в адресе, заданном в списке доступа;
- «1» в поле метасимволов источника означает, что совпадения в этом разряде не требуется.

Практически, если требуется задать условие для всех адресов некоторой подсети, должно использоваться инвертированное значение маски этой подсети. Параметр **any** означает, что любое значение адреса – это более понятная и краткая форма записи значения 255.255.255.255 в поле метасимволов источника.

Пример стандартного списка доступа:

access-list 1 deny 192.78.46.0 0.0.0.255

Здесь 1 – номер списка доступа; deny – действие с пакетом, который удовлетворяет условию данного списка доступа; 192.78.46.0 – адрес источника; 0.0.0.255 – метасимволы источника.

Этот фильтр запрещает передачу пакетов, у которых в старших 3 байтах адреса источника имеется значение 192.78.46.0.

Список доступа может включать более одного условия. В этом случае он состоит из нескольких строк с ключевым словом **access-list** и одним и тем же номером списка доступа.

Например, если мы хотим разрешить прохождение через маршрутизатор пакетов хоста 192.78.46.12, запрещая передачу пакетов одному из хостов сети 192.78.46.0/24, то список доступа будет выглядеть следующим образом:

access-list 1 permit 192.78.46.12 0.0.0.0
access-list 1 deny 192.78.46.0 0.0.0.255
access-list 1 permit any

Примечание. **ACL** (**Access Control List**) – это набор текстовых выражений, разрешающих/запрещающих что-либо. Обычно ACL разрешает или запрещает IP-пакеты, также он может просматривать содержание, тип пакета, TCP и UDP порты.

Условия списка доступа проверяются по очереди. Если какое-либо из условий дает совпадение, то выполняется действие **permit** или **deny**, определенное в этом условии, после чего остальные условия списка уже не проверяются. Считается по умолчанию, что в конце каждого списка имеется неявное условие вида:

[access-list 1 deny any]

Однако, если требуется пропускать все пакеты, не определенные явно в условиях, необходимо добавить в последней строке условие:

access-list 1 permit any

Список доступа можно применять к любому интерфейсу маршрутизатора и в любом направлении: если список применяется с ключевым словом **in**, то он действует на входящие в интерфейс пакеты, если с ключевым словом **out** – то на выходящие.

Например, список доступа 1:

access-list 1 permit 192.78.46.12 0.0.0.0
access-list 1 deny 192.78.46.0 0.0.0.255
access-list 1 permit any

Его можно применить к некоторому интерфейсу для обработки входящего трафика, используя следующую команду:

access-group 1 in

Существуют более мощные типы списков доступа для маршрутизаторов Cisco, например, **расширенные списки доступа**. Общий формат этих списков следующий:

access-list номер_списка_доступа {deny | permit}
{protocol | ключевое_слово_протокола}
{адрес_источника [метасимволы_источника]][порт_источника] | any}

[адрес_приемника [метасимволы_приемника]][порт_приемника]

Пользуясь расширенными списками доступа, можно запретить прохождение во внутреннюю сеть предприятия FTP-пакетов. Как известно, FTP задействует для приема запросов от клиентов протокол TCP с хорошо известным портом 21. Для этого в список доступа нужно включить условие:

access-list 102 deny TCP any 21 any

Затем можно применить его к интерфейсу маршрутизатора, к которому подключена внутренняя сеть, с ключевым словом **out**. Администраторы корпоративных сетей часто запрещают возможность трассировки извне внутренних хостов утилитой **ping**. Это делается с помощью условия:

access-list 101 deny ICMP any 192.78.46.8 0.0.0.0 eq 8

Синтаксис этого условия для протокола ICMP несколько отличается от общего синтаксиса расширенных списков доступа. Параметр **eq 8** означает, что запрещается передача ICMP-сообщений типа 8, соответствующего эхо-запросам, на основе которых разработана утилита **ping**. Еще более гибким является язык фильтров программного маршрутизатора, работающего во многих версиях Unix. Синтаксис этого языка близок к синтаксису языка C, что позволяет строить весьма сложные логические конструкции с помощью условных операторов **if**, **then**, **else**.

Необходимо отметить, что фильтрация пользовательского трафика может существенно замедлять работу маршрутизатора, т. к. обработка каждого пакета требует проверки дополнительных условий. Для того чтобы не создавать еще большую нагрузку на маршрутизатор и не отвлекать его от выполнения основных обязанностей, в фильтрах маршрутизаторов не используется информация о предыстории сеансов. Даже при сложном условии фильтрации маршрутизатора в нем учитываются только параметры текущего пакета и не могут учитываться параметры предыдущих пакетов, уже обработанных маршрутизатором, – это главное отличие маршрутизаторов от брандмауэров – специальных программных систем, которые, используя информацию о предыстории сеансов, выполняют более качественную фильтрацию.

Даже если администратору сети удастся создать эффективные правила фильтрации, их возможности останутся ограниченными. Например, администратор задает правило, в соответствии с которым маршрутизатор будет отбраковывать все пакеты с неизвестным адресом отправителя. Однако в данном случае хакер для проникновения внутрь защищенной сети может осуществить атаку, которую называют подменой адреса. В таких условиях фильтрующий маршрутизатор не сумеет отличить поддельный пакет от настоящего и пропустит его.

К положительным качествам фильтрующих маршрутизаторов можно отнести следующие:

- сравнительно невысокая стоимость;
- гибкость в определении правил фильтрации;
- небольшая задержка при прохождении пакетов.

Недостатки фильтрующих маршрутизаторов:

- внутренняя сеть видна (маршрутизируется) из сети Интернет;
- правила фильтрации пакетов трудны в описании и требуют очень хороших знаний технологий TCP и UDP;
- при нарушении работоспособности межсетевого экрана с фильтрацией пакетов все компьютеры за ним становятся полностью незащищенными либо недоступными;
- отсутствует аутентификация на пользовательском уровне.

Шлюзы сеансового уровня

Данный класс маршрутизаторов представляет собой транслятор TCP-соединения. Шлюз принимает запрос авторизованного клиента на конкретные услуги и после проверки допустимости запрошенного сеанса устанавливает соединение с местом назначения (внешним хостом). После этого шлюз копирует пакеты в обоих направлениях, не осуществляя их фильтрации.

Данный тип шлюза позволяет создать транслятор TCP-соединения для любого определенного пользователем сервиса, базирующегося на TCP, осуществлять контроль доступа к этому сервису и сбор статистики по его использованию.

Шлюз следит за подтверждением (квитированием) связи между авторизованным клиентом и внешним хостом, определяя, является ли запрашиваемый сеанс связи допустимым. Чтобы выявить допустимость запроса на сеанс связи, шлюз выполняет следующую процедуру:

- авторизованный клиент запрашивает некоторый сервис, шлюз принимает этот запрос, проверяя, удовлетворяет ли данный клиент базовым критериям фильтрации;
- действуя от имени клиента, шлюз устанавливает соединение с внешним хостом и следит за выполнением процедуры квитирования связи по протоколу TCP – эта процедура состоит из обмена TCP-пакетами, которые помечаются флагами SYN (синхронизировать) и ACK (подтвердить).

Первый пакет сеанса TCP, помеченный флагом SYN и содержащий произвольное число, является запросом клиента на открытие сеанса. Внешний хост, получивший этот пакет, посылает в ответ другой, помеченный флагом ACK и содержащий число на единицу большее, чем в принятом пакете, подтверждая тем самым прием пакета SYN от клиента.

Далее осуществляется обратная процедура: хост посылает клиенту пакет SYN с исходным числом, а клиент подтверждает его получение передачей пакета ACK. На этом процесс квитирования связи завершается (рис. 37).

Рис. 37. Пример процесса квитирования с передачей пакета ACK

Шлюз сеансового уровня признает завершенное соединение допустимым только в том случае, если при выполнении процедуры квитирования связи флаги SYN и ACK, а также числа, содержащиеся в TCP-пакетах, оказываются логически связанными между собой.

Начиная с этого момента шлюз копирует и перенаправляет пакеты туда и обратно, не проводя фильтрации. Он поддерживает таблицу установленных соединений, пропуская данные, которые относятся к одному из сеансов связи, зафиксированных в данной таблице. Когда сеанс завершается, шлюз удаляет соответствующий элемент из таблицы и разрывает сеть, использовавшуюся в текущем сеансе.

Недостатком шлюзов сеансового уровня является отсутствие проверки содержимого передаваемых пакетов, что дает возможность нарушителю проникнуть через такой шлюз.

Шлюзы уровня приложений

С целью защиты ряда уязвимых мест, присущих фильтрующим маршрутизаторам, межсетевые экраны должны использовать прикладные программы для фильтрации соединений с такими сервисами, как Telnet и FTP. Подобное приложение называется *proxy-службой*, а хост, на котором работает proxy-служба, – *шлюзом уровня приложений*, который исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Посредники прикладного уровня практически не отличаются от шлюзов сеансового уровня, за исключением того, что они также осуществляют посредническую функцию между двумя узлами, исключая их непосредственное взаимодействие, но позволяют проникать в контекст передаваемого трафика, т. к. функционируют на прикладном уровне.

Межсетевые экраны, построенные по этой технологии, содержат т. н. посредников приложений (application proxy), которые, «зная», как функционирует то или иное приложение, могут обрабатывать сгенерированный

ими трафик. Например, разрешать в исходящем трафике команду **get** (получение файла) протокола FTP и запрещать команду **put** (отправка файла) и наоборот. Еще одно отличие от шлюзов сеансового уровня – возможность фильтрации каждого пакета.

Инспекторы состояния

Каждый из названных классов межсетевых экранов обладает рядом достоинств и может применяться для защиты корпоративных сетей. Однако куда более эффективным было бы объединить все названные классы МСЭ в одном устройстве – *инспекторах состояний*, которые совмещают в себе все достоинства названных выше типов экранов, начиная с анализа трафика сетевого/прикладного уровней и обеспечивают высокий уровень производительности и защищенности.

Межсетевые экраны такого типа позволяют контролировать:

- каждый передаваемый пакет на основе имеющейся таблицы правил;
- каждую сессию на основе таблицы состояний;
- каждое приложение на основе разработанных посредников.

В настоящий момент на рынке средств защиты информации в большей степени распространены два класса межсетевых экранов: инспекторы состояний и пакетные фильтры.

4.6. Защита сетевого трафика

Наиболее простым средством для предоставления сервиса защиты сетевого трафика является технология защищенного канала, которая обеспечивает защиту трафика между двумя пользователями публичной сети, т. е. в соответствии с двухточечной топологией. Такая защита осуществляется за счет комплекса средств, опирающихся на различные методы аутентификации пользователей и шифрования их трафика.

В IP-сетях широко применяются две технологии защищенного канала – SSL и IPSec. Протокол SSL работает на уровне представления модели OSI, что делает его непрозрачным для приложений. Протокол IPSec является более универсальным средством, т. к. относится к сетевому уровню и полностью прозрачен для приложений, которые в случае использования IPSec не требуют модификации.

Основное назначение сервиса IPSec (Internet Protocol Security – защищенный протокол IP) состоит в обеспечении безопасной передачи данных по IP-сетям. Применение протокола IPSec гарантирует целостность, аутентичность и конфиденциальность данных. Базовой технологией, на основе которой достигаются эти цели, является шифрование. Для протоколов такого назначения используется обобщенное название – защищенный канал.

Более масштабным средством защиты трафика являются виртуальные частные сети (Virtual Private Network, VPN). Подобная сеть является своего рода «сетью в сети», сервисом, создающим у пользователей иллюзию существования их частной сети внутри публичной сети. Одним из важнейших свойств такой

«частной сети» является защищенность трафика от атак пользователей публичной сети.

Сетям VPN доступна не только возможность имитации частной сети, они дают пользователю возможность задействовать собственное адресное пространство (например, частные IP-адреса, такие как адреса сети 10.0.0.0) и обеспечивать качество обслуживания, близкое к качеству выделенного канала.

Обнаружение вторжений – это активный процесс, при котором происходит обнаружение хакера при его попытках проникнуть в систему.

Обнаружение вторжений помогает при превентивной идентификации активных угроз (немедленная защита от атак сразу после их появления, обеспечивающая защиту от неизвестных угроз и уязвимых мест) посредством оповещений и предупреждений о том, что злоумышленник осуществляет сбор информации, необходимой для проведения атаки.

Системы обнаружения вторжений IDS (Intrusion Detection System) предназначены для разграничения авторизованного входа и несанкционированного проникновения.

При создании политики IDS необходимо выполнить следующие шаги:

- определить цели создания IDS;
- выбрать объекты мониторинга;
- выбрать ответные действия;
- установить пороги;
- применить политику.

Потенциально целями применения IDS являются следующие:

- обнаружение атак;
- предотвращение атак;
- обнаружение нарушений политики;
- принуждение к использованию политик;
- принуждение к следованию политикам соединений;
- сбор доказательств.

Рассмотрим типы таких систем.

Узловая, или хостовая, система обнаружения вторжений (Host-based Intrusion Detection System, HIDS) располагается на отдельном узле и отслеживает признаки атак на данный узел. Узловые IDS (HIDS) представляют собой систему датчиков, загружаемых на различные серверы организации и управляемых центральным диспетчером.

Датчики HIDS отслеживают события, связанные с сервером, на котором они загружены, предпринимают определенные действия на сервере либо передают уведомления. Сенсор HIDS позволяет определить, была ли атака успешной, если атака имела место на той же платформе, на которой установлен датчик. Датчик на сервере может занимать от 5 до 15 % общего процессорного времени, поэтому иногда возникает необходимость приобретать более производительную систему, чтобы присутствие датчика не сказалось отрицательно на ее производительности.

Пять основных типов датчиков HIDS:

- анализаторы журналов;
- датчики признаков;
- анализаторы системных вызовов;
- анализаторы поведения приложений;
- контролеры целостности файлов.

Анализатор журнала. На сервере отслеживаются соответствующие файлы журналов в системе. При соответствии записи в журнале и критерия в процессе датчика HIDS, предпринимается установленное действие. Администратор системы при желании может определить другие записи журнала, представляющие определенный интерес. Анализаторы журналов не предотвращают атаку на систему, а реагируют на событие уже после того, как оно произошло. Их можно использовать для отслеживания активности и перемещения записи об активности персонала в область, недосягаемую для администратора или пользователя.

Датчики признаков – это наборы определенных признаков событий безопасности, сопоставляемых со входящим трафиком или записями журнала. Возможность анализа входящего трафика является отличием данных датчиков от анализаторов журналов. Датчик признаков HIDS является полезным при отслеживании авторизованных пользователей внутри информационных систем.

Анализаторы системных вызовов осуществляют анализ вызовов между приложениями и операционной системой для идентификации событий, связанных с безопасностью. При выполнении приложением действий его вызов операционной системы анализируется и сопоставляется с базой данных признаков, которые являются примерами различных типов поведения, представляющих собой атакующие действия, или объектом интереса для администратора IDS. Анализаторы системных вызовов отличаются от выше перечисленных датчиков тем, что они могут предотвращать действия. Обеспечение неправильной конфигурации датчиков этого типа или их некорректная настройка влечет за собой ошибки в приложениях либо отказы в их работе.

Анализаторы поведения приложений – применяются в виде программной спайки между приложениями и операционной системой, проверяют вызов на предмет того, разрешено ли приложению выполнять данное действие, вместо определения соответствия вызова признакам атак. При конфигурировании таких датчиков необходимо создавать список действий, разрешенных для выполнения каждым приложением. Поставщики датчиков данного типа предоставляют шаблоны для наиболее широко используемых приложений.

Контролеры целостности файлов отслеживают изменения в файлах посредством использования криптографической контрольной суммы или цифровой подписи файла (шифрование). При изменении хотя бы малой части исходного файла (например, атрибутов файла – времени и даты создания) конечная цифровая подпись файла будет изменена. Цель данного алгоритма – максимальное снижение возможности для внесения изменений в файл с сохранением прежней подписи.

Сетевая система обнаружения вторжений (Network Intrusion Detection System, NIDS) находится на отдельной системе, отслеживающей сетевой трафик на наличие признаков атак, проводимых в подконтрольном сегменте сети. *NIDS (Network Intrusion Detection System)* – это программный процесс, работающий на специально выделенной системе и отвечающий за переключение сетевой карты в системе в неразборчивый режим работы, при котором сетевой адаптер пропускает весь сетевой трафик в программное обеспечение NIDS.

Система анализирует трафик, используя набор правил и признаков атак для определения того, представляет ли этот трафик какую-либо угрозу, после чего генерируется соответствующее событие.

На данный момент в большинство систем NIDS встроен набор признаков атак, с которыми сопоставляется трафик в канале связи. При отсутствии признаков атаки в системе обнаружения вторжений система NIDS «не замечает» эту атаку. Данные системы позволяют указывать интересующий трафик по адресу источника, конечному адресу, порту источника или конечному порту, что дает возможность отслеживания трафика, не соответствующего признакам атак.

4.7. Методы мониторинга состояния сети

Выбор способов и объектов мониторинга сети зависит от множества факторов: конфигурации сети, действующих в ней сервисов и служб, конфигурации серверов и установленного на них ПО, возможностей ПО, используемого для мониторинга, и т. п. На общем уровне мониторинга можно говорить о таких элементах, как:

- проверка физической доступности оборудования;
- проверка состояния (работоспособности) служб и сервисов, запущенных в сети;
- детальная проверка важных параметров функционирования сети (производительности, загрузки и т. п.);
- проверка параметров, специфичных для сервисов и служб данного конкретного окружения (наличие некоторых значений в таблицах БД, содержимое лог-файлов).

Системы мониторинга и корреляции событий информационной безопасности представлены следующими вендорами: Symantec, Tenable Network Security, AlienVault, SolarWinds, EMC-RSA, LogLogic, NetIQ, Sensage, EiQ Networks, EventTracker, Trustwave, IBM Qradar, McAfee Nitro, Splunk, RSA Security Analytics, LogRhythm, HP ArcSight.

Исследовательская и консалтинговая компания Gartner на основе анализа мирового рынка выделяет среди вендоров 6 наиболее крупных: IBM Qradar, McAfee Nitro, Splunk, RSA Security Analytics, LogRhythm, HP ArcSight [119].

Рынок Республики Беларусь представлен небольшим числом систем мониторинга и корреляции. В частности в РБ процедуру экспертизы, согласно перечню прошедших экспертизу средств, опубликованному на сайте

Оперативно-аналитического центра при Президенте Республики Беларусь, прошли только 2 из перечисленных решений– IBM QRadar и HP ArcSight.

Основными потребителями систем мониторинга и корреляции событий информационной безопасности HP ArcSight в РБ являются предприятия финансового сектора:

- ОАО «АСБ «Беларусбанк»;
- ОАО «Белгазпромбанк»;
- ОАО «Банковский процессинговый центр»;
- ОАО «Банк БелВЭБ».

Система мониторинга и корреляции событий информационной безопасности IBM QRadar используется в ЗАО «МТБанк».

На данный момент единственной прошедшей сертификацию на соответствие требованиям Технического Регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» и, соответственно, единственной доступной для обращения на рынке средств защиты информации Республики Беларусь является система мониторинга и корреляции событий информационной безопасности **HP ArcSight**, которая поддерживает механизм управления инцидентами, позволяющий использовать СМК в качестве единой точки проведения расследований инцидентов.

Рассмотрим наиболее крупных вендоров систем мониторинга и корреляции событий информационной безопасности в табл. 6.

Таблица 6

Крупнейшие вендоры систем мониторинга и корреляции информационной безопасности

Название	Компоненты	Достоинства	Недостатки
1	2	3	4
IBM QRadar IBM Qradar Integrated Security Solutions	- *QRadar SIEM* – компонент, выполняющий функции по управлению журналами аудита, угрозами и рисками; - *QRadar Risk Manager* – компонент, выполняющий функции моделирования угроз и рисков, анализ их влияния на безопасность системы; - *QRadar QFlow* – компонент, выполняющий функции по анализу сетевого трафика и определению аномалий; - *QRadar VFlow* – компонент, выполняющий функции мониторинга уровня приложений	- Простота развертывания и настройки; - поведенческий анализ и детектирование аномалий; - ориентированность на небольшие, средние и крупные предприятия	- Слабые возможности гибкой настройки

1	2	3	4
Splunk Splunk Enterprise	- *Splunk Indexer* – компонент, выполняющий функции сбора и индексации полученных событий; - *Splunk Search Head* – компонент, выполняющий функции поиска и создания отчетности; - *Splunk App for Enterprise Security* – компонент, выполняющий функции синтаксического анализа событий, а также ограниченного анализа событий VPN	- Интуитивно понятный поиск событий; - гибкие возможности визуализации данных; - возможность разработки дополнений, расширяющих функциональность	- Ограниченные возможности корреляции; - сложность настройки
RSA Security Analytics	- *RSA Security Analytics Decoder* – компонент, выполняющий функции захвата сетевых пакетов и журналов аудита с возможностью анализа и фильтрации; - *RSA Security Analytics Concentrator* – компонент, выполняющий функции агрегации данных, полученных от компонента *Decoder*; - *RSA Security Analytics Broker Server* – компонент, выполняющий функции создания отчетности и управления информацией, полученной в результате работы компонента *Decoder*; - *Event Stream Analysis* – компонент, выполняющий функции корреляции; - *Archiver* – компонент, выполняющий функции долговременного хранения; - *RSA Security Analytics Warehouse* – компонент, выполняющий функции расширенной аналитики.	- Хорошая продуктивность работы с большими объемами данных; - хорошая интегрируемость с другими решениями компании RSA	- Ориентированность исключительно на крупные предприятия; - сложность настройки

Окончание таблицы 6

1	2	3	4
LogRhythm LogRhythm SIEM 2.0 Security Intelligence Platform	- *Log Manager* – компонент, выполняющий функции сбора событий; - *Event Manager* – компонент, выполняющий функции централизованного управления событиями; - *Network Monitor* – компонент, выполняющий функции захвата и инспекции сетевых пакетов, предоставляющий возможность поиска по неструктурированной информации.	Быстрота и простота настройки	- Невысокая производительность; - ориентированность на небольшие и средние предприятия; - невысокая степень интеграции с различными источниками
HP ArcSight	- *ArcSight Enterprise Security Manager (ESM)* – компонент, выполняющий функции корреляции и анализа событий, поиска и создания отчетности и оповещения; - *ArcSight Logger* – компонент, выполняющий функции хранения и поиска; - *ArcSight IdentityView* – компонент, выполняющий функции мониторинга активности пользователей; - *ArcSight Connectors* – компонент, выполняющий функции сбора событий от любых источников	- Широкие возможности по интеграции; - поддержка большого количества источников (более 350); - ориентированность на небольшие, средние и крупные компании; - высокая производительность; - гибкость настройки под необходимые условия заказчика	Сложность развертывания и настройки

ЗАКЛЮЧЕНИЕ

Нормативно-правовая база Республики Беларусь обеспечивает механизмы комплексного подхода государства к обеспечению информационной безопасности, охватывая все сферы жизнедеятельности человека как гражданина и личности. Спектр законов Республики Беларусь в области информационной безопасности и защиты информации, сформированный с учетом развития современных информационных технологий, позволяет обеспечить безопасность персональных данных пользователей интернет-ресурсов, платежных систем, реализовать и внедрить механизмы политики безопасности на предприятиях любой формы собственности. Техническое нормирование и стандартизация в области информационной безопасности, реализованное на базе Оперативно-аналитического центра при Президенте Республики Беларусь, является результатом консолидации усилий и ресурсов государства, институтов гражданского общества и граждан по защите и реализации национальных интересов Республики Беларусь.

Классификация потенциально возможных угроз информационной безопасности на данный момент достаточно обширна, и различные исследователи рассматривают этот вопрос локально, в зависимости от специфики информационной системы или объекта, а также от источников угроз. Угрозы, как правило, возникают через уязвимости, приводящие к нарушению безопасности в информационных системах. На данный момент также существует проблема, связанная с отсутствием единого подхода к идентификации и классификации уязвимостей для информационных систем, который бы учитывал все составляющие комплексного обеспечения информационной безопасности. Степень актуальности программных уязвимостей в современных условиях также постоянно изменяется ввиду появления новых уязвимостей или модификации старых.

Процесс обеспечения безопасности информации на объекте, как правило, начинается с проведения аудита информационной безопасности системы электронного документооборота, по результатам которого проводится оценка рисков реализации угроз. В настоящий момент основой большинства ошибок при принятии решений по вопросам безопасности является неправильная оценка рисков. Результаты аудита влияют на долгосрочные планы развития информационной инфраструктуры организации, политику в области управления службой безопасности, отделом документального обеспечения управления, кадрами, а также выявляют степень необходимости защиты и выбор способов и средств защиты информации: правовые, организационные и технические. В соответствии с законодательством Республики Беларусь в области защиты информации государственным организациям и предприятиям предписывается использование аппаратных и программных средств защиты информации, сертифицированных Оперативно-аналитическим центром при Президенте Республики Беларусь. В настоящее время на рынке средств защиты информации РБ активно работают: ЗАО «БелХард Групп», ИП «С-Терра Бел», ЗАО «Авест», ЗАО «НТЦ

Контакт», Производственно-внедренческое частное унитарное предприятие «СОФТМАРКЕТ», ООО «Энигма», ООО «БАЙТИС», Частное торгово-производственное унитарное предприятие «Авест-Системс», Научно-производственное республиканское унитарное предприятие «НИИ ТЗИ», ЗАО «БЕЛТИМ СБ» СП ООО «Солидекс ПИ», ЗАО «НПП БЕЛСОФТ», ОАО «АГАТ-системы управления» и др. Спектр выпускаемой продукции широк: аппаратные, аппаратно-программные средства защиты документальной и речевой информации, комплексы для реализации инфраструктуры открытых ключей, средства защиты электронной почты и пр.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Безопасность Республики Беларусь в информационной сфере [Электронный ресурс]. – Режим доступа : http://bibliofond.ru/view.aspx?id=443170.

2. Закон Республики Беларусь «Об информации, информатизации и защите информации»: Национальный правовой Интернет-портал Республики Беларусь №455-З 10 ноября 2008 г. [Электронный ресурс]. – Режим доступа : http://pravo.by/document/?guid=3871&p0=h10800455.

3. Киреенко, В. П. Информационные системы в управлении недвижимостью: учеб. пособие / В. П. Кириенко. – Минск : ГИУСТ, БГУ, 2016. – 150 с.

4. Бровка, Г. М. Социально-экономические вызовы при формировании инновационной экономики / Г. М. Бровка // Духовные ипостаси Евфросинии Полоцкой: историческая и современная : материалы международной научной конференции, Минск, 12 мая 2016 г. / Белорусский национальный технический университет ; ред. А. И. Лойко. – Минск, 2016. – С. 19–27.

5. Кубрак, Т. А. Кинодискурс в условиях глобализации информационного пространства: проблема информационно-психологической безопасности / Т. А. Кубрак // Цифровое общество как культурно-исторический контекст развития человека : сборник научных статей и материалов международной конференции «Цифровое общество как культурно-исторический контекст развития человека, Коломна 11–13 февраля 2016 ; под общ. ред. Р. В. Ершовой. – Коломна : Государственный социально-гуманитарный университет, 2016. – С. 210–214.

6. Указ Президента Республики Беларусь от 9 ноября 2010 г. №575 «Об утверждении Концепции национальной безопасности Республики Беларусь» [Электронный ресурс]. – Режим доступа : http://www.pravo.by/pravovaya-informatsiya/normativnye-dokumenty.

7. Абламейко, М. С. Правовое обеспечение информационной безопасности при формировании информационного общества в Республике Беларусь / М. С. Абламейко, Д. А. Марушко // Вес. Нац. акад. навук Беларусі. Сер. гум. навук. – 2011. – №4. – С. 39–45.

8. Национальный правовой Интернет-портал Республики Беларусь, 16.01.2013, 8/26759 [Электронный ресурс]. – Режим доступа : http://www.pravo.by/document/?guid=12551&p0=B21326759&p1=1.

9. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности [Электронный ресурс]. – Режим доступа : http://www.pravo.by/document/?guid=12551&p0=N01300115&p1=1.

10. Постановление Межпарламентской Ассамблеи Евразийского экономического сообщества от 28 мая 2004 г. №5-20 «О типовых проектах законодательных актов МПА ЕврАзЭС в сфере информационных технологий («Об информатизации», «Об информационной безопасности», «Основные принципы электронной торговли»)» [Электронный ресурс]. – Режим доступа : http://spravka-jurist.com/base/part-iq/tx_dswswe/page-4.html.

11. Об утверждении Концепции информационной безопасности государств – участников Содружества Независимых Государств в военной сфере : Решение Совета глав правительств Содружества Независимых Государств, 4 июня 1999 г. / Эталон-Беларусь [Электронный ресурс]. – Минск, Нац. центр правовой информ. Респ. Беларусь, 2014.

12. Бачило, И. Л. Информационное право : учебник / В. Н. Лопатин, М. А. Федотов ; под ред. акад. РАН Б. Н. Топорнина. – 2-е изд., с изм. и доп. – СПб. : Издательство Р. Асланова «Юридический центр Пресс», 2005. – 725 с.

13. Национальная безопасность Республики Беларусь / С. В. Зась [и др.] ; под ред. М. В. Мясниковича и Л. С. Мальцева. – Минск : Беларус. навука, 2011. – 557 с.

14. Лазовский, С. В. Понятие информационной безопасности государства и ее место в правовой системе Республики Беларусь / С. В. Лазовский // Юридический журнал. – 2008. – №3(15). – С. 70–73.

15. Кузнецов, И. Н. Национальная безопасность : учеб.-метод. комплекс [Электронный ресурс]. – 2012.

16. Массмедиа в условиях глобализации : информационно-коммуникационная безопасность / В. И. Василенко, В. В. Василенко, Р. Н. Мамедов, А. Г. Потеенко ; под общ. ред. В. И. Василенко. – Москва : Проспект, 2015. – 163 с.

17. Обеспечение информационной безопасности организации: ICC Russa [Электронный ресурс]. – Режим доступа : http://www.iccwbo.ru/blog/2016/obespechenie-informatsionnoy-bezopasnosti.

18. Домарев, В. В. Оценка эффективности систем защиты информации: Центр информационной безопасности [Электронный ресурс]. – 2005. – Режим доступа : http://www.bezpeka.com/ru/lib/sec/gen/art369.html

19. Ярочкин, В. И. Информационная безопасность / В. И. Ярочкин. – М. : Академический Проект, 2004. – 544 с.

20. Аверченков, В. И. Организационная защита информации / В. И. Аверченков. – М. : Флинта, 2011. – 184 с.

21. Макаров, В. Е. Социальные основы информационной безопасности деловой организации / В. Е. Макаров. – Таганрог : Издатель С. А. Ступин, 2015. – 233 с.

22. Скляров, Д. В. Искусство защиты и взлома информации / Д. В. Скляров. – СПб. : БХВ-Петербург, 2004. – 288 с.

23. О сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 года. СоюзПравоИнформ. Законодательство стран СНГ [Электронный ресурс]. – 2015. – Режим доступа : http://base.spinform.ru/show_doc.fwx?rgn=66894.

24. Постановление Межпарламентская Ассамблея государств – участников Содружества Независимых Государств от 18 ноября 2005 г. №26-7 «О гармонизации законодательства государств – участников СНГ в области информатизации и связи», Право. Законодательство Республики Беларусь [Электронный ресурс]. – 2015. – Режим доступа : http://pravo.kulichki.com/megd2007/spisok/spis2.htm.

25. Соглашение между Правительством Республики Казахстан и Правительством Российской Федерации о сотрудничестве в области защиты информации от 20 января 1995 года, Исполнительный комитет СНГ [Электронный ресурс]. – 2015. – Режим доступа : http://cis.minsk.by/page.php?id=13138.

26. Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области защиты информации от 9 июля 1997 года, Исполнительный комитет СНГ [Электронный ресурс]. – 2015. – Режим доступа : http://www.cis.minsk.by/page.php?id=13156.

27. Постановление Межпарламентского комитета Республики Беларусь, Республики Казахстан, Кыргызской Республики, Российской Федерации и Республики Таджикистан от 15 октября 1999 г. Право. Законодательство Республики Беларусь [Электронный ресурс]. – 2015. – Режим доступа : http://pravo.kulichki.com/zak/megd/meg01770.htm.

28. Конституция Республики Беларусь 1994 года (с изменениями и дополнениями, принятыми на республиканских референдумах 24 ноября 1996 г. и 17 октября 2004 г.), ст. 34, Национальный правовой интернет-портал Республики Беларусь [Электронный ресурс]. – 2015. – Режим доступа : http://pravo.by/pravovaya-informatsiya/normativnye-dokumenty/konstitutsiya-respubliki-belarus.

29. Гражданский Кодекс Республики Беларусь. Статья 140. Служебная и коммерческая тайна. Ст. 140 ГК РБ 218-З от 7.12.1998 г. Национальный правовой интернет-портал Республики Беларусь [Электронный ресурс]. – 2015. – Режим доступа : http://pravo.by/pravovaya-informatsiya/normativnye-dokumenty/kodeksy-respubliki-belarus.

30. Уголовный кодекс Республики Беларусь, стр. 26, раздел XII «Преступления против информационной безопасности», гл. 31 «Преступления против информационной безопасности», Право. Законодательство Республики Беларусь [Электронный ресурс]. – 2015. – Режим доступа : http://pravo.kulichki.com/vip/uk/00000026.htm.

31. Кодекс Республики Беларусь об административных правонарушениях с учетом изменений и дополнений, внесенных Законами Республики Беларусь, 21 апреля 2003 г. № 194-З. Кодексы Республики Беларусь [Электронный ресурс]. – 2015. – Режим доступа : http://kodeksy.by/koap.

32. Трудовой кодекс Республики Беларусь от 26 июля 1999 года №296-З. Законодательство стран СНГ [Электронный ресурс]. – 2015. – Режим доступа : http://www.base.spinform.ru/show_doc.fwx?rgn=56984.

33. Налоговый кодекс Республики Беларусь Статья 82. Обязанности налоговых органов и их должностных лиц. Министерство по налогам и сборам Республики Беларусь [Электронный ресурс]. – 2015. – Режим доступа : http://www.nalog.gov.by/ru/prava-i-obyazannosti-nalog-org-ru.

34. Закон Республики Беларусь от 11 мая 2016 г. №362-З. Национальный правовой Интернет-портал Республики Беларусь, 17.05.2016, 2/2360 [Электронный ресурс]. – 2016. – Режим доступа : http://pravo.by/document/?guid=3871&p0=h10800455.

35. Закон Республики Беларусь от 19 июля 2010 г. №170-З «О государственных секретах». Комитет государственной безопасности Республики Беларусь [Электронный ресурс]. – 2016. – Режим доступа : http://kgb.by/ru/zakon170-3.

36. Закон РБ от 5 января 2013 г. №16-З «О коммерческой тайне». Национальный правовой Интернет-портал Республики Беларусь. [Электронный ресурс]. – 2015. – Режим доступа : http://www.pravo.by/document/?guid=3871&p0=H11300016&p1=1.

37. Об электронном документе и электронной цифровой подписи : Закон Республики Беларусь от 28.12.2009 г. №113-З. Идеи электронного правительства для Беларуси [Электронный ресурс]. – 2015. – Режим доступа : http://e-gov.by/zakony-ob-elektronnom-dokumentooborote/ob-elektronnom-dokumente-i-elektronnoj-cifrovoj-podpisi.

38. Об органах государственной безопасности Республики Беларусь : Закон Республики Беларусь от 10 июля 2012 г. №390-З. Комитет государственной безопасности Республики Беларусь [Электронный ресурс]. – 2016. – Режим доступа : http://www.kgb.by/ru/zakon390-3.

39. Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. – 2015. – Режим доступа : http://pravo.by/pravovaya-informatsiya/normativnye-dokumenty/bank-dannykh-biznes-/pravovye-akty-/po-temam.

40. Об утверждении Концепции национальной безопасности Республики Беларусь : Указ Президента Республики Беларусь от 24 января 2014 г. №49. Комитет государственной безопасности Республики Беларусь [Электронный ресурс]. – 2015. – Режим доступа : http://kgb.by/ru/ukaz575.

41. О некоторых вопросах развития информационного общества в Республике Беларусь : Указ Президента РБ от 11 января 2014 г. №17. Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. – 2015. – Режим доступа : http://pravo.by/document/?guid=3871&p0=P31100515.

42. О некоторых мерах по обеспечению безопасности критически важных объектов информатизации : Указ Президента Республики Беларусь от 16 апреля 2013 г. №196. Национальный правовой Интернет-портал Республики Беларусь, 18.04.2013, 1/14225 [Электронный ресурс]. – 2015. – Режим доступа : http://pravo.by/document/?guid=3871&p0=P31100486.

43. Национальный правовой Интернет-портал Республики Беларусь, 01.02.2010 [Электронный ресурс]. – 2016. – Режим доступа : http://pravo.by/document/?guid=3871&p0=P31000060.

44. Национальный правовой Интернет-портал Республики Беларусь, 29.01.2014, 1/14787 [Электронный ресурс]. – 2015. – Режим доступа : http://pravo.by/document/?guid=3871&p0=P31400046&p1=1.

45. Национальный правовой Интернет-портал Республики Беларусь, 21.05.2013, 5/37263 [Электронный ресурс]. – 2015. – Режим доступа : http://www.pravo.by/document/?guid=3871&p0=C21300375&p1=1.

46. Национальный правовой Интернет-портал Республики Беларусь, 20.08.2013, /37685 [Электронный ресурс]. – 2015. – Режим доступа : http://pravo.by/upload/docs/op/C21300718_1376946000.pdf.

47. Информационная безопасность как составляющая национальной безопасности государства : материалы Междунар. науч.-практ. конф., Минск, 11–13 июля 2013 года. В 3 т. Т. 2. / Ин-т нац. безопасности Респ. Беларусь ; редкол. : С. Н. Князев (гл. ред.) [и др.]. – Минск, 2013. – 332 с.

48. «Доклад Госсекретаря Совета безопасности Станислава Зася» 15 декабря 2016 года. Официальный Интернет-портал Президента Республики Беларусь [Электронный ресурс]. – 2016. – Режим доступа : http://president.gov.by/ru/news_ru/view/vstrecha-s-gossekretarem-soveta-bezopasnosti-stanislavom-zasem-15101.

49. Оперативно-аналитический центр при Президенте Республики Беларусь [Электронный ресурс]. – 2016. – Режим доступа : http://oac.gov.by/info/history.html.

50. Национальный правовой Интернет-портал Республики Беларусь, 21.05.2013, 5/37263 [Электронный ресурс]. – 2016. – Режим доступа : http://www.pravo.by/document/?guid=3871&p0=C21300375&p1=1.

51. Республиканская научно-техническая библиотека Беларуси [Электронный ресурс]. – 2015. – Режим доступа : http://rlst.org.by/temvist/archive/1940.html.

52. Кучеров, А. И. Защита компьютерных сетей и систем. Политика безопасности [Электронный ресурс]. – 2015. – Режим доступа : http://repo.gsu.by/handle/123456789/5123.

53. Основные понятия политики безопасности. Лаборатория Сетевой Безопасности [Электронный ресурс]. – 2015. – Режим доступа : http://ypn.ru/158/introducing-to-security-politics.

54. План-проспект политики безопасности. ИТ-безопасность [Электронный ресурс]. – 2015. – Режим доступа : http://itzashita.ru/designing/plan-prospekt-politiki-bezopasnosti-chast-1-osnovnye-ponyatiya-i-opredeleniya.html

55. Гайкович, В. Ю. Основы безопасности информационных технологий / В. Ю. Гайкович, Д. В. Ершов. – М. : МИФИ, 1995.

56. Романец, Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. – 2-е изд., перераб и доп. – М. : Радио и связь, 2001. – 376 с.

57. Тепляков, А. А. Обеспечение безопасности и надежности информационных систем / А. А. Тепляков, И. В. Гваева, А. В. Орлов. – Минск : Акад. упр. при Президенте Респ. Бел., 2007.

58. Информационная безопасность и анализ угроз. Безопасник [Электронный ресурс]. – 2015. – Режим доступа : http://bezopasnik.org/article/21.html.

59. Уолрэнд, Дж. Телекоммуникационные и компьютерные сети. Вводный курс / Дж. Уолренд. – М. : Постмаркет, 2001. – 358 с.

60. Касперский, Е. Современные угрозы информационной безопасности: классификация, причины и способы устранения / Е. Касперский // Сетевые решения. – 2004. – №4 (32). – С. 72–73.

61. Концепция национальной безопасности Республики Беларусь : Утверждена Указом Президента Республики Беларусь 9 ноября 2010 г. №575. – Минск, 2001. – 55 с.

62. Классификация угроз информационной безопасности [Электронный ресурс]. – 2001. – Режим доступ : http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml.

63. Многокритериальная оценка уровня уязвимости объектов информатизации [Электронный ресурс]. – 2015. – Режим доступа : https://cyberleninka.ru/article/n/mnogokriterialnaya-otsenka-urovnya-uyazvimostiobektov-informatizatsii.

64. Уязвимости информационных систем [Электронный ресурс]. – Режим доступа : http://www.intuit.ru/studies/courses/17846/1242/lecture/27498.

65. Программные уязвимости [Электронный ресурс]. – Режим доступа : https://securelist.ru/threats/programmnye-uyazvimosti.

66. Марков, А. С. Систематика уязвимостей и дефектов безопасности программных ресурсов / А. С. Марков, А. А. Фадин // Защита информации. Инсайд. – 2013. – №3. – С. 56–61.

67. Таксономия угроз качеству функционирования компьютерных систем / Д. С. Багаев, Д. И. Коробкин, А. А. Окрачков, Е. А. Рогозин // Вестник Воронежского государственного технического университета. – 2008. – Т. 4. – №10. – С. 140–142.

68. Емельянов, К. И. Таксономия DOS-атак в беспроводных сенсорных сетях / К. И. Емельянов // Информационное противодействие угрозам терроризма. – 2010. – №14. – С. 53–56.

69. Климовский, А. А. Таксономия кибератак и ее применение к задаче формирования сценариев их проведения / А. А. Климовский // Труды Института системного анализа Российской академии наук. – 2011. – Т. 27. – С. 74–107.

70. Категорирование информации и информационных систем [Электронный ресурс]. – 2008. – Режим доступа : http: // www.jetinfo.ru/stati/kategorirovanie-informatsyonnykh-sistem-obespechenie-bazovogo-urovnya-informatsionnoj.

71. Ярочкин, В. И. Информационная безопасность : учебник для студентов вузов / В. И. Ярочкин. – 2-е изд. – М. : Академический Проект ; Гаудеамус, 2004. – 544 с.

72. Буренин, А. Н. Вопросы безопасности инфокоммуникационных систем и сетей специального назначения: основные угрозы, способы и средства обеспечения комплексной безопасности сетей. / А. Н. Буренин, К. Е. Легков // Наукоемкие технологии в космических исследованиях Земли. – 2015. – Т. 7. – №3. – С. 46–61.

73. Положение о системе резервного копирования [Электронный ресурс]. – Режим доступа : http://securitypolicy.ru.

74. Введение в ИТ-безопасность [Электронный ресурс]. – 2006. – Режим доступа : http://www.alib.spb.ru/blog/page/article-131.

75. Безопасность информации [Электронный ресурс]. – 2008. – Режим доступа : http://isufavt.narod.ru/lekc/infset/page_19.html.

76. Жук, О. Аудит информационной безопасности в системах электронного документооборота / О. Жук // Архивы и делопроизводство. – 2008. – №3. – С. 123.

77. Маликов, В. В. Профили защиты безопасности функционирования объектов и методы их оценки / В. В. Маликов // Сетевые решения. – 2008. – № 4. – С. 68.

78. Арутюнов, В. В. Защита информации: учеб. – метод. Пособие / В. В. Арутунов. – М. : Либерея- Бибинсформ, 2008. – 56 с.

79. Семкин, С. Н. Основы организационного обеспечения информационной безопасности объектов информатизации : учеб. пособие / С. Н. Семкин. – М. : Гелиос АРВ, 2005. – 64 с.

80. Леонов, А. П. Безопасность автоматизированных банковских и офисных систем / А. П. Леонов. К. А. Леонов, Г. В. Фролов. – Минск. : НКПБ, 1996. – 262 с.

81. Давлетханова, Н. А. Роль организационных методов в системе защиты информации / Н. А. Давлетханова // Документ в современном обществе: между прошлым и будущим : тезисы X Всероссийской студенческой научно-практической конференции, Екатеринбург, 7–8 апреля 2017 г. / Урал. федер. ун-т им. Б. Н. Ельцина, Рос. гос. проф.-пед. ун-т. – Екатеринбург : Изд-во Уральского ун-та, 2017. – С. 241-244.

82. Организационные основы защиты информации на предприятии [Электронный ресурс]. – Режим доступа : http://bezopasnik.org/article/19.htm.

83. По каким причинам сотрудники меняли работу в 2016 году [Электронный ресурс]. – 2017. – Режим доступа : http://www.securitylab.ru/blog/company/falcongaze/339581.php.

84. Системы IP-видеонаблюдения [Электронный ресурс]. – Режим доступа : http://www.uni.com.ua/catalogue/index.php?sid=74&r=0.

85. Видеонаблюдение и IP-мониторинг [Электронный ресурс]. – Режим доступа : http://www.taggerd.su/info/sistemy-videonablyudeniya.

86. Охранно-пожарная сигнализация [Электронный ресурс]. – Режим доступа : http://www.taggerd.su/info/ohrannaya-i-pozharnaya-signalizaciya-moskva.

87. Комплексная охрана периметра [Электронный ресурс]. – Режим доступа : http://xn--80ak7acfj.xn--p1ai/montazhnye-raboty/sistema-ohrany-perimetra-zashhita-na-podstupah.

88. Контроль доступа [Электронный ресурс]. – Режим доступа : http://www.spetselectro.by/index.php/uslugi/kontrol-dostupa.

89. Системы контроля доступа [Электронный ресурс]. – Режим доступа : http://www.taggerd.su/info/sistema-kontrolya-dostupa-moskva.

90. Хорев, А. А. Защита информации от утечки по техническим каналам. В 3 т. Т. 1 : Технические каналы утечки информации. / А. А. Хорев. – М. : Гостехкомиссия России, 1998. – 320 с.

91. Устинова, Н. Д. Лазерная локация / Н. Д. Устинова. – Москва : Радио и связь, 1984. – 265 с.

92. Молебный, В. В. Оптико-локационные системы / В. В. Молебный. – М. : Радио и связь, 1981. – 430 с.

93. Боровиков, В. А. Геометрическая теория дифракции / В. А. Боровиков, Б. Е. Кинбер. – М. : Радио и связь, 1978. – 354 с.

94. Фок, В. А. Проблемы дифракции и распространения электромагнитных волн / В. А. Фок. – М. : Радио и связь, 1970. – 214 с.

95 Уфимцев, П. Я. Метод краевых волн физической теории дифракции / П. Я. Уфимцев. – М. : Сов. Радио, 1962. – 187 с.

96. Волков, А. М. Определение спектральных характеристик природных объектов на полигонах и вопросы эффективности космических систем / А. М. Волков. – М. : Гидрометиздат, 1985. – 56 с.

97. Криксунов, Л. З. Справочник по основам инфракрасной техники / Л. З. Криксунов. – М. : Советское радио, 1978. – 400 с.

98. Царегородцев, А. В. Методы и средства защиты информации в государственном управлении: учеб. пособие / А. В. Царегородцев, М. М. Тараскин. – М. : Проспект. – 2017. – 205 с.

99. Лыньков, Л. М. Методы защиты информации по электромагнитному и акустическому каналам [Электронный ресурс]. – Режим доступа : https://libeldoc.bsuir.by/bitstream.pdf.

100. Защита информации [Электронный ресурс]. – Режим доступа : http://helpiks.org/3-89083.html.

101. Методы и средства защиты информации [Электронный ресурс]. – Режим доступа : http://www.crimport.ru/catalogi/anatoli/link5.htm.

102. Защита информации в компьютерных системах [Электронный ресурс]. – Режим доступа : http://bezopasnik.org/article/2.htm.

103. Деднев, М. А. Защита информации в банковском деле и электронном бизнесе. – М. : Кудиц-образ, 2004. – 512 с.

104. Зайцев, А. П. Техническая защита информации / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков. – М. : Горячая линия – Телеком, 2009. – 616 с.

105. Жданов, О. Н. Методы и средства криптографической защиты информации : учеб. пособие / О. Н. Жданов, В. В. Золотарёв. – Красноярск : СибГАУ, 2007. – 217 с.

106. Средство криптографической защиты [Электронный ресурс]. – Режим доступа : http://www.cryptopro.ru/sites/default/files/docs/general_guide_csp_r3.pdf.

107. Средства криптографической защиты информации [Электронный ресурс]. – Режим доступа : http://www.myshared.ru/slide/929719.

108. Реестр средств защиты информации, прошедших экспертизу [Электронный ресурс]. – Режим доступа : http://oac.gov.by/tzi/protection/register_examination.html.

109 Решения по информационной безопасности [Электронный ресурс]. – Режим доступа : http://www.belsoft.by/site/ru/solutions/telecommunication-solutions/information_safety.

110. Разработка и анализ модели политики безопасности компьютерной сети [Электронный ресурс]. – Режим доступа : https://cyberleninka.ru/article/n/razrabotka-i-analiz-modeli-politiki-bezopasnosti-kompyuternoy-seti.

111. Клейменов, С. А. Информационная безопасность и защита информации / С. А. Клейменов. – М. : Академия, 2007. – 336 с.

112. Завгородний, В. И. Комплексная защита информации в компьютерных системах / В. И. Завгородний. – М. : Логос, 2001. – 264 с.

113. Угрозы безопасности информации в компьютерных системах [Электронный ресурс]. – Режим доступа : http://main.tpkelbook.com.

114. DDoS-атака и защита от нее [Электронный ресурс]. – Режим доступа : http://www.nestor.minsk.by/sr/2008/10/sr81004.html.

115. Защита от программных закладок [Электронный ресурс]. – Режим доступа: http://lib.qrz.ru/book/export/html/14342.

116. Классификация компьютерных вирусов [Электронный ресурс]. – Режим доступа : http://sumk.ulstu.ru/docs/mszki/Zavgorodnii/10.1.html.

117. Осовецкий, Л. Построение средств межсетевой защиты [Электронный ресурс]. – Режим доступа : http://citforum.ru/internet/iinet97/6.shtml.

118. Дополнительные функции маршрутизаторов IP-сетей [Электронный ресурс]. – Режим доступа : http://iptcp.net/filtratsiya.html.

119. Обзор SIEM-систем на мировом и российском рынке [Электронный ресурс]. – Режим доступа : https://www.anti-malware.ru/analytics/.

Св. план 2015, поз. 49

Учебное издание

Пулко Татьяна Александровна

ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

УЧЕБНОЕ ПОСОБИЕ

Редактор *А. К. Мяделко*
Компьютерная правка, оригинал-макет *Е. Д. Степусь*

Подписано в печать 05.02.2018. Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л 9,65. Уч.-изд. л. 5,0. Тираж 300 экз. Заказ 62.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
ЛП №02330/264 от 14.04.2014.
220013, Минск, П. Бровки, 6