**БЕЛГОРОДСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ МВД РОССИИ
ИМЕНИ И.Д. ПУТИЛИНА**

# ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ В ДЕЯТЕЛЬНОСТИ СОТРУДНИКОВ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

## Учебное пособие

**Белгород
Белгородский юридический институт МВД России
имени И.Д. Путилина
2023**

УДК 004.056
ББК 67.401.133
О 75

Печатается по решению
редакционно-издательского совета
Бел ЮИ МВД России
имени И.Д. Путилина

Авторы: ***А.Н. Прокопенко,*** кандидат технических наук, доцент; ***А.А. Страхов, Е.Г. Ковалева,*** кандидат технических наук; ***В.Л. Акапьев,*** кандидат педагогических наук, доцент; ***А.П. Гаврющенко,*** кандидат технических наук, доцент; ***А.Ю. Рыбальченко.***

О 75 Основы кибербезопасности в деятельности сотрудников правоохранительных органов : учебное пособие / А. Н. Прокопенко [и др.]. – Белгород : Белгородский юридический институт МВД России имени И.Д. Путилина, 2023. – 153 с.

ISBN 978-5-91776-485-6

**Рецензенты:**

**Старостенко И.Н.,** кандидат физико-математических наук, доцент (Краснодарский университет МВД России);

**Пыхтин И.В.,** начальник отделения технической защиты информации, не содержащей государственную тайну, ЦИТСиЗИ УМВД России по Белгородской области.

В пособии проведен аналитический обзор программного обеспечения, специальных технических средств и методических рекомендаций по их использованию с целью обеспечения защиты от киберугроз.

Предназначено для курсантов и слушателей, профессорско-преподавательского состава, слушателей факультета заочного обучения, слушателей факультета переподготовки и повышения квалификации образовательных организаций системы МВД России, лиц рядового состава и младшего начальствующего состава, впервые принятых на службу в органы внутренних дел Российской Федерации по должности служащего «Полицейский», лиц среднего и старшего начальствующего состава, впервые принятых на службу в органы внутренних дел Российской Федерации по должности служащего «Полицейский», имеющих высшее или среднее профессиональное (неюридическое) образование.

УДК 004.056
ББК 67.401.133

ISBN 978-5-91776-485-6

# ОГЛАВЛЕНИЕ

**Введение** …… **5**
**Глава 1. Кибербезопасность: современные киберугрозы** ……... **8**
1.1. Методы совершения киберпреступлений …… **8**
1.2. Угрозы кибербезопасности и их классификация …… **10**
1.3. Способы совершения кибератак ……... **16**
1.4. Модель нарушителя кибербезопасности …… **22**
1.5. Интернет вещей и его уязвимости ……... **26**
1.6. Критическая информационная инфраструктура …… **31**
*Вопросы для самоконтроля* …… **36**

**Глава 2. Нормативно-правовое обеспечение кибербезопасности** ……. **37**
2.1. Основы государственной политики в области кибербезопасности ….. **37**
2.2. Нормативно-правовое регулирование обеспечения кибербезопасности в Российской Федерации …… **43**
2.3. Классификация информации по степени доступа и понятие информации ограниченного доступа …….. **46**
2.4. Организационные основы обеспечения информационной безопасности России ……. **49**
2.5. Ответственность за нарушения законодательства в сфере кибербезопасности …… **55**
2.6. Административная ответственность за нарушения законодательства в сфере кибербезопасности …….. **57**
2.7. Уголовная ответственность за нарушения законодательства в сфере кибербезопасности …… **60**
*Вопросы для самоконтроля* …… **64**

**Глава 3. Принципы обеспечения компьютерной безопасности** …… **65**
3.1. Основные принципы и меры защиты информации …… **65**
3.2. Организационные меры защиты информации …… **67**
3.3. Основы построения системы кибербезопасности …….. **72**
3.4. Защита автоматизированных информационных систем от кибератак .. **80**
3.5. Влияние на кибербезопасность со стороны различных сотрудников .. **86**
3.6. Регламентация действий пользователей и обслуживающего персонала автоматизированной информационной системы ……. **89**
*Вопросы для самоконтроля* …… **91**

**Глава 4. Источники и каналы утечки информации. Основы технической защиты информации** …… **92**
4.1. Технические каналы утечки информации ……... **92**
4.2. Технические каналы утечки информации при ее передаче по каналам связи ……... **99**

4.3. Техническая защита информации …… **104**
4.4. Меры защиты информации от утечки по техническим каналам …….. **107**
4.5. Средства защиты информации от утечки по техническим каналам …. **109**
*Вопросы для самоконтроля* ……. **116**

**Глава 5. Основы криптографической защиты информации** …… **117**
5.1. Основные понятия криптографии. Кодирование …… **117**
5.2. Основные понятия криптографии. Шифрование …… **120**
5.3. Основные понятия криптографии. Маскирование ……. **127**
5.4. Основные понятия криптографии. Хеширование ……... **129**
5.5. Современные методы и средства криптографической защиты конфиденциальной информации …… **130**
*Вопросы для самоконтроля* ……. **133**

**Глава 6. Реагирование на инциденты кибербезопасности и их обработка** …… **134**

6.1. Понятие инцидента кибербезопасности …….. **134**
6.2. Реагирование на киберинциденты …… **138**
6.3. Системы управления событиями и данными безопасности …….. **147**
*Вопросы для самоконтроля* ……. **149**

**Библиографический список** ……. **150**

# ВВЕДЕНИЕ

Кибербезопасность относится к числу направлений деятельности, развивающихся чрезвычайно быстрыми темпами. Этому способствуют как общий прогресс развития информационных технологий, так и постоянное противоборство различных сторон в процессе сохранности и приобретения информации. Поэтому проблемы, связанные с кибербезопасностью, с каждым годом становятся все более насущными и сложными.

Широкое внедрение информационные технологии получили и в деятельности государственных органов, в том числе подразделений МВД России. Огромный объем аккумулируемой информации (открытой, конфиденциальной, служебной, персональных данных, государственной тайны) ставит органы МВД России в положение одной из наиболее информационноемких государственных структур. Все это делает информационные ресурсы МВД России объектом, представляющим огромный интерес как для отдельных лиц или группировок, так и для организаций антиконституционной направленности, средств массовой информации, стремящихся использовать для своих целей служебную информацию МВД России. Возможность противоправных действий в отношении информационной деятельности подразделений МВД России обуславливает появление различного рода источников угроз информационной безопасности. При этом защитные меры оказываются значительно более дешевыми и эффективными в случае, если они встроены в информационные системы и сервисы на стадиях задания требований и проектирования.

Когда данный момент упущен и информационная система уже находится в эксплуатации, необходимо понимать, что зачастую реальная стоимость информации, циркулирующей в системе, может в разы превышать стоимость самой системы, поэтому актуализируется необходимость защиты информации в составе информационных систем.

Помимо всего прочего, на передний план борьбы за обеспечение информационной безопасности выходят следующие мотивирующие основания:

– обострение противоречий между потребностями общества в свободном обмене информацией и не соответствующими этим потребностям (чрезмерными или наоборот недостаточными) ограничениями на ее распространение и использование;

– повсеместные использование компьютерной техники, информационных технологий, средств коммуникации и связи;

– использование автоматизированных систем управления и обработки информации в критических областях деятельности (в том числе в органах и организациях МВД России);

– вовлечение в процесс информационного взаимодействия все большего числа людей и организаций, резкое возрастание их информационных потребностей, наличие интенсивного обмена информацией между участниками этого процесса;

– концентрация больших объемов информации различного назначения и принадлежности на электронных носителях;

– количественное и качественное совершенствование способов доступа пользователей к информационным ресурсам;

– отношение к информации, как к товару, переход к рыночным отношениям в области предоставления информационных услуг;

– многообразие видов угроз и возникновением новых возможных каналов несанкционированного доступа к информации;

– рост числа квалифицированных пользователей вычислительной техники и возможностей по созданию ими нежелательных воздействий на системы обработки информации;

– увеличение потерь (ущерба) от уничтожения, фальсификации, разглашения или незаконного тиражирования информации (возрастание уязвимости различных затрагиваемых субъектов).

**Острота проблемы обеспечения безопасности субъектов информационной деятельности, защиты их информационных и управляющих систем, хранящейся и обрабатываемой в них информации все более возрастает.** Этому есть четыре объективных причины.

Во-первых, это расширение сферы применения компьютерной техники и возросший уровень доверия к системам управления и обработки информации. Компьютерным системам доверяют самую ответственную работу, от качества выполнения которой зависит жизнь и благосостояние многих людей. Автоматизированные информационные системы управляют технологическими процессами на предприятиях и атомных электростанциях, движением самолетов и поездов, выполняют финансовые операции, обрабатывают секретную и конфиденциальную информацию, в том числе персональные данные миллионов людей. Изменился подход и к самому понятию «информация». Этот термин все чаще используется для обозначения особого товара, стоимость которого зачастую превосходит стоимость информационной системы, в рамках которой он существует. В области создания и предоставления информационных услуг применяются рыночные отношения, используются элементы промышленного шпионажа. При этом информационные ресурсы государственных органов становятся важнейшим источником информации, в том числе инсайдерской, как для коммерческих организаций, так и для иностранных разведок или преступных групп.

Во-вторых, это повсеместное использование информационно-телекоммуникационных сетей, территориально распределенных систем, в том числе облачной обработки информации, систем с удаленным доступом к совместно используемым информационным ресурсам и т.д. Доступность средств компьютерной техники привела к повышению компьютерной грамотности в широких слоях населения, что, в свою очередь, привело к увеличению числа попыток неправомерного вмешательства в работу государственных и коммерческих информационных систем, как со злым умыслом, так и чисто «из спортивного ин-

тереса». К сожалению, эти попытки имеют успех и наносят значительный урон всем участникам информационных отношений.

В-третьих, отсутствие стройной и непротиворечивой системы законодательно-правового регулирования отношений в сфере оборота и защиты информации создает условия для возникновения и широкого распространения «компьютерного хулиганства» и «компьютерной преступности». Несмотря на существенные изменения законодательства в последние годы в сфере информационной безопасности и защиты информации от противоправных действий, проблемы не ликвидированы полностью. Существуют противоправные действия, по которым отсутствует понятийная база, что позволяет преступникам уходить от уголовного преследования. Используются методы социальной инженерии, которые выводят преступника из-под преследования, создавая ситуации якобы добровольной передачи денег, материальных ценностей или информации.

В-четвертых, возрастает количество противоправных действий, совершаемых преступными группами по заранее составленному плану и соответствующему алгоритму. Это деятельность мошенников по получению доступа к банковским картам населения, принявшая в последние годы массовый характер. Шифрование информационных ресурсов, взлом сайтов и серверов с последующим вымогательством денежных средств. Также в составе преступных групп осуществляются попытки доступа к информационным ресурсам государственных органов, промышленный шпионаж. Существенная часть противоправных действий осуществляется под кураторством или непосредственным руководством иностранных разведок. В ряде иностранных государств, таких как США, Великобритания, Украина, созданы специализированные подразделения для проведения противоправных действий в информационном пространстве других стран, в первую очередь России.

# ГЛАВА 1.
# КИБЕРБЕЗОПАСНОСТЬ: СОВРЕМЕННЫЕ КИБЕРУГРОЗЫ

## 1.1. Методы совершения киберпреступлений

В современном обществе компьютеры используются практически во всех областях деятельности. Довольно часто возникает необходимость защиты важной информации. Большие организации, как правило, уже имеют в своем составе специалистов по кибербезопасности. Компании небольшого или среднего размера, как правило, оставляют вопросы обеспечения безопасности информации на усмотрение специалистам информационных технологий (далее – ИТ), административным менеджерам или не занимаются ими вовсе. Откладывают до того момента, пока не происходит потеря денег со счетов компании, пока не начинает возникать проигрыш в тендерах, пока компания не вынуждена платить штрафные санкции за задержку услуг клиентам, пока не происходит потеря клиентов из-за утечки их информации, которая хранилась и обрабатывалась в организации. Перечислять риски, возникающие при нарушении конфиденциальности, целостности и доступности информационных активов можно очень долго. Главный вопрос: что может сделать организация для улучшения ситуации, какие шаги нужно предпринять, чтобы обезопасить себя хотя бы от наиболее вероятных рисков.

К сожалению, не существует готовых рецептов на все случаи жизни, и нет подходов, одинаково применимых для всех организаций. Тем не менее, попытаемся выделить основные типы угроз кибербезопасности, на которые необходимо обратить особое внимание. Учитывая то, что защите от лобовых атак на сетевой периметр уделяется очень большое внимание и практически любое устройство, которое покупается и устанавливается в офисе или дома, к примеру, сетевой маршрутизатор или домашний Wi-Fi роутер, уже изначально имеет базовые средства защиты, мы не будем их рассматривать. Мы попытаемся обратить внимание на те угрозы и методы их устранения, которые выражены не так явно, или их важность, как правило, недооценивается:

- социальная инженерия и фишинг;
- вирусное программное обеспечение;
- использование неактуальных версий программного обеспечения;
- инсайдерские угрозы;
- отсутствие политик и процедур по обращению с информационными ресурсами.

**Социальная инженерия.** Социальная инженерия базируется на эксплуатации человеческих слабостей. В результате успешной психологической обработки жертвы опытный злоумышленник может выявить много базовых моментов в работе организации для планирования взлома, похищения информации. Это и работа системы контроля физического доступа, и работа охраны, график

работы уборщиц, и местонахождение принтеров, мусорных корзин, наличие шредеров и т.д. Подготовка к проникновению в информационную систему организации начинается именно с такой работы.

**Фишинговые атаки** являются продолжением социальной инженерии. Многими специалистами они признаются наиболее массовым и эффективным средством взлома и последующего доступа к ресурсам предприятий и организаций всех форм собственности. По различным оценкам до 90% всех успешных кибератак происходят с использованием этого метода.

Метод по сути очень прост и представляет собой рассылку поддельных писем электронной почты, текст которых побуждает предполагаемую жертву запустить вирусную программу, замаскированную, к примеру, под офисное приложение, или перейти по ссылке на поддельный сайт, на котором предложат ввести свой логин и пароль к почте или другим ресурсам.

**Спам** не только вызывает раздражение у пользователей, но и забивает каналы связи, расходует трафик, отвлекает от работы, вынуждая людей искать важную корреспонденцию среди рекламы. В конечном счете все это приводит к финансовым потерям. Помимо этого, спам также является одним из распространенных каналов внедрения троянских программ и вирусов.

**Вредоносное программное обеспечение** – важнейшее оружие злоумышленников, для защиты от которого необходимо иметь актуальную версию антивирусного программного обеспечения (далее – ПО). Не существует антивирусного программного обеспечения, которое бы защищало от всех вредоносных программ одинаково хорошо. Как показывает практика, очень полезен обмен информацией между специалистами о начале атак и появлении новых вредоносных программ, а также использование служб по анализу подозрительных файлов и ссылок на предмет выявления червей, троянов, вирусов, логических бомб и других всевозможных вредоносных программ. К примеру, очень популярна служба Virus Total.

**Неактуальные версии программного обеспечения.** По сути это уязвимость информационной системы, когда пользователь игнорирует установку необходимых обновлений ПО. Регулярное обновление ПО необходимо по многим причинам, одна из которых – повышение уровня безопасности и защита от вновь выявленных уязвимостей и угроз. Нужно работать с персоналом в этом направлении, делать регулярные рассылки и напоминания для сотрудников, показывать на примерах, к чему может привести использование неактуальной версии ПО.

**Инсайдерские угрозы.** Большая группа угроз, источником которых являются собственные сотрудники. Распространена в организациях, где отсутствует контроль за предоставлением прав доступа высокого уровня, а также отсутствуют разграничения по правам доступа к информационным ресурсам. Очень хорошо, если регулярно проводится хотя бы минимальная оценка лояльности сотрудников при приеме на работу, в процессе работы и при увольнении. Персонал – это всегда самое слабое звено в системе безопасности и с ним нужно постоянно работать. Не зря британские и американские специалисты по безопасности строят свою работу именно с развития культуры безопасности.

**Мир стал цифровым**. Сотовые телефоны теперь обычное дело, в школах планшеты заменили тетради, а компании разрабатывают технологии нового поколения, например автомобили без водителя. Кажется, все связано между собой, особенно в бизнесе. Будь то автоматические системы безопасности или ноутбуки; количество устройств, подключенных к сети и работающих вместе, только растет. Рекомендуется всем организациям максимально подробно изучать собственную инфраструктуру, быстро реагировать на аномалии, сосредоточиться на точках входа в сеть, которые используют удаленные сотрудники. Минимальный набор средств защиты: антивирус, SIEM-система, система анализа сетевого трафика (NTA), межсетевой экран уровня приложений значительно снизит риск реализации киберугроз.

## 1.2. Угрозы кибербезопасности и их классификация

***Угрозой интересам субъектов информационной деятельности*** *называется потенциально возможное событие, вызванное некоторым действием, процессом или явлением, которое посредством воздействия на информацию, ее носители и процессы обработки может прямо или косвенно привести к нанесению ущерба интересам данных субъектов*.

**Нарушением безопасности или атакой** называется реализация угрозы безопасности, то есть наступление соответствующего события.

*Угроза кибербезопасности* – совокупность факторов и условий, создающих опасность нарушения безопасности организации с негативными последствиями (ущерб/вред).

*Действие угрозы кибербезопасности* (далее – КБ) проявляется в виде наступления событий КБ, способных при определенных условиях привести к нарушению КБ.

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

*Событие КБ* рассматривается как угроза КБ, если имеются источник угрозы (нарушитель), объект воздействия, способы реализации угрозы, а реализация угрозы КБ может привести к недопустимым негативным последствиям.

Природные и техногенные факторы, приводящие к непреднамеренному воздействию на информационные ресурсы (далее – ИР) и программно-технические средства (далее – ПТС), несомненно влияют на безопасность автоматизированной информационной системы (далее – АИС), но в рамках КБ будут преимущественно рассматриваться факторы антропогенные.

**В соответствии с ГОСТ Р 50922 06 предусматривается два принципиально разных типа угроз безопасности**[1].

Первый тип угроз связан с так называемым *несанкционированным распространением сведений – утечкой информации* (разглашением, разведкой, несанкционированным доступом к информации).

*Утечка информации* – это неконтролируемое распространение информации путем ее разглашения или несанкционированного доступа к ней заинтересованных субъектов, в том числе путем перехвата по техническим каналам. В данном контексте *заинтересованными субъектами* являются юридические и физические лица, а также иностранные государства. Информация, ставшая доступной посторонним лицам, считается *скомпрометированной*.

Второй тип угроз связан с *несанкционированным воздействием на информацию и ее носители – воздействие на информацию с нарушением установленных прав и/или правил на изменение информации*. Несанкционированное воздействие бывает как целенаправленное (искажение, уничтожение, копирование, блокирование, утрата, сбой функционирования носителя информации), так и непреднамеренное (ошибки пользователей и персонала, сбои и отказы техники, природные явления, другие случайные воздействия).

**Разглашение информации** – действие, в результате которого информация становится известной неконтролируемому количеству лиц.

**Разведка** – целенаправленная деятельность по добыванию сведений в интересах информационного обеспечения военно-политического руководства другого государства либо конкурирующей организации. Разведка может быть агентурной и технической.

*Под **несанкционированным доступом к информации*** (далее – НСД) *понимают действие, в результате которого нарушены правила разграничения доступа, и информацией завладело лицо, не имеющее соответствующего права.*

**Несанкционированное воздействие на информацию подразделяется на следующие виды:**

– *уничтожение информации* (наблюдается при хакерском проникновении в вычислительные системы, при стихийных бедствиях и т.д.);

– *искажение информации*;

– *подделка информации*;

– *блокирование доступа к информации*;

– *хищение носителя*;

– *утрата носителя*.

**Основными источниками угроз безопасности информации являются:**

– стихийные бедствия – наводнение, ураган, землетрясение, пожар и т.п.;

– аварии, сбои и отказы оборудования, в том числе технических средств (далее – ТС) автоматизированных информационных систем;

---

[1] Национальный стандарт РФ ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст). – М.: Стандартинформ.

– ошибки проектирования и разработки компонентов АИС[2] – аппаратных средств, технологии обработки информации, программ, структур данных;

– ошибки эксплуатации – пользователей – операторов и другого персонала;

– преднамеренные действия нарушителей и злоумышленников – обиженных лиц из числа персонала, преступников, шпионов, диверсантов и т.п.

Потенциальные угрозы по природе их возникновения разделяются на два класса: естественные и искусственные.

**Естественные угрозы** – это угрозы, вызванные воздействиями на АИС и ее элементы объективных физических процессов или стихийных природных явлений, не зависящих от человека.

**Искусственные угрозы** – это угрозы АИС, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

– *непреднамеренные* (неумышленные, случайные) угрозы, вызванные ошибками в проектировании АИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.;

– *преднамеренные* (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников).

Источники угроз по отношению к АИС могут быть внешними или внутренними.

**Основные непреднамеренные искусственные угрозы АИС** (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

– частичный или полный отказ системы или разрушение аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);

– неправомерное отключение оборудования или изменение режимов работы устройств и программ;

– неумышленная порча носителей информации;

– запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, 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-

[2] В российских ГОСТ и руководящих документах ФСТЭК России используется три понятия: автоматизированная система (далее – АС, применялось преимущественно до 2010 года), информационная система, в том числе информационная система персональных данных (далее – ИС, ИСПДн, применяется после 2010 года), автоматизированная информационная система (АИС) – используется преимущественно в научной и учебной литературе. В рамках данного учебного пособия мы будем считать все указанные варианты названий равноценными и использовать преимущественно сокращение АИС.

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

– заражение компьютера вирусами;

– неосторожные действия, приводящие к разглашению конфиденциальной информации или делающие ее общедоступной;

– разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);

– проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ с возможностями, представляющими опасность для работоспособности системы и информации;

– игнорирование организационных ограничений (установленных правил) при работе в системе;

– вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.);

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

– пересылка данных по ошибочному адресу абонента (устройства);

– ввод ошибочных данных;

– неумышленное повреждение каналов связи.

**Основные преднамеренные искусственные угрозы** (основные возможные пути умышленной дезорганизации работы, вывода системы из строя, проникновения в систему и несанкционированного доступа к информации):

– физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.);

– отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);

– дезорганизация функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);

– внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);

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

– применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;

– перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на технические средства, непосредственно не участвующие в обработке информации;

– перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;

– хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПК);

– несанкционированное копирование носителей информации;

– хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);

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

– чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, использование в асинхронном режиме недостатков мультизадачных операционных систем и систем программирования;

– незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т.д.) 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, аппаратный блок кодирования и т.п.;

– вскрытие шифров криптозащиты информации;

– внедрение аппаратных «спецвложений», программных «закладок» и «вирусов» («троянских коней» и «жучков»), то есть участков программ, не нужных для осуществления заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;

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

– незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

Следует заметить, что чаще всего для достижения поставленной цели преступники используют не один, а некоторую совокупность из перечисленных выше путей.

**Каналы проникновения в систему и утечки информации разделяют на прямые и косвенные.** Под косвенными понимают такие каналы, использование которых не требует проникновения в помещения, где расположены компоненты системы. Для использования прямых каналов такое проникновение

необходимо. Прямые каналы могут использоваться без внесения изменений в компоненты системы или с изменениями компонентов.

По типу основного средства, используемого для реализации угрозы, все возможные каналы можно условно разделить на три группы, где таковыми средствами являются: человек, программа или аппаратура.

**По способу получения информации потенциальные каналы доступа можно разделить на:**

– *физический;*
– *электромагнитный (перехват излучений);*
– *информационный (программно-математический).*

При контактном НСД (физическом, программно-математическом) возможные угрозы информации реализуются путем доступа к элементам АИС, к носителям информации, к самой вводимой и выводимой информации (и результатам), к программному обеспечению (в том числе к операционным системам), а также путем подключения к линиям связи (см. рис. 1).

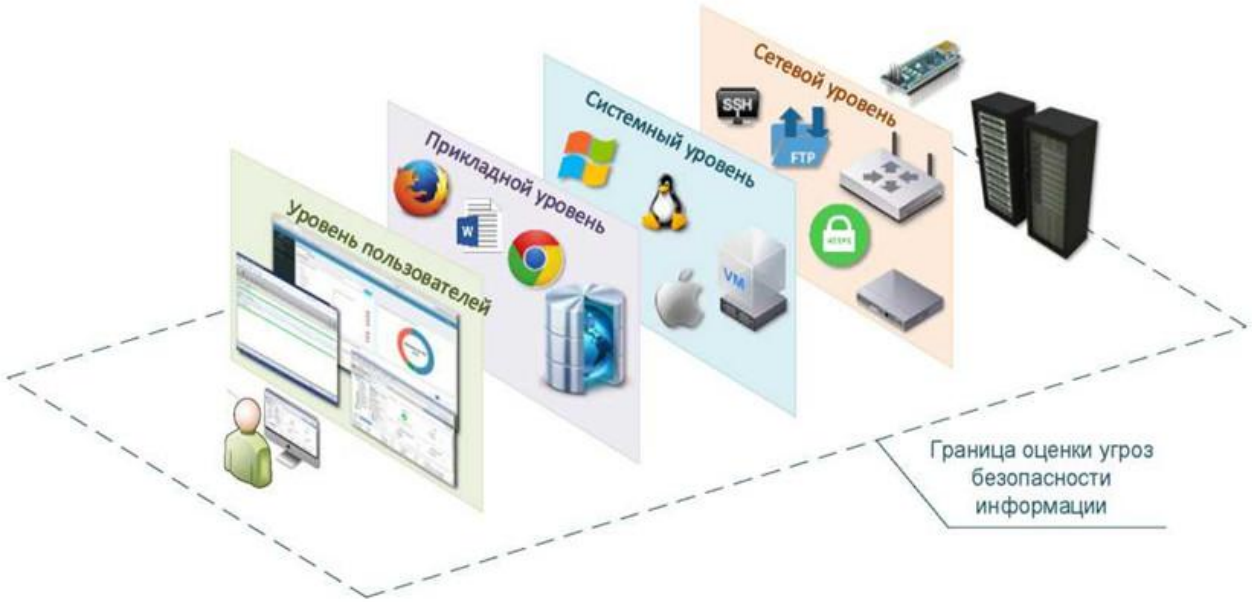


*Рисунок 1. Уровни архитектуры систем и сетей, на которых определяются объекты воздействия*

При бесконтактном доступе (например, по электромагнитному каналу) возможные угрозы информации реализуются перехватом излучений аппаратуры АИС, в том числе наводимых в токопроводящих коммуникациях и цепях питания, перехватом информации в линиях связи, вводом в линии связи ложной информации, визуальным наблюдением (фотографированием) устройств отображения информации, прослушиванием переговоров персонала АИС и пользователей.

Меры обеспечения КБ АИС разрабатываются в соответствии с *моделью угроз КБ*, описание которой, как правило, представляет собой структурированный документ.

Официальный банк данных известных угроз безопасности АИС, который ведет Государственный научно-исследовательский испытательный институт проблем технической защиты информации (ГНИИИ ПТЗИ ФСТЭК России), размещен на сайте: bdu.fstec.ru (см. рис. 2).

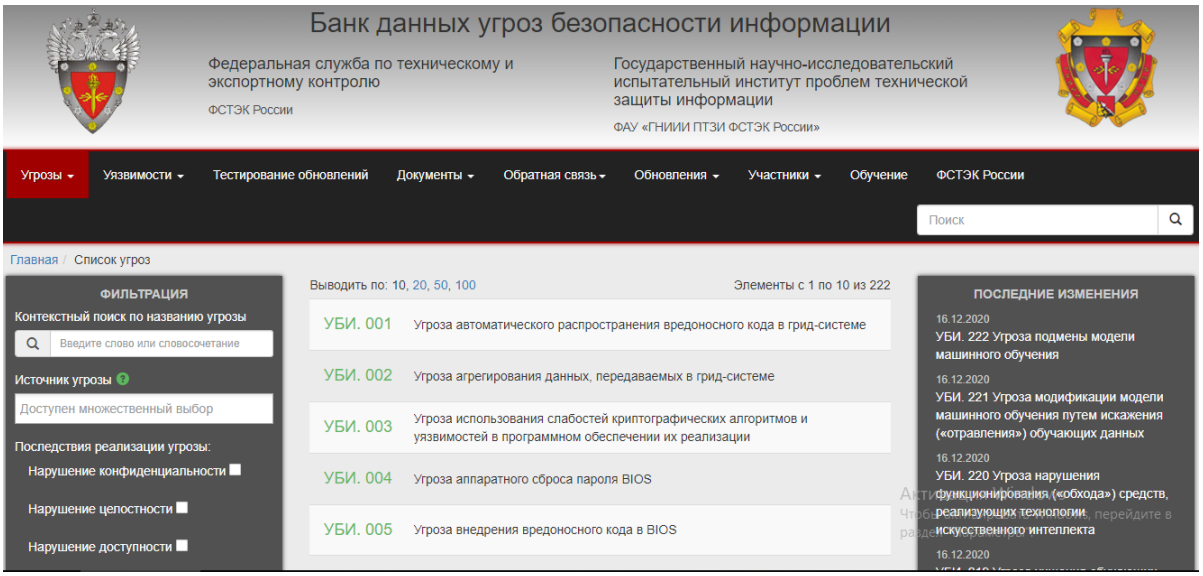


*Рисунок 2. Банк данных угроз безопасности информации*

## 1.3. Способы совершения кибератак

В связи с неоспоримой актуальностью проблемы информационной безопасности рассмотрим более подробно самые распространенные методы воздействия злоумышленников на информационные системы.

**Фишинг (Phishing)**

Вид интернет-мошенничества, цель которого получение доступа к конфиденциальным данным пользователя (например, логинам и паролям). Пользователь думает, что переходит на заявленный сайт, однако фактически его перенаправляют на подставной сайт. Как правило, жертвами фишеров становятся клиенты банков и платежных систем.

*Фишинговые атаки делятся на три категории*:

– фишинговые сайты, которые имитируют реальные ресурсы;

– почтовые рассылки или сообщения в социальных сетях, содержащие ссылки на фишинговые сайты;

– рассылки вредоносного программного обеспечения.

Атаки на организации чаще всего совершают третьим способом. Зараженный файл может нести в себе вирус практически любого типа. Например, вирус-шифровальщик, который распространяется на все компьютеры сети и зашифро-

вывает данные. Еще более тяжелыми последствиями обернется запуск трояна, открывающего злоумышленнику доступ к сети. Тогда он сможет атаковать ее изнутри, похитить денежные средства или конфиденциальную информацию.

Антивирусные программы не способны заблокировать все подозрительные файлы. Поэтому компании, которые заботятся об информационной безопасности, внедряют дополнительные средства активной защиты. Наиболее действенный из них так называемые песочницы. Это искусственная цифровая среда, куда помещают потенциально опасный файл и анализируют, как он себя ведет.

Важно регулярно обновлять установленное ПО. При создании большинства вредоносных программ преступники эксплуатируют известные уязвимости. У крупных разработчиков есть специальные программы (bug bounty), в рамках которых «этичные хакеры» получают вознаграждение за обнаружение уязвимостей. Получив информацию, производители ПО имеют возможность их оперативно закрыть. Соответственно, при запуске зараженного файла встроенные средства безопасности Microsoft Windows заблокируют его.

В последнее время у злоумышленников растет популярность вебфишинга, в исключительных случаях его используют для взлома корпоративных сетей. Преступники могут выяснить, например, какую систему документооборота использует организация, и создать ресурс, копирующий стартовую страницу этой системы. Ничего не подозревающий сотрудник вводит логин и пароль и передает их хакеру.

**Признаки фишингового сайта:**

– *неправильное имя домена*. Например, вместо online.bank.ru можно увидеть onlinebank.ru. Иногда злоумышленники располагают сайт в поддомене bank.site.ru;

– *отсутствие SSL-сертификата*. Адреса настоящих сайтов начинаются на https://. Если адрес начинается с http://, это повод насторожиться;

– *некорректное оформление*: устаревший дизайн, грамматические и орфографические ошибки на странице, сбитая верстка, посторонние элементы дизайна.

***Троян (троянский конь, троянская программа, троянец)*** *– тип вредоносных программ, основной целью которых является вредоносное воздействие на компьютерную систему*. В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

**Основные способы защиты от троянских программ:**

1. *Наличие на компьютере качественного антивирусного пакета*. Любой выход в Интернет приводит к опасности заражения системы, отчего и защищает качественный антивирусный пакет, который к тому же ежедневно обновляется.

2. *Сетевой экран компьютера должен быть постоянно включен*. Это правило стоит соблюдать всем пользователям сети, так как брандмауэр операционной системы (далее – ОС) – это, пусть и слабая, но все-таки защита компьютера от проникновения и работы троянских вирусов.

3. *Постоянно нужно обновлять ОС*. Это позволит исправлять различные уязвимости системы, которыми могли воспользоваться троянские программы для проникновения в систему и навредить их безопасному существованию. Обновления созданы для того, чтобы исправлять ошибки, а также уязвимости устаревших программ и модулей ОС.

4. *Желательно использовать только лицензированное ПО*. Программы из непроверенных источников могут вызвать сбой работы всей системы, а также стать причиной заражения компьютера троянским вирусом. Все программы перед установкой нужно сканировать антивирусом.

5. *Нужно пользоваться только проверенными интернет-ресурсами*. Нужно быть аккуратным при переходе по различным ссылкам и баннерам, которые в огромном количестве есть в современном Интернете. Если ссылка или баннер кажется подозрительным, тогда лучше не нажимать на него.

6. *Нужно использовать безопасные пароли*. Пароли не должны легко угадываться и чем-то быть связаны с владельцем того или иного аккаунта. Пароли не должны храниться в одном месте, а также совпадать между собой. Также в обязательном порядке необходимо «запаролить» учетную запись администратора.

**Червь (сетевой червь)** – тип вредоносных программ, распространяющихся по сетевым каналам, способных к автономному преодолению систем защиты автоматизированных и компьютерных систем, а также к созданию и дальнейшему распространению своих копий, не всегда совпадающих с оригиналом, осуществлению иного вредоносного воздействия.

**Web-черви.** Отдельную категорию составляют черви, использующие для своего распространения web-серверы. Заражение происходит в два этапа. Сначала червь проникает в компьютер-сервер и модифицирует web-страницы сервера. Затем червь «ждет» посетителей, которые запрашивают информацию с зараженного сервера (например, открывают в браузере зараженную web-страницу), и таким образом проникает на другие компьютеры сети.

Разновидностью web-червей являются **скрипты** – активные элементы (программы) на языках JavaScript или VBScript. Профилактическая защита от web-червей состоит в том, что в браузере можно запретить получение активных элементов на локальный компьютер. Еще более эффективны web-антивирусные программы, которые включают межсетевой экран и модуль проверки скриптов на языках JavaScript или VBScript.

**Программы-вымогатели** представляют проблему для предприятий, образовательных учреждений и системы здравоохранения. Исследователи кибербезопасности продемонстрировали, что это семейство вредоносного ПО способно без труда вывести из строя базовую инфраструктуру, необходимую для функционирования городов.

**Вирусы-шифровальщики.** Бум вирусов-шифровальщиков пришелся на 2017 год, когда мир столкнулся с эпидемиями WannaCry, NotPetya, BadRabbit. Но уже в следующем году количество подобных таких атак снизилось на 73%. Атака вируса шифровальщика заключается в том, что внедряется в компьютерную среду жертвы вредоносная программа, которая зашифровывает участок

памяти или весь жесткий диск, делая его недоступным для хозяина компьютера. Вымогатель требует выкуп за расшифровку данного пространства.

Современные средства защиты и обновленное программное обеспечение справляются с большинством вирусов-шифровальщиков. Однако всегда есть вероятность, что преступники сумеют первыми найти уязвимость и воспользоваться ею. Вредоносные программы, использующие уязвимости в ПО, которые еще не были закрыты, называются угрозами нулевого дня.

**Рекомендации по борьбе с вирусами-шифровальщиками:**

1. *Регулярно делать резервные копии всех важных файлов на безопасные внешние носители информации*.

*2. Установить и настроить антифишинговые и антиспамные фильтры.*

3. *Не доверять случайным людям*.

4. *Включить функцию «Показывать расширения файлов» в настройках.* Так будет легче разобраться, какой файл является опасным.

5. *Регулярно устанавливать обновления для ОС, браузера, антивируса и другого ПО.*

6. *Установить надежный антивирус, который умеет бороться с шифровальщиками-вымогателями*.

7. *Если кажется, что обнаружен какой-то подозрительный процесс, отключить компьютер от Интернета*.

8. *Если компьютер уже подвергся заражению, не платить «выкуп», если в этом нет серьезной необходимости*.

9. *Еще один совет для уже «заразившихся»: проверить вирус на принадлежность к старому поколению*.

Кроме того, полиция и специалисты по кибербезопасности (в том числе «Лаборатория Касперского») периодически ловят преступников и выкладывают инструменты для восстановления файлов в Сеть. Стоит проверить, можно ли вернуть свои файлы абсолютно бесплатно с помощью сайта noransom.kaspersky.com.

**Руткит** – это программа, используемая киберпреступниками для получения контроля над компьютером или сетью. Иногда руткиты представляют собой единую программу, но чаще состоят из набора инструментов, позволяющих злоумышленникам управлять устройством на уровне администратора.

*Руткиты устанавливаются на машины несколькими способами:*

– с помощью фишинга или другого типа атак с применением социальной инженерии;

– используя уязвимости (слабые места в программном обеспечении или операционной системе, если они не обновлялись) для принудительной установки руткита на компьютер;

– с помощью связи с другими файлами, такими как зараженные файлы PDF, пиратские носители или приложения из подозрительных сторонних магазинов.

**Виды руткитов:**

1. *Аппаратные руткиты и руткиты для прошивки* могут повлиять на работу жесткого диска, маршрутизатора или BIOS системы, то есть на программное обеспечение, установленное на небольшом чипе памяти на материнской плате компьютера.

2. *Руткиты загрузчика.* Механизм загрузчика отвечает за загрузку операционной системы компьютера. При атаке на систему руткиты загрузчика заменяют подлинный загрузчик взломанным. Это активирует руткит еще до полной загрузки операционной системы компьютера.

3. *Руткиты памяти* скрываются в оперативной памяти компьютера и используют ресурсы компьютера для выполнения вредоносных действий в фоновом режиме. Руткиты памяти влияют на производительность оперативной памяти компьютера. Поскольку руткиты этого типа хранятся только в оперативной памяти компьютера и не внедряют постоянный код, они исчезают при перезагрузке системы. Однако чтобы полностью избавиться от них могут потребоваться дополнительные действия.

4. *Руткиты приложений* заменяют стандартные файлы на компьютере файлами руткитов и даже могут изменить работу стандартных приложений. Эти руткиты поражают приложения Microsoft Office и такие программы как Notepad или Paint. Злоумышленники могут получить доступ к компьютеру при каждом запуске этих приложений. Зараженные приложения по-прежнему работают нормально, поэтому обнаружение руткитов пользователями затруднено.

5. *Руткиты режима ядра* представляют самую серьезную угрозу, поскольку нацелены на ядро операционной системы. Злоумышленники используют их не только для доступа к файлам на компьютере, но и для изменения функций операционной системы, путем добавления собственного кода.

6. *Виртуальные руткиты* загружаются под операционную систему компьютера. Затем они размещают целевые операционные системы как виртуальную машину, что позволяет перехватывать аппаратные вызовы, выполняемые исходной операционной системой. Этот тип руткита не меняет ядро для нарушения работы операционной системы. Его может быть очень сложно обнаружить.

**Возможные признаки руткитов:**

1. *Синий экран*.
2. *Необычное поведение веб-браузера*.
3. *Низкая производительность устройства*.
4. *Изменение параметров Windows без разрешения*.
5. *Веб-страницы работают некорректно*.

Проверка на наличие руткитов – это лучший способ обнаружить заражение руткитами. Проверку может инициировать антивирусное решение. Если есть подозрение на наличие руткита, один из способов обнаружения заражения – выключить компьютер и выполнить проверку из известной чистой системы.

Удаление руткита – это сложный процесс, который обычно требует специальных инструментов, таких как утилита TDSSKiller от «Лаборатории Касперского», позволяющая обнаруживать и удалять руткит TDSS. Иногда единственным способом полностью удалить тщательно спрятанный руткит является

удаление операционной системы компьютера с последующим восстановлением с нуля.

*Для минимизации риска заражения руткитами применимы многие меры, используемые для защиты от компьютерных вирусов*:

- использование комплексных решений кибербезопасности;
- постоянное обновление системы;
- внимательность к фишинговым атакам;
- осуществление загрузки файлов только из надежных источников;
- внимательность к поведению или производительности компьютера.

**Фрод** (fraud) – умышленные действия или бездействие физических и/или юридических лиц с целью получить выгоду за счет компании и/или причинить ей материальный и/или нематериальный ущерб. Простыми словами, фрод (с англ. *fraud* – «обман») – это ситуация, когда мошенник оплачивает услуги ворованным платежным средством. Обычно, это кредитная карта, но иногда фрод бывает и с PayPal.

Практический пример фрода. Вначале, путем фишинга, мошенник овладевает информацией о карте (логин, пароль, номер карты), например, с использованием поддельного сайта. Далее он ищет способы «отоварить» полученные деньги, находит продавца и покупает у него продукт за $100 с украденной карты. Интернет-магазину, например, всегда хорошо иметь anti-fraud систему, которая определит мошенника и не позволит ему совершить оплату на сайте магазина.

Продавец пренебрегает обеспечением безопасности своего бизнеса в Интернете. Он еще не верит во фрод, поэтому идет к своему поставщику и покупает продукт за $80, который позже продает мошеннику, не имея ни малейшего понятия о том, что он на самом деле мошенник, а деньги ворованные. На первый взгляд, продавец заработал $20 и все хорошо. Увы, ненадолго, поэтому, без тщательной проверки платежа нельзя рассчитываться с партнерами.

Через определенное время хозяин банковской карты обращает внимание, что деньги с его карты активно пропадают. Появляются расходы на товары и услуги, которые он реально не оплачивал. Пострадавший обращается в банк и доказывает, что к некоторым тратам он не имеет никакого отношения. Просит вернуть деньги.

Банк удовлетворяет заявку – налицо несанкционированная активность с банковской карты их клиента. Банк запрашивает принудительный возврат средств (чарджбэк) со счета продавца ($100), а также взимает комиссию $20 за то, что произошел «чарджбэк». В обязанность продавца должна входить проверка платежа на мошенничество, а если будет факт мошенничества – банк взыщет штраф. Банк почти всегда удовлетворяет заявку клиента (чарджбэк). В любом случае будут материально пострадавшие: или продавец, если покупатель докажет, что оплата была не санкционирована им, или сам покупатель.

**Флуд** (от англ. *flood* – «наводнение, поток») – это комментарии, сообщения и посты на различных интернет-площадках, предназначенных для общения, не несущие смысловой нагрузки, занимающие большие объемы и не связанные с обсуждаемой темой. Синоним флуда – пустословие.

Основной целью флудеров является вызвать раздражение у других пользователей. Участники беседы начинают отвечать на их сообщения вовлекаясь в новый разговор, тем самым уходят от основной темы.

Флуд внешне напоминает спам, но он имеет отличительные черты. Цель спама имеет коммерческий характер, цель флуда – заставить нервничать других, а самому развлечься. Рассылка спама в большей степени автоматизирована и не требует участия человека. Флуд рассылают только люди. Некоторый спам может быть заражен вредоносными программами и угрожает компьютерной безопасности. Флуд не причинит аналогичного вреда.

## 1.4. Модель нарушителя кибербезопасности

Нарушения и преступления, в том числе и компьютерные, совершаются людьми. Как говорится, *бывают «виртуальные преступления», но «виртуальных преступников» не бывает*. В этом смысле вопросы безопасности автоматизированных систем во многом по своей сути являются вопросами человеческих отношений и человеческого поведения.

Исследования проблемы обеспечения безопасности компьютерных систем ведутся в направлении раскрытия природы явлений, заключающихся в нарушении целостности и конфиденциальности информации, дезорганизации работы компьютерных систем.

*Неформальная модель нарушителя* отражает его практические и теоретические возможности, априорные знания, время и место действия и т.п. Для достижения своих целей нарушитель должен приложить некоторые усилия, затратить определенные ресурсы. Зная причины нарушений, можно либо повлиять на сами эти причины (конечно, если это возможно), либо точнее определить требования к системе защиты от данного вида нарушений или преступлений.

***Нарушитель*** *– это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.*

***При отсутствии правил (запретов и ограничений) не существует и нарушителей (если нет правил, значит, нечего и нарушать). Поэтому борьба с нарушениями всегда должна начинаться с установления четких правил (ограничений, политики безопасности).***

*Злоумышленник* – это нарушитель, намеренно (умышленно, со злым умыслом) идущий на нарушение.

При построении модели нарушителя обычно формулируются предположения:

- о категориях лиц, к которым может принадлежать нарушитель;
- о мотивах действий нарушителя и преследуемых им целях;

– о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средствах);

– о характере возможных действий нарушителей.

**По отношению к АИС нарушители могут быть внутренними (из числа обслуживающего персонала и пользователей системы) или внешними (посторонними лицами).**

*Внешние нарушители* не имеют прав доступа в контролируемую (охраняемую) зону (территорию) и/или к защищаемым ИР и компонентам ПТС систем и сетей (см. рис. 3). Внешние нарушители реализуют угрозы КБ *преднамеренно* с использованием специализированных программно-аппаратных средств или без использования таковых.

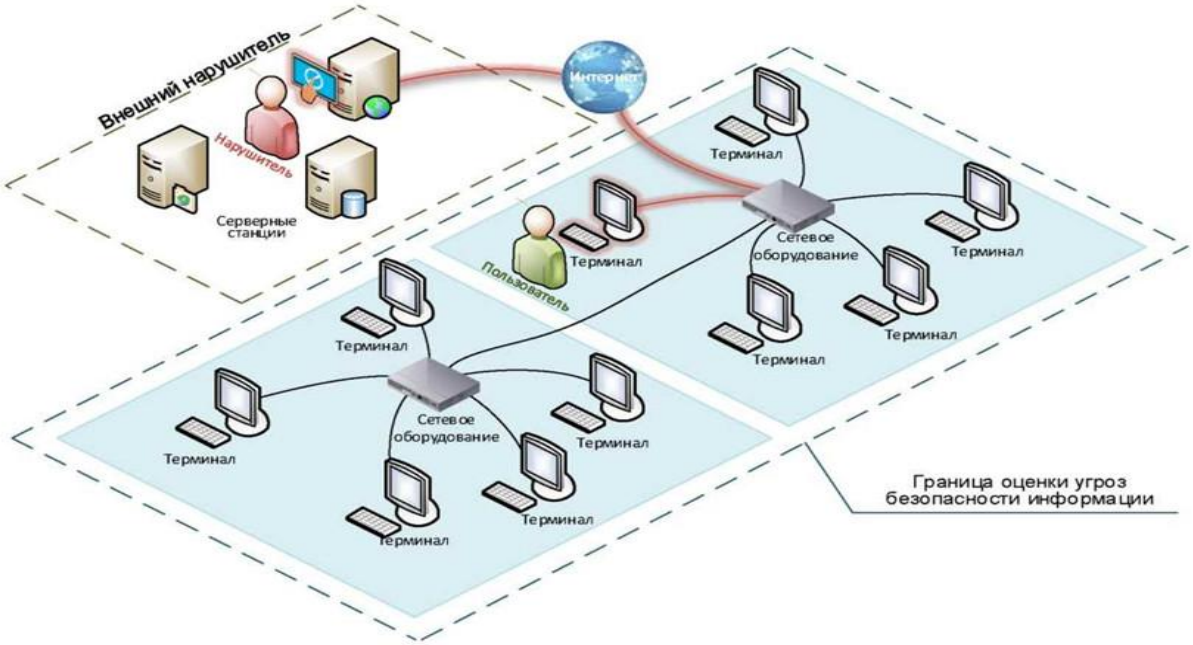


*Рисунок 3. Деятельность внешних нарушителей КБ*

*К внешним нарушителям можно отнести*:

– спецслужбы иностранных государств;

– террористические, экстремистские группировки;

– криминальные структуры;

– физические лица и преступные группы (хакеры);

– конкурирующие организации;

– разработчиков программного обеспечения (далее – ПО) и ТС;

– поставщиков ПО, ТС, обеспечивающих систем;

– технический персонал сторонних организаций, обслуживающих здания и средства вычислительной техники (далее – СВТ) (уборщиков, электриков, сантехников, ремонтников и других сотрудников, имеющих доступ в здания и помещения, где расположены компоненты АИС);

– клиентов и посетителей (представители сторонних организаций и отдельные граждане);

– представителей организаций, взаимодействующих по коммунальным вопросам (энерго-, водо-, теплоснабжения и т.п.).

– уволенных сотрудников (пользователей).

*Внутренние нарушители* имеют права доступа в контролируемую зону и/или к ИР и компонентам ПТС систем и сетей (см. рис. 4). Внутренние нарушители реализуют угрозы информационной безопасности (далее – ИБ) *преднамеренно* или *непреднамеренно*.

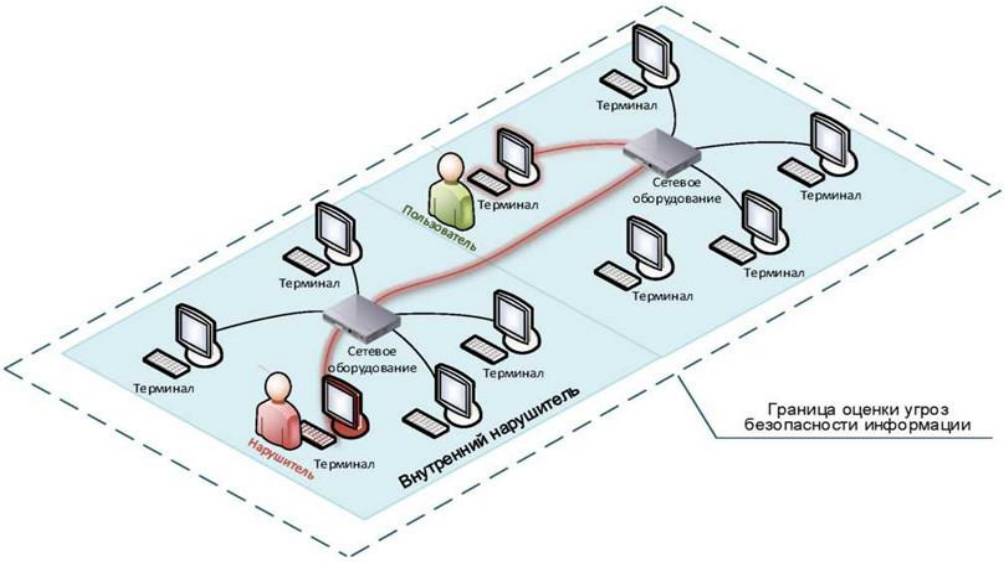


*Рисунок 4. Деятельность внутренних нарушителей КБ*

*Внутренним нарушителем* может быть лицо из следующих категорий сотрудников:

– авторизованных пользователи систем и сетей (инсайдеры);

– персонала, обеспечивающего работу технических средств (инженеры, техники);

– обслуживающего персонала систем и сетей или обеспечивающих систем оператора (администрации, охраны, уборщиков и т.д.);

– сотрудников отделов разработки и сопровождения ПО (прикладных и системных программистов);

– системных администраторов и администраторов безопасности;

– сотрудников службы информационной безопасности;

– руководителей различных уровней.

Условием, позволяющим нарушителям использовать способы реализации угроз КБ, является наличие у них возможности доступа к следующим *типам интерфейсов объектов воздействия*:

– внешним сетевым интерфейсам, обеспечивающим взаимодействие с интернетом или смежными системами (проводным, беспроводным, веб-интерфейсам, интерфейсам удаленного доступа и др.);

– внутренним сетевым интерфейсам, обеспечивающим взаимодействие с компонентами систем и сетей, имеющими внешние сетевые интерфейсы (проводным, беспроводным);

– интерфейсам для подключения пользователей (проводным, беспроводным, веб-интерфейсам, интерфейсам удаленного доступа и др.);

– интерфейсам для подключения съемных машинных носителей информации и периферийного оборудования;

– интерфейсам для установки, настройки, испытаний, пусконаладочных работ (в том числе администрирования, управления, обслуживания) обеспечения функционирования компонентов систем и сетей;

– к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей.

*Основными методами реализации/возникновения угроз КБ* являются:

– использование уязвимостей ПО, архитектуры и конфигурации систем и сетей;

– использование уязвимостей в системе ограничении доступа к ИР и ТС систем и сетей (в том числе физического);

– внедрение вредоносного ПО;

– использование недекларированных возможностей ПО и/или ПТС;

– установка скрытых закладок в ПО и/или ПТС;

– создание и использование скрытых (по времени, по памяти) каналов для передачи конфиденциальных данных;

– перехват (измерение) побочных электромагнитных излучений и наводок (других физических полей) в процессе авторизации пользователей;

– физический доступ к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации (ключам доступа);

– нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию);

– ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке в ПО и/или ПТС.

Сценарии и способы реализации угроз КБ зависят от многих факторов: объектов воздействия, возможностей нарушителя, доступности интерфейсов, архитектуры АИС, системы защиты информации и т.п.

Определение конкретных значений характеристик возможных нарушителей в значительной степени субъективно. Модель нарушителя, построенная с учетом особенностей конкретной предметной области и технологии обработки информации, может быть представлена перечислением нескольких вариантов нарушителей. Каждая категория нарушителей должна быть охарактеризована значениями характеристик, приведенных выше. Для каждой из них можно привести оценку количества сотрудников организации, попадающих в данную категорию нарушителей.

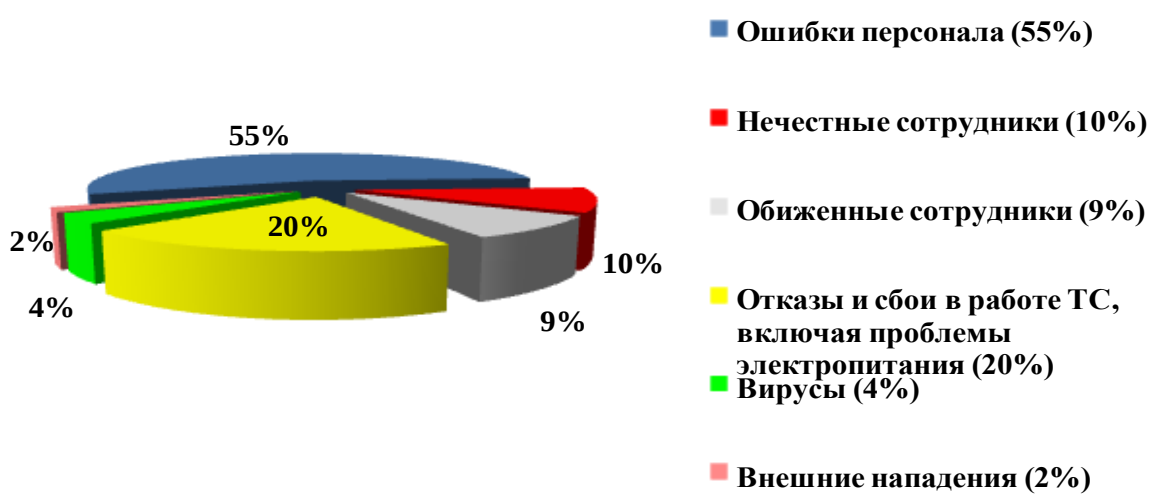


*Рисунок 5. Анализ нарушений и проблем в автоматизированных информационных системах*

Пользователи системы и ее персонал, с одной стороны, являются составной частью, необходимым элементом АИС. С другой стороны, они же являются основным источником угроз и движущей силой нарушений и преступлений. На следующей диаграмме приведены результаты анализа нарушений и проблем в АИС, проведенного Институтом компьютерной безопасности (*Computer Security Institute*) (см. рис. 5).

***Сотрудники организации являются самой массовой категорией нарушителей*** *в силу их многочисленности, наличия у них санкционированного доступа на территорию, в помещения и к ресурсам системы, разнообразия мотивов совершения разного рода небезопасных действий. Причем подавляющее большинство нарушений со стороны сотрудников носит неумышленный характер. Однако ущерб, который они при этом наносят организации, весьма значителен*. Именно поэтому борьба с ошибками пользователей и обслуживающего персонала АИС является одним из основных направлений работ по обеспечению безопасности.

## 1.5. Интернет вещей и его уязвимости

В эпоху всеобщей цифровизации пространство Интернета захватывает новая информационно коммуникационная технология – Интернет вещей, где информационные процессы проходят практически без участия человека. В отличие от Интернета людей в Интернете вещей ведущую роль играют программно-аппаратные комплексы, способные взаимодействовать друг с другом и с управляющим сетевым ПО.

*Конечная точка* – это однозначно идентифицируемое в сетевом пространстве устройство, способное самостоятельно обрабатывать данные для взаимодействия с человеком, с другими устройствами или с внешней физической средой.

В Интернете вещей сетевыми конечными точками являются:

- сенсоры, сервоприводы, контроллеры производственных операций;
- бытовые приборы;
- датчики систем пожарной и охранной сигнализации;
- камеры систем компьютерного зрения;
- point-of-sale терминалы;
- компоненты систем искусственного интеллекта и т.п.

*Интернет вещей (Internet of Things, далее – IoT)* – технология, которая объединяет физические устройства в сеть и позволяет им собирать, обрабатывать и передавать данные другим объектам с помощью программ, приложений или технических устройств.

*Интернет вещей* – инфраструктура взаимосвязанных сущностей, АИС и ИР, а также служб, позволяющих обрабатывать информацию о физическом и виртуальном мире и реагировать на нее.

*Технические устройства для сбора данных* – сенсоры или датчики. Датчики собирают данные, преобразуют их в сигнал и отправляют сигнал платформе.

*Шлюз IoT* – сетевое устройство, предназначенное для передачи данных между устройствами IoT и сетью Интернет.

Концепция IoT предполагает тесную взаимосвязь между информационными технологиями и операционными технологиями.

*Операционные технологии* – это процессы, методы и средства управления в *киберфизических системах*, где вычислительные ресурсы интегрированы с физическими сущностями любого вида, включая биологические и рукотворные объекты.

Технологии IoT используются в различных отраслях: производстве, автомобилестроении, здравоохранении, транспорте, логистике, энергетике, сельском хозяйстве и др. В зависимости от целей конкретной системы IoT интеллектуальные устройства могут варьироваться от простых датчиков освещенности до оборудования для анализа ДНК. Все чаще вокруг встречаются технологии умного дома, умного города, бодинет.

На абстрактном уровне IoT можно сравнить с информационной моделью человека. Тело собирает информацию об окружающей среде через сенсоры – органы чувств (зрение, слух, осязание, обоняние, вкус). Мозг осмысливает поступающие данные, сравнивает с известными образами в своей базе знаний и принимает решение по управлению частями тела. Если принятые образы отсутствуют в базе знаний, то мозг пытается их осознать, пользуясь накопленным опытом и правилами логики, и включить в базу знаний. В 2018 году в сферах транспорта, производства, систем автоматизации и других платформ корпоративного класса во всем мире использовалось около 8 млрд устройств («точек»)

IoT, в 2020 их было около 12 млрд, к 2025 году по разным прогнозам подключенных устройств будет 25 млрд или почти 60 млрд.

*Базовые принципы IoT:*

– распределенная сетевая инфраструктура, позволяющая доставлять данные в конечные точки IoT по оптимальным маршрутам;

– уникальный идентификатор для любого устройства IoT;

– наличие пользовательского интерфейса для ручного управления устройствами IoT;

– гарантированная доступность каждого устройства IoT и возможность коммуникации с управляющим ПО или пользователем в режиме реального времени;

– экономическая эффективность.

По сути IoT – это новая концепция информационно-телекоммуникационной сети, объединяющей на основе архитектуры Интернета множество датчиков и исполнительных устройств для управления технологическими процессами в автоматическом режиме с минимальным участием человека. При этом требования к архитектуре, надежности и функциональным возможностям IoT в некоторых случаях выходят за рамки Интернета людей (см. рис. 6).

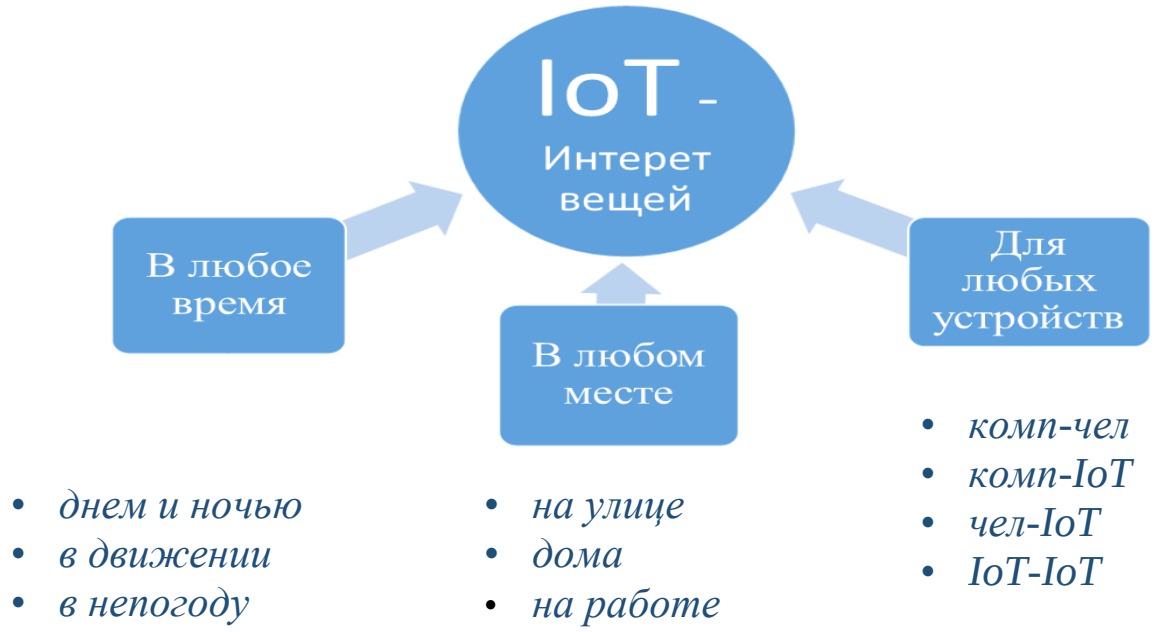


*Рисунок 6. Требования к коммуникации IoT*

С точки зрения информационной безопасности архитектура IoT подразделяется на несколько уровней.

**Физический уровень (уровень вещей)** представляет два типа операций: сбор информации (датчики) и механические действия (актуаторы, исполнительные механизмы).

На физическом уровне функционируют относительно простые датчики (световые, звуковые, емкостные, индуктивные, электрические, концевые выключатели, измерители угла поворота, скорости вращения и т.п.) и сложные сенсоры-анализаторы (спектра, химического состава, компьютерного зрения), собирающие данные в реальном времени.

*Актуаторы IoT* – это, как правило, электронные ключи и контроллеры различных механизмов и технических систем.

*Примерные требования к устройствам IoT* различного применения:

– минимальная цена;

– надежность, защищенность от климатических воздействий;

– низкое энергопотребление и автономное электропитание;

– минимальные затраты на установку и обслуживание;

– машинное обучение;

– для видеокамер – первичная обработка изображения с принятием решения на основе искусственного интеллекта и т.п.

Как видно из примера, в некоторых случаях требования могут быть противоречивыми.

**Сетевой уровень** обеспечивает обмен данными «вещей» с управляющим ПО.

Некоторые системы IoT предполагают размещение устройств и управляющего ПО в одной сети или прямое подключение через сотовую связь, но чаще устройства IoT подключаются к управляющим приложениям в сети Интернет через шлюзы (gateway), которые выступают в роли агрегаторов исходных данных и маршрутизаторов пакетов.

**Прикладной уровень** представляет набор служб и приложений, обеспечивающих автоматизацию бизнес-процессов в IoT.

*В последнее время возникли дополнительные требования к системам IoT*:

– данные должны иметь неограниченный объем;

– являться разнородными (количественными, качественными, текстовыми);

– результаты должны быть конкретны и понятны;

– инструменты для обработки сырых данных должны быть просты в использовании.

Помимо этого методы традиционной математической статистики не подходят для анализа и прогнозирования поведения систем.

В этой связи интеллектуальные возможности IoT расширяются за счет технологий анализа больших данных, в том числе глубинного, а также машинного обучения.

В качестве наглядного примера можно рассмотреть популярную концепцию «умного дома» с автоматическим управлением его инженерной инфраструктурой.

Информационная безопасность IoT подразумевает защиту устройств и сетей, к которым они подключены, от сетевых атак и взломов. Это достигается путем выявления, мониторинга и устранения потенциальных уязвимостей безопасности.

*Основные уязвимости IoT*:

– ненадежные или несменяемые пароли доступа к устройствам IoT;

– сохранение заводских (общеизвестных) паролей;

– сквозная авторизация – для взлома сети достаточно взломать одно устройство;

– отсутствие шифрования сетевого трафика;

– использование небезопасного ПО и протоколов сетевого обмена;

– наличие потенциально опасных сетевых сервисов и открытых портов;

– небезопасные настройки по умолчанию и ограниченное управление устройством;

– отсутствие технической поддержки и безопасных механизмов обновления ПО;

– отсутствие средств защиты от сетевых атак и вредоносного ПО;

– возможность физического доступа к устройству посторонних;

– типовые уязвимости мобильных технологий и облачной инфраструктуры.

Наиболее известные примеры успешных кибератак на IoT.

В 2016 году сотни тысяч скомпрометированных сетевых устройств были вовлечены в ботнет Mirai, который превратил их в прокси-серверы для вредоносного трафика. В результате атаки ботнета Mirai наблюдались сбои в работе таких крупных сервисов и сайтов, как Spotify, Netflix и PayPal.

В 2016 году уязвимость в мобильном и облачном приложениях домашних смарт-устройств SmartThinkQ (LG) позволяла злоумышленникам создать поддельную учетную запись и удаленно получить контроль над всеми видами бытовой смарт-техники LG: телевизорами, пылесосами, холодильниками, электроплитами, посудомоечными и стиральными машинами.

В 2018 году вредоносная программа VPNFilter заразила более полумиллиона маршрутизаторов, установив на устройства IoT вредоносное ПО, которое перехватывает трафик и крадет пароли.

В 2018 году через умный термометр декоративного аквариума в фойе хакеры смогли проникнуть в локальную сеть казино и скопировать базу данных хайроллеров (VIP-игроков на высоких ставках), представляющую коммерческую тайну.

В 2020 году эксперт по кибербезопасности взломал Tesla Model X менее чем за две минуты, воспользовавшись уязвимостью Bluetooth. Аналогичным атакам также подверглись другие автомобили, для открытия и запуска которых используются беспроводные ключи.

В 2021 году швейцарские хакеры получили доступ к 150 000 прямых трансляций с камер компании Verkada. Это были камеры видеонаблюдения внутри зданий государственных организаций, таких как школы, больницы, тюрьмы, и частных компаний.

Требования к КБ индустриального IoT устанавливаются государством или эксплуатирующими организациями исходя из оценки рисков.

В значительной степени с пространством IoT пересекается критическая информационная инфраструктура Российской Федерации.

## 1.6. Критическая информационная инфраструктура

*Критическая информационная инфраструктура (далее – КИИ)* – это совокупность информационных систем (далее – ИС), информационно-телекоммуникационных сетей (далее – ИТКС), автоматизированных системы управления субъектов КИИ, а также сетей электросвязи (далее – СЭС), используемых для организации их взаимодействия. К КИИ обычно относится ИС, сбой или отказ в работе которых кардинально отразится на безопасности граждан, общества государства[3].

*Автоматизированная система управления технологическими процессами* – комплекс программных и технических средств (далее – ПТС), предназначенных для управления технологическими процессами в киберфизических системах.

*Индустриальный (промышленный) Интернет* – концепция построения информационных и коммуникационных инфраструктур на основе подключения к сети Интернет промышленных устройств, технологического оборудования, датчиков, сенсоров, систем управления производственными процессами и т.п.

*Значимые объекты КИИ* – это объекты, которым в установленном порядке присвоена категория значимости и которые включены в реестр КИИ. Правила категорирования объектов КИИ РФ, а также перечень показателей критериев значимости и их значений утвержден постановлением Правительства Российской Федерации от 08.02.2018 № 127[4].

*Основные показатели значимости ущерба от угроз КБ КИИ*:

- смерть или ухудшение здоровья граждан;
- сбои и отказы объектов обеспечения жизнедеятельности;
- нарушение функционирования транспортной инфраструктуры;
- нарушение функционирования сети связи;
- невыполнение органом возложенной на него функции;
- отказ в доступе к государственной услуге;
- нарушение международных обязательств, срыв переговоров;
- недополучение средств в бюджет;
- уменьшение дохода предприятия, организации;
- вредные воздействия на окружающую среду;
- нарушение работы мониторинговых и ситуационных центров;
- невыполнение гособоронзаказа и т.п.

---

[3] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Российская газета. 2017. № 167.

[4] Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» // Собрание законодательства Российской Федерации. 2018. № 8. Ст. 1204.


*Рисунок 7. Основные объекты и субъекты КИИ*

*Безопасность КИИ* – состояние защищенности КИИ, обеспечивающее ее устойчивое функционирование в условиях целенаправленных кибератак и непреднамеренных воздействий.

*Киберинцидент* – факт нарушения безопасности КИИ.

*Кибератаки на объекты КИИ* – это сложные многоходовые процессы, приводящие к несанкционированному воздействию на объекты КИИ или СЭС в целях нарушения их функциональности и/или создания угрозы безопасности данных.

Защита значимых объектов КИИ находится под контролем уполномоченных государственных спецслужб (см. рис. 7).

*Основной регулятор отношений* – Федеральная служба по техническому и экспортному контролю (ФСТЭК России), ответственная за выполнение законодательства в части защиты КИИ.

*Минкомсвязь России* – регулятор в области связи и объектов СЭС.

*Центральный Банк Российской Федерации* регулирует финансовую и банковскую сферу.

В части подключения к Государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) регулятором является ФСБ России.

| Категория | Типы киберинцидентов на объектах КИИ |
|---|---|
| Внедрение и распространение ВПО | заражение вредоносным ПО (ВПО);<br>использование для распространения ВПО;<br>внедрение модулей ВПО |
| Нарушение или замедление работы | компьютерная атака типа DDoS;<br>несанкционированный вывод из строя;<br>непреднамеренное отключение |
| Несанкционированный доступ к ИР и ПТС | эксплуатация уязвимостей;<br>компрометация учетной записи; |

| Категория | Типы киберинцидентов на объектах КИИ |
|---|---|
| | подбор паролей |
| Сбор сведений об АИС | попытки авторизации в АИС;<br>сканирование ресурсов АИС;<br>сканирование ИР;<br>перехват сетевого трафика;<br>социальная инженерия |
| Нарушение конфиденциальности и целостности ИР | разглашение информации;<br>несанкционированное изменение информации |
| Распространение запрещенной информации | рассылка спам-сообщений;<br>публикация запрещенного контента |
| Мошенничество с ИР | подделка личности/организации;<br>публикация мошеннических данных |

Предварительное следствие по правонарушениям в области защиты КИИ ведут следователи ФСБ России.

Защита объектов КИИ является нетривиальной задачей. В промышленных сетях применяются десятки коммуникационных технологий и протоколов. Они позволяют создавать распределенные системы, объединяющие различные датчики, контроллеры и исполнительные устройства. Обмен данными в промышленных сетях обычно осуществляется с помощью сложных специализированных протоколов: Profibus, FIP, ControlNet, Interbus-S, DeviceNet, P-NET, WorldFIP, LongWork или Modbus Plus. Протоколы разработаны с учетом особенностей производства и технических систем, обеспечивают надежные соединения и высокую точность управления в режиме реального времени.

Тенденция комплексной автоматизации опирается и на растущую потребность в использовании производственных данных в бизнес-процессах, бухгалтерском учете, системах планирования и управления ресурсами предприятий (ERP) и взаимодействия с заказчиками (CRM), программах инвентаризации. Современные АСУ ТП используют для коммуникаций сети Ethernet и протоколы TCP/IP.

*Промышленный Ethernet* – спецификация Ethernet для обмена данными между программируемыми контроллерами и АСУ ТП в киберфизических системах.

Довольно часто кибератаки на объекты КИИ начинаются с взлома или заражения SCADA (Supervisory Control And Data Acquisition) – программно-аппаратных комплексов управления киберфизическими системамми с человеко-машинным интерфейсом (HMI, Humane Machine Interface).

Наиболее известной атакой на КИИ считается вывод из строя центрифуг на заводе по обогащению урана в иранском городе Нетензе в 2009–2010 годах. Атака произведена с помощью червя Win32/Stuxnet, внедренного в заводскую сеть при помощи USB-flash накопителей.

По мнению ряда экспертов, Stuxnet представляет собой специализированную разработку спецслужб Израиля и США, направленную против ядерной программы Ирана.

Другой пример связан с атакой государственной информационной инфраструктуры Эстонии в 2007 году. Нападение на сайты правительства Эстонии, эстонских СМИ, банков и других организаций было связано с решением эстонских властей перенести памятник советским солдатам из центра Таллина на воинское кладбище. Против официальных сайтов Эстонии использовалась DDoS-атаки типа Ping of Death и SYN-флуд, Министр иностранных дел Эстонии публично обвинил российские власти в причастности к данным атакам, но не смог предоставить каких-либо доказательств.

12 мая 2017 года начал свое распространение по миру червь WannaCry. Атаке подвергалась информационная инфраструктура различных организаций на Украине, в Индии, Тайване и других странах. Код WannaCry эксплуатировал уязвимость Windows, которая была ранее выявлена Агентством национальной безопасности (АНБ) США.

В Испании были атакованы компьютеры компаний Telefonica, Gas Natural, Iberdrola (поставщик электричества), Centro Nacional de Inteligencia, банке Santander и филиала консалтинговой компании KPMG.

В Великобритании были инфицированы компьютеры в больницах NHS trusts Национальной службы здравоохранения.

В Германии были инфицированы компьютеры основного железнодорожного оператора Deutsche Bahn.

В США кибератакам с применением WannaCry подверглись операционные системы авиастроительной корпорации Boeing. Компанией были оперативно проведены восстановительные мероприятия программного обеспечения, и вирус не повлиял на производственную деятельность Boeing.

В России атаки на информационные системы РЖД, МВД России, МЧС России, Сбербанк были быстро локализованы и не причинили значительного ущерба.

В 2015 году была проведена многоходовая атака на энергосеть Украины. Сначала сотрудникам трех энергетических компаний были направлены фишинговые письма с вложенным документом формата MS Word. Для просмотра документа требовалось включить выполнение макросов, после чего на атакуемый компьютер устанавливалась программа под названием BlackEnergy3 с бэкдором для удаленного доступа.

Фишинговая атака давала злоумышленникам доступ в корпоративную сеть, и далее в течение нескольких месяцев хакеры получили доступ к учетным данным сотрудников, в том числе пароли от VPN-доступа в систему SCADA. Затем хакеры изменили конфигурацию источников бесперебойного питания (UPS) и отключили мощности на подстанциях. Чтобы потребители не могли дозвониться и преждевременно сообщить диспетчерам об отключении света, была организована телефонная TDoS-атака на колл-центры энергетических компаний. Через 90 минут после начала атаки установленные логические бомбы запускали зловред KillDisk, который стер файлы и MBR на компьютерах в центрах управления. Несмотря на то, что атака была краткосрочной и относительно мягкой, блэкаут на Украине создал прецедент для нарушения безопасности электрических сетей по всему миру.

Анализ киберинцидентов, связанных с КИИ, обостряет противоречие классического IoT между простотой управления по сети Интернет и защищенностью от кибератак.

*Меры, повышающие уровень защиты объектов КИИ от кибератак*:

1. Гибридная архитектура, разделяющая коммуникационные ИТ-сети и производственные ОТ-сети, которые непосредственно управляют элементами киберфизических систем, взаимодействующих с физическими объектами.

2. Сегментация сети и максимальная изоляция киберфизических систем от Интернета.

3. Непрерывный мониторинг функционирования объектов КИИ, в том числе с помощью комплексов SCADA.

4. Контроль изменения конфигурации АИС и подключения новых устройств, в том числе съемных носителей.

5. Регулярное обновление ПО.

6. Периодическое тестирование АИС на проникновение и на уязвимости ПТС.

7. Проверка лояльности авторизованных пользователей и обслуживающего персонала АС, в том числе методами OSINT (Open Source INTelligence – разведка по открытым источникам) и социальной инженерии.

Вполне очевидно, что для обнаружения угроз и реагирования на инциденты киберзопасности в режиме реального времени необходимо наличие специального подразделения, оснащенного специализированными средствами автоматизации выявления, реагирования и расследования инцидентов кибербезопасности.

## Вопросы для самоконтроля:

1. Что понимают под угрозой безопасности информации?
2. Что включает в себя информационная безопасность?
3. Что подразумевает понятие информационной безопасности в узком смысле этого слова?
4. Что относят к объектам информационной безопасности?
5. Какие требования предъявляются к защите информации с позиций системного подхода?
6. Какие причинами могут быть обусловлены информационные угрозы?
7. В чем заключается различие активных и пассивных угроз?
8. В чем заключается различие внутренних и внешних угроз?
9. Что такое спам?
10. Что такое фишинг?
11. Что относится к основным угрозам безопасности информации?
12. Каковы пути реализации несанкционированного доступа?
13. Каковы технические угрозы и причины, в результате которых они реализуются?
14. На какие группы подразделяются способы воздействия угроз на информационные объекты?
15. Что относится к информационным способам воздействия угроз на информационные объекты?
16. Что относится к физическим способам воздействия угроз на информационные объекты?
17. Что относится к радиоэлектронным способам воздействия угроз на информационные объекты?
18. Какие объекты АИС могут подвергаться воздействию информационных угроз?

# ГЛАВА 2.
# НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ

## 2.1. Основы государственной политики в области кибербезопасности

В Российской Федерации понятие кибербезопасность рассматривается в рамках информационной безопасности. При этом пока не изданы законодательные документы и подзаконные акты, касающиеся данного понятия. Однако область информационной безопасности проработана достаточно глубоко, имеется достаточное количество законов, подзаконных актов и руководящих документов, регулирующих отношения в этой области. Рассмотрим более детально ряд основных.

Современный этап развития системы обеспечения информационной безопасности государства и общества характеризуется переходом от тотального сокрытия большого объема сведений к гарантированной защищенности принципиально важных данных, обеспечивающей:

– конституционные права и свободы граждан, предприятий и организаций в сфере информатизации;

– необходимый уровень безопасности информации, подлежащей защите;

– защищенность систем формирования и использования информационных ресурсов (технологий, систем обработки и передачи данных).

Ключевым моментом политики государства в данной области является осознание необходимости защиты любых информационных ресурсов и информационных технологий, неправомерное обращение с которыми может нанести ущерб их обладателю (собственнику, владельцу, пользователю) или иному лицу.

**В Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы (Указ Президента Российской Федерации от 09.05.2017 № 203)** установлено, что ***целью развития информационной и коммуникационной инфраструктуры Российской Федерации является*** *обеспечение свободного доступа граждан и организаций, органов государственной власти Российской Федерации, органов местного самоуправления к информации на всех этапах ее создания и распространения*[5].

Стратегия предусматривает, что **для устойчивого функционирования информационной инфраструктуры Российской Федерации необходимо**:

– *обеспечить единство государственного регулирования, централизованные мониторинг и управление функционированием информационной инфраструктуры Российской Федерации* на уровне информационных систем и центров обработки данных, а также на уровне сетей связи;

[5] Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Собрание законодательства Российской Федерации. 2017. № 20. Ст. 2901.

– обеспечить поэтапный переход государственных органов и органов местного самоуправления к *использованию инфраструктуры электронного правительства*, входящей в информационную инфраструктуру России;

– *обеспечить использование российских криптоалгоритмов и средств шифрования* при электронном взаимодействии федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации, государственных внебюджетных фондов, органов местного самоуправления между собой, а также с гражданами и организациями;

– осуществить скоординированные действия, направленные на *подключение объектов к информационной инфраструктуре России*;

– *заменить импортное оборудование, программное обеспечение и электронную компонентную базу российскими аналогами, обеспечить технологическую и производственную независимость и информационную безопасность*;

– *обеспечить комплексную защиту информационной инфраструктуры России*, в том числе с использованием государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы и системы критической информационной инфраструктуры;

– *проводить непрерывный мониторинг и анализ угроз*, возникающих в связи с внедрением новых информационных технологий, для своевременного реагирования на них;

– *обеспечить единство сетей электросвязи Российской Федерации*, в том числе развитие и функционирование сетей связи государственных органов и органов местного самоуправления, а также интегрированной сети связи для нужд обороны страны, безопасности государства и обеспечения правопорядка.

**Для предоставления безопасных и технологически независимых программного обеспечения и сервисов необходимо**:

– *создать российское общесистемное и прикладное программное обеспечение, телекоммуникационное оборудование и пользовательские устройства* для широкого использования гражданами, субъектами малого, среднего и крупного предпринимательства, государственными органами и органами местного самоуправления, в том числе на основе обработки больших объемов данных, применения облачных технологий и интернета вещей;

– *создать встроенные средства защиты информации* для применения в российских информационных и коммуникационных технологиях;

– *обеспечить использование российских информационных и коммуникационных технологий в органах государственной власти Российской Федерации*, компаниях с государственным участием, органах местного самоуправления;

– *создать справедливые условия ведения предпринимательской деятельности для российских разработчиков*.

**Для защиты данных в Российской Федерации необходимо**:

– *совершенствовать нормативно-правовое регулирование в сфере обеспечения безопасной обработки информации* (включая ее поиск, сбор, анализ, использование, сохранение и распространение) и применения новых техноло-

гий, уровень которого должен соответствовать развитию этих технологий и интересам общества;

– *обеспечить баланс между своевременным внедрением современных технологий обработки данных и защитой прав граждан, включая право на личную и семейную тайну*;

– *упорядочить алгоритмы обработки данных и доступа к таким данным*;

– *обеспечить обработку данных на российских серверах* при электронном взаимодействии лиц, находящихся на территории Российской Федерации, а также передачу таких данных на территории Российской Федерации с использованием сетей связи российских операторов;

– *обеспечить государственное регулирование и координацию действий при создании и ведении информационных ресурсов в Российской Федерации в целях соблюдения принципа разумной достаточности при обработке данных*;

– *проводить мероприятия по противодействию незаконным обработке и сбору сведений о гражданах, в том числе персональных данных граждан*, на территории Российской Федерации неуполномоченными и неустановленными лицами, а также используемым ими техническим средствам.

Базовым документом, систематизирующим официальные взгляды на государственную политику, развитие общественных отношений и выработку мер по совершенствованию системы обеспечения ИБ в нашей стране является ***Доктрина информационной безопасности Российской Федерации (Указ Президента Российской Федерации от 05.12.2016 № 646).*** Доктрина информационной безопасности (далее – ИБ) утвердила национальные интересы России в информационной сфере и стратегические направления информационной безопасности в основных отраслях[6].

**Национальные интересы Российской Федерации в информационной сфере:**

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

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

[6] Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

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

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

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

***Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры*** в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации.

**Система обеспечения ИБ является частью системы обеспечения национальной безопасности Российской Федерации**. Обеспечение ИБ осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

6. *Стратегические направления ИБ в области обороны страны*:

– повышение эффективности системы ИБ вооруженных сил Российской Федерации и союзников;

– защита суверенного информационного пространства и общества от технологий ведения информационных войн;

– прогнозирование и противодействие угрозам КБ вооруженных сил;

– пропаганда деятельности государства по обороне Российской Федерации и нейтрализация негативного информационно-психологического воздействия на общественное сознание.

7. *Стратегические направления ИБ в области государственной и общественной безопасности*:

– противодействие использованию ИТ в военно-политических целях, противоречащих международному праву, а также в террористических, экстремистских, криминальных и иных противоправных целях;

– выявление и пресечение противоправной деятельности иностранных технических разведок в информационной сфере Российской Федерации;

– минимизация рисков антропогенного, стихийного или техногенного воздействия на объекты КИИ;

– повышение надежности и безопасности функционирования информационной инфраструктуры государственных и муниципальных органов;

– обеспечение безопасности функционирования высокотехнологичных систем вооружения, военной и специальной техники, АСУ объектами КИИ;

– профилактика и эффективное противодействие киберпреступлениям и правонарушениям, совершаемых с использованием ИТ;

– обеспечение защиты конфиденциальной информации за счет внедрения ПТС, сертифицированных по требованиям ИБ;

– развитие национальной системы управления российским сегментом сети Интернет;

– повышение эффективности информационной поддержки государственной политики;

– нейтрализация вредоносного информационного воздействия, направленного на дискредитацию традиционных российских духовно-нравственных ценностей.

8. *Стратегические направления ИБ в экономической сфере*:

– инновационное развитие ИТ-отрасли и электронной промышленности;

– минимизация зависимости отечественной промышленности от иностранных ИТ и ПТС;

– импортозамещение и переход на отечественную элементную базу в ИТ-отрасли;

– повышение значимости и конкурентоспособности российских компаний в мировой ИТ-индустрии.

9. *Стратегические направления ИБ в области науки, технологий и образования*:

– повышение научно-технического потенциала ИТ-сферы;

– организация фундаментальных исследований ИТ-сфере, электроники и связи;

– поддержка научных исследований и опытных работ по созданию инновационных прикладных ИТ-решений для обеспечения процессов жизнедеятельности;

– подготовка профессиональных кадров для ИТ-сферы;

– повышение уровня компьютерной грамотности и формирование культуры информационной безопасности граждан.

10. *Стратегические направления в области международной ИБ*:

– создание условий для принятия Конвенции ООН об обеспечении международной ИБ;

– создание на постоянной основе диалоговой платформы по вопросам ИБ под эгидой ООН;

– выработка новых принципов и норм международного права, регулирующих деятельность государств в глобальном информационном пространстве;

– достижение и выполнение двусторонних и многосторонних международных договоренностей в области обеспечения ИБ;

– организация и участие в международных форумах и научных проектах по вопросам ИБ и противодействию киберпреступности;

– формирование оргштатной структуры для реализации государственной политики в области международной ИБ;

– гармонизация национальных стандартов в области ИБ с международными;

– развитие международного сотрудничества в целях недопущения кибервойн в глобальном информационном пространстве;

– обеспечение под эгидой ООН принципов и норм международного гуманитарного права применительно к ИТ-сфере;

– развитие международного сотрудничества по вопросам противодействия использованию ИТ в террористических и экстремистских целях;

– развитие международного сотрудничества по вопросам обнаружения, предупреждения, реагирования и расследования инцидентов КБ на объектах КИИ и государственных ИС;

– противодействие монополизации сегментов глобального ИТ-рынка, включая информационные ресурсы, продукты и услуги;

– равноправное участие государств в управлении, развитии и использовании глобальных телекоммуникационных сетей;

– обеспечение равноправного доступа к новейшим ИТ-разработкам, предотвращение технологической зависимости и преодоление цифрового неравенства государств.

Государственное регулирование отношений в сфере ИБ осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

## 2.2. Нормативно-правовое регулирование обеспечения кибербезопасности в Российской Федерации

Среди основных документов, определяющих на сегодняшний день фундаментальные подходы к обеспечению информационной безопасности в Российской Федерации, можно выделить, в первую очередь, следующие:

– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[7];

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»[8];

– Указ Президента Российской Федерации от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности»[9];

– Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

– Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы».

Из современных правовых документов в области безопасности киберпространства следует особо отметить следующие:

– Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

– Указ Президента Российской Федерации 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»[10].

***Кибербезопасность*** согласно стандарту ISO/IEC 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности», разработанный подкомитетом SC 27 «Информационные методы обеспечения безопасности» технического комитета ISO/TC «Информационные технологии», реализуется на стыке следующих трех компонентов системы обеспечения информационной безопасности (см. рис. 8).

---

[7] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Официальный интернет-портал правовой информации [Электронный ресурс]. – Режим доступа: http://pravo.gov.ru. 29.12.2022.

[8] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. 2006. Ч. 1. Ст. 3451.

[9] Указ Президента Российской Федерации от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // Собрание законодательства Российской Федерации. 2021. № 16 (Ч. I). Ст. 2746.

[10] Указ Президента Российской Федерации от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // Собрание законодательства Российской Федерации. 2013. № 3. Ст. 178.

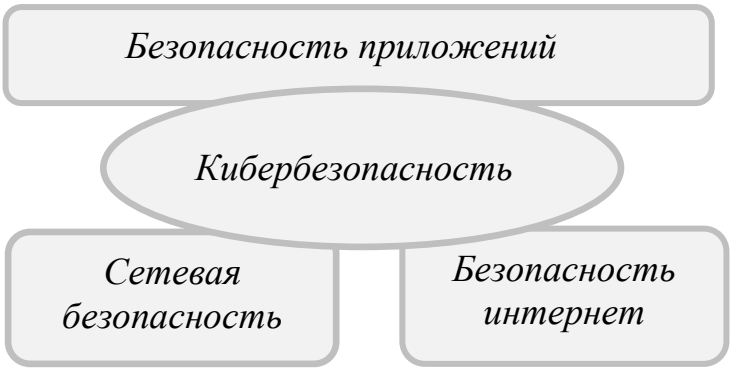


*Рисунок 8. Место понятия кибербезопасность*

Выделяются две основных категории участников информационного взаимодействия (см. рис. 9): провайдеры и потребители.

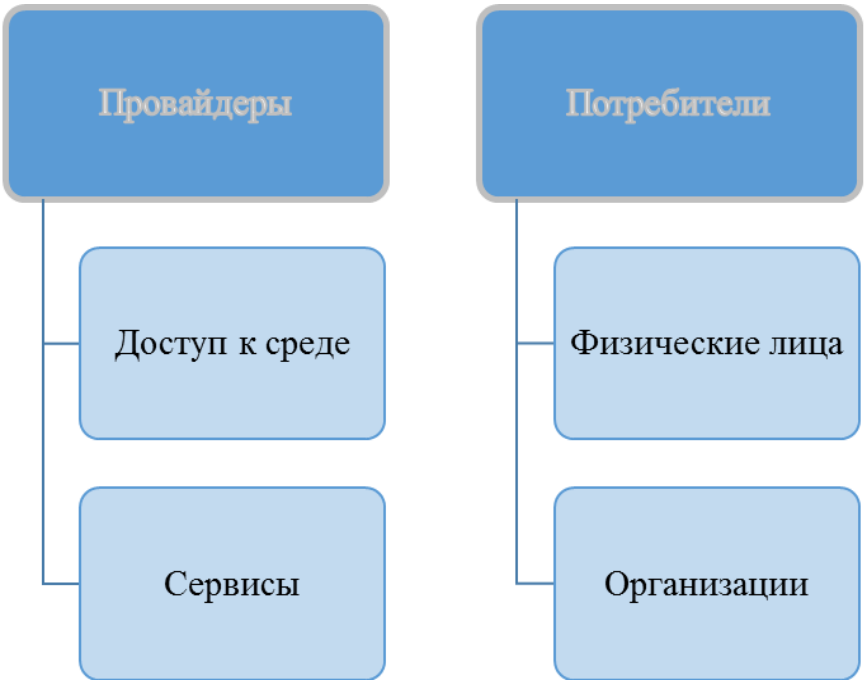


*Рисунок 9. Участники информационного взаимодействия*

*Провайдеры* могут предоставлять как доступ к среде информационного взаимодействия, так и доступ к тем или иным сервисом. В качестве потребителей могут выступать физические лица и организации.

*Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»* (далее – Закон) является базовым законом в информационной сфере. Он определяет ключевые термины, например говорит, что информация – это любые данные, сведения и сообщения, представляемые в любой форме. Также Закон дает понятие таким терминам, как сайт, электронное сообщение и поисковая система. Именно на этот Закон и эти определения нужно ссылаться при составлении документов по информационной безопасности.

Закон определяет, какая информация считается конфиденциальной, а какая – общедоступной, когда и как можно ограничивать доступ к информации, как происходит обмен данными. Также именно в этом Законе закреплены основные требования к защите информации и ответственность за нарушения при работе с ней.

***К ключевые моменты Закона об информационной безопасности:***

1. Нельзя собирать и распространять информацию о жизни человека без его согласия.

2. Все информационные технологии равнозначны – нельзя обязать компанию использовать какие-то конкретные технологии для создания информационной системы.

3. Есть информация, к которой нельзя ограничивать доступ, например, сведения о состоянии окружающей среды.

4. Некоторую информацию распространять запрещено, например, ту, которая пропагандирует насилие или нетерпимость.

5. Тот, кто хранит информацию, обязан ее защищать, например, предотвращать доступ к ней третьих лиц.

6. У государства есть реестр запрещенных сайтов. Роскомнадзор может вносить туда сайты, на которых хранится информация, запрещенная к распространению на территории Российской Федерации. Владелец заблокированного сайта может удалить незаконную информацию и сообщить об этом в Роскомнадзор – тогда его сайт разблокируют.

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» регулирует работу с персональными данными – личными данными конкретных людей. Его обязаны соблюдать те, кто собирает и хранит эти данные. Например, компании, которые ведут базу клиентов или сотрудников.

***Ключевые моменты Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»:***

1. Перед сбором и обработкой персональных данных нужно спрашивать согласие их владельца.

2. Для защиты информации закон обязывает собирать персональные данные только с конкретной целью.

3. Тот, кто собирает персональные данные, обязан держать их в секрете и защищать от посторонних.

4. Если владелец персональных данных потребует их удалить, пользователь обязан сразу же это сделать.

5. При работе с персональными данными пользователи обязаны хранить и обрабатывать их в базах на территории Российской Федерации. При этом последние изменения закона фактически запрещают трансграничную передачу персональных данных.

## 2.3. Классификация информации по степени доступа и понятие информации ограниченного доступа

Рассматривая вопросы защиты информации необходимо особо отметить, что защите подлежит только та информация, относительно которой ее владелец установил соответствующий режим.

В соответствии со ст. 5 *Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»* (Закона) *информация в зависимости от категории доступа к ней подразделяется на* ***общедоступную информацию****, а также на информацию, доступ к которой ограничен федеральными законами (****информация ограниченного доступа****).*

Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

– информацию, свободно распространяемую;

– информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

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

– информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Статья 7 Закона установила, что к общедоступной (открытой) информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен:

– массовая информация (свободно распространяемая информация);

– официальные документы (информация, которая подлежит предоставлению или распространению);

– обязательно предоставляемая документированная информация (информация, которая подлежит предоставлению или распространению);

– информация, являющаяся объектом гражданских правоотношений (информация, предоставляемая по соглашению лиц);

– другая открытая информация.

*Массовая информация* – это информация, содержащая сообщения информационного характера, подготавливаемая и распространяемая средствами массовой информации и через Интернет с целью информирования населения, в том числе реклама.

*Официальные документы* – это законодательные и нормативные акты, принимаемые органами государственной власти и органами местного самоуправления, судебная практика, другие документы законодательного, административного и судебного характера, а также их официальные переводы. Она создается в порядке законотворческой или иной правовой деятельности.

*Обязательно представляемая документированная информация* – это обязательные контрольные экземпляры документов, информация в учетных документах, данные документов, представляемых в органы статистики, налоговая,

регистрационная и другая аналогичная информация. Данный вид документированной информации создается юридическими и физическими лицами в порядке учета и отчетности и направляется в обязательном порядке различным органам и организациям в соответствии с действующим законодательством Российской Федерации.

*Информация, являющаяся объектом гражданских правоотношений* – это произведения науки и литературы, а также информация, содержащаяся в документах, закрепляющих авторские права на изобретения, полезные модели, промышленные образцы (патенты, свидетельства). В отдельных случаях данный вид документированной информации может быть отнесен к информации ограниченного доступа.

На основании ст. 9 Закона **ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства**.

*Документированная информация с ограниченным доступом подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.*

Выделение в отдельный вид информации ограниченного доступа государственной тайны обусловлено конституционными нормами. Конституция Российской Федерации в ч. 4 ст. 29 выделяет государственную тайну в отдельный вид, принципиально отличный от других видов конфиденциальной информации:

«4. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом.»[11]

Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне» в ст. 2 определил, что «*государственной тайной* признаются защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации»[12].

Понятие конфиденциальной информации закреплено в ст. 2 Закона: ***Конфиденциальностью информации*** *называется обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.*

---

[11] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Официальный текст Конституции Российской Федерации, включающий новые субъекты Российской Федерации – Донецкую Народную Республику, Луганскую Народную Республику, Запорожскую область и Херсонскую область, опубликован на Официальном интернет-портале правовой информации [Электронный ресурс]. – Режим доступа: http://pravo.gov.ru, 06.10.2022.

[12] Закон от 21.07.1993 № 5485-1 «О государственной тайне» // Собрание законодательства Российской Федерации. 1997. № 41. Ст. 8220-8235.

Перечень сведений, относящихся к конфиденциальной информации, утвержден Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»[13]. Он включает в себя:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (*персональные данные*), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях. Осуществляется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

2. Сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых в соответствии с федеральными законами от 20.04.1995 № 45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов»[14] и от 20.08.2004 № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства»[15], другими нормативными правовыми актами Российской Федерации принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством Российской Федерации такие сведения не отнесены к сведениям, составляющим государственную тайну.

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (*служебная тайна*).

4. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (*коммерческая тайна*). Обеспечена Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне»[16].

5. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.) (*профессиональная тайна)*.

---

[13] Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» // Собрание законодательства Российской Федерации. 1997. № 10. Ст. 1127.

[14] Федеральный закон от 20.04.1995 № 45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» // Российская газета. 1995. № 82.

[15] Федеральный закон от 20.08.2004 № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» // Собрание законодательства Российской Федерации. 2004. № 34. Ст. 3534.

[16] Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // Российская газета. 2004. № 166.

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них защищаются в соответствии с положениями части 4 Гражданского кодекса Российской Федерации[17].

7. Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии с Федеральным законом от 02.10.2007 № 229-ФЗ «Об исполнительном производстве»[18].

Институт конфиденциальной информации базируется на понятии тайны.

***Тайна*** *– это охраняемая государством конфиденциальная информация, незаконное получение, разглашение, использование которой создает угрозу нанесения вреда правам и законным интересам граждан, общества, государства и влечет за собой привлечение виновных к ответственности в соответствии с законодательством Российской Федерации*[19].

Общим для всех разновидностей тайны является то, что защита информации в режиме тайны предусматривает, во-первых, законодательно установленное право субъекта на введение режима ограниченного доступа, а во-вторых, установление и ограничение объемов прав обладателя на охраняемую информацию и его обязанностей по ее охране и предоставлению по запросам компетентных государственных органов, а также ответственности за нарушение установленных прав и обязанностей[20].

**В настоящий момент в российском законодательстве закреплено более 50 видов тайн. Причем подавляющее большинство из них относятся к служебной или профессиональной тайне.**

## 2.4. Организационные основы обеспечения информационной безопасности России

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

---

[17] Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ // Российская газета. 2006. № 289.

[18] Федеральный закон от 02.10.2007 № 229-ФЗ «Об исполнительном производстве» // Российская газета. 2007. № 223.

[19] Подробнее см.: Проблемы законодательного регулирования оборота информации, относящейся к служебной тайне в органах внутренних дел Российской Федерации: монография / А.Н. Прокопенко [и др.]. – Белгород: Бел ЮИ МВД России имени И.Д. Путилина, 2017. – 120 с.

[20] Волчинская Е.К. Коммерческая тайна в системе конфиденциальной информации // Информационное право. 2005. № 3. С. 17–21.

*Система обеспечения ИБ строится на основе разграничения полномочий* с учетом предметов ведения федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, а также органов местного самоуправления, определяемых законодательством Российской Федерации в области обеспечения безопасности.

***Состав системы обеспечения информационной безопасности определяется Президентом Российской Федерации***.

**Организационную основу системы обеспечения информационной безопасности составляют** принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности:

– Совет Федерации Федерального Собрания Российской Федерации;

– Государственная Дума Федерального Собрания Российской Федерации;

– Правительство Российской Федерации;

– Совет Безопасности Российской Федерации;

– федеральные органы исполнительной власти;

– Центральный банк Российской Федерации;

– Военно-промышленная комиссия Российской Федерации;

– межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации;

– органы исполнительной власти субъектов Российской Федерации;

– органы местного самоуправления;

– органы судебной власти.

**Участниками системы обеспечения информационной безопасности являются:**

– собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты;

– средства массовой информации и массовых коммуникаций;

– организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка;

– операторы связи;

– операторы информационных систем;

– организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи;

– организации, осуществляющие деятельность по разработке, производству и эксплуатации средств обеспечения информационной безопасности

– организации, осуществляющие деятельность по оказанию услуг в области обеспечения информационной безопасности;

– организации, осуществляющие образовательную деятельность в данной области;

– общественные объединения;

– иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационной безопасности.

**К основным задачам государственной системы защиты информации относятся:**

– проведение единой технической политики, организация и координация работ по защите информации в оборонной, экономической, политической, научно-технической и других сферах деятельности;

– исключение или существенное затруднение добывания информации техническими средствами разведки, а также предотвращение ее утечки по техническим каналам, несанкционированного доступа к ней, предупреждение преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе ее обработки, передачи и хранения;

– принятие в пределах компетенции правовых актов, регулирующих отношения в области защиты информации;

– анализ состояния и прогнозирование возможностей технических средств разведки и способов их применения, формирование системы информационного обмена сведениями по осведомленности иностранных разведок;

– организация сил, создание средств защиты информации и контроля за ее эффективностью;

– контроль состояния защиты информации в органах государственной власти и на предприятиях.

**Государственную систему защиты информации образуют (см. рис. 10)**[21]**:**

– Федеральная служба по техническому и экспортному контролю и ее центральный аппарат;

– Федеральная служба безопасности Российской Федерации, Министерство внутренних дел Российской Федерации, Министерство обороны Российской Федерации, Федеральная служба охраны Российской Федерации, Служба внешней разведки Российской Федерации, их структурные подразделения по защите информации;

– структурные и межотраслевые подразделения по защите информации органов государственной власти;

– управления Федеральной службы по техническому и экспортному контролю по федеральным округам;

– головная научно-исследовательская организация в Российской Федерации по защите информации (ФГУП «Научно-исследовательский испытательный институт проблем технической защиты информации» Федеральной службы по техническому и экспортному контролю);

[21] Подробнее см.: Безопасность информационных технологий: руководство слушателя курса. – М.: Учебный центр «Информзащита», 2019. – 301 с.

– головные и ведущие научно-исследовательские, научно-технические, проектные и конструкторские организации по защите информации органов государственной власти;

– предприятия, проводящие работы по оборонной тематике и другие работы с использованием сведений, отнесенных к государственной или служебной тайне, их подразделения по защите информации;

– предприятия, специализирующиеся на проведении работ в области защиты информации;

– высшие учебные заведения и институты повышения квалификации по подготовке и переподготовке кадров в области защиты информации.


*Рисунок 10. Структура государственной системы защиты информации в России*

Права и функции ФСТЭК России и ее центрального аппарата определяются «Положением о Федеральной службе по техническому и экспортному контролю» (Указ Президента Российской Федерации от 16.08.2004 № 1085)[22].

[22] Указ Президента Российской Федерации от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» // Собрание законодательства Российской Федерации. 2004. № 34. Ст. 3541.

*ФСТЭК России является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам*:

– обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

– противодействия иностранным техническим разведкам на территории Российской Федерации;

– обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации (далее – техническая защита информации);

– защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

– осуществления экспортного контроля.

ФСТЭК России является федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, а также специально уполномоченным органом в области экспортного контроля.

ФСТЭК России является органом защиты государственной тайны, наделенным полномочиями по распоряжению сведениями, составляющими государственную тайну. ФСТЭК России организует деятельность государственной системы противодействия техническим разведкам и технической защиты информации и руководит ею.

Руководство деятельностью ФСТЭК России осуществляет Президент Российской Федерации. ФСТЭК России подведомственна Минобороны России.

**Структурные и межотраслевые подразделения по защите информации органов государственной власти (в пределах их компетенции):**

– проводят единую техническую политику, осуществляют координацию и методическое руководство работами по защите информации на подведомственных органу государственной власти предприятиях;

– выполняют функции заказчика по проведению научно-исследовательских и опытно-конструкторских работ по проблемам защиты информации, а также заказчика поисковых научно-исследовательских работ по этим проблемам;

– разрабатывают предложения для федеральных программ по защите информации;

– организуют аттестование подведомственных органу государственной власти объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности,

сертификацию средств защиты информации и контроля за ее эффективностью, систем и средств информатизации и связи в части защищенности информации от утечки по техническим каналам, проведение специальных проверок и специальных исследований технических средств;

– готовят рекомендации и указания по лицензированию деятельности предприятий в области защиты информации.

***Непосредственное руководство работами по защите информации осуществляют руководители органов государственной власти или их заместители.***

*Указанные функции осуществляются подразделениями (штатными специалистами) по защите информации.*

Подразделения по защите информации являются самостоятельными структурными подразделениями или входят в состав одного из главных, технических, научно-технических или специальных управлений органа государственной власти. Назначение на должности и освобождение от должности руководителей этих подразделений производятся по согласованию с ФСТЭК России.

Допускается создание при органе государственной власти в соответствии с актами законодательства Российской Федерации самостоятельных предприятий различных организационно-правовых форм и форм собственности, на которые могут быть возложены функции структурных, а также межотраслевых подразделений по защите информации. В целях обеспечения принципа коллегиальности при рассмотрении важнейших вопросов защиты информации в органах государственной власти могут создаваться технические комиссии, межотраслевые или отраслевые советы.

*Управления ФСТЭК России по федеральным округам, в пределах своих зон ответственности*:

– проверяют и оценивают состояние защиты информации и оказывают методическую помощь на местах в организации и проведении мероприятий по защите информации;

– участвуют в аттестовании объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности.

Организация работ по защите информации ***в организациях*** осуществляется их руководителями. ***В зависимости от объема работ по защите информации руководителем организации создается структурное подразделение по защите информации либо назначаются штатные специалисты по этим вопросам.***

Подразделения по защите информации (штатные специалисты) в организации:

– осуществляют мероприятия по защите информации в ходе выполнения работ с использованием сведений, отнесенных к государственной или служебной тайне;

– определяют совместно с заказчиком работ основные направления комплексной защиты информации;

– участвуют в согласовании технических (тактико-технических) заданий на проведение работ;

– дают заключение о возможности проведения работ с информацией, содержащей сведения, отнесенные к государственной или служебной тайне.

*Указанные подразделения (штатные специалисты) подчиняются непосредственно руководителю организации или его заместителю*. Работники этих подразделений (штатные специалисты) приравниваются по оплате труда к соответствующим категориям работников основных структурных подразделений.

*Для проведения работ по защите информации могут привлекаться на договорной основе специализированные предприятия, имеющие лицензии на право проведения работ в области защиты информации*.

Организации, имеющие намерения заниматься деятельностью в области защиты информации, должны получить соответствующую лицензию на определенный вид этой деятельности. Лицензии выдаются ФСТЭК России и ФСБ России в соответствии со своей компетенцией по представлению органа государственной власти.

*Высшие учебные заведения и институты повышения квалификации по подготовке и переподготовке кадров в области защиты информации* осуществляют:

– первичную подготовку специалистов по комплексной защите информации;

– переподготовку (повышение квалификации) специалистов по защите информации органов государственной власти и предприятий;

– усовершенствование знаний руководителей органов государственной власти и предприятий в области защиты информации.

Подготовка кадров для государственной системы защиты информации осуществляется при методическом руководстве ФСТЭК России.

## 2.5. Ответственность за нарушения законодательства в сфере кибербезопасности

В соответствии со ст. 17 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[23] нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации[24].

[23] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 2006. № 165.

[24] Подробнее см.: Комментарий к Федеральному закону от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (комментарий к закону). Специально для системы ГАРАНТ, 2020 г.

*Институт ответственности* – это общеправовой институт, который оснащается применительно к сфере информационных правоотношений специальными методами и средствами. Иллария Лаврентьевна Бачило отмечала, что «институт ответственности в информационной сфере является системой норм и процедур, реализуемых в целях пресечения и установления вида, формы и мер наказания за совершенные и доказанные преступления и иные правонарушения с учетом их социального вреда и вины правонарушителя»[25].

**Особенности ответственности за правонарушения в сфере информации, информационных технологий и защиты информации:**

– к субъектам ответственности относятся физические лица, организации и их должностные лица, государственные органы и органы местного самоуправления, а также лица, ответственные за исполнение конкретных требований Закона (например, провайдеры, операторы связи, владельцы сайтов и т.д.);

– к субъектам, права которых могут быть нарушены, относится государство и его территориальные подразделения, общегосударственные интересы и интересы общества, частные и общественные организации, физические лица, как граждане России, так и иностранные граждане, лица без гражданства;

– в результате правонарушений в сфере информации могут пострадать неопределенное число субъектов (например, при распространении спама, недостоверной информации, информации, запрещенной к распространению) или возникнуть ситуация с неопределенным виновником правонарушения (например, при осуществлении несанкционированного доступа или распространении вирусов);

– сложность в определении времени и места совершения преступления и правонарушения в связи с совершением их в различных местах мира, за пределами России, во враждебных государствах и юрисдикциях, в том числе таких, где данные действия не являются правонарушением (например, реклама наркотиков в Нидерландах, распространение ложной информации про Великую Отечественную войну в странах Балтии, Польше и на Украине и т.д.);

– сложность в фиксации следов правонарушения и доказывания фактов совершения правонарушений в связи с оборотом документов в электронном виде (например, доказательства, полученные в сети Интернет на иностранных сайтах зачастую не принимаются судом) и необходимостью проведения компьютерной технической экспертизы только тех носителей информации, которые физически находятся у сотрудников правоохранительных органов (кроме того, компьютерная техническая экспертиза может проводиться несколько месяцев в связи с отсутствием необходимых специалистов);

– сложность расследования преступлений в информационной сфере в связи с большой латентностью, пренебрежением субъектами информационной безопасностью, неспособностью установить факт компьютерного преступления.

[25] Бачило И.Л. Информационное право: учебник. – 2-е изд. перераб. и доп. – М.: Юрайт, 2011. С. 472.

## 2.6. Административная ответственность за нарушения законодательства в сфере кибербезопасности

Большая часть норм административной ответственности в сфере информационной безопасности имеет бланкетный характер, отправляя правоприменителя к утвержденным подзаконными актами инструкциям и правилам. Эти нормативные правовые акты устанавливают порядок работы со средствами хранения, обработки или передачи информации ограниченного доступа, информационно-телекоммуникационными сетями и оконечным оборудованием[26].

*Классификация административной ответственности в сфере нарушения кибербезопасности осуществляется на основании разделения области действия угроз кибербезопасности.*

К первой категории правонарушений, нарушающих требования законодательства в области кибербезопасности, относятся **правонарушения в области связи и информатизации, повлекшие за собой угрозы кибербезопасности.** Их можно условно подразделить на три группы правонарушений:

1.1. *Нарушение правил создания и функционирования сетей связи*. К данной группе относятся действия, приводящие к правонарушениям, связанными с техническими вопросами:

– нарушение правил охраны линий или сооружений связи (ст. 13.5 КоАП РФ[27]);

– нарушение требований к использованию радиочастотного спектра, правил радиообмена или использования радиочастот, несоблюдение норм или параметров радиоизлучения (ст. 13.4 КоАП РФ).

К этой же группе отнесены и вопросы организации деятельности сетей:

– нарушение требований законодательства, регулирующих порядок проектирования, строительства и эксплуатации сетей и сооружений связи (ст. 13.7 КоАП РФ);

– нарушение требований централизованного управления сетью связи общего пользования, включая установку требований к устойчивости сети (ст. 13.42, 13.45 КоАП РФ) и спутниковых сетей связи, находящихся под юрисдикцией иностранных государств (ст. 13.47 КоАП РФ).

– правонарушения, связанные с неисполнением обязанностей по реализации требований к сетям и средствам связи, используемым для проведения мероприятий уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации (ст. 13.46 КоАП РФ).

---

[26] Жукова П.Н., Насонова В.А., Прокопенко А.Н. Основы информационной безопасности в ОВД: учебное пособие. – Белгород: Бел ЮИ МВД России имени И.Д. Путилина, 2015. – 72 с.

[27] Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // Российская газета. 2001. № 256.

1.2. *Нарушение правил и норм использования технических средств при эксплуатации сетей связи*. Данная группа правонарушений основана на угрозах кибербезопасности, связанных с изготовлением или использованием различных устройств без специального разрешения (ст. 13.3, 13.6, 13.8 КоАП РФ).

1.3. *Нарушение правил и норм эксплуатации технических средств при эксплуатации информационных систем.* К данной группе относятся:

– правонарушения, которые связаны с нарушением требований российского законодательства о размещении и функционировании технических средств, обеспечивающих работоспособность информационных систем на территории Российской Федерации (ст. 13.27.1 КоАП РФ);

– нарушения при использовании национальной системы доменных имен (ст. 13.44 КоАП РФ).

Ко второй категории правонарушений относятся **правонарушения, связанные с нарушением режима конфиденциальности информации.** К указанной категории также относятся три группы правонарушений:

2.1. *Правонарушения, направленные на нарушение конфиденциальности информации.* В указанную группу входят:

– нарушения законодательства Российской Федерации о порядке оборота информации ограниченного доступа, получении и разглашении информации с ограниченным доступом, в том числе в области персональных данных (ст. 13.11, 13.14, 13.41, 13.14.1 КоАП РФ);

– разглашение сведений о мерах безопасности (ст. 17.13 КоАП РФ).

2.2. *Правонарушения, направленные на нарушения правил организации кибербезопасности.* К данной группе относятся:

– правонарушения, связанные с игнорированием правил защиты информации (ст. 13.12 КоАП РФ);

– нарушения требований законодательства к установке технических средств противодействия известным угрозам безопасности информационно-телекоммуникационных сетей общего пользования (ст. 13.42 КоАП РФ);

– незаконная деятельность в области защиты информации (ст. 13.13 КоАП РФ);

– нарушения правил и норм в области создания и использования электронной подписи (ст. 13.33, 13.33.1 КоАП РФ).

2.3. *Правонарушения в области кибербезопасности в финансовой сфере*. В указанную группу включаются:

– ответственность за несоблюдение порядка сбора, хранения, защиты и обработки сведений, составляющих кредитную историю (ст. 14.30 КоАП РФ);

– нарушение требований законодательства, касающихся представления и раскрытия информации на финансовых рынках (ч. 5 ст. 15.19 КоАП РФ).

В третью категорию правонарушений включаются **правонарушения, связанные с нарушением правил представления, обработки и распространения информации в различных информационных системах**. В данную категорию входит две группы правонарушений:

3.1. *Правонарушения, связанные с несоблюдением установленных ограничений на распространение информации конкретного содержания (кроме информации ограниченного доступа)*. К ним относятся нарушения правил хранения, комплектования, учета или использования архивных документов, в том числе информации, содержащейся в информационных системах (ст. 13.20, 13.25 КоАП РФ).

3.2. *Нарушения кибербезопасности в области критической информационной инфраструктуры*. В них включаются правонарушения, дополнившие административный кодекс в 2021 году и перечисленные в ст. 13.12.1, 19.7.15 КоАП РФ.

Статистика правонарушений за последние годы показывает, что количество совершенных правонарушений в информационной сфере в целом и в области информационной безопасности в частности ежегодно увеличивается. При этом растет не только количество правонарушений в Российской Федерации, но и количество преступлений, причем не только в нашей стране, но и в мире в целом. Кроме того, идущая война между Россией и западным блоком стран привела к тому, что Российскому государству приходится кардинально менять систему правового регулирования организации информационной безопасности в стране. Принимаются новые правила и нормы, ужесточаются условия поведения иностранных компаний на российском рынке, меняется организация защиты информации.

В результате в области административного законодательства в Кодексе Российской Федерации об административных правонарушениях появились новые составы правонарушений, например в области обеспечения безопасности критической информационной инфраструктуры. Также внесены изменения в существующие составы административных правонарушений, например увеличены штрафы за обработку персональных данных с нарушениями законодательства, а также за несоблюдение правил в области обеспечения безопасности критической информационной инфраструктуры.

Особенностью административной ответственности за правонарушения в области законодательства об информации является также то, что использование информационно-телекоммуникационных сетей при совершении деяния может стать квалифицирующим признаком, влекущим более строгое наказание при привлечении к административной ответственности.

## 2.7. Уголовная ответственность за нарушения законодательства в сфере кибербезопасности

В соответствии со статьей 14 Уголовного кодекса Российской Федерации (далее – УК РФ)[28] преступлением признается виновно совершенное общественно опасное деяние, запрещенное УК РФ под угрозой наказания.

Статья 8 УК РФ установила, что основанием уголовной ответственности является совершение деяния, содержащего все признаки состава преступления, предусмотренного УК РФ.

УК РФ содержит значительное количество статей, в соответствии с которыми деяния, совершенные в сфере кибербезопасности, признаются уголовно наказуемыми.

Их можно разделить на три группы. **В первую группу включаются преступления, предусмотренные главой 28 «Преступления в сфере компьютерной информации», которые устанавливают ответственность непосредственно за компьютерные преступления.** Глава 28 включает 5 статей:

*статья 272* «Неправомерный доступ к компьютерной информации»;

*статья 273* «Создание, использование и распространение вредоносных компьютерных программ»;

*статья 274* «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей».

*статья 274.1* «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

*статья 274.2* «Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования» (введена Федеральным законом от 14.07.2022 № 260-ФЗ)[29].

В статьи 272, 273 и 274 УК РФ в 2011 году Федеральным законом от 07.12.2011 № 420-ФЗ[30] были внесены изменения, которые привели указанные статьи в соответствие с текущей реальностью и терминологией. Основным изменением, внесенным в статьи, необходимо признать замену понятия «компьютерной информации, как информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети» на понятие «*компьютерной информации*, как сведений (сообщений, данных), представленных в

[28] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

[29] Федеральный закон от 14.07.2022 № 260-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» // Российская газета. 2022. № 154-155.

[30] Федеральный закон от 07.12.2011 № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» // Российская газета. 2011. № 278.

форме электрических сигналов, независимо от средств их хранения, обработки и передачи». Новое определение закреплено в примечании к статье 272 УК РФ. Оно является более обширным, почти повторяет определение информации, закрепленное в статье 2 Закона, и не содержит практически не употребляемого термина электронно-вычислительная машина (ЭВМ).

Кроме того, существенная часть устройств, которые осуществляют обработку компьютерной информации, например, планшеты, мобильные телефоны и смартфоны, формально не относились к ЭВМ. Соответственно за неправомерный доступ к таким устройствам не наступала уголовная ответственность.

В части 3 статьи 272 УК РФ был указан дополнительный объект преступления – общественные отношения, обеспечивающие интересы службы.

В статье 273 УК РФ уголовная ответственность теперь предусмотрена не за создание программ для ЭВМ, а за создание, распространение или использование компьютерных программ. Причем данные компьютерные программы должны быть заведомо предназначены для противоправных действий: несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

В утвержденных Генпрокуратурой России «Методических рекомендациях по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации» под *компьютерной программой* понимается объективная форма представления совокупности данных и команд, предназначенных для функционирования компьютерного устройства с целью получения определенного результата[31].

Компьютерные программы, предназначенные для совершения противоправных действий, – это как компьютерные вирусы (например, троянские кони, черви, кейлоггеры, руткиты и др.), так и специально созданные программы для осуществления несанкционированного доступа.

В статье 274 УК РФ вместо «нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети» используется понятие «нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям». Таким образом, в статью добавлены новые предметы данного преступления – информационно-телекоммуникационные сети (в том числе Интернет) и оконечное оборудование.

Статьи 272 и 273 УК РФ дополнены частями 4 и 3 соответственно, в которых предусмотрен квалифицирующий признак состава преступления: наступление тяжких последствий или создание угрозы их наступления. В части 2 статьи 274 дополнен квалифицирующий признак состава преступления: создание угрозы их наступления.

---

[31] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации: утв. Генпрокуратурой России // СПС «КонсультантПлюс».

Под тяжкими последствиями необходимо понимать общие последствия, которые наступили или могли наступить в результате преступного деяния. К ним могут относиться нарушение деятельности предприятий и организаций, в том числе в сфере транспорта, связи, здравоохранения, энергетики, обороны и безопасности. В результате возможно наступление аварий или катастроф, а также причинение вреда здоровью и жизни людей. Кроме того, тяжким последствием могут быть причинение особо крупного материального ущерба, действия с привилегированной информацией особой ценности.

Очень важным является добавление такого квалифицирующего признака состава преступления, как *создание угрозы наступления тяжких последствий*. Это позволяет применить к преступнику максимальные санкции даже в случае предотвращения тяжких последствий.

Статья 274.1 введена Федеральным законом от 26.07.2017 № 194-ФЗ[32] после принятия новой Доктрины информационной безопасности России и одновременно с Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Статья 274.2 введена Федеральным законом от 14.07.2022 № 260-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации»[33] и связана с введением особого порядка установки, эксплуатации и модернизации технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования Интернет и сетей связи[34]. Указанные технические средства устанавливаются у всех провайдеров и операторов связи за счет государства и обеспечивают бесперебойную работу Интернет и связи. Именно за противодействие работе таких устройств установлена административная ответственность, а за неоднократное противодействие – уголовная ответственность.

---

[32] Федеральный закон от 26.07.2017 № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»» // Российская газета. 2017. № 167.

[33] Федеральный закон от 14.07.2022 № 260-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» // Официальный интернет-портал правовой информации [Электронный ресурс]. – Режим доступа: http://pravo.gov.ru 14.07.2022.

[34] Постановление Правительства Российской Федерации от 12.02.2020 № 126 (ред. от 28.05.2022) «Об установке, эксплуатации и о модернизации в сети связи оператора связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования» (вместе с «Правилами установки, эксплуатации и модернизации в сети связи оператора связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования») // Собрание законодательства Российской Федерации. 2020. № 8. Ст. 1001.

**Во вторую группу преступлений, совершенных в сфере кибербезопасности, включаются преступления, непосредственно имеющие отношение к объектам регулирования Закона. К ним относятся следующие преступления**:

*статьи 110–110.2* «Доведение до самоубийства посредством Интернет»;

*статья 140* «Отказ в предоставлении гражданину информации»;

*статьи 146–147* «Нарушение авторских, смежных, изобретательских и патентных прав»;

*статья 151.2* «Вовлечение несовершеннолетнего в совершение действий, представляющих опасность для его жизни посредством Интернета»;

*статья 159.3* «Мошенничество с использованием электронных средств платежа»;

*статья 159.6* «Мошенничество в сфере компьютерной информации»;

*статья 171.2* «Незаконные организация и проведение азартных игр через Интернет»;

*статья 183* «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»;

*статья 207* «Заведомо ложное сообщение об акте терроризма, в том числе посредством информационно-телекоммуникационных сетей»;

*статьи 242–242.2* «Незаконные изготовление и оборот порнографических материалов или предметов посредством Интернета»;

*статья 282* «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства»;

*статьи 282.1–282.3* «Организация и финансирование экстремистской деятельности, в том числе посредством информационно-телекоммуникационных сетей»;

*статьи 283–284* «Нарушение законодательства о государственной тайне».

**В третью группу включаются более 50 преступлений, которые опосредованно связанны со сферой кибербезопасности.** Они предусматривают уголовную ответственность за деяния, связанные:

– с искажением информации (например, клевета – ст. 129, фальсификация избирательных документов, документов референдума – ст. 142);

– с неправомерным обращением с информацией (например, неправомерное использование инсайдерской информации – ст. 185.6, разглашение данных предварительного расследования – ст. 310);

– с отказом в предоставлении информации или ее сокрытием (например, отказ в предоставлении информации Федеральному Собранию Российской Федерации или Счетной палате Российской Федерации – ст. 287, сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей – ст. 237).

## Вопросы для самоконтроля:

1. Какие уровни включает в себя правовая защита информации?
2. Какие положения по вопросам информационной безопасности включает Конституция Российской Федерации?
3. Что закрепляет Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности»?
4. Дайте краткую характеристику Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
5. Какие федеральные законы имеют отношение к правовому обеспечению информационной безопасности?
6. Какой правовой режим устанавливает Трудовой кодекс Российской Федерации в области защиты информации?
7. Какими статьями КоАП РФ определяется административная ответственность за правонарушения в области связи и информации?
8. Какие отношения регулирует Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации»?
9. Какой запрет устанавливает Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»?
10. Какие уровни входят в состав политики безопасности?
11. Как можно классифицировать специализированные политики безопасности с учетом особенностей применения?
12. На какие виды делятся угрозы информационной безопасности Российской Федерации?

# ГЛАВА 3.
# ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

## 3.1. Основные принципы и меры защиты информации

**Основные принципы защиты информации:**

1. *Законность* – меры безопасности должны соответствовать требованиям законодательства, технических стандартов, руководящих и нормативно-методических документов в информационной сфере.

2. *Системность* предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности информации.

3. *Комплексность*. Защита должна состоять из правовых, морально-этических, организационных, технологических, физических и технических мер защиты.

4. *Своевременность* предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач и реализацию мер обеспечения безопасности информации на стадии разработки АИС.

5. *Непрерывность*. Защита должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах эксплуатации АИС, в том числе при проведении ремонтных и профилактических работ.

6. *Разумная достаточность*. Стоимость средств защиты информации (далее – СЗИ) не должна превышать стоимость защищаемых информационных активов.

7. *Эффективность и целесообразность*. СЗИ в АИС не должны нарушать функции системных и прикладных средств обработки информации, а также замедлять бизнес-процессы свыше допустимых норм.

8. *Разграничение доступа и минимизация полномочий*. Права доступа к ИР и ПТС каждому субъекту доступа назначаются строго в соответствии с решаемыми задачами.

9. *Персональная ответственность* предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого сотрудника в пределах его полномочий.

10. *Надежность и простота применения средств защиты*. В АИС должны быть предусмотрены средства, обеспечивающие контроль работоспособности и заданной функциональности самих средств защиты информации.

11. *Гибкость системы защиты*. Внешние условия и требования с течением времени меняются. Гибкость системы защиты избавляет владельцев АИС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.

12. *Обязательность контроля* предполагает выявление и пресечение попыток нарушения установленных правил обеспечения безопасности информации на основе используемых систем и средств защиты информации.

**По способам осуществления все меры защиты информации, ее носителей и систем ее обработки подразделяются:**

- на правовые (законодательные);
- морально-этические;
- организационные (административные и процедурные);
- технологические;
- физические;
- технические (аппаратурные и программные).

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

К **морально-этическим мерам защиты** относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и оформленные в некоторый свод (устав, кодекс чести и т.п.) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах пользователей и обслуживающего персонала АИС.

*Правовые и морально-этические меры определяют правила обращения с информацией и ответственность субъектов информационных отношений за их соблюдение*.

**Организационные меры защиты** – это меры административного и процедурного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей и обслуживающего персонала с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

К **технологическим мерам защиты** относятся разного рода технологические решения и приемы, основанные обычно на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

*Организационные и технологические меры защиты – это единственное, что остается, когда другие методы и средства защиты отсутствуют или не могут обеспечить требуемый уровень безопасности*.

Организационные меры необходимы для обеспечения эффективного применения других мер и средств защиты в части, касающейся регламентации действий людей. В то же время организационные меры необходимо поддерживать более надежными физическими и техническими средствами.

**Физические меры защиты** основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также средств визуального наблюдения, связи и охранной сигнализации. К данному типу относятся также меры и средства контроля физической целостности компонентов АИС (пломбы, наклейки и т.п.).

**Технические меры защиты** основаны на использовании различных электронных устройств и специальных программ, входящих в состав АС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты.

*Физические и технические меры защиты призваны устранить недостатки организационных мер и в максимальной степени исключить возможность неумышленных (по ошибке или халатности) нарушений регламента со стороны персонала и пользователей АИС*.

## 3.2. Организационные меры защиты информации

*Организационные меры защиты информации* – это деятельность по регламентации действий сотрудников организации, направленная на обеспечение информационной безопасности.

Необходимо подчеркнуть, что регламентации подлежит не только деятельность, непосредственно связанная с созданием или использованием информационных ресурсов, но и действия, так или иначе затрагивающие поддерживающую инфраструктуру либо обслуживающий персонал.

***Организационная защита информации*** *– это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что несанкционированный доступ к конфиденциальной и секретной информации становится невозможным или существенно затрудняется за счет проведения организационных мероприятий*.

Основой организационных мер защиты является политика информационной безопасности организации.

*Политика информационной безопасности организации* – это документальное оформление правил поведения, процедур, практических приемов или руководящих принципов в отношении защиты данных, которыми руководствуется организация в своей деятельности (см. рис. 11).


*Рисунок 11. Политика информационной безопасности организации*

*Вопросы, регулируемые политикой информационной безопасности организации:*

– управление доступом;
– категорирование и обработка информации;
– физическая безопасность и защита от воздействия окружающей среды;
– ограничения пользователя (доступ к активам; требование «чистого» стола и экрана; предоставление информации; мобильные устройства и дистанционная работа; ограничения на установку и использование ПО);
– резервное копирование;
– порядок информационного обмена;
– защита от вредоносных программ;
– управление техническими уязвимостями;
– применение криптозащиты;
– коммуникационная безопасность;
– конфиденциальность и защита персональных данных;
– профилактика и обслуживание ПТС;
– информационные взаимоотношения с партнерами и т.п.

Политика информационной безопасности доводится до сведения всех работников организации и причастных внешних сторон в актуальной, доступной и понятной форме, например в рамках периодических мероприятий по информированию, обучению и практических тренингах.

*К организационным мероприятиям относятся*:

– мероприятия, осуществляющиеся при проектировании, строительстве и оборудовании служебных и производственных зданий и помещений, исключающих возможность тайного проникновения на территорию и в помещения;
– мероприятия для обеспечения удобства контроля прохода и перемещения людей, проезда транспорта и других средств передвижения;

– мероприятия по созданию отдельных производственных зон по типу конфиденциальности работ с самостоятельными системами доступа и т.п.;

– мероприятия, осуществляющиеся при подборе персонала, включающие ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;

– организацию и поддержание надежного пропускного режима и контроля посетителей;

– организацию надежной охраны помещений и территории.

Организационный элемент системы защиты информации содержит меры управленческого, ограничительного (режимного) и технологического характера, определяющие основы и содержание системы защиты, побуждающие персонал соблюдать правила защиты конфиденциальной информации фирмы. Указанные меры связаны с установлением режима конфиденциальности и определяют:

– формирование и организацию деятельности службы безопасности и службы конфиденциальной документации, обеспечение деятельности сотрудника нормативно-методическими документами по организации и технологии защиты информации;

– организацию составления и регулярного обновления защищаемой информации организации, составления и ведения перечня защищаемых бумажных и электронных документов;

– разрешительную систему разграничения доступа персонала к защищаемой информации;

– методы отбора персонала для работы с защищаемой информацией, методику обучения и инструктирования работников;

– направления и методы воспитательной работы с персоналом, контроль соблюдения работниками порядка защиты информации;

– технологию защиты, обработки и хранения бумажных и электронных документов;

– регламентацию внемашинной технологии защиты электронных документов;

– порядок защиты ценной информации от случайных или умышленных несанкционированных действий персонала;

– порядок защиты информации при проведении совещаний, заседаний, проведении переговоров, приеме посетителей;

– оборудование и аттестацию помещений и рабочих зон, выделенных для работы с ценной информацией, лицензирование технических систем и средств защиты информации и охраны, сертификацию информационных систем, предназначенных для обработки защищаемой информации;

– регламентацию пропускного режима на территории, в здании и помещениях, идентификации персонала и посетителей;

– систему охраны территории, здания, помещений, оборудования, транспорта и персонала организации;

– организационные вопросы приобретения, установки и эксплуатации технических средств защиты информации и охраны;

– организационные вопросы защиты персональных компьютеров, информационных систем, локальных сетей;

– действия службы безопасности и персонала в экстремальных ситуациях;

– регламентацию работы по управлению системой защиты информации;

– критерии и порядок проведения оценочных мероприятий по установлению степени эффективности системы защиты информации.

Структура системы защиты охватывает не только электронные информационные системы, а весь управленческий комплекс организации.

При формировании системы безопасности необходимо четко определить задачи, которые перед ней стоят (см. рис. 12).

Для решения этих задач используется комплекс мероприятий, в число которых входит система организационных мер.

**Система организационных мер по защите информации представляет собой комплекс мероприятий, включающих четыре основных компонента:**

– изучение обстановки на объекте;

– разработку программы защиты;

– деятельность по реализации указанной программы;

– контроль за ее действенностью и выполнением установленных правил.

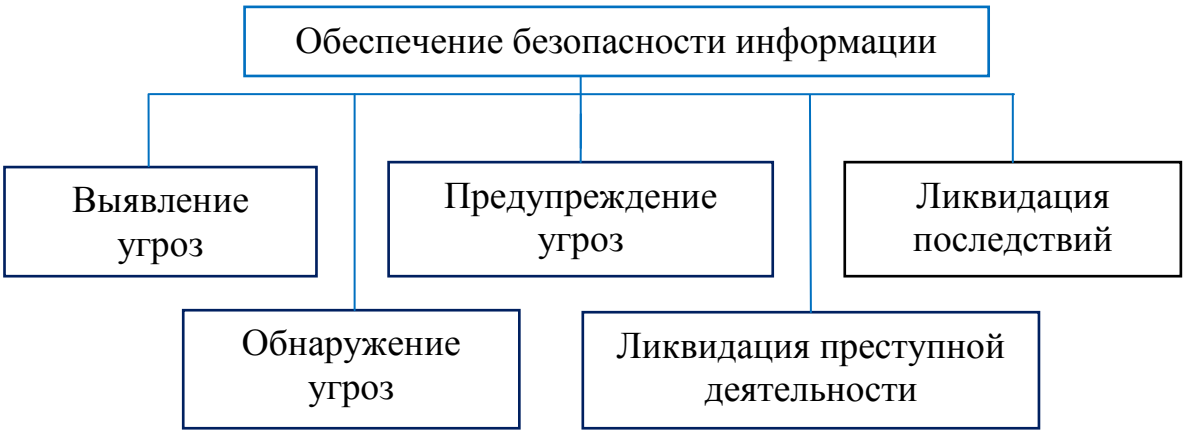


*Рисунок 12. Задачи обеспечения безопасности информации*

*К числу рассматриваемых подсистем организационного плана по защите информации можно отнести следующие мероприятия*:

– ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.;

– организация надежной охраны помещений и территории прохождения линии связи;

– организация, хранение и использование документов и носителей конфиденциальной информации, включая порядок учета, выдачи, исполнения и возвращения;

– создание штатных организационных структур по защите ценной информации или назначение ответственного за защиту информации на конкретных этапах ее обработки и передачи;

– создание порядка взаимоотношений со сторонними организациями;

– организация секретного делопроизводства.

Такой компонент, как разграничение доступа к информации задается одним из важных элементов системы комплексной защиты информации. В основе ее построения лежит положение о том, что каждый из членов коллектива должен обладать только теми сведениями, которые необходимы ему в силу выполняемых обязанностей. В этом случае только руководитель имеет доступ ко всем материалам, независимо от их важности.

Качественная разработка и строгое соблюдение указанных правил – достаточно действенная мера, направленная на то, чтобы привести к минимуму риск утраты наиболее важной информации и определить объем похищенных сведений. При детализации указанных правил предполагается выделение следующих основных позиций:

– права, обязанности и ответственность сотрудников и руководителей по доступу и виды разрешений на доступ к конкретной информации, узлам ее хранения, обработки и передачи по сети;

– порядок доступа к конфиденциальным сведениям представителей государственных структур;

– рассылка носителей информации в другие точки и обмен ими между подразделениями организаций.

*Для минимизации рисков, связанных с несанкционированным доступом в организации или в его отдельных подразделениях, может использоваться метод создания рубежей защиты.*

Это подразумевает, что территория организации разбивается на несколько зон, ранжированных по степени закрытости для сотрудников или посетителей. В результате возникает возможность для разграничения доступа к наиболее важным информационным ресурсам. Тем самым обеспечивается их максимальная защита. Пример организации рубежей защиты приведен на рисунке 13.

Исходя из всего вышесказанного, приходим к выводу, что необходимо четкое разграничение прав доступа различных лиц к информации на различных этапах ее обработки и передачи.

Элемент организационной защиты является стержнем, основной частью рассматриваемой комплексной системы. Меры по организационной защите информации составляют 50–60% в структуре большинства систем защиты информации. Это связано с тем, что важной составной частью организационной защиты информации является подбор, расстановка и обучение персонала, который будет реализовывать на практике систему защиты информации.


*Рисунок 13. Схема рубежей защиты*

Организационные меры защиты отражаются в нормативно-методических документах организации.

В этой связи часто используется единое название двух рассмотренных выше элементов системы защиты – элемент организационно-правовой защиты информации.

Этот элемент является основным в системе защиты информации. Другие элементы носят дополнительный, усиливающий характер, но автономно использоваться не могут.

## 3.3. Основы построения системы кибербезопасности

Независимо от способа кодирования и обработки информационные активы должны быть идентифицированы и надежно защищены. Кибербезопасность достигается путем реализации комплекса мер, определяемых в процессе менеджмента рисков и обеспечивающих их снижение до приемлемого уровня. При этом меры, охватывающие политику, процедуры, организационные струк-

туры, техническое обеспечение не должны негативно влиять на бизнес-процессы.

*Система кибербезопасности* – совокупность объектов защиты информации (далее – ЗИ), организационно-штатной структуры, методов и средств, обеспечивающих функции ЗИ в соответствии с установленными правилами и нормами.

**Типовые меры защиты информации:**

- идентификация и аутентификация субъектов и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- обеспечение целостности ПО;
- обеспечение доступности информации;
- защита среды виртуализации и технических средств;
- защита АИС при взаимодействии с внешними АИС и сетями;
- реагирование на киберинциденты.

*Контрмеры против угроз кибербезопасности должны быть направлены:*

- на совершенствование компетентности подготовки персонала;
- политику организации и применяемые практические рекомендации;
- информационные технологии.

При доступе в АИС должна осуществляться идентификация и аутентификация пользователей, являющихся работниками оператора (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

*Доступ к ИР* – возможность получения информации, ее использования или блокирования.

*Доступ к ПТС АИС* – возможность воздействия на ПТС с целью управления, изменения или отключения функций.

*Правила разграничения доступа (далее – ПРД)* устанавливаются обладателем информации или оператором АИС в соответствии с политикой информационной безопасности и регламентируют порядок доступа субъектов доступа к объектам доступа.

*Субъект доступа* – физическое лицо или информационный процесс, действия которого регламентируются ПРД.

*Объект доступа* – единица ИР, доступ к которой регламентируется ПРД.

*Физический доступ* – непосредственный доступ к объекту доступа (включая место расположения), позволяющий осуществить физическое воздействие на него. Физический доступ нарушителя к ПТС АИС или к внутренней сети – наиболее результативный путь обхода СЗИ (например, загрузка операционной системы с флэшки или несанкционированное подключение к корпоративной сети).

*Логический доступ* – локальный программный доступ к ИР или удаленный по сети, позволяющий ознакомиться или воздействовать на данные ресурсы. *Дискреционный принцип контроля доступа* – контроль доступа именованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам памяти и т.д.). Для каждой пары субъект-объект в ПРД должно быть задано явное и недвусмысленное перечисление допустимых операций, т.е. тех типов доступа, которые являются санкционированными для данного субъекта к данному ИР (объекту) (см. рис. 14).

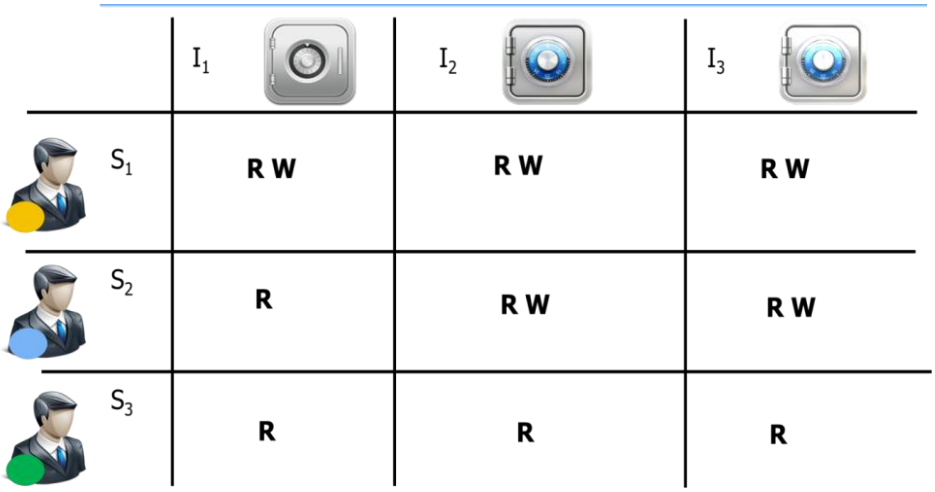


*Рисунок 14. Матрица доступа субъектов S1, S2, S3 к объектам доступа I1, I2, I3*

*Мандатный принцип контроля доступа* – контроль доступа осуществляется путем сопоставления классификационных меток, присваиваемых каждому субъекту и каждому объекту (см. рис. 15).

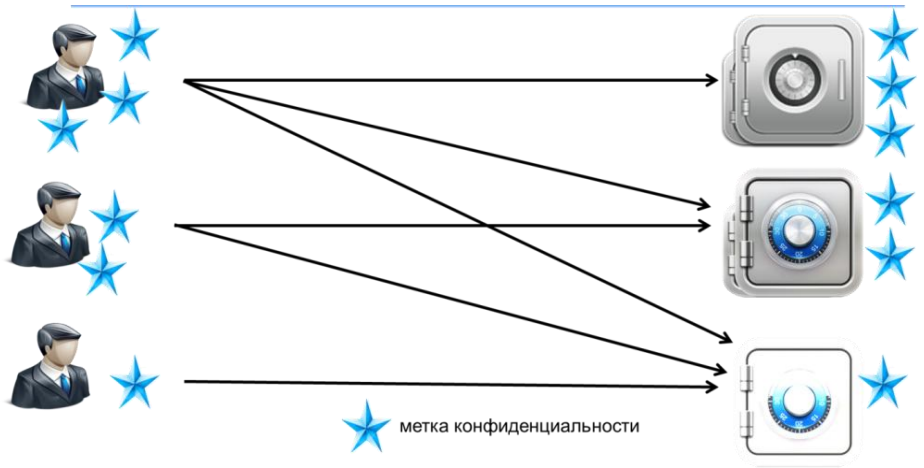


*Рисунок 15. Уровневое разграничение доступа с присвоением мандатных меток*

Посредством этих меток субъекты и объекты распределяются по иерархическим уровням доступа.

*Учетная запись (account)* – сведения, представляющие субъекта доступа в конкретной АИС, включающие логическое имя (логин) и пароль доступа, персональные данные, иную учетную информацию.

*Авторизация (санкционирование доступа)* – проверка и подтверждение прав субъекта доступа с целью предоставления (или отказа) в доступе к ИР. *Принцип необходимого знания* – концепция безопасности, ограничивающая доступ к информации и ресурсам АИС в объеме, необходимом и достаточном для выполнения должностных обязанностей.

*Идентификация* – действия по присвоению субъектам и объектам доступа идентификаторов и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов доступа.

*Идентификатор (доступа)* – признак субъекта (объекта) доступа, как правило в виде последовательности знаков, который однозначно определяет соотнесенную с ними информацию при идентификации.

Идентификация устройств в АИС обеспечивается по логическим именам (NETBIOS, DNS-имя и/или ID), логическим адресам (IP-адресам) и/или по физическим адресам (MAC-адресам, IMEI, SSID) устройства или по комбинации имени, логического и (или) физического адресов устройства.

*Аутентификация* – действия по проверке подлинности субъекта (объекта) доступа, а также по проверке принадлежности субъекту (объекту) доступа предъявленного идентификатора доступа.

*Простая аутентификация* – аутентификация с применением метода однофакторной односторонней аутентификации и соответствующих данному методу протоколов аутентификации.

*Пароль* – конфиденциальная аутентификационная информация субъекта доступа, обычно состоящая из последовательности знаков.

*Многофакторная аутентификация* – аутентификация, при выполнении которой используется не менее двух различных факторов аутентификации. *Фактор* – форма представления информации, используемой при идентификации и аутентификации.

*Биометрические персональные данные* – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

*Биометрическая аутентификация (идентификация)* – аутентификация пользователя (одновременно с идентификацией), осуществляемая путем проверки предъявленного биометрического образа (идентификатора).

*Виды биометрической аутентификации*:

– статический метод аутентификации распознает постоянные физические параметры человека, которыми он обладает с рождения (отпечатки пальцев, отличительные характеристики радужной оболочки глаза, рисунок глазной сетчатки, термограмма, геометрия лица, геометрия кисти руки и даже фрагмент генетического кода);

– динамический метод анализирует характерные признаки пользователя, которые демонстрируются в момент выполнения какого-либо действия (подпись, клавиатурный почерк, голос и другое).

*Взаимная аутентификация* – обоюдная аутентификация, обеспечивающая и субъекту и объекту доступа уверенность в том, что другой участник процесса аутентификации является тем, за кого себя выдает.

*Строгая аутентификация* – аутентификация с применением только метода многофакторной взаимной аутентификации и использованием криптографических протоколов аутентификации.

*Верификация* – процесс проверки подлинности информации путем сопоставления предоставленной информации с доверенной ранее подтвержденной информацией.

*Меры управления доступом* включают:

– управление (создание, активация, назначение прав доступа, блокирование и уничтожение) учетными записями пользователей;

– реализация необходимых методов управления доступом (дискреционный, мандатный, ролевой), прав и правил разграничения доступа (чтение, запись, выполнение);

– управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между компонентами АИС, а также между АИС;

– разделение полномочий (ролей) и назначение минимально необходимых прав и привилегий пользователям, администраторам и техническому персоналу АИС;

– ограничение неуспешных попыток авторизации при входе в АИС;

– ограничение числа параллельных сеансов работы в АИС для каждой учетной записи;

– блокирование сеанса работы в АИС после установленного времени бездействия (неактивности) пользователя или по его запросу;

– реализация возможности защищенного доступа субъектов доступа к объектам доступа через внешние сети;

– регламентация и контроль использования в АИС технологий беспроводного доступа;

– регламентация и контроль использования в АИС мобильных технических средств;

– управление взаимодействием с внешними АИС сторонних организаций;

– исключение НСД к ИР и ПТС на этапе их загрузки (обеспечение доверенной загрузки).

*Меры ограничения программной среды* включают:

– управление запуском (запросами) компонентов ПО (файлов, объектов баз данных, библиотечных процедур и т.п.);

– управление установкой и настройкой параметров доверенных компонентов ПО;

– блокирование установки компонентов не доверенного ПО;

– управление временными файлами (запрет запуска, удаление).

*Защита машинных носителей информации (далее – МНИ)* включает:

– учет МНИ;

– управление доступом к МНИ;

– контроль несанкционированного использования МНИ вне АИС;

– контроль перемещения МНИ за пределы контролируемой зоны;

– контроль использования интерфейсов подключения МНИ;

– контроль ввода-вывода информации на МНИ;

– контроль подключения МНИ;

– гарантирование стирание информации при их передаче МНИ для использования по другому назначению, ремонта или утилизации.

*Регистрация событий безопасности (далее – СБ)* включает:

– определение перечня СБ, подлежащих регистрации;

– определение состава и содержания информации о СБ, подлежащих регистрации, и сроков ее хранения;

– генерирование временных меток и/или синхронизация системного времени в АИС;

– сбор, запись и сохранение информации о СБ;

– мониторинг результатов регистрации СБ и реагирование на них;

– реагирование на сбои и технические ошибки при регистрации СБ;

– защиту информации о СБ;

– обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в АИС.

*Антивирусная защита (далее – АВЗ)* должна предусматривать:

– установку конфигурирование и управление средствами АВЗ на автоматизированных рабочих местах, серверах, средствах защиты информации (межсетевых экранах, прокси-серверах, почтовых шлюзах), ноутбуках и мобильных коммуникаторах, иных устройствах доступа к ИР и ПТС АИС, подверженных заражению вирусами через съемные МНИ или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб-сайты и другие сетевые сервисы);

– предоставление доступа средствам АВЗ к защищаемым объектам;

– проведение ситуационных и периодических проверок ПТС на наличие вирусов;

– проверку в реальном времени файлов из внешних источников при загрузке, открытии или запуске на выполнение (с МНИ, из сети);

– оперативное оповещение администраторов безопасности об обнаружении вирусов или вирусной активности выполняемых программ;

– выполнение установленных действий с подозрительными или зараженными объектами;

– централизованное управление средствами АВЗ (установка, удаление, обновление, конфигурирование и контроль актуальности версий ПО);

– контроль целостности антивирусного ПО и антивирусной базы.

*Вторжениями в АИС (компьютерными атаками)* являются действия, направленные на получение НСД в целях добывания, уничтожения, искажения,

блокирования защищаемой информации или неправомерного воздействия на ПТС АИС и сети.

*Меры обнаружения (предотвращения) вторжений* включают регистрацию всех СБ, распознавание компьютерных атак в реальном времени на внешней границе АС и/или на внутренних сетевых узлах, оповещение и реагирование на вторжение. Анализ СБ осуществляется с помощью базы данных о характерных признаках компьютерных атак и правил принятия решения.

*Меры контроля (анализа) защищенности информации* включают:

– выявление, анализ и устранение уязвимостей АИС;

– контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ;

– контроль обновления ПО из доверенных источников;

– контроль конфигурации ПТС, сети и СЗИ;

– контроль установленных прав и правил разграничения доступа, создания и удаления учетных записей, привилегий пользователей, генерации и смены паролей доступа.

*Меры контроля целостности ПО* включают:

– контроль целостности компонентов ПО, обеспечивающего функциональность АИС, средств разработки и отладки программ по идентификаторам и/или по контрольным суммам компонентов в процессе загрузки и/или в процессе функционирования АИС;

– контроль целостности ПО СЗИ;

– периодическое тестирование ПО на функциональность и попытки НСД;

– обеспечение физической защиты ПТС.

*Меры обеспечения доступности информации* включают:

– использование отказоустойчивых технических средств;

– резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования АИС;

– контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование;

– периодическое резервирование информации в удаленные хранилища или на съемные МНИ;

– обеспечение возможности восстановления информации с резервных копий в течение установленного временного интервала;

– сегментирование и кластеризацию ПТС АИС.

*Меры по защите среды виртуализации* должны исключать НСД и несанкционированное воздействие на виртуальную инфраструктуру.

*Меры по защите технических средств* включают:

– ЗИ от утечки по техническим каналам;

– оборудование контролируемой зоны и управление физическим доступом в помещения, к техническим средствам АИС, СЗИ, средствам обеспечивающей инфраструктуры;

– защиту от внешних техногенных и стихийных воздействий (сбои систем электроснабжения, охлаждения, возгорания, ураганы, наводнения, землетрясения и т.п.).

*Меры по защите АИС* при взаимодействии с внешними АИС и сетями передачи данных включают:

– обеспечение выполнения процессов с высоким приоритетом;

– разделение функций по обработке информации в бизнес-процессах, по администрированию АИС, по администрированию СЗИ, по профилактике и техобслуживанию;

– защиту от раскрытия, модификации и навязывания (ввода ложной информации) при передаче информации за пределы контролируемой зоны, в том числе по беспроводным каналам связи;

– контроль и оповещение пользователей АИС при активации компонентов инженерно-технических средств и систем, способных создать технический канал утечки информации;

– формирование, передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене с другими АИС;

– контроль санкционированного и исключение несанкционированного использования технологий мобильной связи, аудио-, видеотрансляции и т.п.;

– обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе защиту от подмены сетевых устройств и сервисов;

– документальную фиксацию всех фактов информационного взаимодействия между пользователями АИС по сети и иным разрешенным каналам связи;

– защиту данных, конфигурации ПО и параметров настройки СЗИ от несанкционированных изменений;

– выявление, анализ и блокирование скрытых каналов передачи информации и удаленного доступа к ИР и ПТС в обход реализованных мер ЗИ;

– изоляция подозрительных процессов (выполнение программ) в выделенной области памяти;

– защиту беспроводных соединений и мобильных коммуникаторов;

– исключение доступа одного пользователя к информации о действиях предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие ресурсы;

– защиту от сетевых DDoS-атак;

– разрыв канальных соединений по их завершении или по истечении заданного времени неактивности;

– изменение конфигурации АИС и сетей на безопасную в случае отказов (сбоев) в СЗИ.

*Менеджмент инцидентов информационной безопасности* должен обеспечивать непрерывный мониторинг, анализ, обнаружение, идентификацию и предупреждение инцидентов ИБ, а также расследование, устранение последствий и минимизацию ущерба.

В процессе разработки и принятия мер обеспечения кибербезопасности важно также соблюдать еще один принцип – *экономической целесообразности,* суть которого заключается в минимизации материальных затрат за счет сбалансированного применения всех видов ЗИ.

## 3.4. Защита автоматизированных информационных систем от кибератак

Параллельно с расширением диапазона методов и средств проведения кибератак на АИС непрерывно совершенствуются технологии защиты информационных активов. **Для обеспечения информационной безопасности используется специализированное ПО, функционально ориентированное по направлениям защиты. К нему относится**:

– защита от нежелательного контента (антивирус, антиспам, веб-фильтры, анти-шпионы);

– межсетевые экраны и системы обнаружения вторжений;

– управление учетными данными;

– управление привилегированным доступом и управление привилегированными пользователями;

– защита от DDoS-атак;

– защита веб-приложений;

– анализ исходного кода;

– обнаружение мошеннических транзакций, предотвращение мошенничества и анализ мошенничества;

– защита от таргетированных атак;

– управление событиями безопасности;

– системы обнаружения аномального поведения пользователей;

– защита от утечек данных;

– криптографическая защита;

– защита мобильных устройств;

– резервное копирование;

– повышения отказоустойчивости и т.д.

*На рынке производителей ПО при разработке мер обеспечения информационной безопасности АИС и сетей в настоящее время прослеживаются две тенденции*:

– интеграция базовых средств защиты с операционными платформами штатных ПТС;

– создание универсальных программно-аппаратных комплексов защиты АИС с централизованным управлением.

*В соответствии с указанными тенденциями возникли следующие актуальные проблемы в области программно-технической защиты АИС*:

– выполнение сложных задач разбора и анализа инцидентов в условиях нехватки квалифицированных кадров;

– отсутствие программной совместимости и централизованного управления программных СЗИ различного назначения;

– отсутствие единой консоли мониторинга, поддержки и принятия решений по инцидентам ИБ;

– несоответствие СЗИ АИС действующему законодательству и невыполнение требований регулирующих органов.

Для решения данных проблем в настоящее время внедряются интегрированные системы защиты от разнонаправленных угроз информационной безопасности.

**Защита от кибератак данных при их обработке**

У каждой организации есть информационные активы, которые представляют интерес для злоумышленников. Это могут быть базы клиентов, ноу-хау бизнес-процессов, служебная документация, отчеты о деятельности и т.п.

*DLP-система (Data Leakage/Loss Prevention)* – специализированное ПО, предназначенное для предотвращения *утечек* информации и защиты АИС от *потери* данных в результате несанкционированных действий внутренних или внешних нарушителей.

Современные DLP-системы охватывают широкий круг задач по предотвращению внутренних угроз – от перекрытия потенциальных каналов НСД до повседневного наблюдения за работой пользователей АИС, т.к. любой сотрудник организации может стать инсайдером и преднамеренно или случайно создать угрозу ИБ.

*Главный принцип DLP* – максимальный автоматизированный контроль взаимодействия субъектов и объектов доступа внутри АИС и с внешней средой в соответствии с настраиваемыми логическими правилами и алгоритмами реагирования на инциденты кибербезопасности. DLP-система отслеживает не только активность программ на компьютере, но и любые действия пользователей с информацией – ввод данных с клавиатуры, электронный документооборот, электронную почту, обмен сообщениями в соцсетях и мессенджерах, активность на сайтах и даже время простоя.

Примером отечественной DLP-системы является специальный модуль *Kaspersky Security для Microsoft Exchange Servers*, который автоматически анализирует трафик на наличие конфиденциальных данных или данных с заданными характеристиками, к примеру, данных банковских карт, финансовых или персональных данных сотрудников организации. На основании правил, связывающих категории данных DLP и политики DLP, принимается решение о нарушении информационной безопасности АИС, блокировании информационного процесса и внесении в базу данных записи об инциденте. Настройка категорий и политик, а также обработка инцидентов выполняется пользователем, которому назначена роль специалиста по ИБ.

Среди зарубежных DLP-систем на российском рынке хорошо зарекомендовала себя Symantec Data Loss Prevention, которая является частью системы безопасности Endpoint Protection и сочетает в себе механизмы сравнения активности в системе с рисками безопасности данных на серверах, автоматизированных рабочих местах, мобильных устройствах и в облачных хранилищах. При

установке определяются все местоположения конфиденциальных данных, и пользователь получает возможность перенести их на центральный сервер управления или защитить на месте.

**Защита от кибератак данных при информационном обмене**

Автоматизированные рабочие места пользователей по-прежнему остаются основной мишенью злоумышленников при проведении многоходовых кибератак. ***Чтобы перекрыть злоумышленникам канал проникновения в инфраструктуру АИС через конечные устройства, разработаны специальные EDR-системы, которые раскрывают специалистам ИБ полную картину активности рабочих мест и серверов в инфраструктуре АИС и обеспечивают эффективную защиту от сложных угроз и APT-атак.***

*EDR (Endpoint Detection and Response)* – программные продукты для обнаружения и изучения вредоносной активности на конечных устройствах сети (серверах, рабочих станциях, устройствах IoT, терминалах и др.) (см. рис. 16).

Технология EDR в дополнение к антивирусному ПО выполняет проактивное обнаружение угроз (threat hunting), анализируя сигнатуры, атипичное поведение и подозрительную программную активность в конечных точках сети (рабочих станциях, серверах, исполнительных устройствах IoT и др.). EDR-архитектура состоит из программ-агентов на конечных точках и сервисного ПО.


*Рисунок 16. Задачи EDR-систем*

*Функции EDR-продуктов:*

– сбор данных с конечных точек в режиме реального времени;

– ведение журналов с записями о действиях пользователей, сетевой активности и запущенных программах;

– выявление подозрительной активности и нетипичного поведения, в том числе методами проактивного поиска угроз безопасности;

– классификация инцидентов ИБ и уведомление службы безопасности;

– временная блокировка доступа или удаление подозрительных файлов, остановка потенциально опасных процессов, разрыв сетевых соединений;

– интеграция с антивирусами, SIEM-системами и другими средствами защиты данных.

Информация EDR-агентов о сетевых коммуникациях, запущенных процессах, действиях пользователей в конечных точках передается на сетевой сервер в режиме реального времени.

**Защищенность АИС от сетевых атак позволяют повысить IDS/IPS-системы.**

*IDS (Intrusion Detection Systems)* – система обнаружения вторжений, предназначенная для регистрации подозрительных действий в АИС и уведомления о них ответственного за ИБ лица путем передачи сообщения на консоль управления, отправки электронного письма, SMS-сообщения на мобильный телефон и т.п.

*IPS (Intrusion Prevention Systems)* – система предотвращения вторжений, предназначенная для блокировки атак или подозрительных действий в АИС. Классическая IDS состоит из сенсоров, которые просматривают сетевой трафик, журналы событий и отчеты анализаторов трафика.

*В зависимости от места расположения IDS делятся*:

– на сетевые (network-based IDS, NIDS): отслеживают весь сетевой трафик сегмента;

– хостовые (host-based, HIDS): отслеживают входящий/исходящий трафик компьютера.

*Хост* – сетевой компьютер, предоставляющий услуги по запросу в режиме «клиент-сервер». Каждая сервисная программа хоста при запуске сообщает операционной системе, что готова получать и обрабатывать данные, адресованные на определенный порт.

**Детективные методы обнаружения атак:**

*Сигнатурные IDS* – подобно антивирусному ПО отслеживают критические цифровые шаблоны в трафике или в «снимке» состояния АИС. Вектор состояния, которым оперирует IDS, задается набором датчиков, характеризующих информационные процессы в АИС, и любое изменение в работе системы (запуск программного обеспечения, ввод данных, взаимодействие приложений между собой и т.д.) приводит к изменению данного показателя.

*Поведенческие IDS* – отслеживают нештатное поведение системы. Перед началом работы поведенческой СОВ происходит этап обучения нормальному функционированию АИС, и все последующие отклонения воспринимаются как атаки.

*Эвристические IDS*, принимающие решение на основе логических правил, например логического следования «ЕСЛИ (событие), ТО (действие)». Эвристические IDS можно классифицировать как экспертные системы с элементами искусственного интеллекта. Логические выводы по анализируемым данным де-

лаются на основе правил из базы знаний. Например: «ЕСЛИ пользователь administrator авторизовался в System1 И сделал изменение в File2, ЗАТЕМ запустил «Утилиту3», ТОГДА отправить уведомление о нарушении безопасности».

Но в ряде случаев IDS не успевает своевременно среагировать на кибератаку, и тогда прогнозировании и предотвращение вредоносной активности на ранней стадии осуществляется с помощью IPS.

Превентивное предотвращение атак осуществляется за счет того, что сетевые IPS пропускают через себя весь трафик обмена с внешней средой, и на внутренний интерфейс передаются только безопасные данные.

Современные IDS и IPS интегрируются с *межсетевыми экранами*, которые позволяют автоматически блокировать сетевые атаки. МЭ обеспечивает защиту АИС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АИС на основе заданных правил, проводя таким образом разграничение доступа субъектов из одной АИС к объектам другой АИС.

*Правила фильтрации* – перечень условий, по которым с использованием заданных критериев фильтрации осуществляется разрешение или запрещение дальнейшей передачи пакетов данных и перечень действий, производимых МЭ по регистрации и/или осуществлению дополнительных защитных функций. Каждое правило запрещает или разрешает передачу информации определенного вида между субъектами одной АИС и объектами другой АИС. Как следствие, субъекты получают доступ только к разрешенным информационным объектам.

*Функции межсетевых экранов:*

– фильтрация данных на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов;

– скрытие внутренних адресов объектов/субъектов от внешних субъектов;

– идентификация, аутентификация и регистрация входа/выхода администратора МЭ;

– регистрация событий загрузки, инициализации, программного останова;

– контроль целостности;

– регламентное тестирование, восстановление функционала после сбоев и отказов оборудования.

| *Тип* | *Место установки* |
|---|---|
| А | на внешней физической границе АС или между физическими границами ее сегментов |
| Б | на логической границе АС или между логическими границами ее сегментов |
| В | на оконечном узле (хосте) |
| Г | на сервере, обслуживающем сайты, веб-службы и веб-приложения, или на физической границе сегмента таких серверов (Web Application Firewall, WAF) |
| Д | в сети АСУ ТП в целях контроля и фильтрации промышленных протоколов передачи данных |

*NTA (Network Traffic Analysis)* – анализаторы сетевого трафика, перехватывающие потоки данных на периметре АИС и внутри инфраструктуры с целью обнаружения признаков сложных целевых атак (APT).

*SIEM (Security Information And Event Management)* – программно-аппаратные комплексы автоматизации мониторинга и управления событиями безопасности в режиме реального времени.

*Функции SIEM:*

– сбор и накопление данных о событиях ИБ из различных источников (системных журналов серверов и рабочих станций, журналов аудита баз данных, логов сетевых устройств, систем безопасности, сканеров уязвимостей, ИТ-сервисов и т.п.);

– выявление инцидентов ИБ и оповещение в реальном времени администраторов безопасности (через онлайн-интерфейс SIEM, по электронной почте, через SMS и т.п.);

– проактивное выявление потенциальных угроз ИБ с помощью ведения баз данных с цифровыми образцами вредоносных кодов (pattern, signature);

– предварительный анализ инцидентов ИБ и выявление причинно-следственных связей между событиями, приведшими к нарушению ИБ;

– корелляционный анализ и поиск связей инцидентов ИБ с наборами конкретных данных, бизнес-приложениями или пользовтелями АС;

– построение моделей с визуализацией результатов анализа инцидентов КБ и предоставлением инструментов для углубленной экспертизы.

SIEM-системы сами по себе не обеспечивают программно-техническую защиту от киберугроз, они предназначены для сбора данных и предварительного анализа поведения АС с целью раннего обнаружения и эффективного реагирования на киберинциденты, а также своевременного выявления внктренних нарушителей ИБ (инсайдеров) (см. рис. 17).


*Рисунок 17. Алгоритм работы SIEM*

**Защита от кибератак данных при их хранении**

Каждая организация ежедневно генерирует сотни и тысячи файлов, которые хранятся и перемещаются внутри периметра. Сотрудники постоянно создают, копируют и пересылают данные, создавая новых владельцев и уровни доступа. Отсутствие полной картины прав доступа является серьезной угрозой информационной безопасности.

*Проблема аудита и контроля доступа к информационным активам организации решается с помощью продуктов класса DCAP (Data-Centric Audit and Protection), которые автоматически собирают сведения обо всех файлах на серверах и компьютерах сотрудников, в почтовых системах и облачных сервисах. В результате формируется структура данных компании и матрица доступа к ним для каждого объекта и пользователя*.

*DCAP (Data-Centric Audit and Protection)* – система управления доступом и мониторинга безопасности конфиденциальных данных на локальных компьютерах, файловых и почтовых серверах, корпоративных порталах, в облачных хранилищах и т.п.

Базовые требования к DCAP-системам:

1. Обнаружение и идентификация данных.
2. Удобное управление политиками безопасности данных.
3. Мониторинг прав и активности пользователей.
4. Детальная и полноценная отчетность.
5. Уведомление о нарушениях безопасности и предотвращение инцидентов.
6. Защита данных.

## 3.5. Влияние на кибербезопасность со стороны различных сотрудников

*Конечной целью создания системы обеспечения кибербезопасности является предотвращение или минимизация ущерба* (прямого или косвенного, материального, морального или иного), наносимого субъектам информационных отношений посредством нежелательного воздействия на информацию, ее носители и процессы обработки.

***Обеспечение кибербезопасности*** *– это непрерывный процесс, основное содержание которого составляет управление рисками через управление людьми, ресурсами, средствами защиты и т.п.* Люди – обслуживающий персонал и конечные пользователи АИС – являются неотъемлемой частью автоматизированной (то есть «человеко-машинной») системы. От того, каким образом они реализуют свои функции в системе, существенно зависит не только ее функциональность (эффективность решения задач), но и ее безопасность.

**Кибербезопасность организации зависит от деятельности следующих категорий сотрудников и должностных лиц организации** (см. рис. 18):

– руководителей организации, определяющих цели и задачи функционирования АИС, направления ее развития, принимающих стратегические решения

по вопросам безопасности и утверждающих основные документы, регламентирующие порядок безопасной обработки и использования защищаемой информации сотрудниками организации;

– системных администраторов средств защиты (ОС, СУБД и т.п.);

– сотрудников подразделения защиты информации, оценивающих состояние КБ, определяющих требования к системе защиты, разрабатывающих организационно-распорядительные документы по вопросам обеспечения информационной безопасности (аналитиков), внедряющих и администрирующих специализированные дополнительные средства защиты (администраторов безопасности);

– программистов, осуществляющих разработку (приобретение и адаптацию) необходимых прикладных программ (задач) для автоматизации деятельности сотрудников организации;

– сотрудников подразделения внедрения и сопровождения ПО, обеспечивающих нормальное функционирование и установленный порядок инсталляции и модификации прикладных программ (задач);

– сотрудников подразделения эксплуатации ТС, обеспечивающих нормальную работу и обслуживание технических средств обработки и передачи информации и системного программного обеспечения;

– сотрудников структурных подразделений (конечных пользователей АИС), решающих свои функциональные задачи с применением средств автоматизации.

Кроме того, на КБ организации могут оказывать влияние посторонние лица и сторонние организации, предпринимающие попытки вмешательства в процесс нормального функционирования АИС или несанкционированного доступа к информации как локально, так и удаленно.


*Рисунок 18. Субъекты, влияющие на состояние информационной безопасности АИС*

*Руководство принимает стратегические решения по вопросам обеспечения информационной безопасности и утверждает основные документы, регламентирующие порядок функционирования и развития АИС,* обеспечивающий безопасную обработку и использование защищаемой информации. *Руководство определяет критичность процессов, ресурсов и степень их защиты, а также координирует деятельность по управлению и распределению обязанностей по обеспечению КБ между службами безопасности и автоматизации*.

Руководство должно признать комплекс мер по обеспечению КБ частью производственного процесса. Как сказано в стандарте ISO 27002 (BS 7799), *высшее руководство должно поставить четкую цель и показать свою поддержку и заинтересованность в вопросах ИБ, распространения политики ИБ среди сотрудников организации*. В организации должны проводиться регулярные совещания руководства по вопросам корректировки политики ИБ и координации действий персонала.

*Аналитики отвечают за анализ состояния КБ, определение требований к защищенности различных подсистем АИС и выбор методов и средств защиты*.

*Администраторы средств защиты, контроля и управления безопасностью отвечают за эффективное применение специализированных средств защиты*.

*Программисты осуществляют разработку (приобретение и адаптацию) необходимых прикладных программ (задач) для автоматизации деятельности сотрудников организации*. Влияние программистов может быть непреднамеренным (ошибки) и преднамеренным (закладки, люки). Практика показывает, что ошибки кода всегда присутствуют в любой программе.

*Подразделение внедрения и сопровождения ПО обеспечивает нормальное функционирование прикладных программ (задач)*.

*Подразделение эксплуатации обеспечивает нормальную работу и обслуживание технических (вычислительных средств и средств телекоммуникации) и общего (системного) программного обеспечения*.

*Администраторы серверов, приложений, баз данных и т.п. отвечают за эффективное применение штатных средств защиты и разграничения доступа всех используемых ОС и СУБД*.

*Сотрудники структурных подразделений (конечные пользователи системы) решают свои функциональные задачи с применением средств автоматизации.* Совершение ошибок пользователями способствует порождению угроз, которые затем могут быть использованы злоумышленниками для нанесения вреда организации и ее сотрудникам.

*Выполнение сотрудниками ряда ограничительных мероприятий существенно повышает информационную безопасность.* Смысл КБ – жесткая регламентация всей деятельности сотрудников, сочетающаяся с высокой исполнительской дисциплиной. Необходимо учитывать, что регламентация деятельности сотрудников (непосредственно не подчиненных службе безопасности) может привести к конфликтам, поэтому дополнительные функции сотрудников должны быть четко определены в соответствующих утвержденных руководством инструкциях.

## 3.6. Регламентация действий пользователей и обслуживающего персонала автоматизированной информационной системы

Обслуживающий персонал и пользователи, как неотъемлемая часть АИС, является источником внутренних угроз КБ организации и одновременно может являться частью системы защиты АИС. Поэтому *одним из основных направлений обеспечения информационной безопасности является регламентация действий всех пользователей и обслуживающего персонала АИС, целями которой являются*:

– сокращение возможностей лиц из числа пользователей и персонала по совершению нарушений (как неумышленных, так и преднамеренных);

– реализацию специальных мер противодействия другим внутренним и внешним для системы угрозам (связанным с отказами и сбоями оборудования, ошибками в программах, стихийными бедствиями и действиями посторонних лиц, не являющихся частью АИС).

***Регламентация предусматривает*** *введение таких ограничений и внедрение таких приемов работы сотрудников, которые, не создавая помех для исполнения ими своих функциональных обязанностей (технологических функций), минимизируют возможности совершения ими случайных или преднамеренных нарушений (например, наделение каждого сотрудника (пользователя,) минимально необходимыми для выполнения им своих обязанностей полномочиями по доступу к ресурсам АИС).*

*К обеспечению кибербезопасности организации (и в определенной степени к управлению ее безопасностью) должны привлекаться практически все сотрудники, участвующие в процессах автоматизированной обработки информации, и все категории обслуживающего АИС персонала (все кроме посторонних)*.

Роли и функции различных категорий сотрудников и подразделений организации в обеспечении КБ существенно различаются (большинство сотрудников должны лишь исполнять установленные в организации регламенты и правила безопасной работы в АИС).

**Создание (построение, развитие) и эффективное функционирование системы КБ может быть обеспечено только при наличии**:

– правильно разработанной системы организационно-распорядительных и нормативно-методических документов, определяющих политику КБ (регламенты по вопросам безопасности АИС для всех категорий сотрудников организации);

– специальных технических средств защиты и контроля эффективности принятых мер защиты;

– специального подразделения (например, отдела технической защиты информации, далее – ОТЗИ).

За формирование системы защиты и реализацию единой политики КБ организации и осуществление контроля и координации действий всех подразделений и сотрудников организации по вопросам обеспечения КБ должно непосредственно отвечать специальное подразделение (служба) защиты информации (обеспечения КБ).

В силу малочисленности данного подразделения решение им многих процедурных вопросов и эффективный контроль за соблюдением всеми сотрудниками требований по обеспечению КБ возможны только при назначении во всех подразделениях, эксплуатирующих подсистемы АИС, нештатных помощников – ответственных за обеспечение КБ.

Эффективное использование штатных (для ОС и СУБД) и дополнительных средств защиты обеспечивается системными администраторами и администраторами средств защиты. Системные администраторы обычно входят в штат подразделений автоматизации (информатизации). Администраторы дополнительных средств защиты, как правило, являются сотрудниками подразделения защиты информации.

*Таким образом, организационную структуру системы обеспечения безопасности ИТ организации можно представить в виде совокупности следующих уровней:*

Уровень 1. Руководство организации.

Уровень 2. Аналитики подразделения обеспечения ИБ.

Уровень 3. Администраторы штатных и дополнительных средств защиты.

Уровень 4. Ответственные за обеспечение ИБ в подразделениях.

Уровень 5. Конечные пользователи и обслуживающий персонал.

Малочисленное подразделение безопасности должно управлять деятельностью большого числа сотрудников организации. ***Ответственный за обеспечение КБ в подразделении*** *– это посредник между малочисленным подразделением безопасности и многочисленными пользователями (это «представители КБ» на местах).*

Основные функции ответственных за обеспечение КБ – эффективная поддержка реализации разработанных подразделением безопасности и утвержденных руководством регламентов.

*При отсутствии ответственного за обеспечение КБ в подразделении его функции должен выполнять руководитель подразделения*.

Наличие института ответственных за обеспечение КБ в подразделении – признак развитой системы безопасности организации и необходимое условие обеспечения КБ. Основные требования к ответственному за обеспечение КБ – исполнительность, добросовестность, доступность и повышенный уровень знаний по вопросам обеспечения КБ.

## Вопросы для самоконтроля

1. Кто разрабатывает политику безопасности на уровне организации?
2. Где применяется политика безопасности?
3. На каком основании осуществляется классификация моделей разграничения доступа?
4. Какова роль моделей разграничения доступа в теории информационной безопасности?
5. В чем заключаются основные достоинства мандатной политики разграничения доступа?
6. В чем заключаются основные недостатки мандатной политики разграничения доступа?
7. В чем заключается содержание моделей группового доступа?
8. В чем заключается сущность информационной невыводимости?
9. В чем заключается сущность информационного невмешательства?
10. С какой целью строятся многоуровненвые схемы разграничения доступа?

# ГЛАВА 4.
# ИСТОЧНИКИ И КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ. ОСНОВЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

## 4.1. Технические каналы утечки информации

Под **техническим каналом утечки информации** (далее – ТКУИ) понимают совокупность объекта разведки, технического средства разведки (далее – ТСР), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал (см. рис. 20). По сути, под ТКУИ понимают способ получения с помощью ТСР разведывательной информации об объекте. Причем под разведывательной информацией обычно понимаются сведения или совокупность данных об объектах разведки независимо от формы их представления.

Распространение информационного сигнала называют его утечкой.

**Утечка** – бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

**Утечка (информации) по техническому каналу** – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Технический канал утечки информации, так же как и канал передачи информации, состоит из источника сигнала, физической среды его распространения и приемной аппаратуры злоумышленника. На рисунке 19 приведена структура технического канала утечки информации.

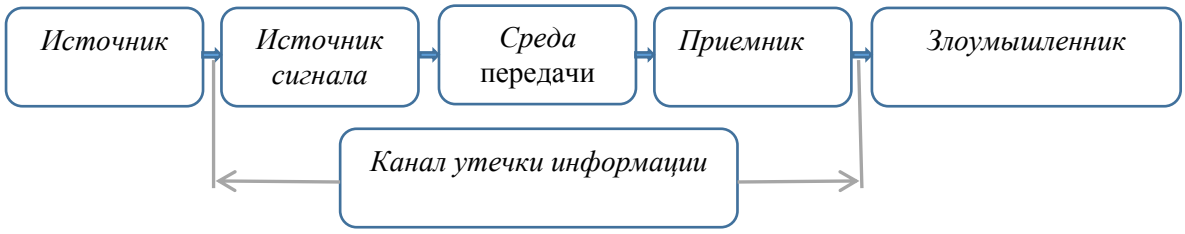


*Рисунок 19. Структура технического канала утечки информации*

На вход канала поступает информация в виде первичного сигнала. Первичный сигнал представляет собой носитель с информацией от ее источника или с выхода предыдущего канала. *В качестве источника сигнала могут быть*:

– объект наблюдения, отражающий электромагнитные и акустические волны;

– объект наблюдения, излучающий собственные (тепловые) электромагнитные волны в оптическом и радиодиапазонах;

– передатчик функционального канала связи;

– закладное устройство;
– источник опасного сигнала;
– источник акустических волн, модулированных информацией.

Сигналы, передающие защищаемую информацию, которые могут быть перехвачены злоумышленником с последующим извлечением этой информации, ***называются опасными***. Опасные сигналы подразделяются на два вида: функциональные и случайные. Функциональные сигналы создаются техническим средством обработки информации для выполнения заданных функций.

*К основным источникам функциональных сигналов относятся*:
– источники систем связи;
– передатчики радиотехнических систем;
– излучатели акустических сигналов;
– люди.

Принципиальным отличием функциональных сигналов от случайных является то, что владелец информации знает о возможных рисках нарушения безопасности информации и может принять соответствующие меры по снижению риска до допустимых значений.


*Рисунок 20. Классификация технических каналов утечки информации*

К техническим средствам, которые могут быть источниками случайных опасных сигналов, относятся:
– средства телефонной проводной связи;
– средства мобильной связи и радиосвязи;
– средства электронной почты;
– СВТ;
– аудиоаппаратура и средства звукоусиления;

– радиоприемные устройства;
– видеоаппаратура;
– телевизионные средства;
– средства линейной радиотрансляции и оповещения.

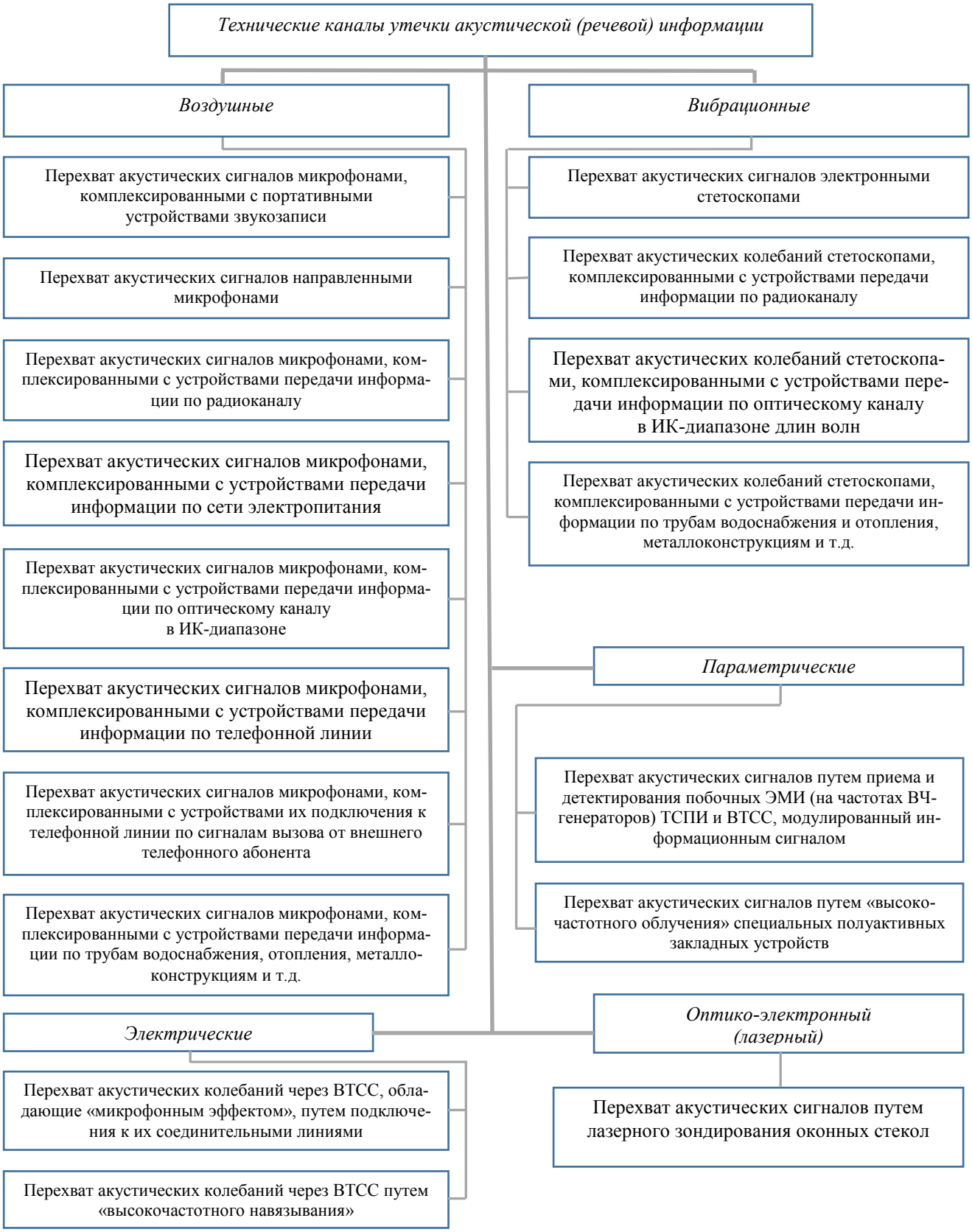


*Рисунок 21. Классификация ТКУ акустической информации*

Случайные опасные сигналы могут создаваться следующими электрическими приборами:

– средствами системы электрочасофикации;
– средствами охранной сигнализации;
– средствами пожарной сигнализации;
– оргтехникой (в частности, принтерами);
– средства системы кондиционирования и вентиляции;
– бытовыми приборами и другой техникой, имеющей в составе элементы преобразования акустической информации в электрические сигналы;
– электропроводящей коммуникацией здания, проходящей через контролируемую зону.

***Под техническим каналом утечки акустической (речевой) информации*** **(*ТКУАИ*)** понимают совокупность объекта разведки (выделенного помещения), технического средства акустической (речевой) разведки (ТСАР), с помощью которого перехватывается речевая информация, и физической среды, в которой распространяется информационный сигнал (см. рис. 21).

***Визуально-оптические каналы*** – это ТКУ, возникающие за счет выхода за пределы контролируемой зоны световой энергии, несущей ту или иную информацию. Защита информации от утечки по визуально оптическим каналам.

Наряду с информацией, обрабатываемой в ТСПИ, и акустической (речевой) информацией, важную роль играет видовая информация, получаемая техническими средствами разведки в виде изображений объектов или документов. Классификация визуально-оптических ТКУИ представлена на рисунке 22.


*Рисунок 22. Классификация визуально-оптических ТКУИ*

В зависимости от характера информации и ее предназначения можно выделить следующие способы ее получения:

– наблюдение за объектом;

– съемка объекта;

– съемка (снятие копий) документов.

Источниками и носителями информации в **материально-вещественных ТКУИ** являются субъекты (люди) и материальные объекты (макро и микрочастицы), которые имеют четкие пространственные границы локализации, за исключением излучений радиоактивных веществ. Утечка информации в этих каналах сопровождается физическим перемещением людей и материальных тел с информацией за пределами контролируемой зоны. Для более четкого описания рассматриваемого канала целесообразно уточнить состав источников и носителей информации.

*Основными источниками информации материально-вещественного канала утечки информации являются*:

– черновики различных документов и макеты материалов, узлов, блоков, устройств, разрабатываемых в ходе научно-исследовательских и опытно-конструкторских работ, ведущихся в организации;

– отходы делопроизводства и издательской деятельности в организации, в том числе использованная копировальная бумага, забракованные листы при оформлении документов и их размножении;

– содержащие защищаемую информацию дискеты ПЭВМ, нечитаемые из-за их физических дефектов и искажений загрузочных или других секторов;

– бракованная продукция и ее элементы;

– отходы производства с демаскирующими веществами в газообразном, жидком и твердом виде;

– радиоактивные материалы.

Перенос информации в этом канале за пределы контролируемой зоны возможен следующими субъектами и объектами (носителями информации):

– сотрудниками организации;

– воздушными массами атмосферы;

– жидкой средой;

– излучениями радиоактивных веществ.

Эти носители могут переносить все виды информации: семантическую и признаковую, а также демаскирующие вещества.

Семантическая информация содержится в черновиках документов, схем, чертежей; информация о видовых и сигнальных демаскирующих признаках в бракованных узлах и деталях, в характеристиках радиоактивных излучений и т.д.; демаскирующие вещества – в газообразных, жидких и твердых отходах производства.

В **воздушных акустических каналах утечки** средой распространения акустических сигналов является воздух, а в качестве основного средства перехвата используется микрофон. Микрофон преобразует акустический сигнал в электрический и соединяется либо с записывающим устройством, либо с ка-

ким-то передатчиком. Передача полученных сигналов злоумышленнику может происходить по многим каналам: радиоканалу, оптическому каналу, по электросети и т.п. (см. рис. 23).

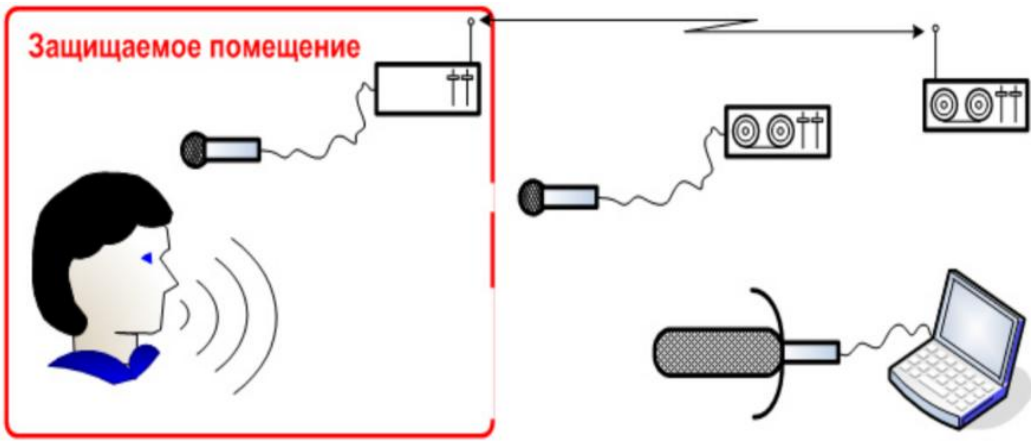


*Рисунок 23. Акустический ТКУИ*

Средой распространения акустических колебаний в вибрационных каналах являются конструкции зданий, стены, потолки, трубы и другие твердые тела (см. рис. 24).

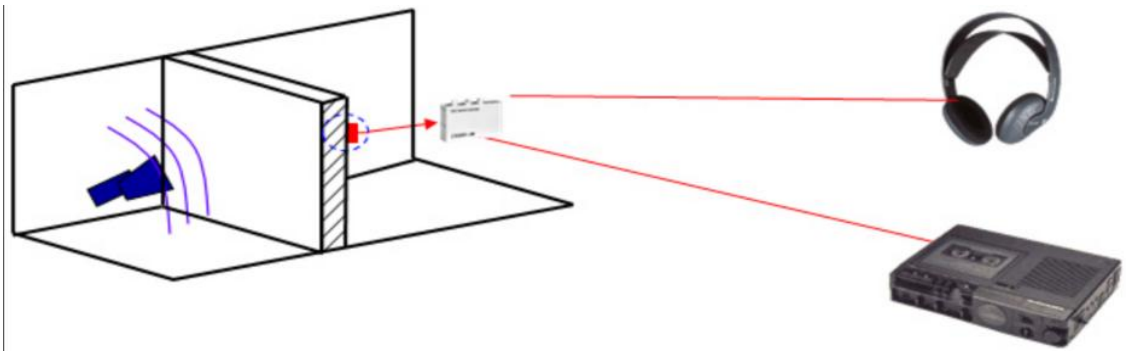

*Рисунок 24. Виброакустический ТКУИ*

Для перехвата информации по виброакустическому каналу используются стетоскопы, в которых в качестве датчиков используются контактные микрофоны.

***Стетоскопы* (*контактные микрофоны*)** – устройства, которые усиливают акустический сигнал, распространяющийся сквозь стены, пол, потолок в 20–30 тыс. раз, а также способны улавливать шорохи и тиканье часов через бетонные стены толщиной до 1 м.

Датчики наиболее часто устанавливаются на наружных поверхностях зданий, на оконных проемах и рамах, в смежных (служебных и технических) помещениях за дверными проемами, ограждающими конструкциями, на перегородках, трубах систем отопления и водоснабжения, коробах воздуховодов вентиляционных и других систем.

Пример электронного стетоскопа представлен на рисунке 25. PKI 2850 является типовым представителем портативных электронных стетоскопов. Размеры его усилительного блока составляют 95x60x25 мм, а контактного микрофона – 50x35x15 мм. Коэффициент усиления стетоскопа не менее 80 дБ. Время работы от встроенного аккумулятора до 800 ч.


*Рисунок 25. Малогабаритный электронный стетоскоп PKI 2850 с контактным микрофоном*

Электроакустические каналы утечки информации возникают за счет электроакустических преобразований, то есть акустические сигналы преобразуются в электрические.

Перехват акустических колебаний в данном канале утечки информации осуществляется путем непосредственного подключения к соединительным линиям ВТСС, обладающих «микрофонным эффектом», специальных высокочувствительных низкочастотных усилителей. Например, подключая такие средства к соединительным линиям телефонных аппаратов с электромеханическими вызывными звонками, можно прослушивать разговоры, ведущиеся в помещениях, где установлены эти аппараты (см. рис. 26).

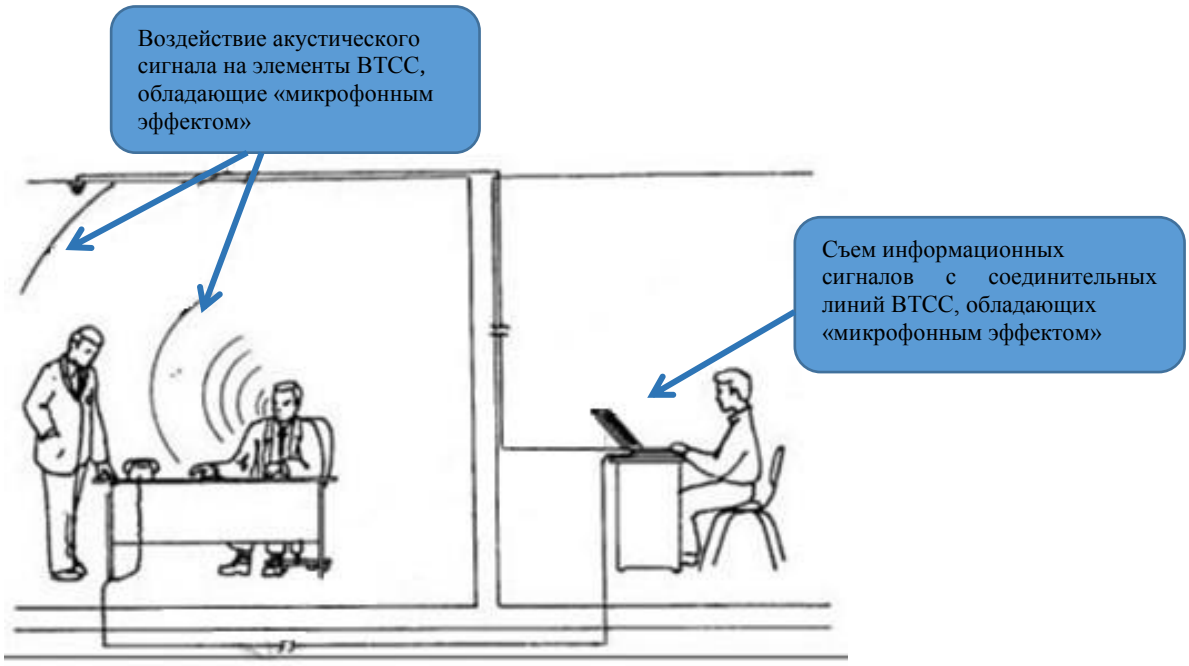


*Рисунок 26. Перехват акустических сигналов через ВТСС, обладающих «микрофонным эффектом»*

Съем информации в *оптико-электронном канале* реализуется с помощью лазера, поэтому иногда этот канал называют лазерным. Под действием звуковой волны тонкие отражающие поверхности, например стекло или зеркало, начинают вибрировать. Если направить на них лазер, отраженное лазерное излучение модулируется и поступает на вход приемника оптического излучения. В приемнике полученный сигнал демодулируется и усиливается, и злоумышленник может получить исходный акустический сигнал (см. рис. 27).

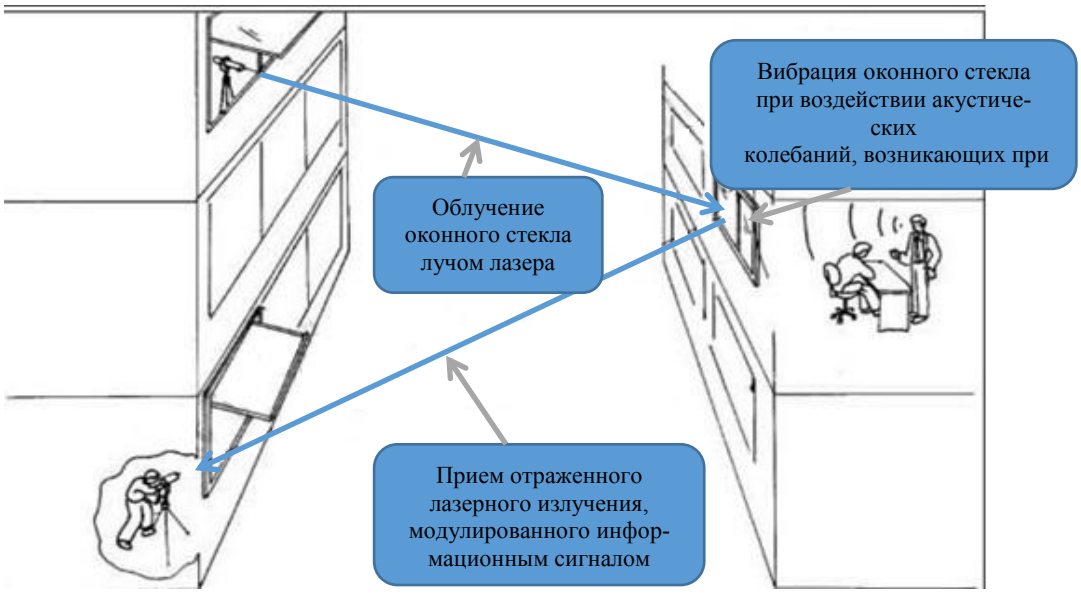


*Рисунок 27. Перехват акустических сигналов путем лазерного зондирования оконных стекол*

Возникновение параметрических каналов обусловлено тем, что под давлением звуковой волны может измениться взаимное расположение элементов схем, проводов и т.п. в ВТСС и ОТСС. Вместе с расположением изменяются индуктивность и емкость. Соответственно, будет наблюдаться модуляция сигналов, проходящих через ВТСС и ОТСС, информационным сигналом, содержащимся в акустической волне. Промодулированные сигналы излучаются в пространство, где могут быть перехвачены средствами радиоразведки.

## 4.2. Технические каналы утечки информации при ее передаче по каналам связи

Защита информации должна осуществляться посредством выполнения комплекса мероприятий и применения средств ЗИ по предотвращению утечки информации или воздействия на нее по техническим каналам, за счет несанкционированного доступа к ней, по предупреждению преднамеренных программно-технических воздействий с целью нарушения целостности информации в процессе ее обработки, передачи и хранения, нарушения ее доступности и работоспособности технических средств.

Организация технической защиты информации – сложный и объемный процесс, который требует наличия определенных знаний и опыта. Не вникая в технические аспекты, рассмотрим только организационную составляющую и отметим основные термины.

***Основные технические средства и системы*** **(*ОТСС*)** – технические средства, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации. К ним относятся технические средства автоматизированных систем различного уровня и назначения на базе средств вычислительной техники, средства и системы связи и передачи данных, используемые для обработки конфиденциальной информации.

Помимо основных технических средств (компьютеры, сетевое оборудование и т.д.) выделяют вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с основными техническими средствами и системами или в защищаемых помещениях. К ним относятся:

- различные телефонные средства и системы;
- средства и системы передачи данных в системе радиосвязи;
- средства и системы охранной и пожарной сигнализации;
- средства и системы оповещения и сигнализации;
- контрольно-измерительная аппаратура;
- средства и системы кондиционирования;
- средства и системы электрочасофикации и иные технические средства.

***Защита информации от несанкционированного доступа*** или воздействия – деятельность, направленная на предотвращение получения информации заинтересованным субъектом с нарушением установленных прав или правил.

***Защищаемые помещения*** **(далее – *ЗП*)** – помещения (служебные кабинеты, конференц-залы), специально предназначенные для проведения конфиденциальных мероприятий.

***Контролируемая зона*** **(далее – *КЗ*)** – это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств. Границей КЗ могут являться: периметр охраняемой территории учреждения; ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории.

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

**ТКУИ при ее передаче по каналам связи**

***Канал связи*** (англ. *channel, data line*) – система технических средств и среда распространения сигналов для передачи сообщений (не только данных) от источника к получателю (и наоборот). Канал связи, понимаемый в узком

смысле (тракт связи), представляет только физическую среду распространения сигналов, например физическую линию связи.

Существует множество видов каналов связи, среди которых наиболее часто выделяют каналы проводной связи (воздушные, кабельные, световодные и др.) и каналы радиосвязи (тропосферные, радиорелейные, спутниковые, собственно радиосвязи и др.).

По типу среды распространения каналы связи делятся на проводные, акустические, оптические, инфракрасные и радиоканалы.

Каналы связи также классифицируются:

– на непрерывные (на входе и выходе канала – непрерывные сигналы);

– дискретные или цифровые (на входе и выходе канала – дискретные сигналы).

В зависимости от вида канала связи ТКУИ можно разделить на электромагнитные, электрические и индукционные (см. рис. 28).


*Рисунок 28. Классификация ТКУИ при ее передаче по каналам связи*

***Электромагнитый ТКУИ*** – перехват электромагнитных излучений на частотах работы передатчиков систем и средств связи. Используется для перехвата информации, передаваемой по каналам радио-, радиорелейной, спутниковой связи. Напряженность электрического поля в точке приема (перехвата) будет прямо пропорциональна величине мощности передатчика, высоте приемной и передающей антенн и обратно пропорциональна расстоянию (см. рис. 29).


*Рисунок 29. Перехват информации по каналам радиосвязи*

***Электрический ТКУИ*** – съем информации путем контактного подключения аппаратуры злоумышленника к кабельным линиям связи. Для подключения аппаратуры злоумышленник может использовать параллельное или последовательное подключение к линии связи.

***Индукционный ТКУИ*** – бесконтактный съем информации с кабельных линий связи. Возможность такого съема информации возникает за счет эффекта возникновения вокруг кабеля связи электромагнитного поля, модулированного информационным сигналом. Это поле перехватывается специальным индукционным датчиком, далее усиливается и демодулируется на аппаратуре злоумышленника. Следует отметить, что бесконтактные закладные устройства обнаружить труднее всего, так как они не изменяют характеристик канала связи (см. рис. 30).


*Рисунок 30. Индукционный и электрический ТКУИ*

**Побочные электромагнитные излучения (ПЭМИ)** – электромагнитные излучения технических средств, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях. Именно для контроля ПЭМИ вводится понятие зоны 2. Зона 2 должна быть меньше контролируемой зоны. В противном случае необходимо использовать активные средства защиты от ПЭМИ, которые будут снижать отношение полезного сигнала к помехе на оборудовании злоумышленника.

**Перехват излучений на частотах работы ВЧ-генераторов** становится возможным из-за того, что в состав ОТСС и ВТСС входят ВЧ-генераторы, например генератор тактовой частоты. Под воздействием внешнего информационного сигнала на их элементах наводятся электрические сигналы. Эти сигналы модулируют собственные высокочастотные колебания генератора и излучаются в окружающее пространство, где могут быть перехвачены злоумышленником.

**Перехват излучений на частотах самовозбуждения** усилителей низких частот. Самовозбуждение УНЧ возможно за счет случайных преобразований отрицательных обратных связей в паразитные положительные, что приводит к

переводу усилителя из режима усиления в режим автогенерации сигналов. Сигнал на частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом и может быть перехвачен злоумышленником.


*Рисунок 31. Классификация технических каналов утечки информации, обрабатываемой ОТСС*

**Параметрический ТКУИ** образуется за счет «высокочастотного облучения» ОТСС. Злоумышленник с помощью специальной аппаратуры направляет на ОТСС электромагнитное поле, которое переизлучается от элементов ОТСС промодурированное информационным сигналом. При переизлучении параметры сигналов меняются, поэтому данный ТКУИ называется параметрическим.

**Электрические каналы утечки** образуются из-за просачивания информационных сигналов в цепи заземления и электропитания ОТСС, а также за счет наводок, которые мы рассмотрели ранее, на линии электропитания ВТСС и другие проводники, выходящие за пределы контролируемой зоны.

Следует отметить, что технические каналы утечки информации могут быть основными источниками несанкционированного доступа к конфиденциальной информации. Для снижения вероятности утечки информации необходимо учитывать наличие ТКУИ и своевременно принимать меры по их ликвидации или, в случае невозможности, применять методы противодействия утечки информации по таким каналам[35].

[35] Особенности реализации компьютерных экспертиз в системе МВД России: учебное пособие / В.Л. Акапьев, А.А. Гуржий, А.А. Дрога [и др.]. – Белгород: Бел ЮИ МВД России имени И.Д. Путилина, 2019. – 99 с.

## 4.3. Техническая защита информации

***Техническая защита информации*** *(далее – ТЗИ) – вид защиты информации некриптографическими методами с применением технических, программных и программно-технических средств*.

Технологии технической защиты информации применяются на объекте информатизации, представляющем совокупность ИР, ПТС АИС и сетей, средств инфраструктуры обеспечения, мест для размещения этих средств и ведения конфиденциальных переговоров (помещений, зданий, сооружений).

*Основные технические средства и системы (далее – ОТСС)* – программно-технические средства АИС и сетей, непосредственно используемые для обработки, хранения и передачи информации.

*Защищаемые помещения* – помещения (служебные кабинеты, переговорные комнаты, актовые залы и т.д.), выделенные для проведения конфиденциальных переговоров, совещаний, конференций и т.п.

*Вспомогательные технические средства и системы (далее – ВТСС)* – технические средства и системы, располагаемые рядом с ОТСС или в защищаемые помещения, но не предназначенные для передачи, обработки и хранения конфиденциальной информации. К ВТСС относятся средства и системы:

- телефонии и мобильной связи;
- радиосвязи;
- оповещения, охранной и пожарной сигнализации;
- климатического контроля, кондиционирования, вентиляции;
- проводной радиотрансляционной сети;
- бытовой и организационной техники и т.п.

Через элементы ВТСС могут создаваться технические каналы утечки информации.

*Технические СЗИ* – это встроенные в ОТСС компоненты или специализированное автономное оборудование, используемое для обеспечения ИБ организации некриптографическими методами.

**Направления технической защиты информации:**

1. *Защита информации от утечки* направлена на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации (иностранными) разведками и другими заинтересованными субъектами (государством, организациями, лицами).

2. *Защита информации от несанкционированного доступа* (НСД) направлена на предотвращение ознакомления с информацией и ее использования с нарушением установленных прав или правил разграничения доступа.

3. *Защита информации от несанкционированного воздействия* (НСВ) направлена на предотвращение НСД и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на ее удаление, блокирование или изменение.

4. *Защита информации от непреднамеренного воздействия* (НПДВ) направлена на предотвращение воздействия на защищаемую информацию ошибок авторизованного пользователя, сбоев ТС, иных техногенных или стихийных факторов.

5. *Защита информации от преднамеренного воздействия* (ПДВ), направлена на предотвращение целенаправленного воздействия (программного, электромагнитного, физического и т.п.), осуществляемого в противоправных целях.

6. *Защита информации от разглашения* направлена на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

7. *Защита информации от* (иностранной, криминальной, коммерческой) *разведки* направлена на предотвращение получения защищаемой информации (иностранной) разведкой.

**Задачи, решаемые с помощью средств ТЗИ:**

– *создание контролируемой зоны безопасности* вокруг защищаемого объекта информатизации;

– *создание физических (механических) препятствий на пути проникновения к носителям информации* (решетки, сейфы, бронированные двери и стекла, замки и др.);

– *выявление и пресечение попыток проникновения* на объект информатизации (охранная сигнализация, средства блокирования доступа на объект);

– *противодействие стихийным угрозам безопасности* (пожарная сигнализация и системы пожаротушения, средства оповещения и т.п.);

– *защита АИС от утечки информации по техническим каналам* (экраны, защитные фильтры, гальваническая развязка в сетях электроснабжения, поиск закладных устройств, зашумление в электромагнитном диапазоне и т.п.);

– *оперативное взаимодействие с обеспечивающими организациями*, подразделениями и другими объектами охраны (радио- и проводные средства связи, сигнальные устройства и т.п.).

– *защита от технических разведок, в том числе путем маскирования и дезинформирования*;

– *защита режимных помещений по требованиям информационной безопасности* (зашумление помещений в акустическом диапазоне, перекрытие каналов несанкционированного видеонаблюдения, обнаружение и вывод из строя подслушивающих устройств и скрытых видеокамер, выявление побочных электромагнитных излучений и наводок и т.п.);

– *блокирование мобильных коммуникаторов* случайных или умышленных нарушителей, способных создавать канал утечки информации за пределы контролируемой зоны;

– *защита ИР АИС от НСД с помощью программных и программно-аппаратных средств*.

**Виды средств технической защиты информационной инфраструктуры на объектах информатизации:**

1. *Средства физической защиты* – это устройства, сооружения и инженерные конструкции, исключающие или затрудняющие физический доступ нарушителей безопасности к ИР и ПТС АИС и сетей.

Механические, электромеханические, электронные, оптические, радиотехнические средства физической защиты можно разделить на *две категории*:

– средства защиты от проникновения нарушителей в пределы контролируемой зоны или на объекты информатизации (заборы, ограждения, усиленные двери, кодовые замки, решетки на окнах);

– средства обнаружения и ликвидации угроз безопасности, связанных с преднамеренным или непреднамеренным воздействием на ресурсы АС или обеспечивающую инфраструктуру (системы контроля и управления доступом, видеонаблюдение, пожарная и охранная сигнализация, системы пожаротушения, резервного электропитания, автоматического блокирования доступа в защищаемые помещения).

2. *Технические средства защиты* – это любые электрические, механические, оптические устройства, которые встраиваются в ИР и ПТС АИС и сетей или устанавливаются на объекте информатизации: системы контроля и управления доступом сотрудников (в том числе по биометрическим признакам), гарантированного уничтожения данных на внешних носителях, средства экранирования ПТС АИС и сетей. Они препятствуют доступу к информации, ресурсам АИС, ИТКС со стороны внутренних и внешних нарушителей, в том числе иностранных разведок. К техническим средствам защиты также относятся генераторы шума, сетевые фильтры подавления паразитного информативного сигнала, сканирующие радиоприемники и множество других устройств, обнаруживающих и/или перекрывающих технические каналы утечки информации.

3. *Программные средства* – это совокупность специализированных программ, обеспечивающих гарантии конфиденциальности целостности и доступности информации (ПО разграничения доступа и авторизации пользователей по ключам доступа, архиваторы резервных копий, ПО гарантированного стирания донных и т.п.).

Состав и эффективность принимаемых мер ЗИ зависит от качества определения модели угроз ИБ для конкретной АИС в конкретных условиях ее функционирования, а также от требований регулятора отношений в области ТЗИ.

*Основным регулятором вопросов ТЗИ в государственных или ведомственных АИС, обрабатывающих информацию ограниченного доступа (гостайну, служебную тайну, персональные данные), является ФСТЭК России*.

В соответствии приказом ФСТЭК России от 11 февраля 2013 г. № 17[36] для АИС устанавливаются четыре класса требований к защищенности в зави-

[36] Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Официальный интернет-портал правовой информации [Электронный ресурс]. – Режим доступа: http://www.pravo.gov.ru 16.09.2019.

симости от уровня значимости информации (не составляющей гостайну) и масштаба АИС (федеральный, региональный, объектовый).

Нормы ФСТЭК в целом регламентируют:

– классифицирование и набор требований к программным и техническим СЗИ в каждом классе;

– состав и соответствие мер защиты информации уровню угроз;

– порядок разработки и эксплуатации системы ТЗИ АИС;

– лицензирование деятельности в области ТЗИ и сертификацию некриптографических СЗИ.

***Аттестация объектов информатизации*** *– комплекс организационных и технических мероприятий, в результате которых подтверждается соответствие системы защиты информации требованиям безопасности*.

Аттестация объекта информатизации проводится при его создании, модернизации или повышении категории ограничения доступа к обрабатываемой информации. Аттестация предусматривает проведение комплекса организационных и технических мероприятий, по результатам которых выдается аттестат соответствии защиты объекта информации в условиях его эксплуатации установленным требованиям.

## 4.4. Меры защиты информации от утечки по техническим каналам

Перечень необходимых мер ЗИ определяется по результатам обследования объекта информатизации с учетом соотношения затрат на защиту информации с возможным ущербом от ее разглашения, утраты, уничтожения, искажения, нарушения санкционированной доступности информации и работоспособности технических средств, обрабатывающих эту информацию, а также с учетом реальных возможностей ее перехвата и раскрытия ее содержания.

*Приоритетное внимание должно быть уделено защите информации, в отношении которой угрозы безопасности информации реализуются без применения сложных технических средств перехвата информации*:

– речевой информации, циркулирующей в защищаемых помещениях;

– информации, обрабатываемой штатными ПТС АИС и сетей;

– информации, хранимой на отторгаемых носителях;

– информации, выводимой на экраны видеомониторов;

– информации, передаваемой по каналам связи, выходящим за пределы контролируемой зоны.

*Рекомендуемые меры ЗИ от утечки по техническим каналам:*

– использование основных технических средств и систем в защищенном исполнении;

– использование шифрования при передаче файлов по каналам связи или сохранении на съемные носители;

– использование сертифицированных СЗИ;

– размещение защищаемых объектов информатизации строго в соответствии с предписанием на эксплуатацию;

– размещение в пределах контролируемой зоны понижающих трансформаторных подстанций электропитания и контуров заземления технических средств;

– обеспечение развязки цепей электропитания ПТС с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;

– экранирование линий связи между ПТС передачи информации;

– обеспечение электромагнитной развязки между линиями передачи защищаемой информации и вспомогательных технических средств и систем, выходящими за пределы контролируемой зоны;

– использование ПТС АИС и сетей, удовлетворяющих требованиям национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации;

– реализация организационных и технических мер обеспечения звукоизоляции ограждающих конструкций помещений, в которых расположены ПТС АИС, систем вентиляции и кондиционирования, не позволяющей вести прослушивание речевой информации при разговоре или воспроизведении;

– размещение устройств отображения информации ПТС АИС таким образом, чтобы была исключена возможность ее просмотра;

– установка на объекте информатизации систем ограничения доступа, охранного видеонаблюдения и сигнализации.

*Организационные (режимные) и инженерно-технические меры КБ*:

– исключить обработку информации с грифом, превышающим разрешенный для ОИ;

– исключить физический доступ к информации (в том числе акустической) посторонних лиц;

– исключить неконтролируемый доступ посторонних лиц в помещение (включая инженерно-технические сооружения), где расположены ОТСС;

– строго соблюдать технические условия и правила эксплуатации защищаемого помещения, технических средств и инженерно-технических устройств, расположенных в этом помещении;

– не допускать изменение условий расположения, комплектации и эксплуатации помещения, ОТСС и ВТСС без согласования со службой защиты информации;

– эксплуатация в помещении нештатных технических средств любой номенклатуры не допускается (включая мобильные коммуникаторы);

– не допускать передачу компонентов ОТСС вместе с защищаемой информацией посторонним лицам (в ремонт, на баланс, на списание и в иных случаях);

– исключить возможность визуального считывания (просмотра) информации (с экранов дисплеев, с бумажных носителей и других возможных источников информации), обрабатываемой в помещении;

– ремонт, установку, замену ограждающих (строительных) конструкций, систем приточно-вытяжной вентиляции и кондиционирования, инженерно-технических сооружений, оборудования или предметов интерьера помещения производить только по согласованию со службой защиты информации;

– обеспечить присутствие ответственного должностного лица при проведении уборки помещения;

– в нерабочее время запирать, опечатывать и сдавать под охрану помещение, при этом окна помещения должны быть закрыты на запирающие устройства и полностью зашторены;

– исключить доступ к ИР и ПТС АС с нарушением установленных прав;

– осуществлять постоянный контроль СЗИ;

– осуществлять постоянный контроль целостности кабелей и кабель-каналов связи, электропитания (освещения), пожарной и охранной сигнализации, инженерно-технических сооружений, расположенных в помещениях.

Разрабатывая механизм защиты информации от утечки, следует также учитывать особенные *свойства информации*, отличающие ее от материальных объектов:

– утечку информации трудно обнаружить методами контроля ее количества, т.к. емкость информации, подвергшейся разглашению, НСД или перехвату по техническим каналам не изменяется;

– утечка информации в большинстве случаев наносит ущерб владельцу только при попадании ее к заинтересованному злоумышленнику;

– ценность украденной информации снижается при расширении круга ознакомленных с ней потребителей.

## 4.5. Средства защиты информации от утечки по техническим каналам

*Средство защиты информации от утечки по техническим каналам* – техническое средство, вещество или материал, предназначенное и/или используемое для защиты информации от утечки по техническим каналам.

*Сертификация СЗИ на соответствие требованиям по безопасности информации* – форма подтверждения соответствия объектов оценки требованиям по ИБ, установленным техническими регламентами, стандартами или условиями договоров.

К объектам оценки могут относиться средства защиты информации или средства контроля эффективности защиты информации.

Сертификацию СЗИ от утечки по техническим каналам осуществляют подразделения ФСТЭК России (кроме средств криптозащиты).

*Инженерно-техническая защита объектов (территорий, зданий, помещений)* – это совокупность инженерных и технических мероприятий, направленных на предупреждение и предотвращение несанкционированных проникновений, чрезвычайных ситуаций, противоправных действий, а также мер по минимизации их последствий (см. рис. 32).


*Рисунок 32. Общая схема инженерно-технической защиты объекта*

**Основные средства инженерно-технической защиты:**

1. Естественные и искусственные преграды (барьеры, заборы, ограждения), располагаемые по периметру территории, в стратегически важных зонах и на возможных путях проникновения и передвижения злоумышленников, оборудованные специальными средствами обеспечения пропускного режима и досмотра вносимого/выносимого имущества.

2. Системы контроля и управления доступом на объекты информатизации (СКУД).

3. Системы видеонаблюдения и охранно-пожарной сигнализации.

4. Использование дверных замков и запоров с биометрической идентификацией.

5. Средства защиты элементов зданий, помещений, коммуникаций (стен, окон, потолков, дверных конструкций, кабель-каналов, отопления, водопровода) от возникновения возможных каналов утечки информации.

6. Устройства зашумления и средства постановки контрпомех.

Под ПЭМИН понимают *паразитные электромагнитные излучения радиодиапазона* в окружающем пространстве и высокочастотные наводки на токопроводящие коммуникации, создаваемые устройствами, специальным образом для этого не предназначенными (средства ЭВТ, связи и т.д.).

*СЗИ от утечки по каналам ПЭМИН* подразделяются на активные и пассивные. Главным принципом защиты информации от утечки по каналам ПЭМИН является уменьшение отношения $\frac{\text{Информативный сигнал}}{\text{Шум}}$ на границе контролируемой зоны до значения, при котором техническое устройство зло-

умышленника не сможет выделить информативную составляющую. Пассивные устройства снижают уровень информативного сигнала, активные – повышают уровень шума.

*Пассивные средства защиты информации от ПЭМИН:*

– трансформаторы и фильтры;

– электромагнитные, электростатические (емкостные), магнитостатические (индуктивные) экраны;

– устройства одноточечного и многоточечного заземления.

*Активные средства защиты информации от ПЭМИН:*

– устройства пространственного зашумления;

– устройства активной маскировки;

– устройства линейного зашумления.

*Рисунок 33. Генераторы шума «Соната Р3», «ГАММА ГШ-18» и «Покров»*

*Рисунок 34. Клавиатура со сверхмалой зоной утечки «Фарватер-КВ1»*


*Рисунок 35. Программно-аппаратный комплекс защиты объектов информатизации от разведки ПЭМИ ЛГШ-504*

По аналогии с ПЭМИН средства акустической защиты от утечки речевой информации также можно разделить на пассивные и активные.

*Пассивные средства акустической защиты*:

– строительные и отделочные материалы звукоизоляции помещений;
– звукоизолирующие кабины;
– акустические экраны.

*Активные средства акустической защиты*:

– генераторы акустических помех в звуковом и ультразвуковом диапазоне;
– генераторы электрических помех и устройства активной маскировки в проводных линиях связи ВТСС;
– виброакустические излучатели активной маскировки;
– нелинейные локаторы закладок и детекторы диктофонов;
– ультразвуковые подавители прослушивающих устройств;
– помехоподавляющие фильтры сетей электропитания.


*Рисунок 36. Сетевые фильтры и подавители помех ФСПК-10 и ЛФС-40-1Ф*

*Рисунок 37. Устройство защиты цепей электросети и заземления SEL SP-44*

*Рисунок 38. Устройства обнаружения жучков и скрытых камер ХВ-68 и ST 033P*

*Рисунок 39. Ультразвуковые подавители диктофонов и микрофонов SEL-310 «КОМАР» и «Бубен-Ультра» в двух исполнениях*

*Рисунок 40. Комплекс акустической маскировки конфиденциальных переговоров «Комфорт-4»*

Акустический сейф предназначен для защиты речевой информации циркулирующей в местах пребывания владельца сотового телефона в случае его активизации с целью прослушивания.

*Рисунок 41. Акустический сейф «Ладья DM»*


*Рисунок 42. Устройство защиты акустической речевой информации от утечки по волоконно-оптической линии связи «Фотон-М»*


*Рисунок 43. Подавитель сигналов мобильной связи «Завеса-12СТ» и WiFi*

Для защиты речевой информации, циркулирующей в выделенных и защищаемых помещениях, от лазерных микрофонов, а также от просмотра с использованием оптико-электронных средств артикуляции говорящего человека используются защитные экраны, которые устанавливаются на окна.

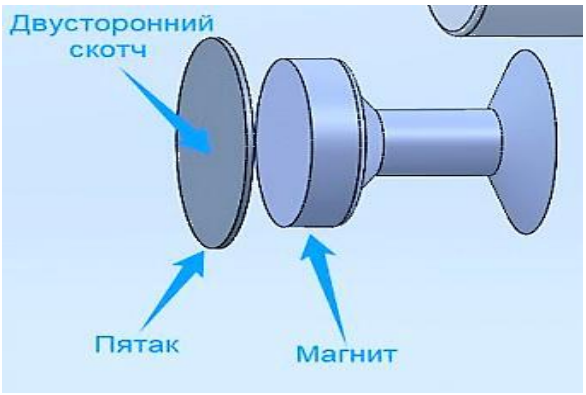


*Рисунок 44. Экран защитный «Пелена-256»*

Иногда бывает недостаточно защитить данные на внешних носителях, необходимо еще их гарантированно уничтожить без возможности восстановления.

*Рисунок 45. Устройство для хранения, транспортировки и экстренного уничтожения информации на магнитных носителях «Раскат» (Кейс)*

Сертификация средств защиты информации осуществляется на соответствие требованиям по безопасности информации, установленным нормативными правовыми актами ФСТЭК России, а также техническими условиями, техническим заданиям, заданиям по безопасности, согласованными заявителями на сертификацию с ФСТЭК России.

Государственный реестр сертифицированных средств защиты информации размещен на сайте ФСТЭК России в сети Интернет по адресу: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00.

## Вопросы для самоконтроля:

1. В чем выражается утечка (информации) по техническому каналу?
2. Из чего состоит технический канал утечки информации?
3. Какие сигналы называют опасными?
4. Какие технические средства могут быть источниками случайных опасных сигналов?
5. Что понимается под визуально-оптическими ТКУИ?
6. Что в радиоэлектронном канале утечки используется в качестве носителей информации?
7. Что является основными источниками информации материально-вещественного канала утечки информации?
8. Что такое защита информации от несанкционированного доступа?
9. Что такое защищаемое помещение?
10. Что такое основные технические средства и системы (ОТСС)?
11. Что такое канал связи?
12. Что такое стетоскоп?
13. Как образуется параметрический ТКУИ?
14. Как образуются электрические каналы утечки?
15. Что называется акустоэлектрическим преобразователем?
16. Какие случайные акустоэлектрические преобразователи относятся к наиболее распространенным?
17. Какие выделяют три вида паразитной связи?
18. Что называется радио- и радиотехнической разведкой?

# ГЛАВА 5.
# ОСНОВЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

## 5.1. Основные понятия криптографии. Кодирование

Криптографическая защита информации в АИС обычно применяется в ситуациях, где сложно или дорого обеспечить заданный уровень кибербезопасности организационно-техническими мерами, либо применение криптографических средств установлено требованиями к процессам передачи и хранения данных (например, электронная подпись в системах электронного документооборота).

*Криптография* (κρυπτός + γράφω, тайнопись) – это совокупность методов и средств скрытия информации в процессе ее передачи и хранения, а также обеспечения аутентичности информации (подлинности и неизменности) при ее передаче.

*Криптографические методы защиты информации* – это специальные методы преобразования информации, в результате которого ее содержание становится недоступным без предъявления ключа обратного преобразования.

*Криптоанализ* – это совокупность методов и средств раскрытия информации путем анализа криптографических систем. Методы криптографии и криптоанализа во многом схожи.

Способность криптосистемы противостоять возможным криптоаналитическим атакам называется ее *криптографической стойкостью.*

Абсолютно криптостойкой считается криптоситема, для взлома которой требуется неограниченное количество материальных ресурсов, вычислительных сверхмощностей и временных затрат, после которых исходная информация будет уже не актуальна.

Взаимосвязь криптографии и криптоанализа и общность методов привели к возникновению *криптологии* – науки о защите информации с помощью математических преобразований (см. рис. 46).


*Рисунок 46. Связь криптографии, криптоанализа и криптологии*

Современная криптология базируется на математических дисциплинах, таких как модульная арифметика, линейная алгебра, теория групп, полугрупп, теория автоматов, математический анализ, теория дискретных функций, теория чисел, комбинаторный анализ, теория вероятностей и математическая стати-

стика, теория кодирования, теория информации, теория сложности вычислений. Соответственно, большинство криптографических систем описываются математическими моделями.

Любая информация в процессе ее обработки, передачи или хранения представляется в форме знаковой последовательности. Упорядоченное множество знаков (набор знаков), принятых для конкретной формы представления информации, называется *алфавитом*. Русский алфавит в информатике называется *кириллицей*. Цифровой алфавит машинных кодов (слов) состоит из двух знаков *0* и *1*.

Отношение исходного алфавита и конечного алфавита в ходе криптографического преобразования может быть задано словесным описанием, графическим отображением, кодовой таблицей или математической функцией y = f (x).

Основные *методы криптографии:*

- кодирование;
- шифрование;
- маскирование;
- хеширование.

*Кодирование (encoding)* – это процесс взаимно-однозначного обратимого преобразования информации посредством замены знаков одного алфавита на соответствующие знаки другого алфавита или их перестановки в пределах исходного алфавита.

Примером простейшего кодирования является присвоение символам алфавита их порядкового номера (а-1, б-2, в-3,…).

Другим примером служит транслитерация или перевод русских букв в английские буквы или их сочетания. ГОСТ Р 52535.1-2006 для загранпаспортов обеспечивает однозначность преобразования в обе стороны (см. рис. 47).

| А | Б | В | Г | Д | Е | Е | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ы | Э | Ю | Я |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | V | G | D | E | E | ZH | Z | I | I | K | L | M | N | O | P | R | S | T | U | F | KH | TS | CH | SH | SH CH | Y | E | IU | IA |

*Ющина Жанна Яковлевна ⇒ IUshchina ZHanna IAkovlevna*

*Рисунок 47. Транслитерация кириллицы для загранпаспорта*

Текстовые сообщения можно также посимвольно передавать с помощью звуковых сигналов или графических образов (см. рис. 48).

*Ющина Жанна Яковлевна*

*Рисунок 48. QR-код*

Системы текстовой кодировки, принятые в компьютерах, сопоставляют символьные наборы с одно- или двухбайтовыми двоичными кодами.

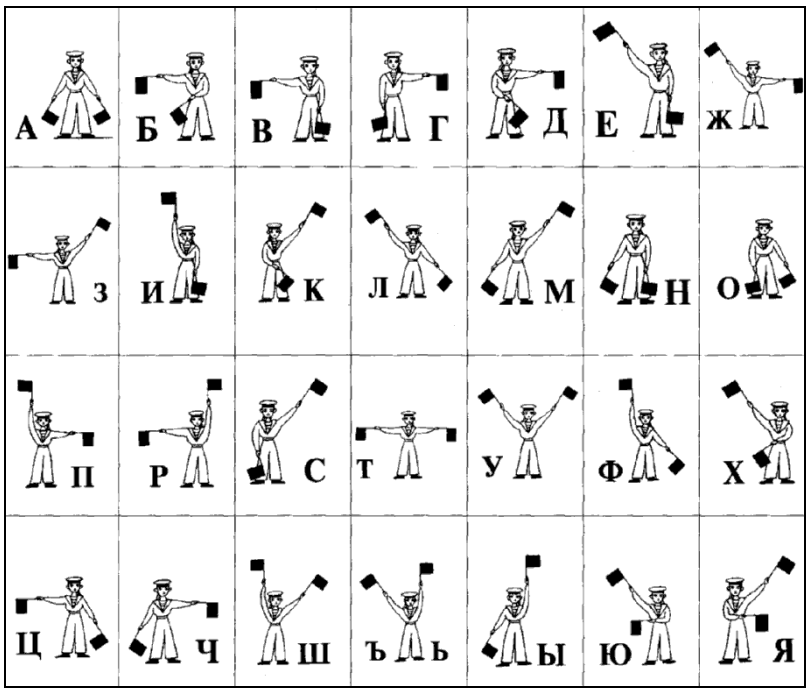


*Рисунок 49. Русская семафорная азбука, принятая на флоте*

| Символ | Unicode | | UTF-8 | | Windows-1251 |
|---|---|---|---|---|---|
| | 16-ричн. | 10-тичн. | 16-ричн. | 10-тичн. | |
| **А** | 0410 | 1040 | D090 | 208 144 | 192 |
| **Б** | 0411 | 1041 | D091 | 208 145 | 193 |
| **В** | 0412 | 1042 | D092 | 208 146 | 194 |
| **Г** | 0413 | 1043 | D093 | 208 147 | 195 |
| **Д** | 0414 | 1044 | D094 | 208 148 | 196 |
| **Е** | 0415 | 1045 | D095 | 208 149 | 197 |
| **Ж** | 0416 | 1046 | D096 | 208 150 | 198 |
| **З** | 0417 | 1047 | D097 | 208 151 | 199 |
| **И** | 0418 | 1048 | D098 | 208 152 | 200 |
| **Й** | 0419 | 1049 | D099 | 208 153 | 201 |
| **К** | 041A | 1050 | D09A | 208 154 | 202 |

*Рисунок 50. Наиболее известные кодировки*

*Раскодирование, декодирование (decoding)* – обратный кодированию процесс, направленный на восстановление исходного сообщения.

Простое кодирование заменой одного знака на другой без дополнительного секретного ключа в криптографии практически не используется. Если таблица кодов или алгоритм преобразования не меняется, то взломать подобную систему кодирования можно за считанные часы без применения компьютера.

Классические криптографические системы обычно состоят из открытых правил преобразования информации и специальных параметров (ключей), которые в этих правилах обеспечивают тайную часть скрытия/раскрытия информации.

## 5.2. Основные понятия криптографии. Шифрование

*Кодирование с ключом* уже считается *шифрованием*. В качестве ключа в общем случае может быть что угодно.

*Шифр (cipher)* – криптографический метод скрытия информации путем обратимых преобразований, зависящих от некоторого секретного параметра (ключа). Шифры обычно включают алгоритм *зашифрования* и алгоритм *расшифрования*.

*Открытый текст (plaintext)* – незашифрованная информация.

*Шифрование (encryption)* – преобразование открытого текста с целью скрытия его содержания.

*Шифротекст (ciphertext)* – данные, полученные в результате шифрования открытого текста.

*Расшифрование, дешифрование (decryption)* – операция, обратная шифрованию (см. рис. 51).

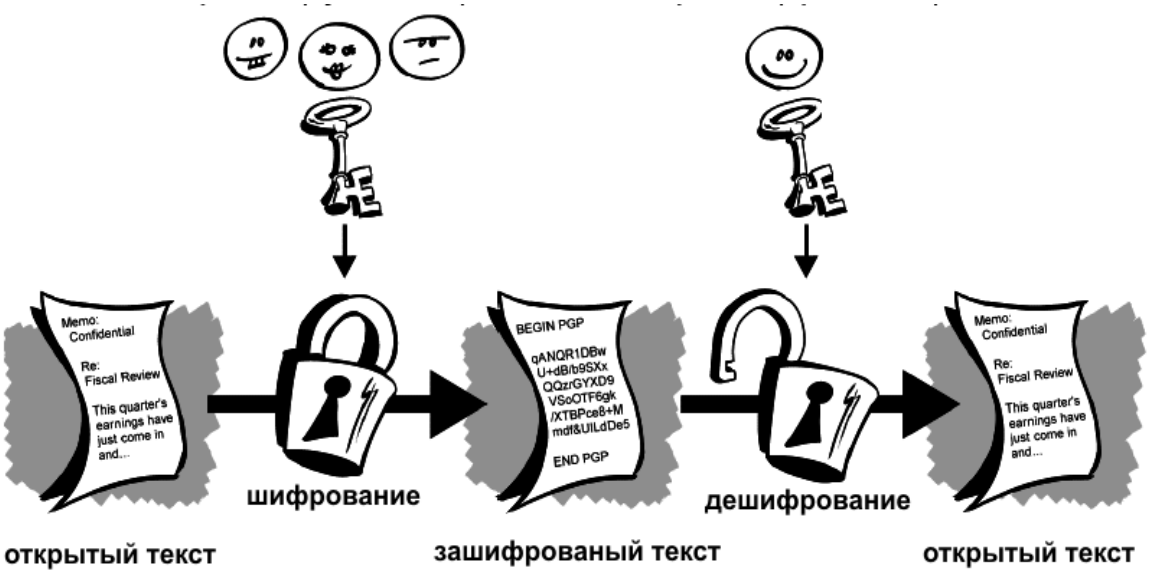


*Рисунок 51. Универсальная модель криптографической защиты*

Появление первых моноалфавитных шифров, которые использовали замену знаков одного алфавита на кодовые знаки другого, относят к 3-му тысячелетию до н.э. Позднее появились шифры перестановки, в которых скрытие текста осуществляется посредством изменения исходного порядка следования знаков.

Например, шифрование с помощью *скиталы (σκυτάλη)* – многогранного жезла, на который по спирали наматывалась полоска пергамента. Текст писался на пергаменте вдоль жезла, после чего полоска разматывалась (см. рис. 52).


*Рисунок 52. Скитала*

*Принцип шифрования с помощью скиталы можно описать следующей математической моделью*.

Зашифрованное с помощью скиталы сообщение – это последовательность знаков обычного письменного алфавита, в котором к исходному сообщению принадлежат только знаки с порядковым номером в строке:

n (i) = k * i, где

k – ключ шифра, равный количеству символов в одном обороте вокруг жезла;

i = 0, 1, 2 … – количество витков, зависящее от длины жезла.

Пользуясь символами русского алфавита, зашифруем с помощью модели скиталы сообщение: *ШИФР*

Пусть диаметр жезла позволяет разместить на одном витке условной ленты k = 6 знаков.

Расставим на условной ленте знаки исходного сообщения:

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ш | | | | | | И | | | | | | Ф | | | | | | Р | | |

Затем заполним оставшиеся позиции произвольными знаками русского алфавита:

Ш В Л И Р Д И Н Р Е К У Ф Ц М Н В Ф Р Ы Ц

Расшифровка осуществляется в обратном порядке.

Условный маркер устанавливается на первую позицию, и это будет первый знак сообщения. Затем к нему добавляется каждый шестой знак.

Иногда в математической модели скиталы используется дополнительная константа-ключ, устанавливающая смещение первого знака исходного сообщения от начала шифрованного текста.

Очевидно, что, зная модель шифрования и язык алфавита, прочитать зашифрованное скиталой сообщение достаточно легко даже без жезла.

*Книжные шифры* основаны на использовании обоими участниками переписки одной и той же заранее оговоренной книги в качестве ключа. Конкретный механизм шифрования может варьироваться от более простого, когда каждая буква кодируется номером страницы/строки/знака в строке, до более сложного, когда текст из книги используется как гамма-последовательность символов, используемая для шифрования текста.

В стихотворном шифре ключом является заранее оговоренное стихотворение, которое записывается в прямоугольник согласованного размера. Этот прямоугольник является ключевой страницей книжного шифра.

*Решетка Кардано* – таблица-трафарет, которая накладывается на лист бумаги для записи слов исходного текста в вырезанные ячейки. Оставшиеся пустые места для маскировки заполняются произвольным текстом в том же формате. В идеале зашифрованное сообщение должно выглядеть как осмысленный текст (см. рис. 53).

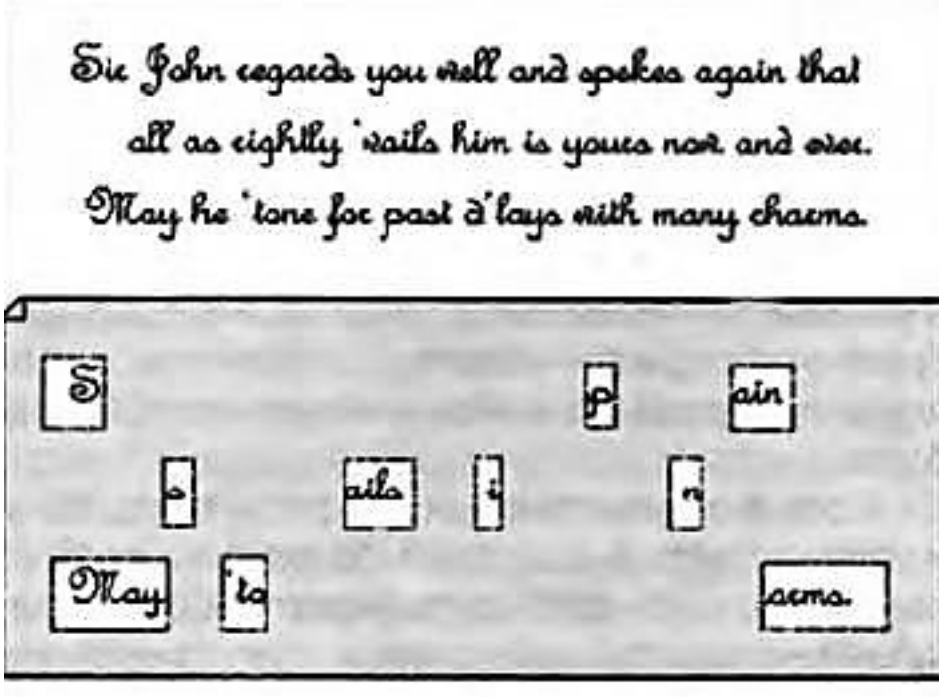


*Рисунок 53. Решетка Кардано*

Существуют варианты решетки Кардано с посимвольным заполнением и поворотом. После заполнения вырезанных ячеек в одном положении, решетка поворачивается по часовой стрелке на 180 или 90 градусов. Вырезанные ячейки в новом положении должны попасть на пустые места, которые также можно заполнить полезным текстом. В отличие от классического варианта Кардано, при данном способе сразу бросается в глаза сам факт шифрования (см. рис. 54).

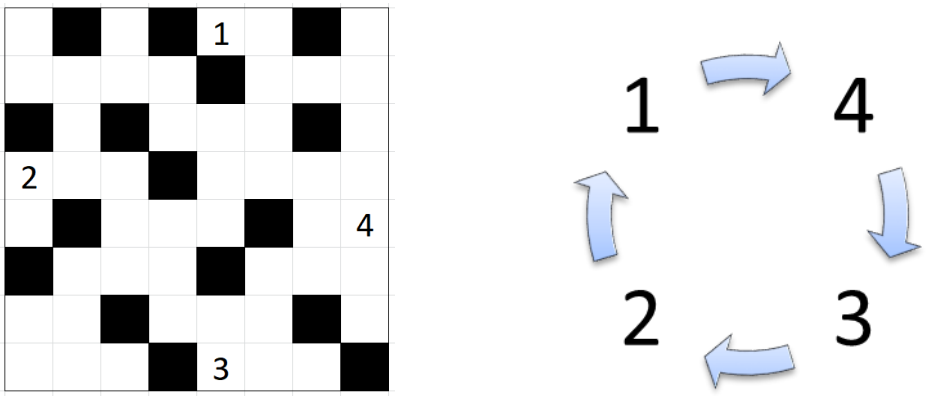


*Рисунок 54. Решетка Кардано 8x8 с возможностью 4 поворотов на $90^0$*

В шифре *табличной маршрутной перестановки* исходный (открытый) текст записывается последовательно по строкам заданной таблицы, начиная с первой ячейки (см. рис. 55).

Например, размерность таблицы 5×6. Шифрованный (скрытый) текст формируется последовательно сверху вниз по столбцам в порядке, заданном ключом, например, {3, 4, 2, 5, 1}.

| 3 | 4 | 2 | 5 | 1 |
|---|---|---|---|---|
| Т | А | Й | Н | О |
| Е | В | С | Е | Г |
| Д | А | С | Т | А |
| Н | О | В | И | Т |
| С | Я | Я | В | Н |
| Ы | М | А | Б | В |

*Рисунок 55. Таблица перестановок*

В результате получим текст:

ОГАТНВЙССВЯАТЕДНСЫФВАОЯМНЕТИВБ.

Зная ключ и размерность таблицы, расшифровать текст довольно легко. Нужно записать его последовательно по столбцам, пронумерованным в соответствии с ключом, и прочитать по строкам.

Альтернативой шифрам перестановки являются *шифры подстановки*, когда знаки открытого текста заменяются на другие знаки того же или другого алфавита в соответствии с некоторым правилом. Другими словами, знаки исходного текста не меняют свою последовательность, а изменяются сами. Простейший шифр подстановки можно получить, печатая русскими буквами в английской раскладке клавиатуры компьютера.

В качестве другого известного примера можно привести *шифр Цезаря* (см. рис. 56). Процесс шифрования заключается в замене каждой буквы исходного текста на другую букву из этого же алфавита, но отстоящую от исходной на заданное количество позиций вправо или влево. Причем при сдвиге цепочка

символов замыкается, т.е. за последним символом следует первый. Раскрытие шифротекста осуществляется соответственно обратным сдвигом.

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| А | Б | В | Г | Д | Е | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я |
| ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ |
| Г | Д | Е | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 0 | 1 | 2 |

*ЮЩИНА ЖАННА ЯКОВЛЕВНА ⇒ БЬЛРГ ЙГРРГ ВНСЕОИЕРГ*

*Рисунок 56. Шифр Цезаря с ключом +3*

С одной стороны, шифр Цезаря можно рассматривать как простое кодирование путем прямого отображения одного алфавита на другой, и при разных ключах можно формировать табличное отношение.

С другой стороны, если символы алфавита пронумеровать, начиная с 0, то шифрование и дешифрование можно выразить формулами модульной арифметики:

$y = (x + k) \bmod n;$ $x = (y - k) \bmod n,$

где y – символ шифротекста, x – символ открытого текста, k – ключ, n – мощность алфавита.

В отличие от шифров сдвига в шифрах замены исходному алфавиту соотносится тот же набор символов, но не сдвинутых, а переставленных по какому-то правилу. Причем, моноалфавитные шифры замены также легко взламываются путем анализа частоты использования символов или устойчивых для данного языка символьных комбинаций.

В основе *шифра Виженера* лежит матрица из алфавитных строк, расположенных друг под другом и циклически сдвинутых на одну позицию влево, как в шифре Цезаря с ключом – 1 (иногда этот частный случай называют *шифром ROT1*). Таким образом, в каждой строке матрицы набор знаков один и тот же, но упорядочены они по-разному, следовательно, речь уже идет о *полиалфавитной криптосистеме*. Например, для русского языка в матрице будут 32 алфавита замены (вместо «е» в шифрах обычно используют букву «е»). Размерность квадратной матрицы совпадает с мощностью исходного алфавита, а названия строк и столбцов совпадают с его первыми буквами.

*Гаммирование или шифр XOR* – метод, при котором шифротекст формируется как битовая строка, где каждый бит является результатом сложения по модулю 2 (XOR) соответствующих битов из открытого текста и псевдослучайной последовательности. Ключевая последовательность псевдослучайных битов (гамма) определяется для шифрования/дешифрования каждого нового сообщения. Сложение по модулю 2 примененное к шифротексту и гамме восстанавливает исходный открытый текст (см. рис. 57).

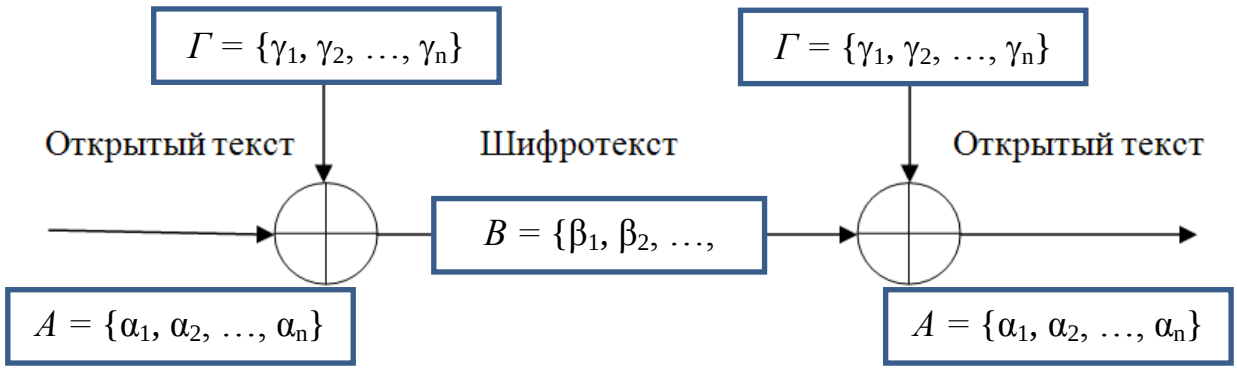


*Рисунок 57. Схема шифра XOR*

Для удобства использования шифров замены, а также повышения их криптоустойчивости были созданы шифровальные механические устройства. Например, диск с двумя алфавитами, один из которых в соответствии с кодовой фразой-ключом сдвигался относительно другого при выбора очередной буквы шифротекста (см. рис. 58).


*Рисунок 58. Шифродиск, использовавшийся во время гражданской войны в США*

Наиболее известным представителем шифровальных устройств с полиалфавитным шифром замены является «Энигма».

*«Энигма» (Änigma, загадка)* – переносная электромеханическая шифровальная машина, использовавшаяся для обмена секретными сообщениями в первой половине XX века. В семействе «Энигма» было выпущено около 100 000 шифровальных машин различной модификации, созданных на основе первоначальной модели Артура Шербиуса, запатентованной в 1918 году. Высокая надежность и криптоустойчивость «Энигмы» способствовали ее широкому применению в военной и коммерческой сфере в разных странах, включая нацистскую Германию.

«Энигма» была сконструирована из механических и электрических компонентов. Механическая часть включала в себя клавиатуру, набор коммутационных дисков, размещенных на одной оси, и ступенчатого механизма вращения этих дисков при каждом нажатии на клавишу. Электрическая часть состояла из схемы, соединяющей клавиатуру, коммутационную панель, лампочки и скользящие контакты дисков (см. рис. 59).

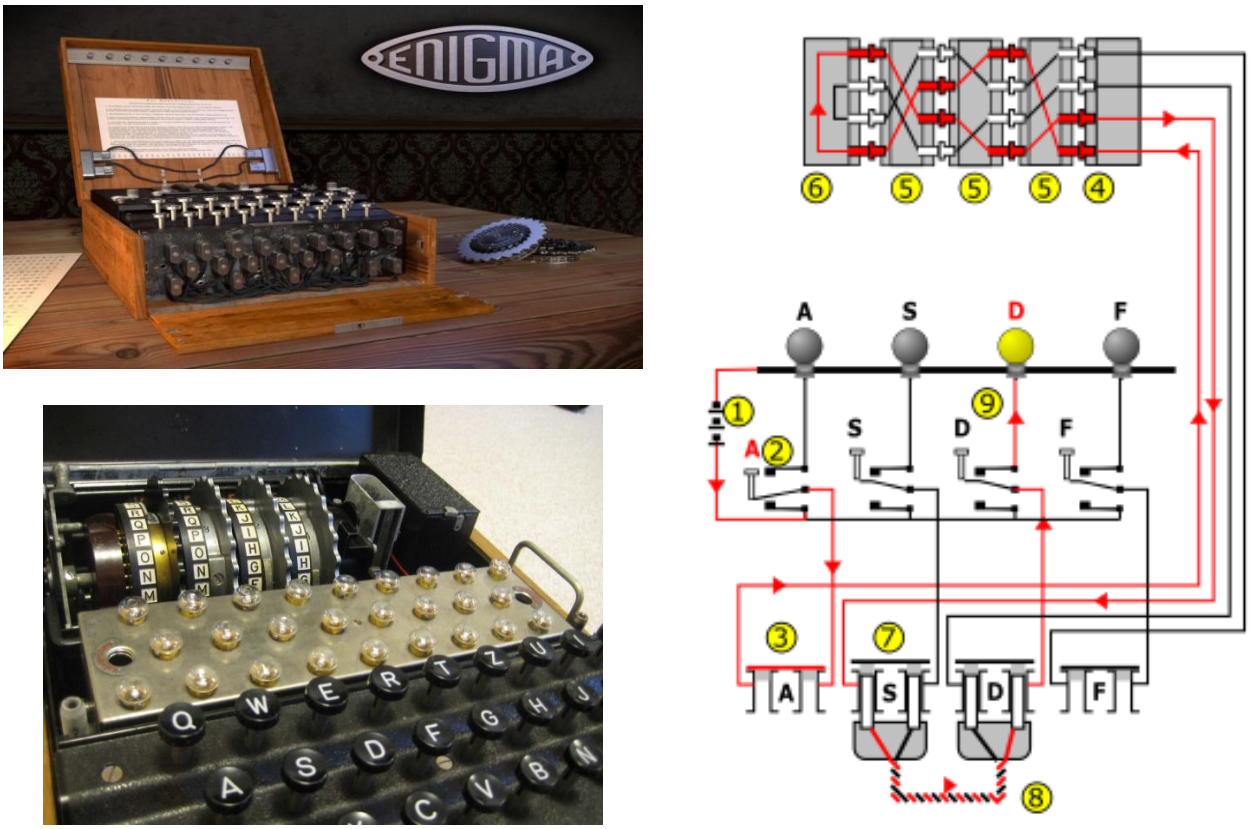


*Рисунок 59. «Энигма» и ее схема коммутации для 4 букв английского алфавита*

Перед началом шифрования устанавливалась стартовая позиция алфавитных колес и перемычки на коммутационной панели. При каждом нажатии на клавишу роторы сдвигаются, в результате чего образуется новая электрическая цепь, зажигающая лампочку у соответствующей буквы.

При нажатии клавиши с буквой А на барабане прокручиваются роторы 5, замыкается переключатель 2, и ток от батареи 1 поступает в коммутационную панель, которая с помощью сменных перемычек позволяет создавать разные цепи между клавишами клавиатуры и контактами неподвижного входного колеса. В данном примере ток проходит через разъем коммутационной панели 3 (А), не имеющий перемычки. Далее ток подается на неподвижный входной диск 4, находящийся на одной оси с тремя (на флоте – четырьмя) дисками-роторами (5), проходит сквозь электрическую цепь, образованную контактами роторов, и от рефлектора (6) через роторы возвращается на входное колесо, но уже по другой цепи. С входного колеса ток идет на разъем коммутационной па-

нели 7 (S), соединенный с разъемом 8 (D) перемычкой и через переключатель 9 зажигает лампочку D.

Ключами в «Энигме» служили сменные диски-роторы, которые прошивались по-разному для разных сетей связи, а также коммутационная панель, перемычки которой устанавливались шифровальщиками вручную в соответствии с инструкцией. Каждый ротор имел по 26 контактов на каждой стороне, соединенных друг с другом проводами произвольным образом. При нажатии буквенной клавиши первый ротор автоматически поворачивался на одну позицию, создавая новую цепь коммутации. После совершения полного оборота первым ротором на одну позицию прокручивался второй ротор, а после оборота второго – третий. Таким образом, внутренняя топология электрической схемы менялась с каждым нажатием буквы открытого текста.

*Во время 2-й Мировой войны в немецкой армии каждой машине «Энигма» регулярно назначались свои настройки на определенный период времени или на один сеанс передачи.*

Шифр «Энигмы» симметричен, и для обмена шифрованными сообщениями было достаточно иметь машины с дисками одинаковой прошивки, знать их стартовое расположение и настройки коммутационной панели. Процесс подготовки сообщения для передачи состоял в том, что шифровальщик настраивал «Энигму» в соответствии с инструкцией на определенный день, нажимал последовательно кнопки с символами открытого текста и по индикации лампочек определял символы шифротекста. Затем радист передавал шифротекст с помощью азбуки Морзе. На принимающей стороне коды Морзе преобразовывались в шифротекст, который вводился в «Энигму» с такими же ключевыми настройками и адресат получал исходный текст.

## 5.3. Основные понятия криптографии. Маскирование

Шифрование помогает сохранять данные в секрете, но шифротекст при этом привлекает лишнее внимание. Если сообщение так просто не прочитать, значит, в нем наверняка есть что-то ценное. Поэтому довольно часто бывает важно скрыть само наличие секретной информации.

*Маскирование информации* – процесс скрытия информации путем ее обратимой подмены или смешивания с другой информацией.

*Стеганография* – самостоятельное направление тайнописи, где скрывается сам факт наличия защищаемого сообщения.

Не вдаваясь в исторические подробности и древние способы маскировки посланий, в рамках данного курса будет целесообразно рассмотреть *цифровую стеганографию*, которая как наука возникла в середине XX в. на базе теории информации.

Цифровую стеганографию можно разделить на три больших направления. Первое – это собственно тайнопись или скрытие сообщений внутри файлов-контейнеров текстового, графического или мультимедиа формата. После запол-

нения сообщением контейнер внешне не меняется и полностью сохраняет свою функциональность.

Второе направление изучает методы добавления к сообщению скрытых стегометок (stegomarks), позволяющих впоследствии доказать его принадлежность конкретному автору, как личное клеймо. Например, стегометки записываются в цифровые фотографии.

Третье направление отвечает за внедрение уникальных для каждого сообщения цифровых отпечатков (digital fingerprints) или водяных знаков (digital watermark). Они служат в основном для защиты интересов правообладателей, позволяя обеспечить оригинальность контента. К примеру, многие интернет-магазины внедряют цифровые отпечатки в продаваемые книги и музыкальные композиции. В них кодируется информация о дате продажи и аккаунте купившего (имя, IP-адрес и прочее). Если купленные файлы позже появятся среди торрентов или на файлообменниках, то правообладатели смогут установить источник утечки. Для этого будет достаточно считать из контрафактного файла вкрапленный цифровой отпечаток.

Стеганографию эффективнее всего использовать не вместо шифрования, а вместе с ним. Такое сочетание позволяет скрыть как саму информацию, так и факт ее хранения или передачи.

Например, профессиональный программный продукт OpenPuff поддерживает двойную защиту: скрытие данных в файле и подписывание файла цифровым кодом (см. рис. 60).

OpenPuff работает с такими форматами, как:

– изображения (BMP, JPG, PCX, PNG, TGA);
– аудио (AIFF, MP3, NEXT/SUN, WAV);
– видео (3GP, MP4, MPG, VOB);
– Adobe flash (FLV, SWF, PDF).

Скрытые данные (до 256 МБ) распределяются между цепочкой заданных файлов и шифруются с использованием трех 256-битных ключевых фраз.

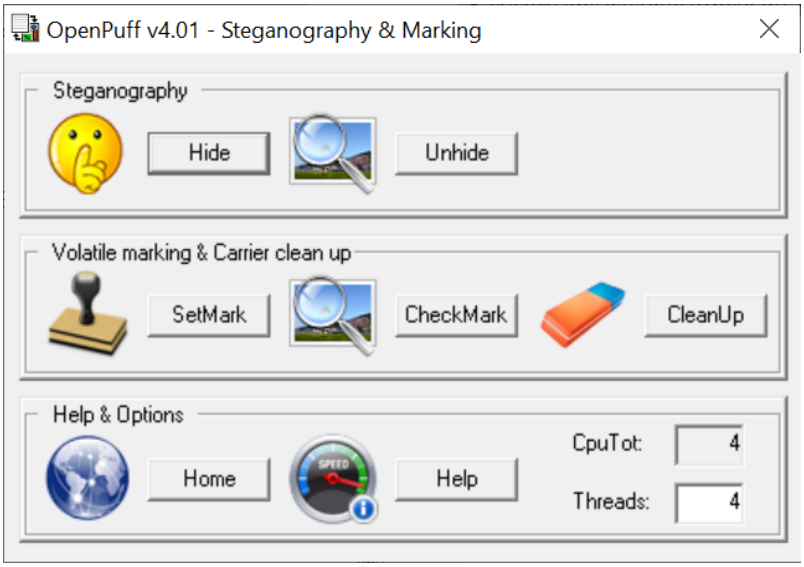


*Рисунок 60. Стеганографическая утилита OpenPuff*

## 5.4. Основные понятия криптографии. Хеширование

*Хеширование* – процесс преобразования открытого текста в хэш-код.

*Хэш-код (hash-code)* – строка бит, являющаяся выходным результатом хэш-функции.

*Хэш-функция (collision-resistant hash-function)* – функция, отображающая строки бит произвольной длины в строки бит фиксированной длины и удовлетворяющая следующим свойствам:

– по хэш-коду сложно вычислить исходные данные, отображаемые в это значение;

– для заданных исходных данных сложно вычислить другие исходные данные, отображаемые в тот же хэш-код;

– сложно вычислить какую-либо пару исходных данных, отображаемых в один и то же хэш-код.

*Хеширование (hashing)* – криптографическое преобразование исходного массива данных произвольной длины в выходную битовую строку фиксированной длины. Такие преобразования также называются *хеш-функциями* или функциями свертки, а их результаты называют *хешем*, *хеш-кодом* или *сводкой сообщения (message digest)*.

Хеш-коды применяются в качестве уникальных идентификаторов наборов данных при формировании ассоциативных массивов, контрольных кодов для проверки данных при передаче, образов паролей доступа при их хранении, кодов исходных сообщений для электронной подписи и т.п. В криптовалютных операциях присутствует множество этапов, которые реализуются с помощью хэш-функций: майнинг, проверка баланса, связывание входов и выходов транзакций, хеширование всех операций в блоке для формирования дерева Меркла.

Очевидно, что количество неповторяющихся значений хеш-функций значительно меньше, чем количество вариантов исходных наборов данных, и возможны совпадения хеш-кодов.

*Принцип Дирихле (комбинаторика*) – если кролики рассажены в клетки, причем число кроликов больше числа клеток, то хотя бы в одной из клеток находится более одного кролика. То есть фиксированные ограничения на выход означают, что существует фиксированная степень перестановок, на которых возникнет коллизия. Вероятность возникновения подобных коллизий отражает качество алгоритмов хеш-функций.

Свойства хеш-функции:

– хеш-функция является детерминированной, т.е. одно и то же сообщение приводит к одному и тому же хеш-коду;

– хеш-функция является необратимой, т.е. по хеш коду нельзя восстановить исходное сообщение;

– минимальная вероятность существования двух разных сообщений с одинаковым хеш-кодом;

– значение хеш-функции быстро вычисляется для любого сообщения;

– хеш-функция должна противостоять всем известным типам криптоаналитических атак;

– любое изменение исходного сообщения приводит к существенному изменению хеш-кода.

Длина хеш-кода зависит от алгоритма хеширования, например SHA-2 (Secure Hash Algorithm) объединяет семейство алгоритмов: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/256 и SHA-512/224, где число в названии отражает фиксированную длину битовой строки на выходе.

В таблице ниже представлены шестнадцатеричные хеш-коды вариантов текста, пропущенного через алгоритм хеширования SHA-256, который используется в криптовалюте.

| | |
|---|---|
| андрей | 6992DD2D09A63C039C93728FDCEBA18FCCD4F16CABE2E0188E4DBD87FC1ACA6D |
| Андрей | 7951B5AB1EADA31D7E5425AD3A4FF50E63A592411666EC597057DB5C2A4CCF1D |
| Андрей Александрович | 67D79D5CB18CEFB74D5C6549A149E974598B81F62E0E50DBD63142647EA232CF |

Независимо от исходных текстов, в каждом все хеш-коде 256 бит (64 шестнадцатеричные цифры) и все хеш-коды существенно отличаются. Вероятность повторения хеш-кода на другом входном наборе – очень малая величина ($2^{-256}$).

## 5.5. Современные методы и средства криптографической защиты конфиденциальной информации

Методы и средства криптографической защиты информации нацелены обеспечить конфиденциальность, подлинность (аутентичность) и целостность информации.

При зашифровывании информации может использоваться один общий ключ, а могут два – один для скрытия, другой для расшифровывания.

*Криптографический ключ (криптоключ)* – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптосистеме.

*Ключевая информация* – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

*Ключевые документы* – электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах.

Для криптографических преобразований СКЗИ (шифрование, электронная подпись) используется ключевая информация, а людям выдаются ключевые документы, ее содержащие.

*Ключевой носитель* – физический носитель определенной структуры, предназначенный для размещения и хранения на нем ключевой информации и/или инициализирующей последовательности.

Криптосистемы с одним секретным ключом (Secret Key Systems), общим для шифрования и расшифровывания сообщений, принято называть *симметричными*.

Криптосистемы с открытым (публичным) и закрытым (приватным) ключами, функционально связанными друг с другом, называют *ассиметричными* (Open Key Systems) (см. рис. 61).

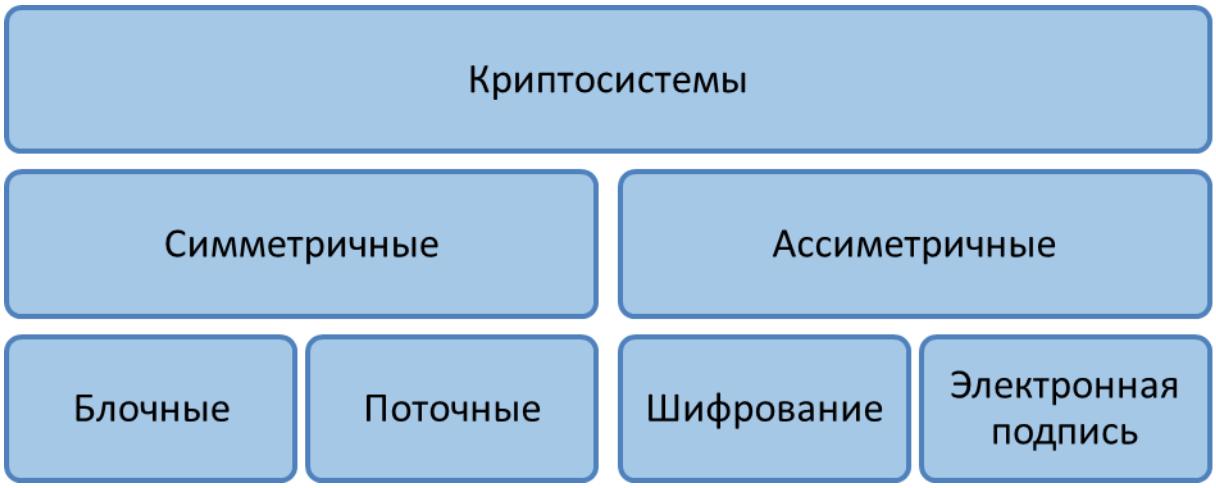


*Рисунок 61. Классификация криптосистем*

*Симметричные криптосистемы* используют два вида шифров:

– блочные шифры, которые разбивают открытый текст на блоки фиксированной длины (64, 128, 256 бит) и затем каждый блок зашифровывается;

– поточные шифры, в которых преобразование каждого символа открытого текста в символ шифрованного текста зависит не только от используемого ключа, но и от его позиции в текстовой строке (например, на открытый текст накладывается гамма-код).

Симметричные системы обладают относительно высоким быстродействием, но есть проблема – передача участникам обмена секретного ключа. Если передавать секретный ключ по незащищенным каналам, его могут перехватить и получить доступ к зашифрованным данным.

*Асимметричные* криптографические системы с открытым ключом применяются как для шифрования информации, так и для электронной подписи (ЭП), причем в обоих случаях открытый ключ передается участникам обмена по открытому каналу.

Для получения сообщения владелец сертификата ключей отправляет открытый ключ своим корреспондентам, количество которых не имеет значения. Автор сообщения зашифровывает свой конфиденциальный контент открытым

ключом, после чего, независимо от способа передачи, прочитать шифротекст может только владелец закрытого ключа.

При формировании электронной подписи владелец пары ключей применяет закрытый ключ и направляет подписанное сообщение адресатам вместе с открытым ключом для проверки аутентичности.

*Инфраструктура открытых ключей* – набор принципов, методов и средств, позволяющих управлять процессами шифрования с открытым ключом.

**Виды средств криптографической защиты информации (СКЗИ):**

1. *Средства шифрования* – программно-аппаратные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации от НСД при ее обработке, передаче и хранении.

2. *Средства имитозащиты* – программно-аппаратные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для обеспечения ее целостности и защиты от навязывания ложной информации.

3. *Средства электронной (цифровой) подписи* – аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций:

– создание электронной подписи с использованием закрытого ключа;

– подтверждение подлинности электронной подписи с использованием открытого ключа;

– создание закрытых и открытых ключей электронной подписи.

4. *Средства кодирования* – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций.

5. *Ключевые документы и средства изготовления ключевых документов* (независимо от вида носителя ключевой информации).

## Вопросы для самоконтроля:

1. Какие используются криптографические методы симметричного шифрования?
2. В чем заключается принцип действия метода симметричного шифрования «Гаммирование»?
3. Что содержит понятие метода симметричного шифрования «Перестановки»?
4. В чем заключается метод симметричного шифрования «Подстановка»?
5. В чем заключается принцип действия асимметричных методов шифрования в целях обеспечения конфиденциальности передаваемого сообщения?
6. Какие существуют достоинства и недостатки симметричной и асимметричной систем шифрования?
7. В чем заключается метод симметричного шифрования «Блочные шифры».
8. Что такое электронная подпись?
9. Какие существуют разновидности мошенничества с электронными подписями?
10. Что такое инфраструктура открытых ключей?

# ГЛАВА 6.
# РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ КИБЕРБЕЗОПАСНОСТИ И ИХ ОБРАБОТКА

## 6.1. Понятие инцидента кибербезопасности

*Мониторинг КБ* – процесс постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления нарушений безопасности информации, компьютерных атак и компьютерных инцидентов.

*Событие КБ* – идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики КБ или неработоспособность защитных мер, а также возникновение неизвестной ранее ситуации, которая может иметь отношение к КБ.

*Инцидент КБ* – непредвиденное или нежелательное событие КБ, которое привело к негативным последствиям для активов организации (см. рис. 62).

*Компьютерный инцидент* – факт нарушения и (или) прекращения функционирования информационного ресурса и (или) нарушения безопасности, обрабатываемой таким информационным ресурсом информации, в том числе произошедший в результате компьютерной атаки.

***События КБ возникают*** как после преднамеренных попыток нарушения конфиденциальности, целостности и доступности информационных активов, так и после случайных ошибок вполне лояльных пользователей, и сам факт события КБ еще не означает, что попытка завершилась успешно и привела к инциденту КБ. С другой стороны, типовые политики и соответствующие меры КБ не могут обеспечить стопроцентную защиту ИР и ПТС АИС организации, поэтому управление инцидентами КБ – это процесс планомерный, непрерывный, динамически развивающийся.


*Рисунок 62. Анализ инцидента КБ*

*Основными задачами управления инцидентами КБ* являются:

– обеспечение непрерывности деятельности организации;

– обнаружение и анализ всех событий КБ, выявление среди них инцидентов КБ, оповещение заинтересованных лиц;

– оценка и классификация идентифицированных инцидентов КБ в целях наиболее эффективного реагирования;

– результативное реагирование на инциденты КБ, включая активацию мер для их предотвращения, минимизации ущерба и полнофункционального восстановления;

– всестороннее изучение КБ и извлечение выводов с целью выработки превентивных защитных мер и корректировке общего подхода к менеджменту инцидентов КБ.


*Рисунок 63. Этапы цикла управления инцидентами КБ*

Процесс решения задач управления инцидентами КБ – это циклическая последовательность действий, направленных на улучшение качества структурных компонентов системы КБ (см. рис. 63).

**Действия на этапе планирования управления инцидентами КБ**:

– документирование политики обработки сообщений о событиях и инцидентах КБ и системе, соответствующей этой политике (включая родственные процедуры);

– создание подходящей структуры менеджмента инцидентов КБ в организации и подбор соответствующего персонала;

– создание программы обучения и проведения инструктажа с целью обеспечения осведомленности о менеджменте инцидентов.

*Группа реагирования на инциденты КБ (далее – ГРИКБ)* формируется из профессионально подготовленных и доверенных сотрудников организации, а также внешних экспертов, например, для реагирования на специфические кибер-инциденты. После завершения этого этапа организация должна быть полностью готова к надлежащей обработке инцидентов КБ.

**Действия на этапе реагирования на инциденты КБ:**

1. Автоматическое или обнаружение непосредственно пользователем события ИБ, оповещение о нем уполномоченных лиц (например, сигналом тревоги от межсетевого экрана или устно по телефону).

2. Сбор и первичная оценка информации о событии КБ, проводимая эксплуатационным персоналам АИС, принятие решения, является ли событие инцидентом КБ или ложным сигналом тревоги.

3. Квалифицированная оценка события КБ специалистами ГРИКБ и немедленное реагирование в случае инцидента КБ, при необходимости, проведение правовой экспертизы и защитных действий по дальнейшей обработке информации.

4. Анализ ГРИКБ о возможности контроля над инцидентом КБ:

– в положительном случае продолжение действий по реагированию на инцидент КБ, сбор и подготовка информации для анализа последствий инцидента КБ;

– при отсутствии контроля уведомление руководства и антикризисные действия, предусмотренные политикой безопасности для обеспечения непрерывности деятельности организации;

5. Расширение круга заинтересованных лиц для дальнейших оценок и/или принятия решений в соответствии с политикой безопасности.

6. Регистрация принятых мер (всеми причастными лицами, в особенности членами ГРИКБ) для дальнейшего анализа.

7. Обеспечение сбора и защищенного хранения свидетельств в электронном виде и постоянного мониторинга защищенного хранения этих свидетельств на случай их востребованности для судебного преследования или внутреннего дисциплинарного разбирательства.

8. Поддержка режима контроля изменений, включая отслеживание инцидентов КБ и обновления отчетов по инцидентам с тем, чтобы база данных событий/инцидентов КБ постоянно соответствовала действительности.

После обнаружения события КБ и оповещения о нем типовыми задачами менеджмента являются:

– обеспечение формальных процедур реагирования на событие КБ и актуализация информации о нем, включая оценку ущерба;

– оценка принятых решений и действий лиц, ответственных и просто причастных к событию КБ;

– документирование информации о событии КБ и ведение базы данных в установленном порядке.

Вся собранная информация, касающаяся событий КБ, должна храниться в базе данных (событий/инцидентов КБ), сопровождаемой ГРИКБ. Вносимая в базу информация должна быть полной и достоверной для обеспечения качественной информационной поддержки принятия решений и результативного противодействия выявленным инцидентам КБ в дальнейшем.

После принятия решения о закрытии инцидента КБ необходимо провести углубленную экспертизу принятых мер, извлечь выводы и выработать рекомендации по улучшению всей *системы КБ организации*, в частности.

**Действия на этапе анализа инцидентов КБ:**

1. Правовая экспертиза.

2. Подготовка выводов о необходимости внесения изменений:

– в политику информационной безопасности организации;

– в состав и содержание мер обеспечения КБ (в том числе дополнительные инструктажи и обучение персонала);

– в процессы, организацию, формы документирования СМИБ и менеджмента инцидентов ИБ и т.д.;

3. Выявление закономерностей, характерных для конкретных инцидентов ИБ, и выработка превентивных мер.

4. Тестирование АИС на уязвимости и возможность проникновения.

5. Обмен знаниями и опытом идентификации инцидентов КБ с заинтересованными организациями.

6. Подготовка рекомендаций по улучшению безопасности.

Обобщенный анализ инцидентов КБ, выводы и предложения по устранению недостатков должны регулярно рассматриваться на совещаниях при руководстве организации, принятые решения – документироваться и выполняться.

**Действия на этапе улучшения системы реагирования на инциденты КБ:**

– устранение уязвимостей АИС, модернизация СЗИ организации;

– реконфигурация АИС и СЗИ;

– обновление политики и процедур обеспечения КБ;

– модернизация процессов менеджмента КБ;

– иные действия по устранению недостатков, выявленных на этапе анализа.

***Тип компьютерного инцидента*** *– классификация разновидностей фактов нарушения кибербезопасности и/или прекращения функционирования ИР АИС, в том числе в результате компьютерной атаки.*

**Типы компьютерных инцидентов:**

1. Внедрение в АИС модулей ВПО, предназначенного для получения НСД к ИР и ПТС АИС, с целью несанкционированного использования его ресурсов или нанесения ущерба владельцу ИР.

2. Использование ИР для распространения ВПО с целью заражения других ИР.

3. Компьютерная атака типа «отказ в обслуживании» (DoS, DDoS), направленная на ИР, последствия которой привели к нарушению функциональности данного ИР.

4. Несанкционированный вывод информационного ресурса из строя путем проведения компьютерной атаки, в результате которой информационный ресурс не способен выполнять возложенную на него функцию должным образом.

5. Случайное блокирование доступа или нарушение функциональности ИР, произошедшее в результате непреднамеренных действий или обстоятельств.

6. Успешная эксплуатация нарушителем уязвимости ПТС АИС путем проведения компьютерной атаки.

7. Компрометация учетной записи в АИС путем проведения компьютерной атаки, в ходе которой нарушитель получил идентификационные и аутентификационные данные авторизованного пользователя АИС.

8. Прослушивание сетевого трафика в информационной инфраструктуре АИС, перехват и раскрытие нарушителем содержания сетевых пакетов путем проведения компьютерной атаки.

9. Социальная инженерия, направленная на получение НСД путем проведения компьютерной атаки и компрометацию ИР.

10. Противоправное разглашение защищаемой информации и ознакомление с ней посторонних лиц в результате умышленных или неосторожных действий.

11. Несанкционированное изменение защищаемой информации при ее обработке, хранении или передаче с нарушением установленных прав и правил разграничения доступа.

12. Использование сервисов ИР для рассылки спам-сообщений, содержание которых может быть вредоносным и/или мошенническим.

13. Публикация в ИР запрещенной законодательством Российской Федерации информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

14. Злоупотребление и использование ИР и ПТС АИС организации в личных целях, повлекшее нарушение функциональности и/или снижение производительности АИС.

15. Публикация мошеннической информации, заведомо ложных данных, предназначенных для хищения идентификационных и аутентификационных данных путем обмана или злоупотребления доверием.

## 6.2. Реагирование на киберинциденты

*Основные цели процесса реагирования на киберинциденты:*

– не допустить или минимизировать последствия компьютерного инцидента, сохраняя непрерывность критических функций организации;

– обеспечить эффективное и своевременное восстановление работоспособности (штатного функционирования) ИР;

– повысить уровень обеспечения КБ и эффективность СМИБ в организации.

*Основные правила реагирования на киберинциденты:*

– поиск и сбор данных обо всех событиях КБ со всех конечных устройств АИС (хостов) и активного сетевого оборудования;

– сохранение в базе всех относящихся к инциденту данных (в т.ч. находящихся в ОЗУ);

– сбор доказательной базы, протоколирование логов и журналов устройств, дампов ОЗУ, образов жестких дисков, логов интернет/телеком-провайдеров, СКУД, записи систем видеонаблюдения и т.п.;

– идентификация атакующих (квалификация, специализация, степень опасности) для понимания проблемы и адекватных мер реагирования;

– широкое использование средств автоматизации для уменьшения времени реагирования и, соответственно, снижения ущерба;

– быстрое восстановление ПТС АИС в исходное состояние «до инцидента»;

– обмен данными в рамках концепции Threat Intelligence;

– выводы из инцидента: перенастройка СЗИ, изменение регламентов реагирования, обучение.

Процесс реагирования на киберинциденты состоит из следующих последовательных этапов (см. рис. 64).

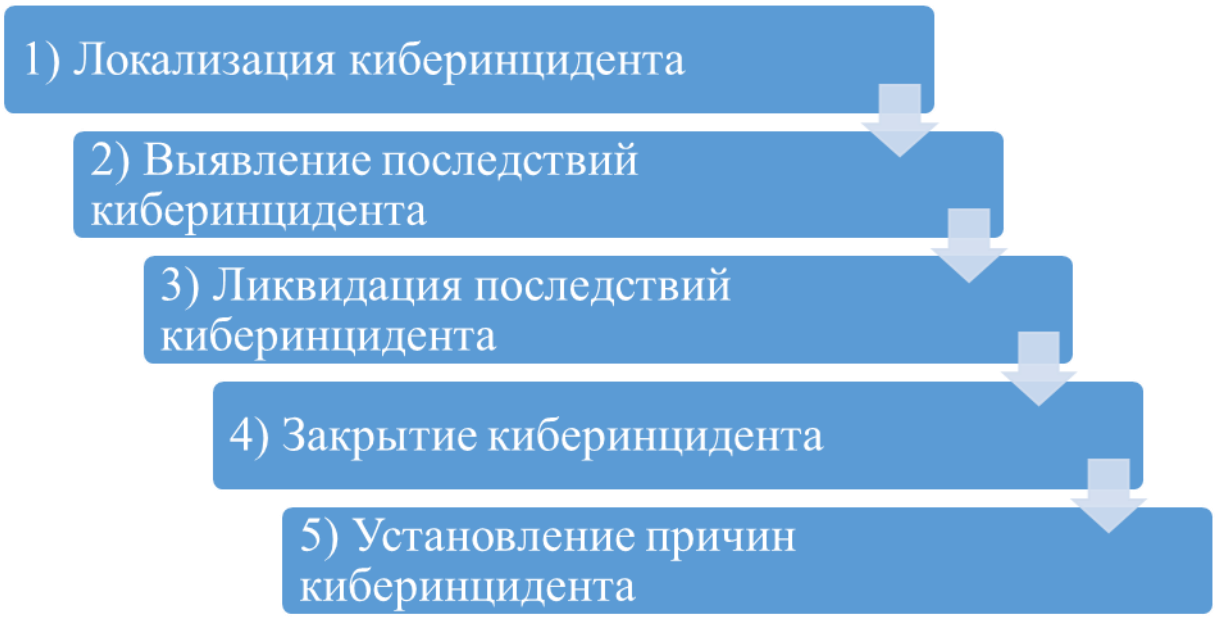


*Рисунок 64. Этапы процесса реагирования на компьютерные инциденты*

**Этап локализации киберинцидента** представляет собой действия, направленные на определение и ограничение функционирования ИР, на которых обнаружены признаки зарегистрированного киберинцидента с целью предотвращения его дальнейшего распространения.

*Цель локализации киберинцидента* состоит в том, чтобы предотвратить следующие возможные действия нарушителя:

– нарушение конфиденциальности, целостности или доступности информации вследствие НСД;

– несанкционированное вмешательство в IT-инфраструктуру организации;

– использование ИР и/или ПТС АИС и сетей для атаки на другие АИС.

**Способы локализации киберинцидента** (см. рис. 65)**:**

1. *Применение блокировок (использование межсетевого экрана)*.

Блокировки с использованием межсетевых экранов используются для предотвращения несанкционированного воздействия со стороны идентифицированной внешней системы. Например, с использованием межсетевого экрана можно заблокировать информационные потоки с IP-адресов, с которых распространяется вредоносное ПО, шпионское ПО, неразрешенное ПО, а также IP-адресов почтовых ретрансляторов, источников «фишинга» и «спама» или известных IP-адресов хостов нарушителей.

Почтовые блокировки включают фильтрацию вложений, строк темы и адреса отправителей. Для предотвращения доступа к неразрешенным или вредоносным веб-сайтам, или хостам (узлам) могут применяться блокировки URL-адресов и доменных имен.


*Рисунок 65. Действия на этапе локализации киберинцидента*

2. *Отключение (изоляция, исключение)*.

Отключение зараженных ИР от сети электросвязи, может помочь предотвратить заражение остальной части сети.

Отключение ИР от Интернета и/или других общедоступных ИТКС может помочь предотвратить НСД и, соответственно, нарушение конфиденциальности, целостности и доступности информации. В некоторых случаях целесооб-

разно просто осуществлять наблюдение за вредоносной активностью, ограничив при этом возможности нарушителя атаковать другие ИР.

Отключение (изоляция, исключение) сегмента сети связи, где размещен ИР, от остальной части сети также может помочь предотвратить дальнейшее заражение или сдерживание злонамеренных действий в IT-инфраструктуре. Атакованный ИР сможет функционировать, не распространяя вредоносную активность на остальную часть IT-инфраструктуры.

3. *Выключение*. Если дальнейшее функционирование ИР приведет к уничтожению (потере, утечке) данных в IT-инфраструктуре, то в качестве меры сдерживания может быть принято решение о прекращении функционирования данного ИР. Например, установлено, что с сервера электронной почты или веб-сервера распространяется ВПО. Функционирование данного сервера должно быть приостановлено, но это может отрицательно сказаться на деятельности организации, и решение должно приниматься в координации с лицами, заинтересованными в функционировании данного ИР.

4. *Изменения маршрутизации*. Изменения маршрутизации осуществляются с целью устранения маршрута, по которому нарушитель получил доступ к ИР, ставшему объектом атаки, а также блокирования маршрутов распространения ВПО.

5. *Отключение процессов*. Данный способ подразумевает отключение процессов, которые могли быть использованы при компьютерной атаке.

6. *Отключение учетных записей пользователей*. Данный способ подразумевает отключение учетных записей пользователей, которые могли быть использованы при компьютерной атаке.

Перед внесением каких-либо системных изменений следует убедиться, что вся необходимая для установления причины киберинцидента информация собрана в полном объеме. Любые изменения ИР, включая действия по локализации, могут привести к потере цифровых свидетельств о киберинциденте.

**На этапе выявления последствий киберинцидента** специалисты, принимающие участие в реагировании, должны провести анализ, который включает:

– выявление признаков негативного воздействия на элементы IT-инфраструктуры в результате киберинцидента;

– оценку негативного влияния киберинцидента на ИР.

При выявлении признаков негативного воздействия на элементы IT-инфраструктуры специалистами, ответственными за реагирование на киберинцидент проводится детальный анализ полученных ранее технических данных. В общем случае порядок проведения такого анализа не может быть формализован, а результат анализа определяется опытом и компетенцией специалистов, участвующих в его проведении, а также наличием у специалистов, осуществляющих реагирование, доступа к информации о действиях, которые выполнялись при выявлении последствий аналогичных киберинцидентов (см. рис. 66).

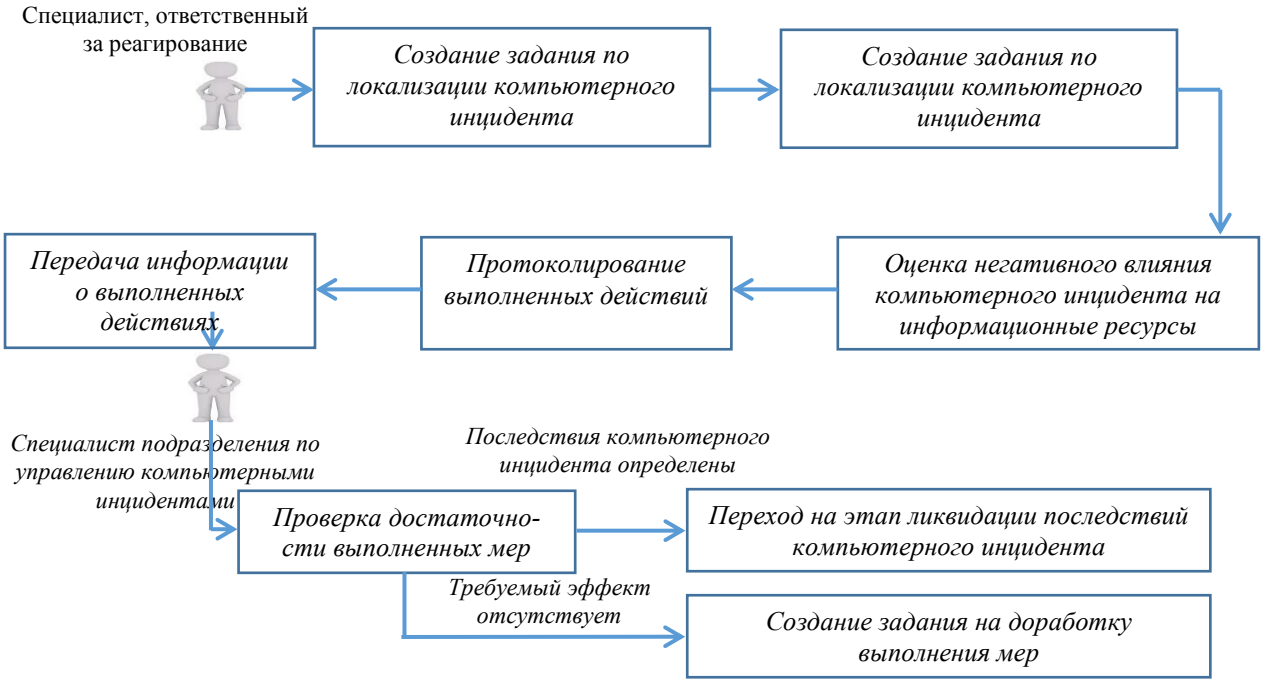


*Рисунок 66. Действия на этапе выявления последствий киберинцидента*

*Признаки негативного воздействия* на элементы информационной инфраструктуры, которые выявляются в ходе анализа:

– нештатная сетевая активность объекта воздействия компьютерной атаки;

– созданные, модифицированные, удаленные файлы, каталоги, параметры настройки ПО, включая ПО средств ЗИ;

– отклонения от эталонных (допустимых) параметров конфигурации операционной системы (ОС), и ПО, включая ПО средств ЗИ;

– отклонения от эталонного (допустимого) состава, установленного в ОС, ПО;

– отклонения от эталонного (допустимого) содержания системных и защищаемых файлов;

– выполненные потенциально вредоносные команды, в том числе расположенные в оперативной памяти СВТ – объекта воздействия компьютерной атаки;

– признаки, идентифицирующие источник компьютерной атаки;

– признаки сбоев, перезагрузок, остановок и других нарушений в штатной работе ПО, признаки нарушений функционирования сетевых служб, аномального использования системных ресурсов;

– другая информация, характерная для отдельных типов компьютерных инцидентов, компьютерных атак.

*Оценка негативного воздействия* на элементы IT-инфраструктуры в результате киберинцидента должна учитывать:

– трудозатраты, связанные с проведением мероприятий по реагированию на киберинцидент;

– время простоя ИР;

– вред, причиненный заинтересованным лицам, в том числе связанный с нарушением конфиденциальности, целостности и доступности обрабатываемой информации;

– вред, причиненный организации, в том числе репутационные потери, экономический ущерб и т.п.;

– финансовые затраты на восстановление штатного функционирования информационных ресурсов.

Переход на следующий этап реагирования на киберинцидент осуществляется после того, как ответственный руководитель службы управления киберинцидентами убедится в достаточности выполненных действий и правильном заполнении карточки киберинцидента.

**На этапе ликвидации последствий киберинцидента** специалисты, принимающие участие в реагировании, должны выполнить удаление следов киберинцидента и/или восстановление объекта воздействия компьютерной атаки в состояние, предшествующее нарушению безопасности информации.

Первоначально специалисты, принимающие участие в реагировании на киберинциденты, планируют стратегию выполнения работ и согласовывают ее с лицом, ответственным за эксплуатацию объекта воздействия компьютерной атаки. В зависимости от уровня воздействия компьютерной атаки и объема негативных воздействий определяются необходимые работы по отмене обнаруженных на объекте воздействия изменений от компьютерной атаки (см. рис. 67).

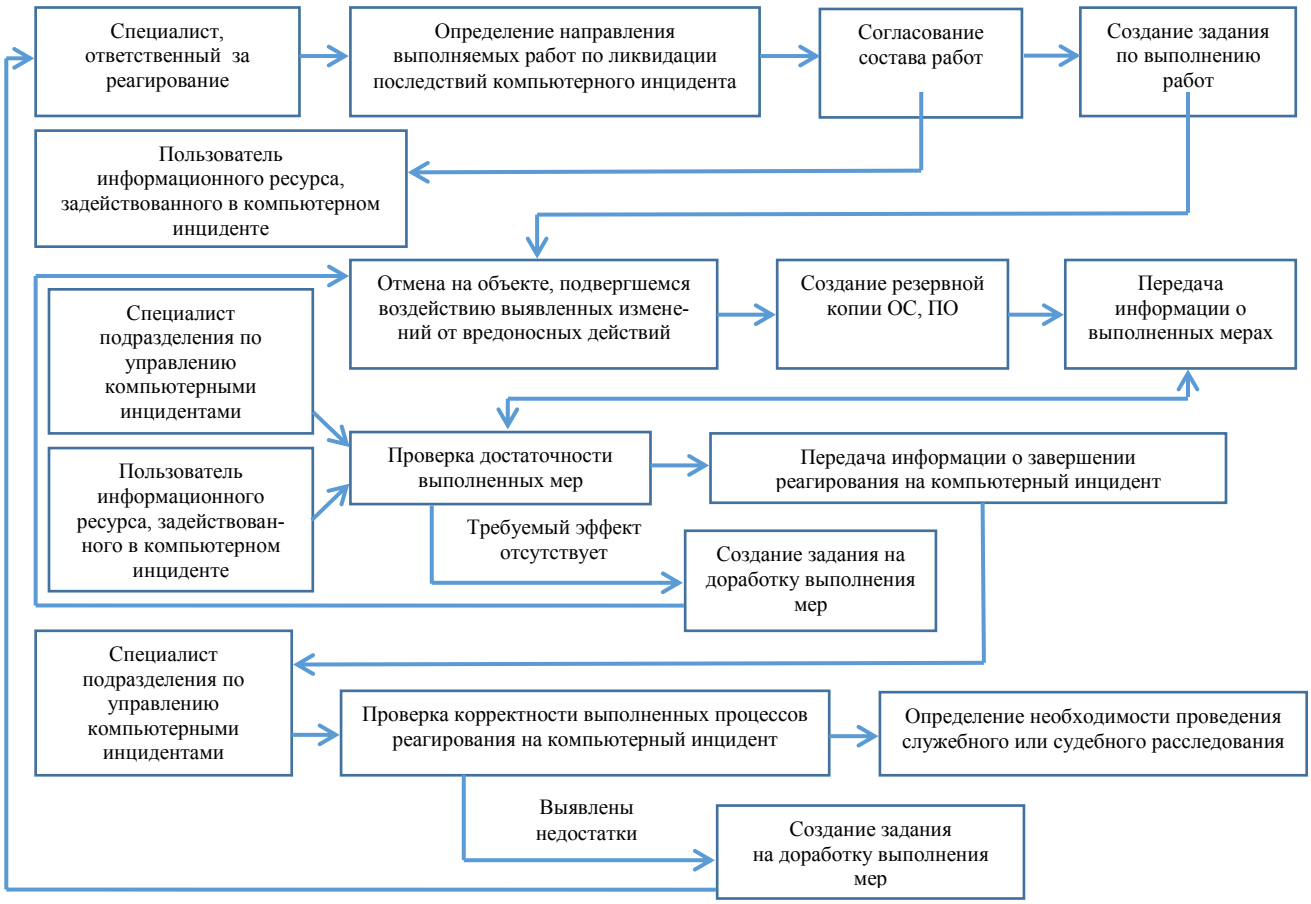


*Рисунок 67. Действия на этапе ликвидации последствий киберинцидента*

Необходимо отметить, что данные работы выполняются вне зависимости от компетенции специалистов, принимающих участие в реагировании на киберинциденты, и уровня критичности объекта воздействия компьютерной атаки. При недостаточной квалификации своих специалистов руководителем команды реагирования на киберинциденты должно приниматься решение о необходимости привлечения внешних специалистов.

*Типовые меры ликвидации последствий киберинцидента на уровне сети:*

– внесение изменений в параметры настроек ПО ИР, вовлеченных в киберинцидент;

– подключение резервных ресурсов (каналы связи, серверное оборудование, виртуальные машины, оборудование из состава запасных инструментов и принадлежностей);

– внесение изменений в архитектуру ИР, вовлеченных в киберинцидент, с корректировкой проектной документации;

– миграция (перемещение) виртуальных машин в сторонние виртуальные инфраструктуры.

*Типовые меры ликвидации последствий киберинцидента на уровне ПО:*

– выполнение настройки безопасной конфигурации ИР, вовлеченного в киберинцидент;

– восстановление из актуальных резервных копий файлов, баз данных, конфигурационных файлов, подвергшихся несанкционированному изменению;

– восстановление удаленных файлов, в том числе с использованием специальных инструментальных средств;

– удаление ПО, вовлеченного в компьютерный инцидент и всех его файлов с последующей установкой актуальной версии данного ПО и актуальных обновлений безопасности.

*Типовые меры ликвидации последствий киберинцидента на уровне операционной платформы:*

– удаление следов вредоносной активности;

– восстановление ОС на объекте воздействия;

– настройка безопасной конфигурации ОС.

– переустановка ОС с актуальными обновлениями безопасности.

При проведении всех мероприятий фиксируются технические данные, результаты проводимых исследований носителей информации, результаты анализа технических данных и иные цифровые свидетельства.

После завершения работ руководитель службы реагирования совместно с ответственным за эксплуатацию ИР проверяет достаточность принятых мер и при положительном результате принимает решение о закрытии киберинцидента.

**Закрытие киберинцидента** может быть выполнено только после принятия необходимых и достаточных мер на этапах локализации, выявления и ликвидации его последствий. Решение о закрытии киберинцидента принимается по результатам проверки руководителем службы реагирования, в ходе которой определяется полнота выполненных и запротоколированных мероприятий на всех

этапах. В случае получения неудовлетворительных результатов меры могут выполняться повторно.

Закрытый киберинцидент считается полностью устраненным. После этого любой выявленный киберинцидент с идентичными признаками регистрируется как новый.

**Деятельность по установлению причин киберинцидента** направлена на определение факторов, способствовавших его возникновению.

1. *Анализ действий пользователей*. Анализ действий пользователей является процессом изучения сведений, задокументированных в ходе опроса причастных к киберинциденту лиц, о действиях или бездействии в целях определения причины, которая могла способствовать возникновению компьютерного инцидента.

*Сведения, изучаемые в ходе анализа действий пользователей:*

– информация о действиях пользователей (администраторов), которые выполнялись с ИР до и во время регистрации киберинцидента (например, посещение веб-сайта, открытие сообщения электронной почты, открытие электронного документа, подключение носителя информации к компьютеру, подключение компьютера к сетевой розетке);

– сведения об игнорировании пользователем (администратором) появляющихся сигналов ОС, ПО (например, о необходимости выполнить обновление ОС, ее перезагрузку, о необходимости ввести в определенные поля учетные данные пользователя, о выявленном потенциально вредоносном файле).

2. *Системный анализ*. Системный анализ является процессом изучения системных настроек и логов системных событий, которые происходили до и во время возникновения киберинцидента.

*Лог* – файл с записями о событиях в хронологическом порядке, является простейшим средством журналирования.

*Сведения, изучаемые в ходе системного анализа:*

– содержимое логов и журналов автоматической регистрации событий ОС и ПО;

– информация о запущенных программных процессах;

– информация об установленных сетевых сессиях и открытых сетевых портах;

– реестр ОС;

– информация об атрибутах объектов файловой системы;

– состав учетных записей пользователей и их прав.

3. *Анализ защищенности*. Анализ защищенности является процессом изучения информации об актуальных уязвимостях ОС и ПО объекта киберинцидента.

*Сведения, изучаемые в ходе анализа защищенности:*

– существующие результаты проведенных мероприятий по анализу защищенности АС и тестированию ее СЗИ;

– состав ПТС объекта киберинцидента;

– сетевая конфигурация ОС, ПО;

– групповые политики безопасности ОС;

– функциональные параметры настроек ПО, служб ОС;

– состав установленных (неустановленных) актуальных обновлений безопасности ОС и ПО.

4. *Сетевой анализ*. Сетевой анализ является процессом изучения сетевого трафика до, во время и после возникновения киберинцидента.

*Сведения, изучаемые в ходе сетевого анализа:*

– копии сетевого трафика между сегментами ИТКС, в которой расположен объект киберинцидента, сохраненные средствами записи (анализа) сетевого трафика;

– копия сетевого трафика или его фрагменты, зафиксированные средством обнаружения компьютерных атак (системой обнаружения вторжений) или иными средствами выявления угроз кибербезопасности;

– статистическая и иная информация о потоках сетевого трафика между объектом киберинцидента и вероятным источником угрозы кибербезопасности, а также между объектом киберинцидента и другими сетевыми устройствами ИТКС;

– статистическая и иная информация о потоках сетевого трафика, зафиксированная телекоммуникационным оборудованием или специализированными средствами.

Потоком данных считается набор сетевых кадров канального уровня стека TCP/IP, проходящих в одном направлении к одному сетевому устройству в рамках одного сетевого сеанса.

5. *Анализ программных и информационных объектов*. *Задачи анализа программных и информационных объектов*:

– выявление вредоносного программного кода в объектах файловой системы, в оперативной памяти ПТС и в ИР (веб-ссылки, программный код веб-страницы, карточные транзакции и др.);

– выявление в них связей с вредоносными ресурсами или ресурсами, предположительно используемыми нарушителями;

– определение принципа их работы.

Методы анализа программных объектов:

– декомпиляция и дизассемблирование машинного кода (представление на языке ассемблера) в режиме отладки ПО;

– запуск и изучение поведения программных кодов в изолированной программной среде (режим песочницы).

*Примерный перечень организационно-распорядительных документов для реагирования на инциденты КБ*:

– общая политика реагирования;

– регламенты (инструкции) реагирования на отдельные типы инцидентов;

– условия передачи полномочий в группе реагирования от сотрудника 1-го уровня к сотруднику 2-го уровня к киберкриминалисту (форензик-эксперту), реверс-инженеру, в специализированные организации (матрица эскалации);

– инструкции по взаимодействию при инциденте пользователя, ответственного за актив, владельца актива, ИТ-службы, КБ-службы, СБ-службы, руководства организации (матрица коммуникации).

## 6.3. Системы управления событиями и данными безопасности

К управлению инцидентами киербезопасности предъявляются все большие требования компаний и регуляторов. SIEM-системы помогают обеспечить последовательный и эффективный подход к работе с инцидентами КБ, чем значительно облегчают жизнь специалистов по безопасности.

Разработчики SIEM объединили функциональные возможности SIM-систем управления информацией о безопасности и SEM-систем управления событиями безопасности, которые применялись для автоматизации деятельности специалистов по реагированию на киберинциденты. Сами по себе SIEM-продукты не способны предотвращать киберинциденты, но при помощи SIEM специалисты центров оперативного управления (SOC) могут своевременно выявить нарушения политик безопасности и кибератаки, чтобы минимизировать ущерб от них. Решения SIEM также помогают оценить степень защиты информационных активов, актуальные для организации риски. Базы данных SIEM-систем используются при расследовании инцидентов.

*Задачи SIEM-систем:*

– централизованный сбор данных о событиях безопасности и визуализация поведения АИС (диаграммы, таблицы, списки);

– ведение базы данных о событиях безопасности;

– идентификация и автоматическое оповещение о киберинцидентах владельцев ИР и сотрудников заинтересованных служб;

– проактивный поиск угроз безопасности;

– контроль защищенности критически важных ресурсов АИС;

– автоматизация подготовки отчетных документов и выработка рекомендаций по реагированию на киберинциденты и устранению уязвимостей СЗИ и др.

*Виды событий безопасности для SIEM:*

– срабатывание датчиков угроз на традиционных СЗИ;

– появление приоритетного индикатора компрометации;

– одновременное обнаружение нескольких индикаторов компрометации.

*Индикатор компрометации* – признак поведения объекта, который с большой долей вероятности указывает на угрозу кибербезопасности.

В информации о событиях кибербезопасности могут указываться различные источники и разнотипные индикаторы, следовательно, для принятия решения по факту инцидента кибербезопасности возникает необходимость выявления корреляционных связей между ними.

Корреляционный анализ событий кибербезопасности в SIEM производится на основе заранее определенных логических правил, сформированных на основе баз данных о тактике, технике и процедурах, применяемых нарушителями при подготовке и реализации кибератак.

*С помощью набора правил корреляции современные SIEM-системы способны автоматически выявлять*:

– известные угрозы безопасности;

– потенциальные угрозы безопасности;

– аномальную активность компонентов АИС;

– действия или процессы запрещенные политикой безопасности;

– причинно-следственную связь между событиями безопасности и информационными процессами в АИС;

– ненадежные компоненты АИС и др.

Базовый набор правил логики корреляционного анализа в SIEM-системы закладывается на этапе их разработки и настройки, а затем в процессе эксплуатации корректируется и дополняется с учетом особенностей IT-инфраструктуры, правил разграничения доступа и политики безопасности организации.

*Архитектура SIEM-систем* разворачивается над инфраструктурой защищаемой АИС и состоит из следующих компонентов:

– агенты (подготовка и отправка данных о событии безопасности);

– сервер-коллектор (сбор информации из различных источников);

– сервер баз данных (хранение в репозитории);

– сервер-коррелятор (анализ).

Российские SIEM-системы развиваются стремительными шагами и меньше, чем за 10 лет догнали и перегнали зарубежных вендоров во многих аспектах.

**КОМРАД.** Отечественная SIEM-система компании НПО «Эшелон», которая осуществляет централизованный мониторинг событий ИБ, выявляет инциденты КБ, реагирует на возникающие угрозы и выполняет требования, предъявляемые регуляторами к защите персональных данных.

Преимуществами использования данной системы можно считать:

– поддержку большого количества платформ;

– быстрое оповещение и реагирование на различные виды угроз;

– возможность гибкой настройки;

– удаленное управление конфигурациями;

– сбор информации с нестандартных источников событий.

**RUSIEM**. Основное преимущество RUSIEM заключается в невысокой стоимости внедрения и поддержки, а также широкой функциональности. Существует три версии продукта:

– RuSIEM free, бесплатно распространяемая версия с урезанным функционалом;

– RuSIEM, имеющая расширенные возможности корреляции, инцидент-менеджмента и риск-менеджмента, то есть являющаяся полноценной системой класса SIEM.

– RuSIEM Analytics, дополняющая RuSIEM возможностями по управлению активами и выявлению аномалий на базе машинного обучения.

Видимыми отличиями от конкурирующих компаний являются: собственные модульные агенты, высокая производительность и безлимитное количество источников информации о событиях безопасности.

**MAXPATROL SIEM**. Особенностью MaxPatrol SIEM является активориентированный подход, который обеспечивает устойчивость работы системы к изменениям в ИТ-инфраструктуре организации. В продукте активы разбиваются по динамическим группам согласно сформулированным при создании групп критериям.

## Вопросы для самоконтроля:

1. Что представляет собой система VERIS?
2. В чем заключаются цели создания VERIS?
3. На решение какой проблемы направлен фреймворк VERIS?
4. Что представляет собой диаграмма Венна?
5. Из каких разделов состоит схема VERIS?
6. Из каких этапов состоит процесс реагирования на инциденты в сфере сетевой безопасности?
7. В чем заключается содержание этапа локализации компьютерного инцидента?
8. В чем заключается применение блокировок как способа локализации компьютерных инцидентов?
9. В чем заключается смысл отключения зараженного информационного ресурса?
10. С какой целью осуществляется изменение маршрутизации?
11. Какие элементы включает в себя анализ последствий компьютерных инцидентов?
12. Что должно оцениваться при оценке негативного воздействия на элементы информационной инфраструктуры в результате компьютерного инцидента?
13. В чем заключается закрытие компьютерного инцидента?
14. В чем заключается анализ программных и информационных объектов?

# БИБЛИОГРАФИЧЕСКИЙ СПИСОК


1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993, с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) [Электронный ресурс]. – Режим доступа: https://consultant.ru.
2. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 30.12.2021) // Собрание законодательства Российской Федерации. 2002. № 1 (ч. 1). Ст. 1.
3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 14.07.2022, с изм. от 18.07.2022) (с изм. и доп., вступ. в силу с 25.07.2022) [Электронный ресурс]. – Режим доступа: https://consultant.ru.
4. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. – Режим доступа: https://consultant.ru.
5. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности» [Электронный ресурс]. – Режим доступа: https://consultant.ru.
6. Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» [Электронный ресурс]. – Режим доступа: https://consultant.ru.
7. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» [Электронный ресурс]. – Режим доступа: https://consultant.ru.
8. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. – Режим доступа: https://consultant.ru.
9. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне» [Электронный ресурс]. – Режим доступа: https://consultant.ru.
10. Доктрина информационной безопасности Российской Федерации: утверждена Указом Президента Российской Федерации от 05.12.2016 № 646 [Электронный ресурс]. – Режим доступа: https://consultant.ru.
11. Указ Президента Российской Федерации от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» [Электронный ресурс]. – Режим доступа: https://consultant.ru.
12. Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс]. – Режим доступа: https://consultant.ru.
13. Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. – Режим доступа: https://consultant.ru.
14. Приказ Минкомсвязи Российской Федерации от 22.09.2020 № 486 «Об утверждении классификатора программ для электронных вычислительных машин и баз данных» [Электронный ресурс]. – Режим доступа: https://consultant.ru.

15. Приказ ФСТЭК России от 09.08.2018 № 138, от 26.03.2019 № 60, от 20.02.2020 № 35 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»» [Электронный ресурс]. – Режим доступа: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/.

16. План мероприятий по направлению Информационная безопасность программы Цифровая экономика Российской Федерации: Приложение № 4 к протоколу заседания Правительственной комиссии по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 18.12.2017 № 2 [Электронный ресурс]. – Режим доступа: http://static.government.ru.

17. Андресс Дж. Защита данных. От авторизации до аудита. – Санкт-Петербург: Питер, 2021. – 275 с.

18. Ашманов И., Касперская Н. Цифровая гигиена. – Санкт-Петербург: Питер, 2022. – 340 с.

19. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации: учебу пособие. – 4-е изд., перераб. и доп. – Москва: РИОР: ИНФРА-М, 2022. – 336 с.

20. Белоус А.И., Солодуха В.А. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения. – Москва: Техносфера, 2021. – 482 с.

21. Гизатуллин М.Г. Правовая информатика: учебное пособие. – Екатеринбург: Уральский юридический институт МВД России, 2020. – 44 с.

22. Грей Дж. Социальная инженерия и этичный хакинг на практике. – Москва: ДМК, 2023. – 228 с.

23. Деза Е.И., Котова Л.В. Введение в криптографию. – Москва: Ленард, 2022. – 376 с.

24. Ищейнов В.Я., Мецатунян М.В. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации: учебное пособие. – 2-е изд., перераб. и доп. – Москва: ИНФРА-М, 2021. – 256 с.

25. Казарин О.В., Забабурин А.С. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум. – Москва: Юрайт, 2022. – 312 с.

26. Келдыш Н.В. Системная защита информации компьютерных сетей. – Москва: Мир науки, 2022. – 100 с.

27. Кемпф В.А. Обеспечение информационной безопасности в органах внутренних дел: учебное пособие. – Барнаул: Барнаульский юридический институт МВД России, 2019. – 63 с.

28. Кирюшин С., Борисов Е. Цифровая трансформация мировой экономики: учебное пособие. – Москва: Озон, 2022.

29. Колисниченко Д.Н. Хакинг на LINUX. – Санкт-Петербург: Наука и Техника, 2022. – 320 с.

30. Комиссаров И. Взлом. Приемы, трюки и секреты хакеров. – Москва: BHV, 2020. – 194 с.

31. Криптографическая защита информации: учебное пособие / науч. ред.: Васильева И.Н., Локнов А.И., Примакин А.И. – Санкт-Петербург: СПб. ун-т МВД России, 2022 – 186 с.

32. Маккарти Б. Кибердзюцу. Кибербезопасность для современных ниндзя. – Санкт-Петербург: Питер, 2022. – 224 с.

33. Матросов А., Родионов Е. Руткиты и буткиты. Обратная разработка вредоносных программ и угрозы следующего поколения. – Москва: ДМК Пресс, 2022. – 442 с.

34. Основы и нформационной безопасности в органах внутренних дел: учебно-практическое пособие / авт.-сост. Ю.Э. Голодков, В.И. Демаков, Е.Ю. Ларионова, Е.Е. Ровина. – Иркутск: ВСИ МВД России, 2018. – 75 с.

35. Паренти Т., Домет Дж. Кибербезопасность. Что руководителям нужно знать и делать. – Москва: ЛитРес, 2021. – 200 с.

36. Пиз Э. Активное выявление угроз с Elastic Stack. – Москва: ДМК Пресс, 2022. – 326 с.

37. Райтман М. Старший брат следит за тобой. Как защитить себя в цифровом мире. – Москва: Альпина Диджитал, 2022. – 485 с.

38. Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учебное пособие. – Москва: ИНФРА-М, 2021. – 223 с.

39. Цымбаленко С.В. Основы информационной безопасности в органах внутренних дел: учебное пособие. – Ставрополь: Ставропольский филиал Краснодарского университета МВД России, 2018. – 110 с.

40. Чанцис Ф., Стаис И. Практический хакинг интернета вещей. Подробное руководство по атакам на устройства интернета вещей. – Москва: ДМК Пресс, 2022. – 482 с.

УЧЕБНОЕ ИЗДАНИЕ

***Прокопенко Алексей Николаевич,***
кандидат технических наук, доцент;
***Страхов Андрей Александрович,***
***Ковалева Екатерина Геннадьевна,***
кандидат технических наук;
***Акапьев Виктор Львович,***
кандидат педагогических наук, доцент;
***Гаврющенко Александр Павлович,***
кандидат технических наук, доцент;
***Рыбальченко Антон Юрьевич***

**Основы кибербезопасности**
**в деятельности сотрудников правоохранительных органов**

Учебное пособие

Редактор *О.И. Шаповал*
Комп. верстка *И.Ю. Чернышева*

---

Подписано в печать 2023. Формат 60x90/16
Усл. печ. л. 7 Тираж 74 экз. Заказ 22

---

Отпечатано в отделении полиграфической и оперативной печати
Белгородского юридического института МВД России имени И.Д. Путилина
г. Белгород, ул. Горького, 71

ISBN 978-5-91776-485-6