ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОСТОВСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ МИНИСТЕРСТВА
ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(ФГКОУ ВО РЮИ МВД России)

С. В. Лемайкина, А. Г. Карпика,
В. Б. Гунько, В.В. Комерцов

ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

Учебное пособие

Ростов-на-Дону
2023

УДК 004.056(075.8)
ББК 32.973
О 753

***Рецензенты**:*
Л. Д. Матросова, кандидат юридических наук, доцент
(Орловский юридический институт МВД России им. В.В. Лукьянова);
Т. Л. Васютина, кандидат технических наук, доцент
(Санкт-Петербургский университет МВД России).

Лемайкина, Светлана Владимировна.

О 753 **Основы кибербезопасности**: учебное пособие / С. В. Лемайкина, А. Г. Карпика, В. Б. Гунько и др. – Ростов-на-Дону : ФГКОУ ВО РЮИ МВД России, 2023. – 64 с.
ISBN 978-5-89288-506-5

В учебном пособии изложены основы кибербезопасности – основополагающие вопросы теории и практики решения проблем защиты информации. Это, в первую очередь, сущность и основные проблемы защиты информации наряду с перечнем возможных киберугроз. Отражены составляющие национальных интересов Российской Федерации в информационной сфере, приведены концептуальные основы подходов к построению защищенных систем, освещен основной понятийный аппарат. Рассмотрено нормативно-правовое обеспечение информационной безопасности и представлен анализ методов, технологий и средств защиты информации в компьютерных системах.

Предназначено для преподавателей, курсантов и слушателей образовательных организаций МВД России.

Печатается по решению редакционно-издательского совета

ФГКОУ ВО РЮИ МВД России.

ISBN 978-5-89288-506-5

УДК 004.056(075.8)
ББК 32.973

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В учебном пособии представлен необходимый объем информации для формирования профессиональной компетентности у обучающихся в области основ кибербезопасности посредством теоретико-методологических знаний. В значительной мере безопасность общества зависит от безопасности используемых информационно-коммуникационных технологий, применение которых требует неустанного внимания к вопросам обеспечения кибербезопасности. Интенсификация процессов обеспечения кибербезопасности невозможна без формирования научно-методологического базиса защиты информации и рационализации подходов к созданию систем защиты объектов разного уровня.

В связи с этим проблемы кибербезопасности приобретают первостепенное значение, актуальность и важность которых обусловлена основными факторами:

− быстрый прогресс информационно-коммуникационных технологий;

− несоответствие значительной доли внедряемых аппаратно-программных средств и технологий современным требованиям безопасности;

− широкое использование сетевых технологий, формирование единой глобальной информационно-коммуникационной среды на основе сети Интернет, в которой не обеспечивается достаточный уровень кибербезопасности.

Указанные выше факторы создают целый спектр угроз для кибербезопасности на уровне личности, общества и государства. Для средств нейтрализации таковых необходимым условием является формирование теоретических и методологических основ кибербезопасности у сотрудников ОВД.

ТЕМА 1. ОБЩИЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

1.1. Кибербезопасность: современные киберугрозы. Методы совершения киберпреступлений

В настоящее время эффективное функционирование органов государственной власти и Министерства внутренних дел Российской Федерации (далее – МВД) в том числе основывается на использовании цифровых технологий. В течение последних лет МВД России включило в свои основные процессы и системы управления облачные технологии, большие данные, Интернет, искусственный интеллект, что позволило систематизировать и интегрировать большие объемы информации в единые информационные базы данных. Результатом стало существенное увеличение эффективности работы МВД России в его основной сфере деятельности – обеспечении общественной безопасности и противодействии преступности. Вместе с тем широкое использование цифровых технологий в деятельности МВД России чревато серьезной потенциальной угрозой, обусловленной наличием обработкой органами внутренних дел большого объема конфиденциальной информации. В МВД России такой информацией является информация в различных единых базах данных. Что будем понимать под термином «кибербезопасность»?

Кибербезопасность можно определить как совокупность процессов, методов и лучших практик, предназначенных для защиты компьютерных данных, информационных систем и сетей от цифровых атак злоумышленников.

Роль инструментов защиты компьютерных систем и мер, принимаемых в рамках кибербезопасности, в современных условиях огромна. И чем большим количеством высокотехнологичных устройств мы себя окружаем, тем больше увеличиваем риск стать жертвой киберкриминала. Соответственно, растет и важность кибербезопасности – и как области информационных технологий, и как комплекс инструментов для обеспечения защиты конфиденциальных данных.

Основные типы угроз кибербезопасности:

Вредоносное программное обеспечение (ВПО). К ВПО относятся любые программы или файлы, предназначенные для причинения ущерба компьютеру, сети или серверу. Вредоносные программы способны украсть,

зашифровать, изменить или удалить компьютерную информацию, захватить основные вычислительные функции, отслеживать активность компьютеров или приложений (см. раздел 3). ВПО зачастую используется киберпреступниками с целью вымогательства. Сущность данного вида киберпреступлений заключается в том, что на компьютеры пользователя или корпоративной сети компании в результате кибератаки происходит загрузка вредоносной программы, которая выполняет шифрование файлов. Возможен вариант, когда предварительно похищается конфиденциальная информация (персональные данные сотрудников, клиентов или пациентов, документы, содержащие коммерческую тайну, и т. п.). Затем от преступников под угрозой публикации или продажи конфиденциальной информации третьим лицам или за восстановление файлов поступает требование об оплате в криптовалюте.

SQL-инъекция. Это вид кибератак, используемый для неправомерного доступа к информации в базах данных. Киберпреступники эксплуатируют уязвимости в приложениях, управляемых данными, для внедрения вредоносного кода на языке управления базами данных (SQL).

Социальная инженерия. Метод атак, использующий различные психологические приемы при человеческом взаимодействии. Злоумышленники втираются в доверие к пользователям и побуждают их выдать конфиденциальную информацию, нарушить процедуры информационной безопасности.

Фишинг. Форма социальной инженерии. Мошенники рассылают пользователям электронные письма или текстовые сообщения, напоминающие сообщения из доверенных источников. При фишинговых атаках злоумышленники зачастую выманивают у пользователей данные банковских карт или учетные данные.

Целевая (таргетированная) атака. Продолжительная и целенаправленная кибератака, при которой злоумышленник получает доступ к сети и остается незамеченным в течение длительного периода времени. Целевые атаки обычно направлены на кражу данных у крупных предприятий или правительственных организаций.

Внутренние угрозы. Нарушения безопасности или потери, спровоцированные инсайдерами – сотрудниками, подрядчиками или клиентами – со злым умыслом или из-за небрежности.

DoS-атака (Denial of Service – «отказ в обслуживании»). Атака, при которой злоумышленники пытаются сделать невозможным предоставление услуги. При DoS-атаке вредоносные запросы отправляет одна

система. **DDoS-атака** (Distributed Denial of Service – «распределенный отказ в обслуживании»**)** исходит из нескольких систем. В результате атаки можно заблокировать доступ практически ко всему: серверам, устройствам, службам, сетям, приложениям и даже определенным транзакциям внутри приложений.

Сталкерское ПО. Программное обеспечение, предназначенное для скрытой слежки за пользователями, часто распространяемое под видом легального ПО. Такие программы позволяют злоумышленникам просматривать фотографии и файлы на устройстве жертвы, подглядывать через камеру смартфона в режиме реального времени, узнавать информацию о местоположении, читать переписку в мессенджерах и записывать разговоры.

Криптоджекинг. Относительно новый тип киберпреступлений, при которых вредоносное ПО устанавливается в системе и использует вычислительные ресурсы устройства с целью добычи криптовалюты для злоумышленника.

Атака Man-in-the-Middle («человек посередине»). В ходе атаки киберпреступник перехватывает данные во время их передачи – он как бы становится промежуточным звеном в цепи, и жертвы об этом не подозревают. Такой атаке можно подвергнуться при подключении к незащищенной сети Wi- Fi.

Атаки на цепочку поставок. При атаках подобного типа злоумышленники используют отношения доверия между организацией и ее контрагентами (клиентами). Если одна организация имеет надежную систему безопасности, но сеть ее доверенного клиента имеет слабую защиту, то преступники могут предпринять попытку взломать систему этого клиента, чтобы затем проникнуть в сеть целевой организации.

Атаки на системы искусственного интеллекта. Цель подобных атак – обмануть алгоритм искусственного интеллекта, функционирующего в составе системы кибербезопасностии, предназначенного для распознавания новых вредоносных программ, провоцируя его принимать неверное решение. Чаще всего злоумышленники используют так называемое «отравление данных», предлагая нейросети для обучения заведомо некорректную обучающую выборку.

1.2. Киберпреступления: понятие, виды и методы защиты

Киберпреступность – это преступная деятельность, в рамках которой используются либо атакуются компьютер, компьютерная сеть или сетевое устройство.

Киберпреступления совершаются как отдельными частными лицами, так и хорошо организованными и технически подготовленными преступными группировками.

Провести классификацию киберпреступлений достаточно сложно, т. к. их варианты в различных сочетаниях постоянно пополняются новыми разновидностями. Тем не менее известны варианты классификации киберпреступлений как на международном уровне, так и в законодательствах многих государств и работах отдельных исследователей. Рассмотрим некоторые примеры.

В 1991 г. Генеральный секретариат Интерпола ввел кодификатор компьютерных преступлений и способов их совершения. В соответствии с данным кодификатором каждому виду киберпреступлений поставлен в соответствие идентификатор, начинающийся с буквы Q. Для детализации описания преступления могут применяться до пяти кодов, расположенных в порядке убывания значимости. Всего выделено шесть групп компьютерных преступлений, каждая из которых делится на некоторое количество подгрупп:

1. QA – несанкционированный доступ и перехват;
2. QD – изменение компьютерных данных;
3. QF – компьютерное мошенничество;
4. QR – незаконное копирование;
5. QS – компьютерный саботаж;
6. QZ – прочие компьютерные преступления.

В 2001 г. Совет Европы принял Будапештскую Конвенцию «О преступлениях в сфере компьютерной информации», в которой определены четыре группы преступлений, каждая из которых включает по несколько составов:

1. Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:

– противозаконный доступ;
– неправомерный перехват;
– воздействие на данные;
– воздействие на функционирование системы;
– противозаконное использование устройств.

2. Правонарушения, связанные с использованием компьютерных средств:

– подлог с использованием компьютерных технологий;
– мошенничество с использованием компьютерных технологий.

3. Правонарушения, связанные с содержанием данных:

– преступления, связанные с детской порнографией.

4. Правонарушения, связанные с нарушением авторского права и смежных прав.

Российская Федерация не ратифицировала Будапештскую Конвенцию в связи с наличием в ней положений, предусматривающих трансграничный доступ к хранящимся компьютерным данным. Несмотря на это наиболее существенные положения Конвенции фактически имплементированы в российское уголовное законодательство.

В Уголовном кодексе Российской Федерации к киберпреступлениям отнесены правонарушения, предусмотренные гл. 28 «Преступления в сфере компьютерной информации»:

1. Статья 272. Неправомерный доступ к компьютерной информации.

2. Статья 273. Создание, использование и распространение вредоносных компьютерных программ.

3. Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

4. Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

5. 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.

В качестве мер защиты от киберпреступлений следует придерживаться ряда несложных правил:

– регулярно проводить аудиты безопасности и тесты на наличие уязвимостей;

– использовать актуальные средства защиты (брандмауэры, антивирусное программное обеспечение);

– регулярно обновлять операционную систему и используемые приложения;

– не открывать файлы, вложения или ссылки из писем от неизвестных адресатов;

– проявлять осторожность при открытии ссылок в письмах, мгновенных сообщениях и социальных сетях, даже если они пришли от адресатов, которые кажутся известными;

– периодически выполнять резервное копирование наиболее важной информации.

1.3. Риски и угрозы в интернете вещей

Интернет вещей (Internet of Things, IoT) – это множество предметов бытовой техники, оборудования, транспорта, имеющих электронные блоки управления, способные подключаться к Интернету и обмену данными. Широкое внедрение IoT может существенно улучшить многие сферы жизни людей и помочь создать более удобный, «умный» и безопасный мир. Примеры интернета вещей варьируются от носимых вещей, таких как «умные» часы, до «умного» дома, который умеет, например, контролировать и автоматически менять степень освещения и отопления. Многие из них не имеют защиты от атак. Злоумышленники могут легко получить доступ к таким устройствам, используя подбор пароля (brute force – метод грубой силы).

Среди основных направлений использования взломанных устройств IoT рассматривается их использование для организации DDoS-атак и в качестве узлов выхода VPN. В обоих случаях преступники продают свои услуги другим участникам сообщества.

1.4. Центры мониторинга информационной безопасности

Центр мониторинга информационной безопасности (кибербезопасности) или SOC-центр (от англ. Security Operations Center) –это структурное подразделение, осуществляющее непрерывный мониторинг работы систем защиты информации и реагирующее на инциденты информационной безопасности. SOC-центр включает не только аппаратно-программные системы, непрерывно передающие дежурной смене сообщения от средств защиты информации, но и собственно экспертов, анализирующих поступающую информацию с целью выявить как можно раньше начало инцидента кибербезопасности и предотвратить или уменьшить ущерб от компьютерной атаки. В принятии решений они опираются на информацию, предоставляемую специализированными аппаратно-программными системами, например: SIEM (Security Information and Event

Management, системы управления информацией о безопасности и событиями информационной безопасности), IRP (Incident Response Platform, платформы реагирования на инциденты информационной безопасности), SOAR (Security Orchestration, Automation and Response, системы управления, автоматизации и реагирования на инциденты), SGRC (Security Governance, Risk-management and Compliance, системы управления информационной безопасностью, рисками и соответствием законодательству).

SOC-центры могут быть внутренними и внешними. Внутренний SOC-центр – это структурное подразделение организации (компании), выполняющее указанные выше функции. Внешний SOC-центр – это сторонняя организация, предоставляющая на условиях договора услуги по оперативному реагированию на инциденты информационной безопасности.

Поступающая от систем контроля безопасности информация непрерывно обрабатываются дежурной сменой центра, которая включает в себя, как правило, следующих специалистов:

– системный администратор выполняет настройку внутренних систем SOC-центра, используемых в обработке инцидентов заказчиков;

– аналитик 1-го уровня выполняет первичную обработку инцидентов ИБ. Его задача – отсеять явные ложные срабатывания систем защиты. При этом аналитик 1-го уровня использует заранее разработанные сценарии реагирования, которые предписывают последовательность действий, предпринимаемых в случае того или иного типа инцидента. Если аналитик 1-го уровня может самостоятельно нейтрализовать инцидент, он осуществляет реагирование своими силами. В противном случае инцидент передается на следующий уровень аналитику 2-го уровня.

Другими словами, аналитику 2-го уровня приходится анализировать нетипичную ситуацию, применяя свои экспертные знания и опыт реагирования на инциденты, сопоставляя различные события и факты. В случае, если в расследуемой кибератаке применялось ранее неизвестное вредоносное ПО или вообще непонятно, что произошло, аналитик 2-го уровня передает инцидент еще выше – специалисту по реверс-инжинирингу, форензик-эксперту или в специализированные компьютерные лаборатории.

Специалист по реверс-инжинирингу – эксперт высшей категории, как правило, профессиональный программист. Его задача – понять, что делает и как функционирует вредоносное программное обеспечение. Для этого он может запустить вирус в изолированной среде («песочнице») для анализа его поведения, провести процедуру обратной разработки и полу-

чить из файла-образца первоначальный программный код, чтобы уже в нем найти особенности, которые помогут понять, что именно делает данный вирус и как ему лучше противостоять.

Форензик-эксперт (англ. forensics) – компьютерный криминалист. Его задача – понять, что изменилось в атакованной системе, какие данные были стерты, изменены или похищены вирусом, какие еще системы в компании-заказчике были атакованы.

Менеджер взаимодействует с руководством компании-заказчика, разъясняет, насколько серьезным был ущерб или какую именно угрозу удалось предотвратить. SOC-менеджер также координируют работу всей команды SOC-центра, связывает друг с другом заказчиков и исполнителей, выполняет организационную работу.

1.5. Безопасность объектов критической информационной инфраструктуры

Обработка инцидентов информационной безопасности требует высокой оперативности реагирования, в первую очередь, когда возникает угроза безопасности информационных систем наиболее важных отраслей экономики или всего государства. Подобные системы составляют критическую информационную инфраструктуру (далее – КИИ). В целях обеспечения информационной безопасности КИИ был принят Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (вступил в силу 01.01.2018).

Критическая информационная инфраструктура – это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ, а также сети электросвязи, используемые для организации их взаимодействия.

Кроме подписания данного Закона о КИИ, были назначены федеральные органы исполнительной власти (далее – ФОИВ), отвечающие за реализацию норм данного закона. Так, Федеральная служба по техническому и экспортному контролю (далее – ФСТЭК) России была назначена уполномоченным ФОИВ в области обеспечения безопасности критической информационной инфраструктуры РФ. На Федеральную службу безопасности (далее – ФСБ) РФ были возложены функции обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (далее –

ГосСОПКА). Приказом ФСБ РФ был создан Национальный координационный центр по компьютерным инцидентам (далее – НКЦКИ), который координирует деятельность субъектов КИИ и чья техническая инфраструктура используется для функционирования системы ГосСОПКА. Упрощенно, НКЦКИ – это Центр SOC в государственном масштабе, а система ГосСОПКА – это такая большая система SIEM для всей страны.

Также, как и во всех случаях защиты информации, важно определить меры по защите информации в КИИ, а для того, чтобы это осуществить, следует понять, какие объекты КИИ являются более важными и, соответственно, требуют большей защиты, а какие – не столь важны. Для этого было введено понятие категорирования объектов КИИ и подписано Постановление Правительства РФ от 8 февраля 2018 г. №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». В данном документе приведены требования для субъектов КИИ по осуществлению категорирования объектов КИИ и указаны перечень критерии значимости объектов КИИ.

Объектам КИИ могут быть назначены первая (самая высокая), вторая, третья категория значимости, или объект может быть признан не имеющим категории (при низкой значимости). Процедура категорирования объектов КИИ должна проводиться внутренней комиссией по категорированию субъекта КИИ, которая определяет список объектов КИИ с категориями значимости. Список затем отправляется в ФСТЭК России, которая эти сведения вносит в специальный реестр объектов КИИ.

ФСТЭК России издала ряд нормативных документов, детально описывающих организацию защиты информации в КИИ. Одним из основных является приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». Он применяется после того, как организацией – субъектом КИИ была проведена процедура категорирования своих объектов и определено, что среди них есть значимые. В соответствии с данным приказом разработка мер защиты информации значимого объекта КИИ включает анализ угроз безопасности и построение модели угроз безопасности КИИ.

ТЕМА 2. НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ

2.1. Задача нормативно-правового регулирования обеспечения кибербезопасности в Российской Федерации как компонент государственной политики развития национального сектора применения информационных технологий

Основными документами, определяющими в настоящий момент подходы к обеспечению информационной безопасности в Российской Федерации, являются следующие:

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.
2. Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ.
3. Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ.
4. Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ.
5. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ.
6. Федеральный закон «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» от 19.12.2005 № 160-ФЗ.
7. Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» от 21.07.2014 № 242-ФЗ.
8. Закон РФ «О государственной тайне» от 21.07.1993 № 5485-1.
9. Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ.
10. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.
11. Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона “О безопасности критической информационной инфраструктуры Российской Федерации”» от 26.07.2017 № 193-ФЗ.
12. Федеральный закон «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”» от 26.07.2017 № 194-ФЗ.

13. Федеральный закон «О банках и банковской деятельности» от 02.12.1990 № 395-1.

14. Федеральный закон «О лицензировании отдельных видов деятельности» от 04.05.2011 № 99-ФЗ.

15. Федеральный закон «Об экспортном контроле» от 18.07.1999 г. № 183-ФЗ.

16. Федеральный закон «О техническом регулировании» от 27.12.2002 № 184-ФЗ.

17. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ.

18. Гражданский кодекс Российской Федерации часть 4 (ГК РФ ч.4) 18.12.2006 № 230-ФЗ.

19. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ.

20. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ.

Перечисленные выше, а также сопутствующие им ведомственные нормативные документы на сегодняшний день формируют комплексную систему требований по обеспечению информационной безопасности для информационных систем различного уровня.

В настоящее время существует ряд нормативных актов, регулирующих отношения, связанные с информационной безопасностью. Центральное место занимает Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.

В 149-ФЗ сказано, какая информация считается конфиденциальной, а какая – общедоступной, когда и как можно ограничивать доступ к информации, как происходит обмен данными. Также именно здесь прописаны основные требования к защите информации и ответственность за нарушения при работе с ней.

Ключевые положения закона № 149-ФЗ:

1. Сбор и распространение информации о жизни любого человека без его согласия недопустимы.

2. Для создания собственной информационной системы компания, организация имеет право использовать любую информационную технологию. Принуждать компании к выбору конкретных технологий никто не вправе.

3. Определены категории информации, ограничение доступа к которой запрещено (сведения о состоянии окружающей среды, о техногенных или природных катастрофах и т. п.).

4. Определены категории информации, распространение которой на территории Российской Федерации запрещено (пропаганда терроризма, насилия,расовой, религиозной или иной нетерпимости).

5. Физическое или юридическое лицо, обладающее конфиденциальной информацией, обязано обеспечить ее защиту.

6. Роскомнадзор проводит мониторинг информации, размещаемой на сайтах в Интернете. При обнаружении информация, запрещенной к распространению на территории РФ и неудалении ее в установленные сроки, сайт может быть заблокирован и внесен в реестр запрещенных сайтов.

7. Для разблокировки сайта владелец обязан удалить незаконную информацию и уведомить об этом в Роскомнадзор.

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» регулирует работу с персональными данными – личными данными конкретных людей. Его требования обязаны соблюдать все юридические и физические лица, которые собирают и хранят эти данные.

Ключевые положения закона № 152-ФЗ:

1. Прежде чем получить и обрабатывать персональные данные, необходимо получить письменное согласие их владельца.

2. Сбор персональных данных может производиться только в конкретных целях.

3. Организация, имеющая базу персональных данных (сотрудников, клиентов и т. п.), обязана обеспечить ее защиту от утечек и доступа к ней третьих лиц.

4. Персональные данные должны быть удалены из базы по первому требованию их владельца.

5. Базы данных с персональной информацией должны храниться и обрабатываться на территории Российской Федерации. Передача данных за границу возможна только при соблюдении условий, прописанных в законе.

Федеральный закон № 63-ФЗ «Об электронной подписи». Электронная цифровая подпись (далее – ЭЦП) – цифровой аналог физической подписи. ЭЦП является подтверждением подлинности информации и исключает возможность ее модификации или подделки. В закон определено понятие электронной подписи, сфера ее применения, юридическая сила ЭЦП.

Ключевые положения Федерального закона № 63-ФЗ «Об электронной подписи»:

1. Создание ЭЦП возможно с помощью любого сертифицированного программного обеспечения и технических средств, которые обеспечивают требуемую надежность подписи.

2. Установлены три категории ЭЦП: простая, усиленная неквалифицированная и усиленная квалифицированная. Они имеют разные технические особенности, разные сферы применения и разную юридическую силу. Наиболее надежные – усиленные квалифицированные подписи, они полностью аналогичны физической подписи на документе.

3. Владелец ЭЦП обязан охранять ключ подписи.

4. Выдачу ЭЦП и сертификатов, подтверждающих их действительность, осуществляет только специальный удостоверяющий центр.

2.2. Законодательство Российской Федерации в области защиты информации

Все специалисты по информационной безопасности рано или поздно сталкиваются с вопросами законодательного регулирования своей деятельности. Первой проблемой при этом обычно является поиск документов, где прописаны те или иные требования.

Во главе этой схемы стоит Федеральный закон «Об информации, информационных технологиях и о защите информации» (от 27.07.2006 № 149-ФЗ). Перечень конфиденциальной информации определен в Указе Президента «Об утверждении перечня сведений конфиденциального характера» (от 6 марта 1997 г. № 188). Это справочный документ, никаких особых указаний там нет. Но из перечня ясно, что в конфиденциальную информацию входит целое семейство тайн: коммерческая, служебная, профессиональная и многие другие. Всего более 50 разновидностей. Каждой посвящен отдельный нормативный акт, например, Федеральный закон «О коммерческой тайне» (от 29.07.2004 № 98-ФЗ). Работе с персональными данными посвящен отдельный Федеральный закон «О персональных данных» (от 27.07.2006 № 152-ФЗ). Он перечисляет категории персональных данных, из его положений вытекают обязательства, связанные с их обработкой. Их можно детально изучить в отдельных нормативных правовых актах. Постановление правительства № 1119 (от 1.11.2012) поможет установить тип информационной системы и необходимый уровень защищенности в зависимости от объема данных, а приказ № 21 ФСТЭК (от 18.02.2013) подскажет базовый перечень необходимых защитных мер. Это уже информация, необходимая на практике. Согласно п. 6 приказа

№ 21 ФСТЭК необходимо как минимум раз в три года проводить оценку эффективности и соответствия закону мер по безопасности персональных данных. Чтобы подобрать защиту под конкретную информационную систему, придется также определить, каким угрозам подвергаются персональные данные при обработке. Для решения этой задачи служит методика оценки безопасности от ФСТЭК.

Банк угроз БДУ. Там собрано описание более 200 различных угроз с возможными источниками и объектами, которые им подвержены.

Чтобы найти списки сертифицированных СЗИ, можно воспользоваться Положением о сертификации средств защиты информации.

Системы сертификации создаются ФСТЭК, ФСБ, Министерством обороны, которые уполномочены проводить работы по сертификации СЗИ в пределах компетенции, определенной для них законодательными и иными нормативными актами Российской Федерации (далее именуются – федеральные органы по сертификации).

Закон № 152-ФЗ также указывает на необходимость создания целого пакета локальных нормативных актов по обработке и защите персональных данных, предъявляет требования к техническим организационным мерам защиты.

Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» регулирует отношения в области обеспечения безопасности КИИ Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

2.3. Основы государственной политики Российской Федерации в области международной информационной безопасности

12 апреля 2021 г. Президентом Российской Федерации был подписан Указ № 213 «Об утверждении основ государственной политики Российской Федерации в области международной информационной безопасности». Данным Указом были утверждены основы государственной политики России в области международной информационной безопасности, призванные способствовать продвижению российских подходов к формированию системы обеспечения международной информационной безопасности и российских инициатив в этой сфере, содействию создания международно-правовых механизмов предотвращения и урегулирования

межгосударственных конфликтов в информационном пространстве, организации межведомственного взаимодействия.

В Указе определены основные угрозы в информационной сфере: использование IT-технологий в военно-политической и иной сферах для подрыва суверенитета государств, нарушения их территориальной целостности, а также в террористических, экстремистских и преступных целях.

В общих положениях документа указано, что «основы являются документом стратегического планирования Российской Федерации и отражают официальные взгляды на сущность международной информационной безопасности».

Во втором разделе Указа раскрыты сущность международной информационной безопасности и основные угрозы международной информационной безопасности.

Третий раздел документа содержит формулировки цели и задач государственной политики в области международной информационной безопасности. Указано, что цель государственной политики в области международной информационной безопасности заключается в содействии установлению международно-правового режима, при котором создаются условия для предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве, а также для формирования с учетом национальных интересов Российской Федерации системы обеспечения международной информационной безопасности.

В четвертом разделе Указа определены основные направления реализации государственной политики в области международной информационной безопасности.

В пятом разделе Указа – задачи федеральных органов исполнительной власти Российской Федерации по созданию механизмов реализации государственной политики в области международной информационной безопасности

2.4. Международные стандарты в области обеспечения кибербезопасности

Стандарты кибербезопасности – опубликованные и многократно проверенные методы защиты информационных систем от различного рода киберугроз.

Основная цель применения стандартов кибербезопасности – снижение рисков, предотвращение или уменьшение ущерба в случае

возникновения инцидента кибербезопасности. Стандарты кибербезопасности включают описание инструментов, политик, концепций и мер безопасности, руководств, подходов к управлению рисками, действий, обучения, передовых методов, гарантий и технологий.

Каждый специалист, работающий в сфере кибербезопасности, должен знать наиболее эффективные методологии в этой области и владеть их практическим применением.

Международные стандарты кибербезопасности развивались и совершенствовались годами, вбирая в себя лучший практический опыт.

Освоение общепризнанных стандартов кибербезопасности позволяет специалистам продуктивно взаимодействовать между собой и с подразделениями компаний, ответственных за ИБ с использованием принятых терминов и определений.

Методы классификации стандартов кибербезопасности могут различаться по целям и задачам применения. Один из возможных подходов – разделение стандартов: технические (прикладные) и процессно-ориентированные.

Технические стандарты регламентируют различные аспекты реализации мер защиты, помогают выполнить выстраивание технической защиты информации – выбрать необходимый комплекс защитных мер и провести их грамотную настройку. Процессно-ориентированные стандарты описывают поход к выстраиванию отдельных процессов.

Краткий обзор стандартов кибербезопасности

COBIT. Международная ассоциация ISACA (Information Systems Audit and Control Association), известная разработкой стандартов по управлению ИТ в корпоративной среде, и Институт руководства ИТ (IT Governance Institute – ITGI) совместно разработали подход к управлению информационными технологиями. В 1996 г. на его основе была выпущена первая версия стандарта COBIT. В настоящее время самой новой версией методологии является COBIT 2019, которая описывает набор процессов, лучших практик и метрик для выстраивания эффективного управления и контроля, а также достижения максимальной выгоды от использования ИТ.

ITIL и ITSM. Библиотека инфраструктуры информационных технологий, или ITIL (The IT Infrastructure Library) – это набор публикаций (библиотека), описывающий общие принципы эффективного использования ИТ-сервисов. Библиотека ITIL применяется для практического внедрения подходов IT Service Management (ITSM) – проектирования сервисов и ИТ-инфраструктуры компании, а также обеспечения их связности.

ITIL можно рассматривать в том числе с точки зрения информационной безопасности, т. к. для успешного использования ИТ и поддерживаемых услуг необходимо обеспечивать доступность, целостность и конфиденциальность ИТ-инфраструктуры.

Серия ISO/IEC 27XXX. Наиболее известным и популярным набором стандартов, к которому обращаются в первую очередь при внедрении СУИБ, являются документы из серии ИБ-стандартов ISO/IEC 27XXX.

Стандарт ISO/IEC 27001:2013 имеет российский аналог ГОСТ Р ИСО/МЭК 27001.

Разработанная совместно с Международной электротехнической комиссией (МЭК) техническая спецификация ISO/IEC TS 27110 «Информационные технологии, кибербезопасность и защита частной жизни – Руководящие принципы разработки рамок кибербезопасности» содержит информацию о том, как создать или усовершенствовать надежную систему защиты от кибератак. Эта техническая спецификация призвана упростить задачу как для создателей, так и для пользователей путем предоставления согласованного на международном уровне минимального набора концепций и определений.

NIST (National Institute of Standards and Technology) – американский национальный институт стандартизации, аналог отечественного Госстандарта. В состав института входит Центр по компьютерной безопасности, который публикует с начала 1990-х годов Стандарты (FIPS), а также детальные разъяснения/рекомендации (Special Publications) в области информационной безопасности.

SANS. CIS 20.SANS – организация по обучению и сертификации в области ИБ, наиболее известна своими руководствами по безопасной настройке различных систем (Benchmarks) и перечнем ключевых мер защиты Top 20 Critical Security Controls (CSC), включающим 20 рекомендаций по защите ИТ-инфраструктуры. ИБ-специалисты могут использовать этот документ как контрольный список при проверке безопасности систем.

ТЕМА 3. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

3.1. Уязвимости оконечных устройств, реализующих информационные процессы

В настоящее время так называемые оконечные устройства (далее – ОУ) являются частью онлайн-сетей многих организаций. Подобные устройства предоставляют сотрудникам и разработчикам географическую независимость при работе на различных уровнях, что позволяет повысить эффективность их работы, т. к. они могут быстрее выполнять задания, держа при этом данные в организованном и доступном виде.

При этом важно понимать потенциальные угрозы, которые сопутствуют оконечным устройствам, и знать, что можно сделать, чтобы защитить организацию.

Что такое оконечное устройство?

Оконечное устройство (оконечное оборудование обработки данных, (ООД), терминальное оборудование) – оборудование, преобразующее пользовательскую информацию в данные для передачи по линии связи и осуществляющее обратное преобразование.

Это обобщенное понятие, используемое для описания оконечного прибора пользователя или его части. ОУ может являться источником информации, ее получателем или тем и другим одновременно. Оно передает и/или принимает данные посредством использования оконечного оборудования линии связи и канала связи.

Примеры оконечных устройств: настольные компьютеры, серверы, ноутбуки, планшеты, смартфоны, принтеры, POS-терминалы, сетевые камеры наблюдения, любое другое оборудование, способное передавать или принимать данные.

Еще одна специфичная черта оконечных устройств: некоторые из них могут получать доступ к нескольким сетям, и многие из них это делают на регулярной основе. Это подвергает их множеству угроз, когда злоумышленники из других сетей могут украсть информацию.

Так, сотрудники могут выносить их из офиса и подключать к небезопасным Wi-Fi сетям в соседнем кафе или в гостинице в любом городе страны. Такая практика усиливает уязвимости системы безопасности так, что хакеры

могут получать конфиденциальные данные, которые хранятся на корпоративных устройствах или к которым получают доступ с таких устройств.

Угрозы безопасности оконечных устройств

Утечка данных с ОУ. Использование имеющегося или организация нового канала утечки информации с ОУ. Кроме того, утечка может быть и случайной, например, в случае потери телефона.

Блокирование ОУ. Нарушение нормального функционирования устройства с целью временного исключения его из информационного поля организации.

Уничтожение ОУ. Выведение из строя устройства с целью нанесения его исключения из информационного поля организации и нанесения материального вреда.

Использование ОУ. Использование вычислительных мощностей устройства для решения задач, не связанных с его назначением.

3.2. Способы совершения кибератак на средства хранения, обработки и передачи данных

Типовые виды атак на оконечные устройства описаны в п. 1.1.

Большинство атак происходит следующими методами:

1. Социальная инженерия.
2. Через вредоносные программы.
3. Комбинация первого и второго.

Рассмотрим их более подробно.

Методы социальной инженерии

Социальная инженерия в контексте информационной безопасности – психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации.

Первым шагом в противостоянии такого вида уловкам является понимание самих тактик злоумышленников. Ниже перечислены семь основных подходов в социальной инженерии:

- теория шести рукопожатий;
- изучение корпоративного языка;
- заимствование музыки для ожидания во время звонков;
- спуфинг (подмена) телефонного номера;
- использование новостей против вас;

– использование доверия к социальным платформам;
– тайпсквоттинг.

Вредоносные программы

Вредоносная программа или вредоносное программное обеспечение (далее – ВПО) – это программа, разработанная с целью нанесения вреда устройствам и данным. Как правило, вредоносные программы создаются злоумышленниками для похищения конфиденциальной информации (персональных, учетных, данных, данных платежных карт), шифрования файлов на компьютере жертвы и последующего вымогательства. Атакам ВПО могут подвергаться все виды устройств и операционных систем. Известно, что ежегодно совершается более 5 млрд таких атак. Более 90 % из них начинаются с доставки ВПО по электронной почте. В последние годы резко увеличилось количество вредоносных программ для мобильных устройств. Поэтому важно распознавать все виды вредоносных программ. Ниже перечислены несколько различных типов вредоносных программ.

Червь – ВПО, которое может создавать собственные копии и автоматически распространяться по сети. Червь может попасть в компьютер или смартфон в виде вложений в мгновенные сообщения или спам, распространяемый по электронной почте, а также может проникнуть через уязвимости программного обеспечения. Установившись на компьютере, червь начинает работать в фоновом режиме незаметно для пользователя. Он может внедрять вредоносный код в файлы операционной системы, изменять или удалять файлы.

Кейлоггер – это ВПО, выполняющее скрытый контроль за клавиатурой и запись всех нажатий клавиш в файл, который позднее может быть передан злоумышленнику.

Руткиты – различные вредоносные программы для предоставления несанкционированного доступа к программному обеспечению компьютера, включая операционную систему. Руткиты могут содержать множество различных кодов – от программ, отключающих защитное ПО и отслеживающих все, что вводится на компьютере, до скриптов, позволяющих злоумышленникам украсть пароли и банковскую информацию. Поэтому их трудно обнаружить. Они могут жить на устройстве в течение долгого времени (недель или даже месяцев), нанося существенный ущерб. Если руткит поселился в ядре операционной системы, удаление его может быть практически невозможно. В этом случае единственный способ избавиться от руткита – установить новую операционную систему.

Бесфайловые вредоносные программы часто используют программу автоматизации задач и управления конфигурацией Microsoft Power Shell. Вредоносные программы этого типа не хранятся на диске и не устанавливаются непосредственно на устройство. Они проникают в основную память, не зависят от других файлов, не имеют сигнатур и не оставляют следов. Это значительно затрудняет их обнаружение и удаление. Так как они могут существовать только в оперативной памяти, их жизнеспособность сохраняется до перезагрузки системы.

Adware (рекламное ПО). Рекламное ПО отображает рекламу на экране устройства и отслеживает запросы пользователей в маркетинговых целях. Основная цель создания рекламного ПО – получение прибыли за счет показа рекламы пользователям при установке приложений или просмотре веб-страниц.

Вредоносные боты. Интернет-боты (веб-роботы) предназначены для выполнения автоматизированных задач (скриптов) через Интернет. Они эффективно выполняют простые и повторяющиеся задачи – например, собирать данные с миллиардов веб-страниц. Сложные боты, созданные с использованием методов машинного обучения, могут имитировать поведение человека. Вредоносные боты могут заражать большое количество устройств, создавая сеть, называемую ботнетом. Ботнеты часто используются злоумышленниками для рассылки спама, выполнения DDoS-атак и похищения информации.

RAM Scraper («скребок» оперативной памяти). Это вредоносная программа, которая атакует терминал, используемый для обработки розничных транзакций (атака на точку продажи – POS). Стандарты безопасности данных, используемые в платежных системах, предусматривают сквозное шифрование конфиденциальной информации. Эта информация расшифровывается в оперативной памяти POS для обработки, и именно в этот момент срабатывает RAM Scraper. Другими словами, RAM Scraper – это тип ВПО, способный украсть информацию о кредитной карте и ее владельце во время оплаты.

Бэкдор – это ВПО для получения доступа к системе или приложению путем обхода обычных процедур аутентификации, а также других стандартных методов обеспечения безопасности. Это дает злоумышленникам возможность удаленно управлять системой. Как правило, установка бэкдора достигается за счет использования уязвимостей в программном обеспечении. Бэкдоры входят в пятерку наиболее распространенных угроз.

Программа-вымогатель шифрует файлы заданного типа либо всю операционную систему. Затем от злоумышленника поступает требование выкупа в установленный срок для восстановления доступа после оплаты. Если жертва не заплатит до истечения срока, то сумма выкупа увеличивается или файлы остаются зашифрованными.

Шпионские программы устанавливаются на оконечное устройство и скрытно отслеживают поведение пользователя в Интернете.

Троян. Троянская программа маскируется под легитимное ПО. Троян может быть внедрен в загружаемые файлы или электронные письма. После установки он может похитить данные, загрузить другие вредоносные программы, открыть бэкдор. В отличие от компьютерных вирусов и червей, троянские программы не способны к самовоспроизведению.

Компьютерный вирус – это ВПО, которое может распространять свои копии в сети, заражая другие компьютеры. Вирус проникает в систему из Интернета, с зараженных носителей, от других устройств сети.

3.3. Способы защиты от вредоносного программного обеспечения

Для борьбы с ВПО разработано специальное ПО для распознавания и обезвреживания компьютерных вирусов (антивирусные программы).

Антивирусное ПО – это программы, предназначенные для профилактики заражения, обнаружения, удаления вредоносных программ и последующего восстановления работоспособности компьютера.

В настоящее время для этих целей используются два основных подхода: сигнатурный и проактивный (эвристический).

Сигнатурные методы обнаружения вирусов основаны на сравнении проверяемого файла с известными образцами (сигнатурами) вирусов.

Проактивные (эвристические методы) – приблизительные методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл заражен.

Главный недостаток сигнатурного метода – невозможность обнаружения нового вируса, если его сигнатура отсутствует в базе. Создать сигнатуру вируса можно только после того, как вирус попал на анализ к экспертам. Поэтому сигнатуры всегда появляются только через некоторое время после появления нового вируса.

Проактивные методы ориентированы на предотвращение заражения системы пользователя, а не на обнаружение уже известных вирусов.

Проактивная защита строится, как правило, на основе эвристических анализаторов и поведенческих блокираторов.

Брандмауэр (фаэрвол) – это программа, контролирующая сетевой трафик и разрешающая или запрещающая поступление извне пакетов на основании заданного набора правил.

Правило брандмауэра задается несколькими атрибутами: приложение, протокол, адреса, порт и т. д. Реакция может быть следующей: разрешить, запретить или спросить у пользователя.

3.4. Принципы обеспечения сетевой безопасности

Для защиты современных компьютерных сетей и ИТ-инфраструктуры требуется комплексный подход, четкое понимание всех уязвимых мест, а также соответствующих необходимых мер защиты. И хотя одно такое знание не сможет предотвратить все попытки проникновения в сеть или атаки на систему, но оно даст возможность сетевым администраторам устранить определенные глобальные проблемы, значительно сократить возможный ущерб и позволит быстро находить пробелы в защите. Из-за постоянного растущего числа и сложности атак злоумышленников необходимы бдительные методы обеспечения безопасности систем как для больших, так и для малых предприятий.

Во всем мире частота атак на корпоративные компьютерные сети возрастает каждый год. Незнание и невыполнение принципов безопасности сети – главная причина сложившейся ситуации. Корпоративные сети становятся более уязвимыми в результате установки дополнительных приложений, подключения новых устройств и пользователей сети.

Несмотря на то, что основные угрозы являются следствием перечисленных событий, они необходимы для развития любой организации, расширения ее возможностей и решения более широкого круга задач.

С учетом этого целесообразно сформулировать пять основных принципов, лежащих в основе поддержания компьютерной сети в безопасном состоянии.

Принцип 1. Обучение сотрудников требованиям сетевой безопасности.

Человеческий фактор – одна из самых больших угроз безопасности организации. Сюда входят такие ошибки, как загрузка вредоносных

файлов, передача паролей и невозможность их регулярного обновления, а также фишинг.

Эффективным способом смягчения проблем кибербезопасности является обучение сотрудников передовым методам обеспечения безопасности в сети. Необходимо обучить сотрудников способам выявления фишинг-атак и способам реагирования на них. При этом следует обратить их внимание на важность обновления установленного программного обеспечения, особенно если они работают с личных устройств.

Создание политики безопасности, касающейся частоты смены паролей, доступа к сети, процедуры сообщения о потерянных устройствах, безопасных способов обмена файлами и многого другого. Необходимо обучить сотрудников этой политике и убедиться, что они понимают ее.

Принцип 2. Постоянное обновление программного обеспечения и создание резервных копий критически важных ресурсов.

Резервное копирование (англ. backupcopy) – процесс создания копии данных на носителе (жестком диске и т. д.), предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения.

Любой организации необходим план сетевой безопасности на случай повреждения данных недобросовестными сотрудниками, злоумышленниками, проникновением вредоносных программ и природных явлений, таких как наводнения, пожары и землетрясения.

Инвестирование в управляемые ИТ-услуги – это один из лучших способов использовать круглосуточный мониторинг информационной безопасности антивирусной защитой, консультациями по сетевой безопасности, обновлениями системы, резервным копированием данных и облачными услугами. Необходимо иметь расписание обновления данных и резервного копирования системы.

Принцип 3. Реагирование на инциденты.

Реагирование на инциденты (Incident Response) – комплекс мероприятий по обнаружению и прекращению кибератаки или утечки данных из инфраструктуры организации и устранению последствий.

Порой сложно отслеживать и реагировать на все, что происходит в ваших сетях и устройствах, своими силами. Здесь на помощь приходят различные инструменты, позволяющие автоматизировать эти процессы.

Принцип 4. Защита беспроводных сетей и точек возможного проводного подключения.

Одной из точек входа для взлома является беспроводная сеть организации. Тем не менее выполнить эту задачу относительно легко.

Во-первых, необходимо использовать брандмауэр сети и шифрование данных. Во-вторых, необходимо защитить панель администрирования роутера паролем и использовать привязку беспроводных устройств по их MAC-адресу, тем самым исключив возможность несанкционированного подключения к нему незарегистрированным устройствам посторонних лиц. Можно также скрыть идентификатор сети (SSID), настроив роутер таким образом, чтобы он не отображал имя вашей сети.

Принцип 5. Двухфакторная аутентификация.

Двухфакторная аутентификация – это метод идентификации пользователя в каком-либо сервисе (как правило, в глобальной сети) при помощи запроса аутентификационных данных двух разных типов, что обеспечивает двухслойную, а значит, более эффективную защиту аккаунта от несанкционированного проникновения. Это одна из самых игнорируемых угроз безопасности сетей небольших организаций!

Большинство злоумышленников получают доступ к облачным ресурсам организации, потому что предприятия не включают двухфакторную аутентификацию.

Принцип 6. Сегментация сети.

Сегментация сети – метод обеспечения безопасности сети, который заключается в разделении сети на более мелкие отдельные подсети. При этом специалисты по сети могут распределять эти подсети по сегментам и предоставлять уникальные средства и службы управления безопасностью для каждой из них. В случае взлома, когда сеть не сегментирована, угроза может легко распространиться. Сегментация помогает изолировать угрозы.

Сетевая безопасность является серьезной проблемой для всех организаций (малых или крупных), но при надлежащих мерах кибербезопасности есть реальная возможность максимально снизить последствия возможной кибератаки.

3.5. Обнаружение вторжений и управление рисками

Система обнаружения вторжений (СОВ) – программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет.

Соответствующий английский термин – Intrusion Detection System (IDS). Системы обнаружения вторжений используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей).

Управление рисками (менеджмент риска)

Одним из важнейших аспектов обеспечения нормального функционирования любой организации является задача анализа и управления информационными рисками.

В аспекте информационной безопасности риск можно связать с событием реализации угрозы ресурсам информационной системы, вследствие которого произошло нарушение одной или более их базовых характеристик безопасности – конфиденциальности, целостности, доступности.

Риск информационной безопасности (information security risk) – возможность того, что угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации.

Информационный актив – информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для организации и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

Процесс менеджмента риска ИБ может быть применен ко всей организации, к любой отдельной части организации (например, подразделению, филиалу, службе), к любой информационной системе, к имеющимся, планируемым или специфическим аспектам управления (например, к планированию непрерывности бизнеса).

Процесс менеджмента риска ИБ состоит из установления контекста, оценки риска, обработки риска, принятия риска, коммуникаций риска, а также мониторинга и переоценки риска информационной безопасности.

Как показано на рисунке 1, в процессе менеджмента риска ИБ процедуры оценки риска и/или обработки риска могут выполняться итеративно. Итеративный подход к проведению оценки риска может увеличить глубину и детализацию оценки при каждой последующей итерации. Итеративный подход позволяет сбалансированно затрачивать время и усилия на выбор мер и средств контроля и управления, в то же время по-прежнему обеспечивая соответствующую оценку высокоуровневых рисков.

Оценка уровня рисков проводится на основании сопоставления оценок вероятности реализации угрозы информационной безопасности критичным информационным активам и оценок соответствующих потенциальных убытков.

Обработка риска – процесс выбора и осуществления защитных мер, снижающих риск нарушения ИБ, или мер по переносу, принятию или уходу от риска.

Принятие риска – решение о покрытии возможных потерь в результате рискового события за счет собственных средств организации.

Коммуникация риска – процесс обмена информацией о различных видах риска между заинтересованными сторонами (государственные учреждения, промышленные предприятия, профсоюзы, СМИ, ученые-исследователи, общественные организации и отдельные граждане).

Мониторинг и переоценка риска – процесс отслеживания идентифицированных рисков, определение остаточных рисков, идентификации новых рисков.

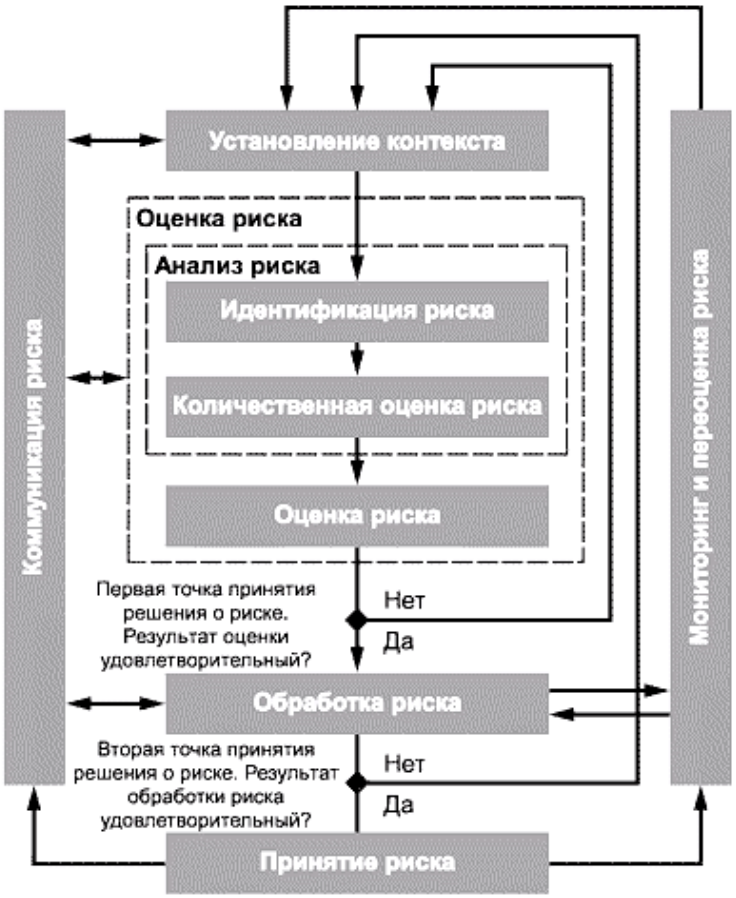

Рис. 1. Процесс менеджмента (управления) риска

3.6. Обеспечение безопасности операционных систем

Программные средства защиты информации являются, как правило, прикладными программами, которые функционируют под управлением операционной системы (далее – ОС). Окружение, в котором функционирует ОС, называется доверенной вычислительной базой (ДВБ). Она включает в себя полный набор элементов, обеспечивающих информационную безопасность: ОС, программы, сетевое оборудование, средства физической защиты и даже организационные процедуры.

Краеугольным камнем этой пирамиды является защищенная ОС.

Угрозы безопасности ОС

ОС может подвергнуться следующим типичным атакам:

- сканирование файловой системы;
- подбор пароля;
- кража ключевой информации;
- сборка мусора;
- превышение полномочий;
- программные закладки;
- жадные программы.

Журналирование событий в Windows

ОС Windows оснащена функцией, которая регистрирует все, что происходит в компьютере. Данные записываются в Журнал событий, даже если пользователь ничего не делал. В нем отображаются ошибки и предупреждения.

Журнал событий Windows – функция, позволяющая просматривать все действия, происходящие в ОС. Записываются сообщения, ошибки работы драйверов, приложений и программ в лог, который называется Журналом событий.

Просмотр сообщений помогает найти проблемы в защите устройства. Это полезно для серверов и рабочих станций. Основное предназначение – сбор информации для устранения неисправностей.

Это файлы расширением EVTX. Находится по адресу:

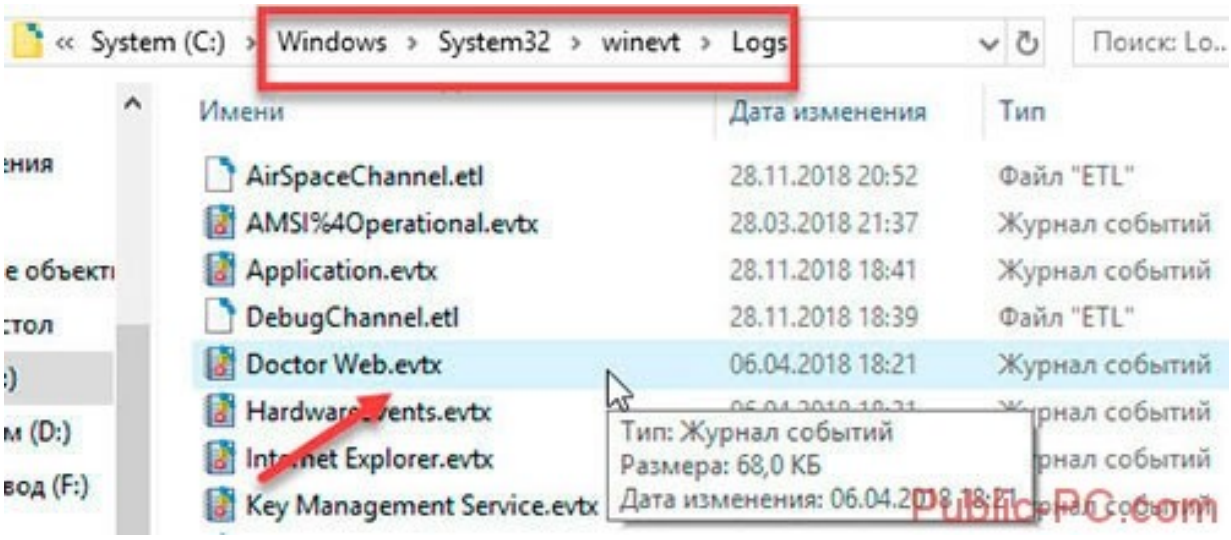

Рис. 2. Расположение файлов сообщений ОС

Содержание файлов – текстовая информация, но открыть их текстовым редактором не получится. Они содержат двоичный формат. Для просмотра используется утилита eventvwr.

Для запуска утилиты следует нажать Win+R, прописать control либо нажать Win+R, прописать eventvwr.msc.

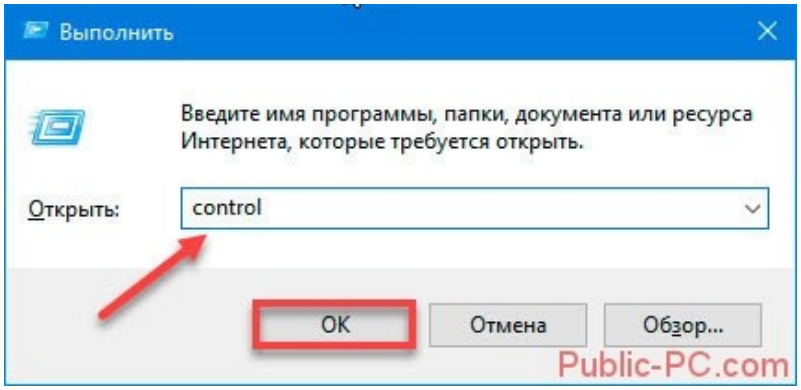

Рис. 3. Запуск утилиты eventvwr

Слева расположены журналы.

Средняя колонка отображает события. Правая – действия. Ниже – сведения о выбранной записи. Работа происходит с разделом «Журналы», в который входят 5 категории. Основными являются:

− **Система**. Содержит действия, которые созданы драйверами и модулями ОС.

− **Установка**.

− **Безопасность**. Информация о входе в аккаунты, учетные записи, доступ к файлам, установки процессов.

− **Приложение**. Информация об ошибках, созданных установленным программным обеспечением. Используется для того, чтобы найти причину неработоспособности приложений.

− **Перенаправление**.

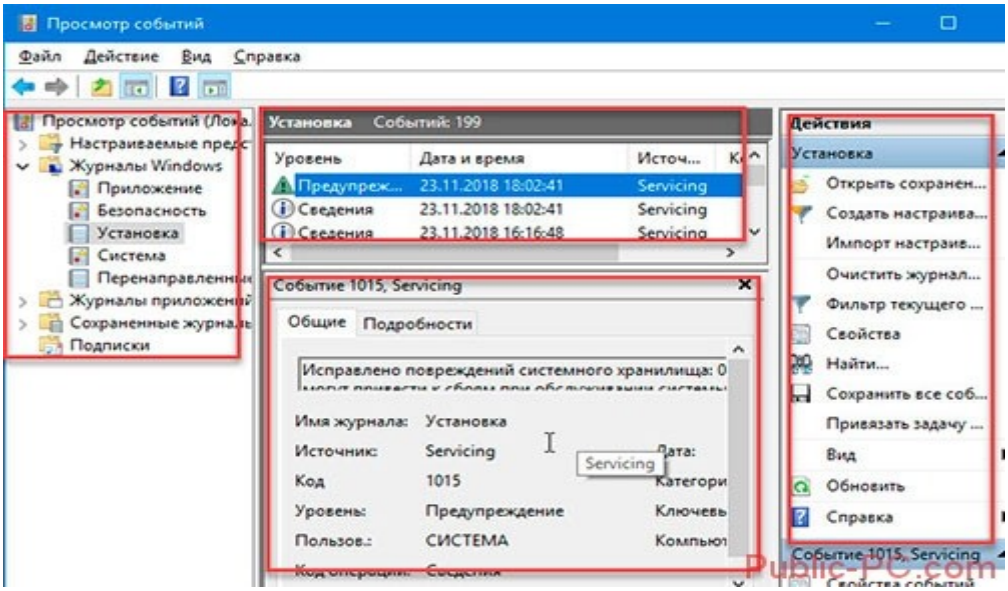

Рис. 4. Вид окна утилиты eventvwr

ТЕМА 4. ИСТОЧНИКИ И КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ. ОСНОВЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

4.1. Технические каналы утечки информации

Технический канал утечки информации (далее – ТКУИ) – совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Утечка (информации) по техническому каналу – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

На рис. 5 показана структура ТКУИ.

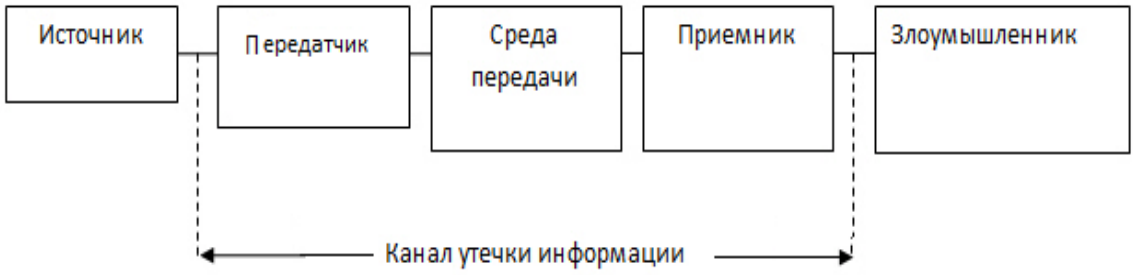

Рис. 5.Структура технического канала утечки информации

Информация от источника поступает на вход канала в форме первичного сигнала. В качестве источника сигнала могут выступать объект наблюдения, отражающий (излучающий) электромагнитные или акустические волны, передатчик легитимного канала связи, закладное устройство и т. п.

Передатчик ТКУИ преобразует первичный сигнал в форму, обеспечивающую его распространение (передачу) в среде передачи.

Среда передачи – физическая среда, по которой информативный сигнал может распространяться и регистрироваться приемником.

Приемник выполняет обратное преобразование сигнала, позволяющее выделить полезную информацию.

Классификация технических каналов утечки информации может быть представлена следующей структурой (рис. 6).

По физической природе носителя можно выделить следующие виды ТКУИ:

- оптические;
- радиоэлектронные;
- акустические;
- материально-вещественные.

Рис. 6. Классификация технических каналов утечки информации

Носителем информации в **оптическом канале** является электромагнитное поле в оптическом диапазоне (световой поток).

В **радиоэлектронном канале** носителями являются электромагнитные поля в радиодиапазоне, а также электрический ток в металлическом проводнике.

В **акустическом канале** носителями информации являются упругие акустические волны, распространяющиеся в среде.

В **материально-вещественном канале** утечка информации производится путем несанкционированного распространения за пределы контролируемой зоны вещественных (например, бумажных) носителей с защищаемой информацией.

В зависимости от ценности передаваемой информации можно выделить **информативные, малоинформативные и неинформативные** ТКУИ**.**

По времени проявления каналы делятся на **постоянные, периодические и эпизодические**. В постоянном канале утечка информации носит достаточно регулярный характер. К эпизодическим каналам относятся каналы, утечка информации в которых имеет случайный разовый характер.

В контексте изучения ТКУИ необходимо ознакомиться со следующими понятиями:

Основные технические средства и системы (далее – ОТСС) – это средства и системы, в которых непосредственно передается, обрабатывается и (или) хранится защищаемая информация.

Вспомогательные технические средства и системы (далее – ВТСС) – технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, размещаемые совместно с основными техническими средствами или в защищаемых помещениях (системы пожарной и охранной сигнализации, кондиционирования и т. п.).

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

«Микрофонный эффект» – нежелательное преобразование акустического сигнала в электрический элементами ОТСС и ВТСС.

В зависимости от вида канала связи ТКУИ можно разделить на электромагнитные, электрические и индукционные.

Электромагнитый ТКУИ – электромагнитные излучения передатчиков систем и средств связи. Используется для перехвата информации, передаваемой по каналам радио-, радиорелейной, спутниковой связи (рис. 7).

Рис. 7. Перехват информации по каналам радиосвязи

Электрический ТКУИ – съем информации с кабельных линий связи путем контактного подключения аппаратуры злоумышленника.

Индукционный (бесконтактный) ТКУИ обеспечивает получение злоумышленником информации за счет эффекта возникновения вокруг кабеля связи электромагнитного поля, модулированного информационным сигналом, которое может восприниматься специальным индукционным датчиком, усиливаться и демодулироваться аппаратурой злоумышленника. На рис. 8 показаны индукционный и электрический ТКУИ.

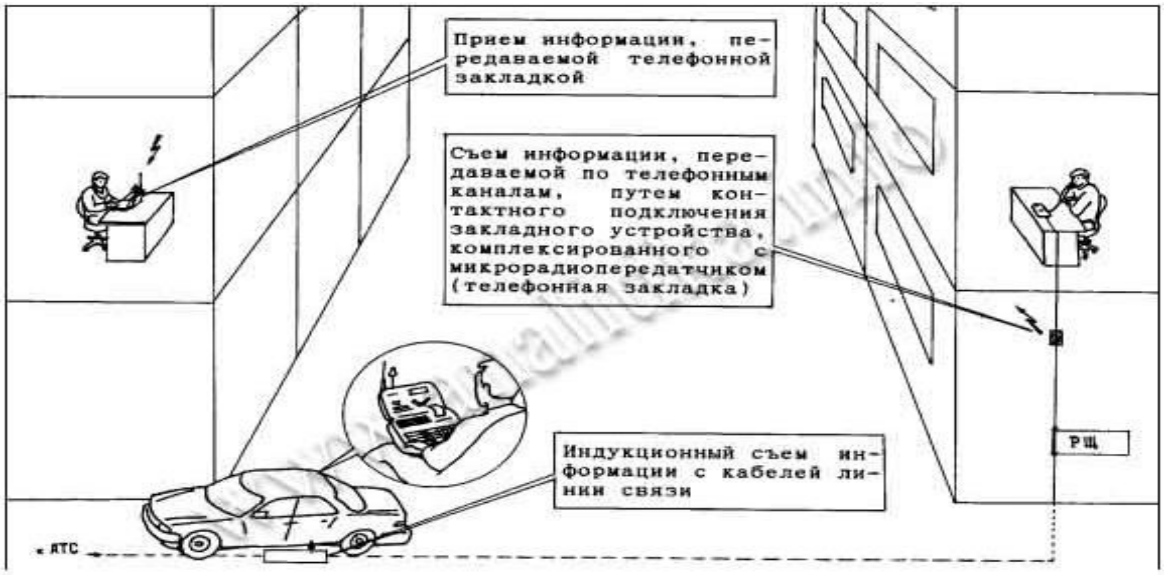

Рис. 8. Перехват информации по индукционному и электрическому ТКУИ

4.2. Каналы утечки акустической информации

Первичными источниками акустических колебаний являются механические системы, например, органы речи человека, а вторичными – преобразователи различного типа, в том числе электроакустические.

Выделяют воздушные, вибрационные, электроакустические, оптико-электронные и параметрические каналы утечки акустической информации.

В воздушных каналах утечки средой распространения акустических сигналов является воздух. Основным средством перехвата информации является микрофон, преобразующий акустический сигнал в электрический, который записывается запоминающим устройством или поступает на передатчик злоумышленника (рис. 9).

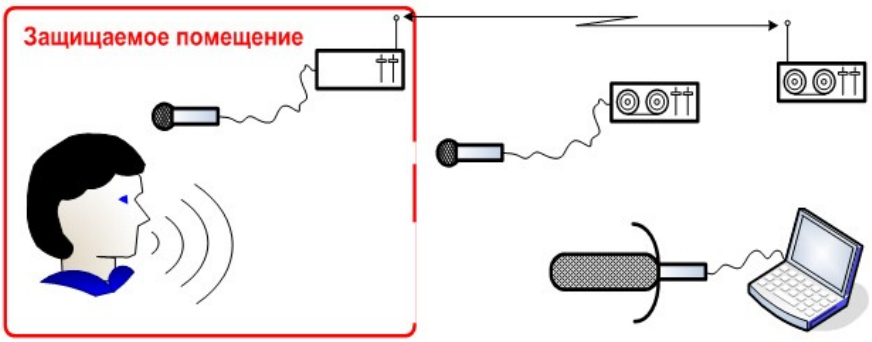

Рис. 9. Акустический ТКУИ

В вибрационных каналах в качестве среды распространения акустических колебаний используются строительные конструкции зданий, стены, потолки, трубы и другие твердые тела (рис. 10).

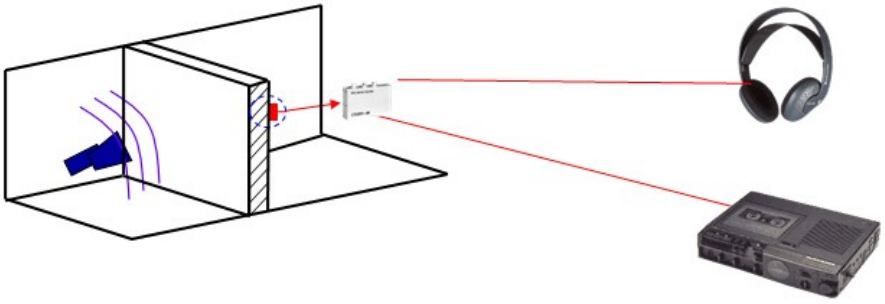

Рис. 10. Виброакустический ТКУИ

Для перехвата информации по виброакустическому каналу используются стетоскопы, в которых в качестве датчиков используются контактные микрофоны (стетоскопы), обладающие высокой чувствительностью.

Стетоскопы наиболее часто устанавливаются на наружных поверхностях зданий, на оконных проемах и рамах, в смежных (служебных и технических) помещениях, за дверными проемами, на перегородках, трубах систем отопления и водоснабжения, коробах воздуховодов вентиляционных и других систем.

Электроакустические каналы утечки информации возникают за счет «микрофонного эффекта», которым обладают некоторые элементы ВТСС (трансформаторы, электромагниты электрочасов, дроссели ламп дневного света и т. п.). Под действием переменного акустического давления они могут изменять свои параметры (емкость, индуктивность, сопротивление).

Перехват акустической информации осуществляется путем непосредственного подключения к соединительным линиям ВТСС, обладающих «микрофонным эффектом», специальных высокочувствительных низкочастотных усилителей (рис. 11).

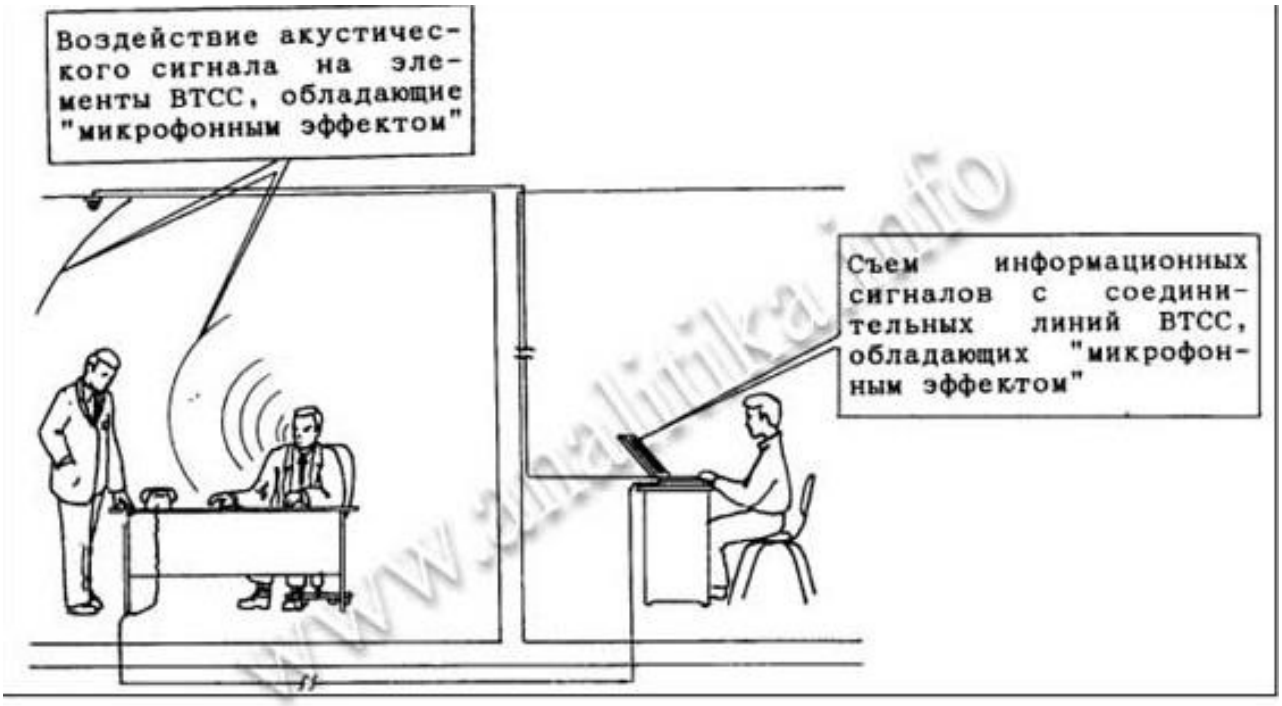

Рис. 11. Перехват акустических сигналов через ВТСС, обладающих «микрофонным эффектом»

Оптико-электронный (лазерный) канал. Под действием звуковой волны тонкие отражающие поверхности (оконные стекла) 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 (рис. 12).

Если в помещении установлены закладные устройства с элементами, параметры которых могут изменяться под действием акустической волны, возможен съем информации с помощью высокочастотного навязывания. При облучении мощным высокочастотным сигналом в закладном устройстве при взаимодействии облучающего электромагнитного поля со специальными элементами закладки (например, четвертьволновым вибратором) происходит образование вторичных радиоволн («переизлучение»). Специальное устройство закладки (например, объемный

резонатор) обеспечивает модуляцию вторичных радиоволн по закону изменения речевого сигнала. Подобного вида закладки иногда называют **полуактивными**. Для перехвата информации по данному каналу кроме закладного устройства необходимы специальный передатчик с направленным излучением и приемник.

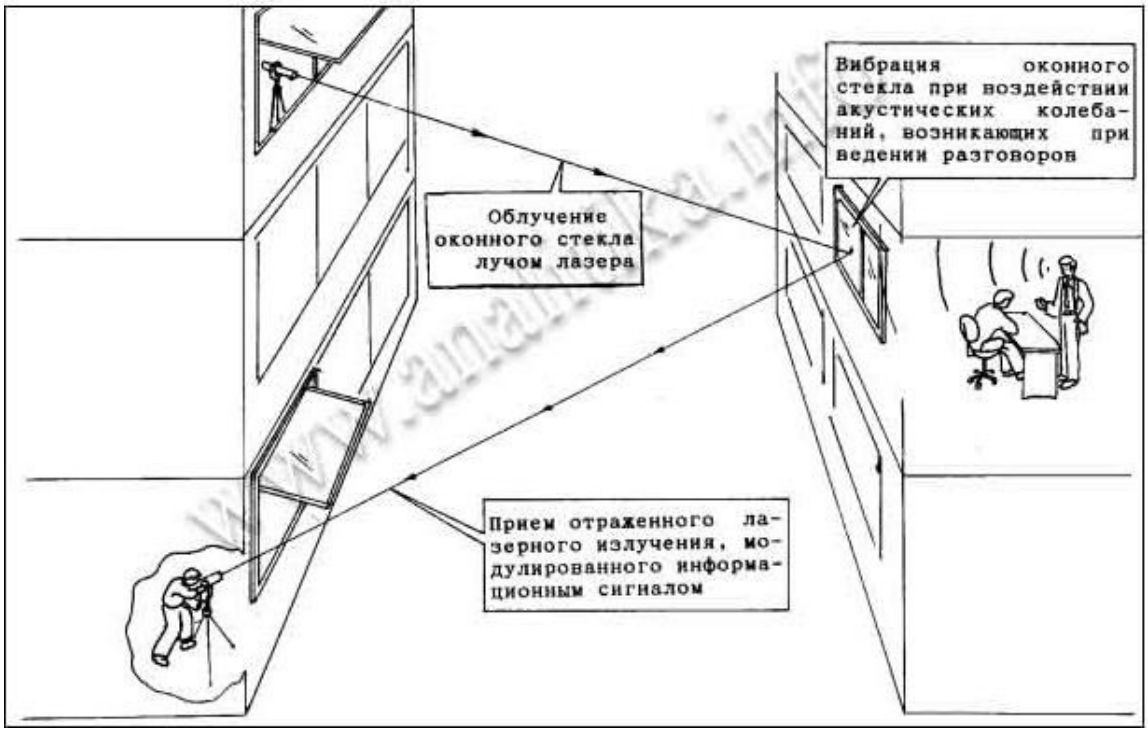

Рис. 12. Перехват акустических сигналов путем лазерного зондирования оконных стекол

4.3. Каналы утечки в технических средствах и системах

Классификация технических каналов утечки информации, обрабатываемой ОТСС, приведена на рис. 13.

Переносчиком информации в ОТСС является электрический ток, параметры которого изменяются по закону информационного сигнала. При прохождении электрического тока по токоведущим элементам вокруг них образуется электромагнитное поле (поля), модулированное информационным сигналом, т. е. возникает побочное электромагнитное излучение.

Рис. 13. Классификация технических каналов утечки информации, обрабатываемой ОТСС

Побочные электромагнитные излучения (ПЭМИ) – побочное явление возникновения электромагнитного излучения технических средств, вызванное электрическими сигналами, действующими в их электрических цепях.

Электромагнитные поля создаются зарядами и токами переменной частоты. Поэтому при проектировании технических средств и систем большое внимание уделяется снижению паразитных связей и наводок до допустимых значений. Однако сделать их равными нулю не представляется возможным. По этой причине любое радиоэлектронное средство и электрический прибор представляют собой потенциальную угрозу с точки зрения защиты информации.

Перехват излучений на частотах работы ВЧ-генераторов становится возможным из-за того, что в состав ОТСС и ВТСС входят высокочастотные генераторы, например, генераторы тактовых импульсов.

Под воздействием внешнего информационного сигнала на их элементах наводятся электрические сигналы, которые модулируют собственные высокочастотные колебания генератора и излучаются в окружающее пространство, где могут быть перехвачены злоумышленником.

Параметрический ТКУИ образуется за счет «высокочастотного облучения» ОТСС. Злоумышленник с помощью специальной аппаратуры направляет на ОТСС электромагнитные волны высокой частоты, которые переизлучаются от элементов ОТСС, промодулированные информационным сигналом.

Электрические каналы утечки образуются при попадании информационных сигналов в цепи заземления и электропитания ОТСС, на линии электропитания ВТСС и другие проводники (за счет наводок), выходящие за пределы контролируемой зоны.

Технические каналы утечки видовой информации

Видовая информация – информация, получаемая в виде изображений объектов или документов.

Способы получения видовой информации можно разделить на три группы (рис.14).

Рис. 14. Способы получения видовой информации

4.4. Защита информации от утечки по техническим каналам

Инженерно-техническая защита информации представляет собой комплекс мероприятий по защите информации от несанкционированного доступа по различным каналам, а также нейтрализацию уничтожения, искажения или блокирования доступа.

Эффективная техническая защита информационных ресурсов является неотъемлемой частью комплексной системы обеспечения информационной безопасности.

Задачами технической защиты информации являются:

− предотвращение проникновения злоумышленника к источникам информации;

− защита носителей информации;

− предотвращение утечки информации по техническим каналам.

Методы защиты информации от утечки по каналу ПЭМИ

Для защиты информации от утечки через ПЭМИ используются пассивные и активные методы, имеющие целью уменьшение отношения сигнал/шум в канале утечки.

В пассивных методах защиты эта задача решается путем снижения уровня опасного сигнала, в активных методах – путем увеличения уровня шума.

Примеры пассивных методов защиты:

− применение разделительных трансформаторов и помехоподавляющих фильтров;

− экранирование;

− заземление всех устройств.

Активные методы защиты информации направлены на создание маскирующих электромагнитных помех.

Защита речевой информации

Для защиты акустической (речевой) информации также используются пассивные и активные методы.

Пассивные методы защиты акустической (речевой) информации направлены на:

− ослабление акустических сигналов на границе контролируемой зоны;

− ослабление информационных электрических сигналов;

− обнаружение излучений акустических закладок и несанкционированных подключений к телефонным линиям связи.

Звукоизоляция помещений направлена на локализацию источников акустических сигналов внутри них.

Обнаружение и подавление акустических закладок

Наиболее эффективным средством обнаружения акустических закладок является нелинейный локатор, устанавливаемый на входе в выделенное помещение и работающий в составе системы контроля доступа.

Системы ультразвукового подавления излучают мощные неслышимые человеческим ухом ультразвуковые колебания (обычно частота излучения около 20 кГц), воздействующие непосредственно на микрофоны акустических закладок, что является их преимуществом.

Поиск и обнаружение закладных устройств может осуществляться визуально, а также с использованием специальной аппаратуры: детекторов диктофонов и видеокамер, индикаторов поля, радиочастотомеров и интерсепторов, сканерных приемников и анализаторов спектра и т. п.

Защита информации от утечки по визуально-оптическим каналам

С целью защиты информации от утечки по визуально-оптическому каналу рекомендуется:

− располагать объекты защиты так, чтобы исключить отражение света в стороны возможного расположения злоумышленника;

− уменьшить отражательные свойства объекта защиты;

− уменьшить освещенность объекта защиты;

− использовать средства преграждения или значительного ослабления отраженного света;

− применять средства маскирования, имитации.

Защита информации от утечки в каналах связи

Методы защиты информации в канале радиосвязи можно разделить на две группы:

− ограничивающие физический доступ к линии и аппаратуре связи;

− преобразующие сигналы в линии к форме, исключающей (затрудняющей) восприятие передачи.

Другим возможным способом активного противодействия съему информации является постановка радиоэлектронных помех. Радиоэлектронные помехи – это непоражающие электромагнитные излучения, которые нарушают или затрудняют работу радиолинии «передатчик-приемник».

ТЕМА 5. ОСНОВЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

5.1. Основные понятия и определения криптографии

Защитой информации при ее передаче люди были озабочены на протяжении многих веков. Было изобретено множество способов решения данной задачи. Основными из них являются следующие.

1. **Физическая защита** материального носителя информации. Методы физической защиты информации используются и в современных условиях. Комплексные системы защиты информации предусматривают наличие систем ограждения, охраны и сигнализации.

2. **Стеганография.** Метод направлен на сокрытие самого факта наличия носителя или факта передачи секретной информации. Раньше это было «запрятывание» носителя с тайной информацией в несекретном месте: под маркой на почтовом конверте, в корешке книги, в предметах одежды и обуви и т. д. С развитием информационных технологий появились новые способы стеганографии. Например, секретное сообщение может быть укрыто в файле графического изображения следующим образом: младший бит в двоичной последовательности, кодирующей цвет каждого пикселя изображения, отводится под бит сообщения. Так как человеческий глаз различает ограниченное количество цветов, то визуально графическое изображение практически не изменится. Например, графический файл с разрешением всего 64 × 64= 4096 точки может содержать секретное сообщение объемом 512 байт (символов).

3. **Криптография** (с греч. – «тайнопись») разрабатывает методы такого преобразования информации, чтобы ее смысл был скрыт от злоумышленника.

Современная криптография решает следующие основные задачи:

– защита информации от несанкционированного доступа путем ее шифрования;

– удостоверение подлинности сообщений (получатель сообщения имеет возможность проверить источник сообщения);

– удостоверение в целостности полученного сообщения (возможность гарантировать, что сообщение не было модифицировано или подменено в процессе передачи);

– обеспечение невозможности отказа (как получатель, так отправительне могут опровергнуть факт передачи).

Основные термины и определения

Шифр – совокупность способов преобразования исходного сообщения (открытого текста) с целью его защиты.

Алфавит – конечное множество символов, используемых для кодирования информации. Например, латинский алфавит содержит 26 букв от A до Z. Любое сообщение может быть записано также с помощью двоичного алфавита, содержащего только два символа: 0 и 1.

Шифрованное сообщение (закрытый текст, криптограмма) – сообщение, полученное в результате преобразования исходного сообщения путем использования некоторого шифра.

Преобразование открытого текста в криптограмму называется **зашифрованием.** Обратное действие называется **расшифрованием.**

Ключ – информация, используемая для шифрования и расшифрования сообщений.

Криптостойкость – свойство шифра противостоять дешифрованию без знания ключа (криптоанализу).

Таким образом, **криптография** изучает построение и использование систем шифрования, в том числе их стойкость, слабости и степень уязвимости относительно различных методов вскрытия.

Все методы преобразования информации с целью защиты от несанкционированного доступа делятся на две большие группы: методы шифрования с закрытым ключом и методы шифрования с открытым ключом.

5.2. Симметричное шифрование

Классическая криптография использует симметричные алгоритмы шифрования, в которых применяется один и тот же секретный ключ, как для шифрования, так и для расшифрования сообщения. Каждый из абонентов может, используя секретный ключ, как зашифровать, так и расшифровать сообщение. Структуру системы с закрытым ключом иллюстрирует рис. 15.

Источник шифрует открытое сообщение ***M***с использованием выбранного ключа ***K***. Полученное зашифрованное сообщение ***E*** (криптограмма) передается по открытому каналу связи. Оно может быть перехвачено противником. Приемник сообщений с помощью ключа ***K*** расшифровывает криптограмму ***E*** и получает исходное сообщение ***M***.

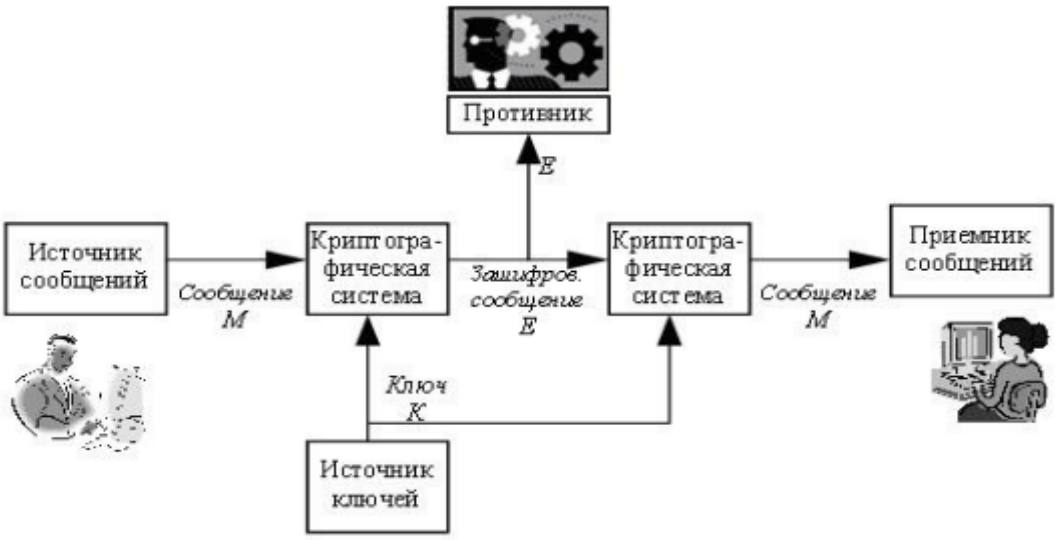

Рис. 15. Система шифрования с закрытым ключом

Классификация методов шифрования с закрытым ключом представлена на рис. 16.

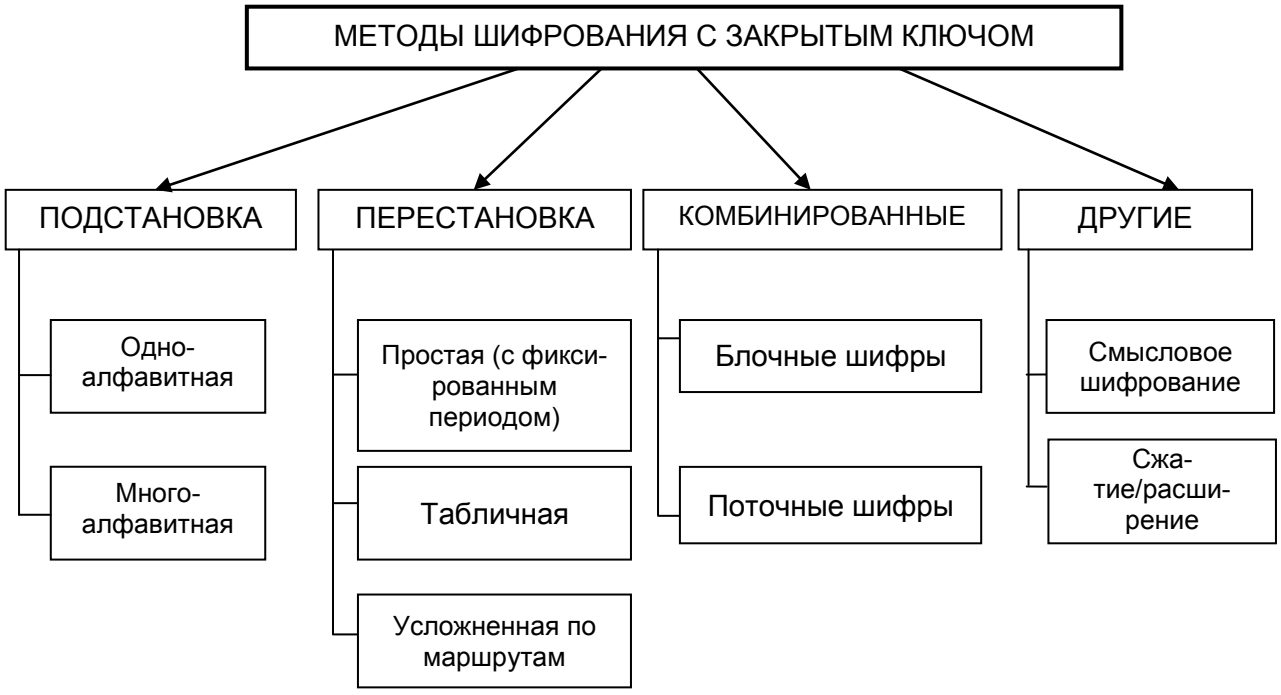

Рис. 16. Методы шифрования с закрытым ключом

Методы замены основаны на том, что символы исходного текста заменяются символами другого алфавита в соответствии с принятым правилом.

Представителями методов замены являются одноалфавитные (моноалфавитные) подстановки, в которых каждому символу исходного алфавита соответствует определенный символ алфавита, используемого для шифрования. Классический пример одноалфавитной замены – шифр Цезаря, при использовании которого каждая буква исходного сообщения заменяется на другую, отстоящую от исходной, например, на три позиции вправо.

Другими словами, при одноалфавитной подстановке выполняется однозначная замена исходных символов их эквивалентами из таблицы замен. Таким образом, таблица замен является ключом такого шифра.

Так как зашифрованный текст сохраняет статистические закономерности исходного текста, подобные шифры имеют низкую стойкость к криптоанализу.

Многоалфавитную подстановку может иллюстрировать шифр, описанный французом Блезом Вижинером в «Трактате о шифрах» (1585 г.).

Ключом является некоторое слово или просто последовательность символов, которая подписывается с повторением под сообщением. Числовой эквивалент каждого символа криптограммы определяется в результате сложения с приведением по модулю N числовых эквивалентов символа сообщения и лежащего под ней символа ключа.

Формула получения шифрограммы:

$e_i(K)=(t_i+ k_j) \ mod N$.

Формула для расшифровки:

$t_i(K)=(e_i- k_j+ N) \ mod N$ **,**

где e_j – порядковый номер символа шифротекста в алфавите,

t_i –порядковый номер символа сообщения в алфавите,

k_j – порядковый номер символа ключа в алфавите,

i– номер символа в сообщении,

j – номер символа в ключе, $j \in \{1, ..., L\}$,

N – мощность алфавита,

L – длина ключа.

В первой половине XX в. широкое применение нашли роторные шифровальные машины, позволяющие автоматизировать процесс выполнения многоалфавитных подстановок. Наиболее известное устройство подобного класса – немецкая роторная шифровальная машина «Энигма» (лат. enigma – загадка), использовавшаяся во время Второй мировой войны.

Гаммирование. Шифрование выполняется путем сложения кодов символов исходного текста и ключа по модулю, равному числу букв в алфавите. Данный процесс называется наложением гаммы. Наиболее часто на практике используется двоичный алфавит, содержащий два символа – 0 и 1. Таким образом, при наложении гаммы производится сложение по модулю два, которое на компьютере выполняется очень быстро. То есть гаммирование даже очень большого исходного текста выполняется практически без задержек.

В **методах перестановки** исходный текст делится на блоки равной длины, в каждом из которых выполняется перестановка символов по определенному правилу (ключу). Например, пусть длина блока d=8, а ключом является последовательность 75213864. При шифровании в каждом блоке седьмой символ переставляется на первое место, пятый символ – на второе место, второй – на третье и т. д.

Еще один пример метода перестановки – перестановка по таблице. Например, заполнение ячеек таблицы производится по заранее определенному маршруту, а затем выполняется перестановка строк и столбцов в соответствии с двумя ключами, длина которых равна количеству строк и столбцов соответственно.

Существуют и другие способы перестановки, которые можно реализовать программным и аппаратным путем. При передаче двоичных данных можно использовать блок, в котором с помощью соответствующей электрической схемы перемешиваются разряды исходного сообщения. Если установить размер блока, равный одному байту, можно использовать блок перестановки, представленный на рис. 17. Подобная перестановка широко используется на практике как составная часть некоторых современных шифров.

Последовательное применение к одному исходному сообщению нескольких простых шифров (например, перестановки или подстановки) называется **комбинированным шифром**. Такие шифры обладают более

высокой криптостойкостью, чем перестановка или подстановка по отдельности.

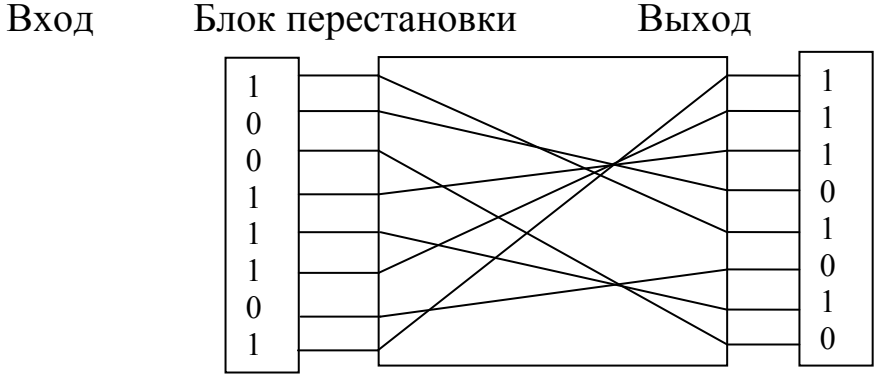

Рис. 17. Аппаратная реализация блока перестановки

Блочные шифры представляют собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к блоку (части) шифруемого текста. Примерами блочных шифров являются алгоритмы шифрования DES (США) и ГОСТ 28147-89 (Россия).

Поточные шифры. Одним из первых и наиболее известных в истории криптографии шифров поточного шифрования стал шифр гаммирования Вернама (1917 г.). Устройство для автоматического шифрования телеграфных сообщений осуществляло электромеханическое сложение по модулю 2 пятиразрядных кодов телеграфных символов Бодо с кодами гаммы, предварительно нанесенными на склеенную в кольцо телеграфную перфоленту. На основании свойства обратимости операции сложения по модулю 2 расшифрование сообщения выполнялось с помощью аналогичного устройства сложением шифртекста с той же гаммой.

Достижениями шифра Вернама стали автоматизация процесса преобразования сообщений и фактически объединение процедур зашифрования и расшифрования информации и ее передачи по каналу связи, исключившие процедуру предварительного шифрования.

Известно, что шифр, в котором размер гаммы равен размеру шифруемого сообщения, а каждый ее бит является независимой случайной величиной, обеспечивает абсолютную криптографическую стойкость. Однако обмен пользователями криптографической системы секретными параметрами, размер которых равен объему передаваемых сообщений,

нерационален. В связи с этим на практике гамма формируется как псевдослучайная последовательность, полученная на основе относительно короткого криптографического ключа, обмен значениями которого для криптографии выступает традиционной задачей.

Для получения таких последовательностей используются различные датчики псевдослучайных чисел, которые в большинстве случаев построены на основе регистров сдвига (аппаратных или программных) с линейными обратными связями.

Начальное заполнение регистра сдвига (векториниципализации), одинаковое на передающей и приемной стороне, является криптографическим ключом соответствующего шифра.

5.3. Асимметричное шифрование

Для решения проблемы передачи секретных ключей были разработаны алгоритмы асимметричного шифрования (системы с открытым ключом). Идея состоит в том, что каждый участник обмена создает два ключа, математически связанных между собой.

Один из ключей является открытым и может быть известен неопределенному кругу лиц. Второй ключ является закрытым (секретным). Исходное сообщение шифруется открытым ключом и передается адресату. Зашифрованный текст не может быть расшифрован тем же открытым ключом. Дешифрование сообщения возможно лишь с использованием закрытого ключа, который известен только адресату (рис. 18).

Асимметричные криптографические системы используют так называемые необратимые (односторонние) функции, обладающие следующим свойством: при заданном значении x относительно просто вычислить значение функции $y=f(x)$. При этом если известно значение y, то нахождение значения x является сложной вычислительной задачей. Алгоритмы шифрования с открытым ключом получили широкое распространение в современных информационных системах.

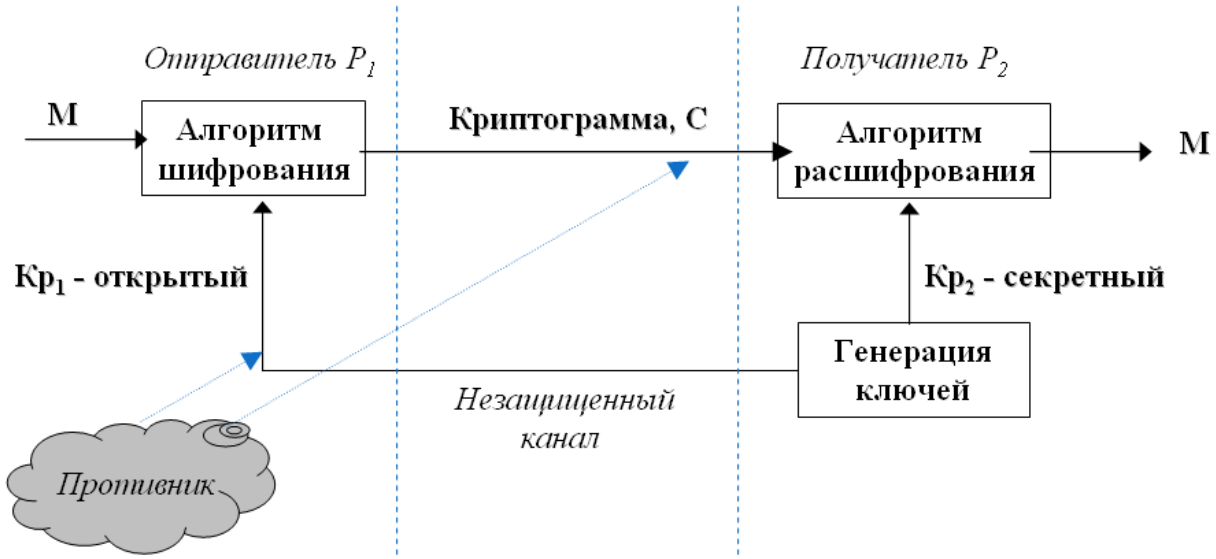

Рис. 18. Общая схема асимметричной криптосистемы

Алгоритмы криптосистем с открытым ключом более сложны, чем симметричные системы шифрования, поэтому использование их в качестве самостоятельных средств защиты нерационально. На практике с помощью криптосистем с открытым ключом распределяют ключи, а потом с помощью симметричных алгоритмов производят обмен большими информационными потоками.

Алгоритм Диффи-Хеллмана (Diffie-Hellman)

Передача ключа по открытым каналам была большой проблемой криптографии XX в., но эту проблему удалось решить после появления метода Диффи-Хеллмана.

Открытое распространение ключей Диффи-Хеллмана позволяет паре пользователей системы выработать общий секретный ключ, не обмениваясь секретными данными. Схема алгоритма Диффи-Хеллмана представлена на рис. 19.

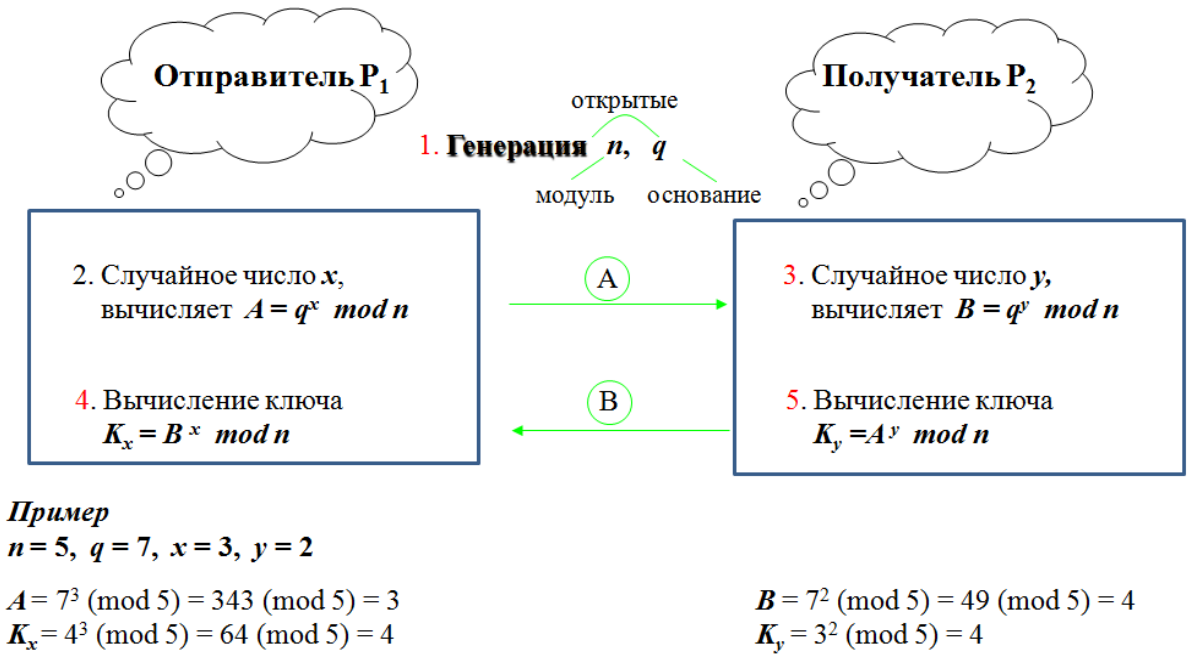

Рис. 19. Схема алгоритма Диффи-Хеллмана

На первом шаге генерируются два больших простых числа n и q, которые являются несекретными и могут быть открыты для неопределенного круга лиц. Затем партнер P1 генерирует случайное число x, вычисляет и передает партнеру P2 число

$A =$ ^{x} od ,

где функция od – возвращает остаток от деления ^{x} на . При получении значения A партнер P2 генерирует случайное число y, вычисляет и посылает партнеру P1 значение

$B =$ $^{y}modn.$

Партнер P1 вычисляет значение = $modn = q^{yx}modn$, а партнер P2 вычисляет = $modn = q^{xy}modn$. Мы видим, что числа и равны и могут быть использованы в качестве секретного ключа для шифрования. Даже в случае перехвата чисел A и B, вычисление значений или является сложной задачей.

ТЕМА 6. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ КИБЕРБЕЗОПАСНОСТИ И ИХ ОБРАБОТКА

6.1. Банк данных угроз безопасности информации

При построении модели угроз безопасности (далее – УБ) необходимо выявить и оценить факторы риска, которые могут быть реализованы в информационной системе (ИС). Для упрощения решения данной задачи можно использовать **банк данных угроз (далее – БДУ) безопасности информации ГНИИИ ПТЗИ ФСТЭК[1] России**, который представляет собой, по сути, базу данных, в которой собрано описание условий, способствующих реализации несан*кционированного доступа (НСД) к конфиденциальной информации и выпол*нению других неправомерных действий.

Основные сведения о БДУ:

1. БДУ, кроме основных УБ, содержит список киберугроз.
2. Цель создания БДУ – обеспечение поддержки (информационной и методической) организациям, деятельность которых связана с обработкой персональных данных, управлением критически важными объектами и т. п.
3. Сведения из БДУ призваны помочь выявить и предупредить УБ в процессе разработки, оптимизации информационных систем, средств защиты информации и программного обеспечения.
4. Ознакомиться с БДУ можно на официальном сайте ФСТЭК России в разделе «Техническая защита информации» или перейти по прямой ссылке *bdu.fstec.ru*.
5. За ведение БДУ отвечает ГНИИИ ПТЗИ, при этом подать заявление на добавление УБ есть возможность у любого пользователя.
6. На текущий момент в банке представлено описание более 200 угроз безопасности и около 50 тысяч уязвимостей.

Особенностью банка данных угроз ФСТЭК России является то, что доступ в БДУ свободный, регистрация не требуется.

---

[1] Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»).

Таким образом, Банк данных угроз безопасности информации ФСТЭК является источником актуальных сведений об уязвимостях, но чтобы грамотно применять их при построении частной модели УБ, необходимы узкоспециализированные знания и немалый опыт.

6.2. Уровневая структура описания инцидентов в международной базе данных VERIS

Словарь для записи событий и обмена инцидентами (VERIS) представляет собой набор метрик, предназначенных для обеспечения общего языка описания инцидентов безопасности структурированным и повторяемым образом. VERIS – это ответ на одну из самых острых и постоянных проблем в индустрии безопасности – нехватку качественной информации. VERIS решает эту проблему, помогая организациям собирать полезную информацию, связанную с инцидентами, и делиться этой информацией.

Платформа VERIS была разработана для решения проблемы, воспринимаемой ее создателями. VERIS разработан как набор показателей, которые обеспечивают его через свой собственный веб-сайт, как способ выражения показателей в общем формате для описания событий безопасности. VERIS преследует несколько целей.

Во-первых, создать сообщество пользователей, которые могут собрать библиотеку качественной информации о безопасности и поделиться этой информацией анонимно и с другими членами этого сообщества

Структура VERIS

Пять основных разделов, каждый из которых предназначен для отражения различных аспектов повествования об инциденте. При просмотре в совокупности они дают видимое представление о причине и серьезности инцидента:

1. Отслеживание инцидентов.
2. Демография жертв.
3. Описание инцидента.
4. Обнаружение и реагирование.
5. Оценка воздействия.

Каждый раздел содержит элементы, совпадающие с описанными в схеме. База данных VERIS пытается найти баланс между полезной

и полной информацией об инциденте. Если что-то интересно с исследовательской точки зрения, но напрямую не предоставляет управлению безопасностью полезную информацию, оно, скорее всего, не будет включено в базу данных. В некоторых разделах есть дополнительные метрики, которые, хотя и не включены формально, но могут представлять интерес, если пользователи захотят их собрать. При правильном выполнении VERIS может создавать не только представление о том, что произошло в конкретном инциденте, но и позволяет рассматривать инцидент в контексте более широкого массива знаний.

Платформа VERIS и база данных сообщества VERIS доступны на GitHub. Платформа VERIS – https://github.com/vz-risk/veris. База данных сообщества VERIS – https://github.com/vz-risk/VCDB.

6.3. Реагирование на уязвимости, связанные с компьютерной безопасностью

Расследование инцидентов информационной безопасности (далее – ИБ) и реагирование на них (независимо от вида) требует работы команды опытных специалистов, которые осуществят целый комплекс мероприятий, включающий ряд последовательных шагов:

1. Подготовка. В случае возникновения инцидента ключевую роль играет оперативность и правильность предпринимаемых сотрудниками действий. Для предотвращения (уменьшения) ущерба от компьютерных атак важна тщательная подготовка персонала по вопросам ИБ.

2. Обнаружение. Специалисты по ИБ выясняют, является ли произошедшее в системе или сети событие инцидентом. Используются различные аналитические средства, данные об угрозах, остальные информационные источники.

3. Сдерживание. Специалисты выявляют скомпрометированные компьютеры, локализуют угрозу таким образом, чтобы остальные компьютеры не подверглись заражению. В результате система должна продолжать работать без зараженных объектов.

4. Удаление. Специалисты удаляют вредоносное программное обеспечение, приводят подвергшиеся атаке системы в первоначальное состояние.

5. Восстановление. Функционирование сети постепенно восстанавливается, «вылеченные» системы вводятся в работу. Чтобы удостовериться в полной ликвидации угрозы, наблюдение за ними продолжается.

6. Выводы. Проводится анализ ситуации, факторов, способствующих возникновению инцидента, проведенных мероприятий, корректировка средств защиты информации, составляются рекомендации для недопущения в будущем подобных атак, а также оперативного реагирования на них.

При возникновении инцидента от сотрудников службы информационной безопасности требуются быстрые и точные действия для минимизации ущерба от инцидента. Для безошибочного совершения этих шагов необходимо наличие инструкции по реагированию на инциденты ИБ, созданной экспертами ИБ. Если сотрудники подразделений, ответственных за ИБ, не знают, как реагировать на возникший инцидент и как обеспечить оперативный сбор данных, необходимых для проведения расследования, атакованная организация понесет значительные убытки. Ошибки в реагировании на инциденты ИБ приводят к достижению злоумышленником целей атаки и дают ему возможность удаления следов в информационной системе.

6.4. Системы обнаружения вторжений. Принципы построения и использования

В настоящее время существует большое количество как коммерческих (проприетарных), так и решений с открытым исходным кодом, способных обеспечить необходимый уровень защиты внутренней сети организации. К ним относятся системы обнаружения вторжений (Intrusion Detection Systems – **IDS**) и системы предотвращения вторжений (Intrusion Prevention Systems – **IPS**).

IDS – система обнаружения вторжений, предназначенная для регистрации подозрительных действий в сети и уведомления о них службы информационной безопасности.

IDS включает в свой состав сенсоры, мониторящие сетевой трафик или журналы, и передающие информацию анализаторам. Анализаторы ищут в полученных данных вредоносный характер и при необходимости отправляют результаты администратору. В зависимости от места расположения

IDS делятся на *сетевые* (network-based IDS, NIDS) и *хостовые* (host-based, HIDS). Первые отслеживают весь сетевой трафик того сегмента, где они установлены, а вторые – в пределах единственного компьютера.

Таким образом, IDS может предупреждать о вредоносной активности, но не имеет возможности локализовать вредоносную активность на ранней стадии. В этом может помочь IPS. IPS основана на тех же методах обнаружения атак, что и IDS, и может работать как на уровне сети (NIPS), так и на уровне хоста (HIPS). Возможность предотвращения атак реализована за счет того, что сетевая IPS, как правило, встраивается «в разрыв» сети и пропускает через себя весь трафик, а также имеет внешний интерфейс, на который приходит трафик и внутренний интерфейс, который пропускает трафик далее, если он признается безопасным.

Мониторинг кибербезопасности включает комплекс мероприятий по сбору, систематизации и анализу сведений о состоянии информационной системы и действиях пользователей, проводимых с целью выявления несанкционированных действий как сотрудников организации, так и посторонних лиц, проникших в сеть.

Современные системы мониторинга кибербезопасности позволяют обнаруживать такие действия и сигнализировать о них, что позволяет своевременно их пресекать и минимизировать риски возникновения инцидентов ИБ.

В настоящее время существует ряд средств для решения данных задач. Любая система мониторинга событий информационной безопасности может быть отнесена к одной из следующих категорий:

1. **SIEM (Security Information and Event Management)** – системы, позволяющие отслеживать и анализировать события в реальном времени.
2. **UBA (User Behavioral Analytics)** – системы, собирающие данные о действиях пользователей в сети для последующего анализа и выявления возможных угроз.
3. **UEBA (User and Entity Behavioral Analytics)** – системы для обнаружения подозрительных действий пользователей и аномальности в работе сети.
4. **Решения, контролирующие эффективность сотрудников и отслеживающие внутри сети все их действия**, которые касаются работы с корпоративными конфиденциальными данными.

5. **Системы поиска и выявления различного рода атак**, ориентированные на улучшение общей защищенности корпоративной сети.

6.5. Анализ данных сетевых вторжений. Системы управления событиями и данными безопасности (SIEM)

Угрозы для безопасности сетей либо данных могут быть реализованы с помощью некоторых следующих типов сетевых атак:

1. ***Анализ трафика*** (снифинг) – перехват всех сетевых пакетов, которые передаются через определенный сегмент сети.

2. ***IP-спуфинг*** *(подмена IP-адреса)* – злоумышленник выдает себя за легитимного пользователя.

3. ***Перехват сообщений на маршрутизаторе*** – злоумышленник, получив доступ к сетевому маршрутизатору, получает и возможность перехватывать все сообщения, проходящие через него.

4. ***Создание ложного маршрутизатора*** – злоумышленник добивается, чтобы его компьютер стал маршрутизатором сети, после чего получает доступ ко всем проходящим через него сообщениям.

5. ***Отказ в обслуживании*** *(DoS).*

6. ***Парольные атаки*** – подбор (хищение) паролей пользователей ТКС (простой перебор, IP-спуфинг, сниффинг пакетов).

7. ***Атаки Man-in-the-Middle*** (атака посредника, или «человек посередине») – злоумышленник перехватывает и, возможно, подменяет сообщения, которыми обмениваются пользователи.

8. ***Атаки на уровне приложений*** – использование известных уязвимостей серверного программного обеспечения.

9. ***Сетевая разведка*** – сбор информации о сети с помощью общедоступных данных и приложений.

SIEM-системы объединяют функции SIM (управление информацией о безопасности) и SEM (управление событиями безопасности) в единую систему.

Основная цель SIEM-системы – объединение больших объемов данных для использования их специалистами по ИБ. Для этого она выполняет:

– сбор и анализ данных из различных источников в информационной инфраструктуре организации;

– формирование полной картины ИБ организации.

Инструменты SIEM представляют собой важную часть системы ИБ. SIEM собирает журналы событий со всех офисных устройств и технических служб организации.

SIEM выполняет мониторинг:

– журнала приложений;

– активности пользователей;

– целостности файлов;

– системы и журнала устройств.

Таким образом, задача SIEM заключается в сборе и консолидации данных журналов, которые генерируются во всей технологической инфраструктуре организации. Сюда входят компьютеры и приложения, сетевые устройства и устройства безопасности (брандмауэры, антивирусные фильтры). Система управления инцидентами информационной безопасности идентифицирует и классифицирует события, чтобы проанализировать их в дальнейшем.

Программное обеспечение SIEM значительно снижает влияние нарушений безопасности на работу информационных систем. Быстрое реагирование на инциденты безопасности уменьшает ущерб организации.

Решения SIEM могут быть установлены локально или в облаке. При выборе SIEM необходимо учитывать возможность интегрировать сторонние источники информации об угрозах для более точного обнаружения угроз. Данные журнала должны анализироваться в режиме реального времени, чтобы позволить быстро выявлять и блокировать атаки. Хорошее программное обеспечение для управления инцидентами ИБ должно обеспечивать быстрый анализ и визуальное установление корреляции между событиями. SIEM должна уметь отслеживать доступ к критически важным ресурсам, выявлять необычное поведение пользователя или попытки удаленного входа в систему.

ЗАКЛЮЧЕНИЕ

Обеспечение кибербезопасности призвано минимизировать ущерб в результате хищения, уничтожения, блокирования, искажения или подделки информации. Комплексная защита информации должна проводиться в полном соответствии с действующим законодательством, нормативными документами информационной безопасности, интересами и требованиями потребителей информации. Каждый сотрудник органов внутренних дел должен обладать необходимыми знаниями и навыками в сфере информационных технологий и их применении в профессиональной деятельности, а также в области обеспечения кибербезопасности. Поэтому вопросам защиты информации и обеспечения кибербезопасности должно уделяться особое внимание в процессе сбора, обработки, хранения, передачи служебной информации и эксплуатации систем информационно-аналитического обеспечения деятельности органов внутренних дел.

ЛИТЕРАТУРА

1. Журавленко Н.И., Тутова О.В. Информационные технологии в правоохранительной деятельности: учебное пособие. Краснодар, 2016. URL: http://ios.ruimvd.ru/mod/resource/view.php?id=5733.

2. Белоус А.И., В.А. Солодуха. Кибероружие и кибербезопасность. О сложных вещах простыми словами. М., 2020. URL: https://www.iprbookshop.ru/98349.html.

3. Гультяева Т.А. Основы информационной безопасности: учебное пособие. Новосибирск, 2018. URL: https://www.iprbookshop.ru/91640.html.

Учебное издание

ЛЕМАЙКИНА Светлана Владимировна,
КАРПИКА Анатолий Григорьевич,
кандидат технических наук, доцент;
ГУНЬКО Виталий Борисович,
кандидат технических наук, доцент;
КОМЕРЦОВ Вячеслав Викторович

Учебное пособие

Редактор *Н.А. Чуб*
Корректор *Л.Н. Кожоридзе*
Компьютерная верстка – *Е.Е. Пелехатой*

Подписано в печать 28.09.2023.
Формат 60х84/16. Объем 4 п. л. Набор компьютерный.
Гарнитура Times New Roman. Печать лазерная.
Бумага офисная. Тираж 40 экз. Заказ № 123.
Редакционно-издательское отделение НИиРИО
ФГКОУ ВО РЮИ МВД России.
Отпечатано в ГПиОП НИиРИО
ФГКОУ ВО РЮИ МВД России.
344015, г. Ростов-на-Дону, ул. Еременко, 83.

ISBN 978-5-89288-506-5