ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

УЧЕБНИК

Воронеж
2022

Авторский коллектив: Винокуров С. А., Минаев В. А., Симоненко Д. А., Жуков М. М., Поликарпов Е. С., Телков А. Ю., Авсентьев А. О., Полухин Д. И.

Основы кибербезопасности: учебник / С. А. Винокуров [и др]. – Воронеж-Москва: Воронежский институт МВД России, Московский университет МВД России им. В.Я. Кикотя, 2022. – 392 с.

Рецензенты:

Учебник является результатом работы авторов по обобщению российских и зарубежных исследований по обеспечению кибербезопасности. Учебник предназначен для подготовки сотрудников органов внутренних дел по направлениям подготовки (специальностям), не связанным с обучением специалистов в области информационной безопасности, эксплуатации средств связи, радиоэлектронных средств и радиоэлектронных систем различного назначения.

СОДЕРЖАНИЕ

Принятые сокращения

АБС – автоматизированная банковская система
АО – аппаратное обеспечение
АС – автоматизированная система
АСЕАН – Ассоциация государств Юго-Восточной Азии
АСУ – автоматизированная система управления
АСУТП – автоматизированная система управления технологическим процессом
БД – база данных
БРИКС – группа из пяти стран: Бразилии, России, Индии, КНР, ЮАР
ВТСС – вспомогательные технические средства и системы
ВЧС – виртуальная частная сеть
ГосСОПКА – Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак
ЕИТКС – единая информационно-телекоммуникационная система органов внутренних дел
ЕПП – единое пространство пользователей
ИБ – информационная безопасность
КБ – компьютерная безопасность, кибербезопасность
ИКТ – инфокомуникационные технологии
ИС – информационная система
ИСО – Международная организация по стандартизации
ИСОД – система информационно-аналитического обеспечения деятельности
ИТ – информационные технологии
ИТВ – информационно-технологическое воздействие
КИИ – критическая информационная инфраструктура
КЦД – конфиденциальность, целостность, доступность
ЛПР – лицо, принимающее решение
МСЭ – межсетевой экран
МЭК – Международная электротехническая комиссия
НКЦКИ – Национальный координационный центр по компьютерным инцидентам
НСД – несанкционированный доступ
ОБСЕ – организация по безопасности и сотрудничеству в Европе
ОВД – органы внутренних дел
ОДКБ – Организация Договора о коллективной безопасности
ОКБ – обеспечение компьютерной безопасности
ООН – Организация Объединенных Наций
ОС – операционная система
ОТСС – основные технические средства и системы
ПО – программное обеспечение

ПолИБ – политика информационной безопасности
ПолКБ – политика компьютерной безопасности
ПЭМИН – побочные электромагнитные излучения
СЗИ – средства защиты информации
СОВ – система обнаружения вторжений
СПВ – система предотвращения вторжений
СОИБ – система обеспечения информационной безопасности
СОКБ – система обеспечения компьютерной безопасности
СУКБ – система управления кибербезопасностью
СУБД – система управления базами данных
СУДИС – сервис управления доступом к информационным ресурсам и системам
СУИБ – система управления информационной безопасностью
СУКБ – система управления компьютерной безопасностью
ТКЭ – технико-криминалистическая экспертиза
ТКУИ – технический канал утечки информации
ТСОИ – технические средства обработки информации
ТСР – техническое средство разведки
УБИ – угроза безопасности информации
УНЧ – усилитель низкой частоты
УЦ – удостоверяющий центр
ФСТЭК – Федеральная служба по техническому и экспортному контролю
ШОС – Шанхайская организация сотрудничества
ЭМИ – электромагнитное излучение
ЭЦП – электронная цифровая подпись

Введение

К сегодняшнему дню информация представляет собой один из самых главных активов любой организации, имеющий ценность для нее, находящийся в ее распоряжении, обеспечивающий ее эффективное функционирование и вследствие этого нуждающийся в защите. Система МВД России не является здесь исключением.

Между тем, вовремя не нейтрализованные и доступные злоумышленникам уязвимости в обеспечении безопасности информационных систем организации могут привести к катастрофическим потерям финансового и репутационного характера, нанести непоправимый ущерб бизнес-процессам, а применительно к деятельности органов внутренних дел (ОВД) – оперативно-служебным процессам. Поэтому вопрос разработки адекватной потребностям той или иной структуры эффективной системы управления компьютерной безопасностью (СУКБ), ее квалифицированного внедрения и использования сегодня, как никогда прежде, актуален. Если говорить образно, это вопрос из ряда «быть или не быть» для любой организации.

Осуществление операций с применением инфокоммуникационных технологий (ИКТ) в современной организации выходит далеко за рамки ограничений, присущих защищенным центрам обработки данных со строго определенными физическими и логическими параметрами. Это связано с тем, что в процессе эволюции усложнились программные и аппаратные средства. Многочисленные операции теперь выполняют серверы, рабочие станции, ноутбуки, мобильные телефоны, умные часы и другие устройства, которые сотрудники организации, смежные с ними структуры могут использовать в любое время. Доступ к ресурсам информационных систем получает значительное число пользователей различных категорий, подключающихся к корпоративным сетям через интернет как по выделенным линиям, так и по коммутируемым каналам и радиоканалам.

Обработка информационных потоков в системе МВД России требует высоких темпов и точности. Сбор и хранение крупных информационных баз на защищенных электронных носителях, объединение в общий массив данных, имеющих сложную территориально-динамическую структуру, увеличение стоимости информационных ресурсов, большая зависимость от характеристик конфиденциальности, целостности, доступности и других значимых свойств информационных активов – это только часть важных проблем, требующих четкой организации управления кибербезопасностью (КБ).

Российские организации осознают необходимость эффективного управления своей информационной безопасностью, приобретающего все большее значение по мере их роста и продвижения в своей деятельности.

Выбирающим их продукцию и услуги важно понимать, как осуществляется защита их персональных данных. Инвесторам необходима уверенность в том, что активы организации находятся в безопасности. Смежные структуры ожидают, что организация будет функционировать без сбоев, вызванных ошибками в работе информационных систем (ИС) на всех стадиях их жизненного цикла, умышленными или неумышленными действиями персонала, вредоносным программным обеспечением (ПО) и другими деструктивными факторами.

В начале 80-х годов прошедшего века защита информации могла быть эффективно обеспечена при помощи специальных организационных мер и различных программно-аппаратных средств. С развитием локальных и глобальных сетей, каналов спутниковой связи остро встал вопрос об обесппечении кибербезопасности.

Очевидно, что несистемная организация защитных мер ИС не может обеспечить требуемый уровень КБ. Чтобы надежно защитить свою информацию, необходимо интегрировать решение вопросов защиты в единый для всей организации процесс управления КБ, связанный со снижением рисков ее деятельности.

В современных условиях достаточно много сделано для обеспечения КБ организаций, но при этом пока не достигнут необходимый уровень управления защитными комплексами и мерами, которые применяются в них. Зачастую специалисты в организациях не полностью осознают, какие их активы являются наиболее критичными, какие риски КБ связаны с этими активами, какие защитные меры в этой связи необходимо спланировать. Все указанные проблемы решаются за счет построения СУКБ.

Разработка централизованной СУКБ на уровне организации зависит от множества внутренних и внешних факторов, которые часто противоречат друг другу, конфликтуют. Что хорошо для одной организации, совсем не подходит для других. В этой связи требуются различные комбинации структур, процессов и механизмов, наилучшим образом обеспечивающих защищенное состояние существующей информационной инфраструктуры в каждом регионе в конкретный период времени.

Управление КБ не может рассматриваться только с технической и технологической точек зрения, поскольку это – комплексный, непрерывно реализуемый процесс, имеющий правовую, организационную, документальную, кадровую и другие составляющие.

Следует отметить, что система подготовки кадров в области борьбы с киберпреступностью находится в стадии становления, отсутствует необходимое хорошо адаптированное учебно-методическое обеспечение, не налажены устойчивые связи между ведомствами, отвечающими за свои

участки работы в этой сфере. Собственно, на решение указанных и возникающих новых проблем и направлен учебник.

Комплексно, со всеми важными деталями, как хотелось бы, вопросы кадрового обеспечения в период развертывания новой для образовательной системы МВД России дисциплины с учетом направленности учебника раскрыть очень сложно. Однако и обойти их в учебнике для целевого контингента – полицейских – было бы ошибкой.

В учебнике рассмотрены основополагающие аспекты обеспечения КБ, состоящего из многих направлений независимо от масштаба и области деятельности организации.

В то же время, по мере развития и становления дисциплины, прояснения системных взаимосвязей раскрываемых в ней проблем, уточнения и совершенствования нормативной правовой базы, будет не только желательно, но и необходимо расширение и совершенствование целого ряда разделов учебника.

Глава 1. Общие вопросы обеспечения кибербезопасности

1.1. Кибербезопасность в системной защите государства, общества, человека

Кибербезопасность и информационная безопасность. Становление обоих понятий в России связано с активным развитием науки и практики в области защиты информации, регулируемой со стороны государства, и формированием теоретических и методических основ в научных институтах, учебных заведениях страны, включая научно-образовательные учреждения системы МВД Российской Федерации.

Чтобы дать максимально корректное понимание относительно нового научно-практического направления – кибербезопасности (КБ), осуществим краткий сравнительный анализ указанных двух взаимосвязанных и взаимозависимых течений в области обеспечения безопасности.

Несмотря на то что кибербезопасность заявлена в области естественных наук, претендуя на определенную фундаментальность, она, на наш взгляд, не может быть изолирована, сама в себе [1] и должна, с одной стороны, открывать новые возможности и методы решения практических задач, в том числе стоящих перед органами внутренних дел, а с другой – отражать преемственность в историческом плане. А именно давать понимание того, каким мировым тенденциям развитие кибербезопасности соответствует, на каких устоявшихся концепциях она базируется, где востребованы её изыскания, включая усложняющуюся картину киберпреступности.

Исходя из этого, рассмотрим:

- эволюцию понятийного аппарата, соответствующего существу и названиям указанных направлений в сфере защиты информации;
- сравнение структур двух названных направлений, сложившихся к сегодняшнему дню;
- последние нормативные и профессиональные стандарты как отражение современных веяний обеспечения безопасности.

Понятийный аппарат в области информационной безопасности (ИБ) в российской науке и практической деятельности сложился, опираясь на международные стандарты европейского происхождения [1, 2].

Согласно ГОСТ Р ИСО/МЭК 27000, информационная безопасность характеризует сохранение свойств конфиденциальности, целостности и доступности информации. Часто эту совокупность свойств называют КЦД. Они – основные. По ГОСТ, кроме КЦД, нередко добавляются свойства подлинности, подотчетности, неотказуемости, надежности, а по ISO – еще и свойство доверия.

Некоторые авторы, развивая названный спектр свойств, добавляют и другие, например, контролируемость информации владельцем, ее

полезность. В литературе встречаются и иные подходы к определению ИБ. Так, ряд авторов декларирует ИБ не как состояние, а как процесс «обеспечения ИБ» или в узком понимании – процесс «защиты данных».

Общее соотношение свойств информационных систем (ИС) и факторов деструктивного воздействия на эти свойства, а также соотношения ИБ и КБ с видами угроз приведены на рисунке 1.1.1.

Рис. 1.1.1. Информационные системы, информационная безопасность, кибербезопасность и факторы деструктивного воздействия

Из рисунка 1.1.1 следует, что основополагающим фактором деструктивного воздействия на ИБ и КБ являются угрозы в информационной сфере. Они входят в тройку последовательно реализуемых и связанных факторов: уязвимость – угроза – риск.

Понятие «кибербезопасность», в отличие от ИБ, имеет американское происхождение, часто отождествляясь с военными операциями в киберпространстве как современном театре военных действий [3].

В стандартах указанное понятие представлено двумя трактовками, а именно как свойство защищённости:

- компьютерных ресурсов от компьютерных атак;
- сегмента компьютерных ресурсов (данных в электронном виде, виртуальных приложений) от компьютерных угроз в традиционной совокупности КЦД.

Первый вариант определения приводится в документах Комитета по системам национальной безопасности США (CNSSI) и Национального института стандартов и технологий США (NIST) [4].

Ряд американских авторов сводят дефиницию к предотвращению,

обнаружению и реагированию на атаки. При этом виды, техники, методики и средства проведения компьютерных атак составляют суть проблематики кибербезопасности.

Второй, по существу – сленговый, вариант весьма распространен, используясь в американских документах, словарях и т.п. [5].

Что касается всего научно-технического мира, то понятие кибербезопасности пока дискуссионно [1], хотя во всех трех системах международной стандартизации ISO, IEC и ITU этот термин применяется. Так, новый стандарт ISO/IEC 27100:2020 дает определение кибербезопасности как свойства защищенности активов (общества, организации, человека) от киберрисков, связанных с эксплуатацией уязвимостей в киберпространстве – цифровой среде.

На сегодняшний день можно констатировать, что американизм не прижился повсеместно. Так, Совет Безопасности Российской Федерации и МИД России вместо термина «кибербезопасность» используют формулировку «безопасность в ИКТ-среде» [5].

По мнению одного из лидеров в области разработки и внедрения телекоммуникационного оборудования компании Cisco, кибербезопасность – это деятельность, направленная на защиту систем, сетей и программ от цифровых атак. Целью таких кибератак обычно является получение доступа к конфиденциальной информации, ее изменение или уничтожение, вымогательство денег у пользователей.

Если обобщить соотношение кибербезопасности и информационной безопасности, то совершенно очевидно, что мировое сообщество рассматривает КБ как часть ИБ [1]. При этом методы ИБ и КБ, имея выраженные прикладные цели и задачи, лежат главным образом в плоскости технических наук, в то же время любая сложная проблематика, решаемая на их основе – на пересечениях целого ряда наук – военных, социальных, юридических, политических и др.

В настоящее время российская наука, связанная с обеспечением защиты информации, делает шаг вперед. Появились научные специальности в сфере информационной безопасности, разведенные по разным областям науки: естественным и техническим. Это, с одной стороны, влечет распараллеливание научных структур [6], порождение неопределённости выбора, с другой стороны, добавляет новую степень свободы в научном творчестве и образовательном процессе, не угрожая строгости научных положений.

Онтология безопасности, включая кибербезопасность, представлена на рисунке 1.1.2, который представляет собой адаптацию соответствующей схемы из ISO/IEC 15408-1. Как видно из рисунка, более пристальное внимание в области кибербезопасности уделяется злонамеренным угрозам.

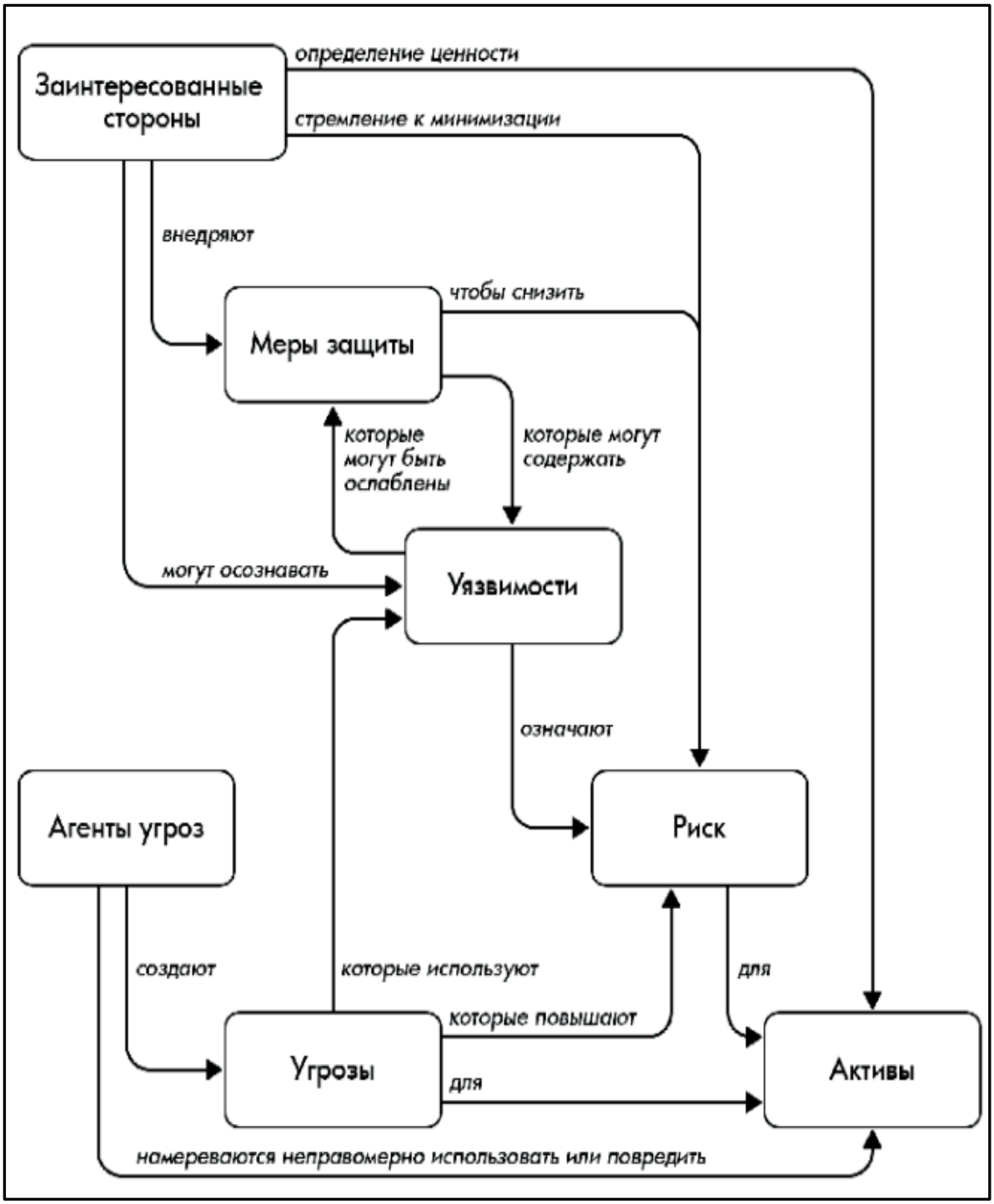


Рис. 1.1.2. Основные понятия безопасности и характер связей между ними

1.2. Базовые понятия в сфере кибербезопасности

Базовые понятия в сфере кибербезопасности связаны с определениями управленческого характера. И это – обоснованно. Чтобы не снижать уровень безопасности в киберпространстве, необходимо постоянно совершенствовать систему управления кибербезопасностью. Рассмотрим основные понятия.

Система (от греч. *systema* – целое, составленное из частей) *управления кибербезопасностью – это единство взаимосвязанных и взаимодействующих элементов, характеризующихся общей целью* поддержания *кибербезопасности в определенных границах* [7, 8].

Если говорить более детально, система – это состоящее из двух или более элементов множество, которое удовлетворяет следующим трем условиям [9]:

1. Поведение каждого элемента воздействует на поведение целого (например, организм человека). Каждая его часть, сердце, легкие, желудок и другие, влияет на функционирование организма в целом.

2. Воздействие на целое взаимозависимо, что означает – поведение каждого элемента и его влияние на целое зависит от того, как ведет себя, по крайней мере, еще какой-то элемент. При этом ни один элемент самостоятельно не воздействует на систему в целом.

3. Элементы системы связаны таким образом, что образование ими независимых подгрупп невозможно.

Уточняя определение, данное выше, систему можно определить, как множество элементов любой природы, взаимодействующих между собой для достижения общей цели, обладающее системным свойством/свойствами, и этого свойства не имеет ни один из элементов и ни одно из их подмножеств.

Свойствами системы являются [10]:

- целостность – первичность целого по отношению к элементам;
- неаддитивность – несводимость свойств системы к сумме свойств составляющих ее элементов;
- синергетичность – целенаправленность действий совокупности элементов системы, усиливающая эффективность ее функционирования;
- эмерджентность – наличие новых свойств у множества элементов системы, которых не было до их объединения; элемент обладает свойствами, которые он теряет в случае отделения от системы;
- мультипликативность – эффекты умножения, а не сложения свойств функционирования элементов в системе;
- взаимодействие и взаимозависимость системы и внешней среды;
- структурность – возможность декомпозиции системы на части и установление связей между частями;

- иерархичность – каждая часть системы может быть рассмотрена как подсистема общей системы;
- непрерывность функционирования;
- целенаправленность – система всегда рассматривается относительно некоторой цели/целей;
- адаптивность – стремление системы к состоянию устойчивого равновесия, предполагающее постоянную адаптацию ее параметров к изменению характеристик внешней среды;
- альтернативность развития – существование нескольких альтернативных путей достижения конкретной цели;
- наследственность – передача наиболее сильных признаков эволюции системы от ее старой версии к новой;
- приоритетность – преобладание целей системы более глобального уровня перед целями ее частей или подсистем.

Системный подход – методология исследования объекта как системы в разных аспектах, комплексно, учитывая всю совокупность связей между ее элементами [7].

Системный подход ориентирован на раскрытие целостности объекта, выявление многообразных типов связей и отношений как внутри исследуемого объекта, так и в его взаимоотношениях с внешней средой.

Установлением структурных связей между элементами системы, базируясь на комплексе общенаучных, естественнонаучных, статистических, математических методов, занимается *системный анализ,* представляющий совокупность методов и средств изучения сложных объектов. Системный анализ используется как эффективный инструмент решения сложных, не всегда четко сформулированных проблем, к числу которых относится управление различными объектами в сфере кибербезопасности. Системный анализ позволяет структурировать проблемы, разложить их в серию решаемых с помощью различных методов задач, найти критерии их решения, детализировать цели.

При системном подходе в рамках моделирования систем необходимо прежде всего четко определить его цель. Реализации этой цели способствует корректный отбор элементов системы, описание структуры и связей между ними, выбор критериев оценки адекватности модели.

Основными целями при системном подходе являются:

- повышение синергетичности;
- мультипликативность в организации;
- устойчивость функционирования организации;
- адаптивность работы организации;
- совместимость работы различных подсистем организации;
- эффективная работа обратных связей в организации.

Системный подход предполагает этапность решения проблемы, включающую:

- изучение предметной области (качественный анализ);
- выявление и формулирование проблемы;
- математическую (количественную) формулировку проблемы;
- натурное и/или математическое моделирование исследуемых объектов и процессов.

Термин «процесс» (от лат. *processus* – продвижение) может быть рассмотрен в нескольких аспектах:

1) последовательная смена явлений, состояний в развитии конкретной системы;

2) цепь логически связанных, повторяющихся действий, в результате которых используются ресурсы организации с целью достижения определенных измеримых результатов [11];

3) поиск и оценка альтернативных решений, обработка результатов исследования, формулирование выводов по решению проблемы.

Обобщая различные дефиниции, можно определить процесс как совокупность взаимосвязанных видов деятельности, преобразующей характеристики входов в характеристики выходов, потребляющей для этого различные ресурсы и обеспечивающей управляющие воздействия (управления) (рис. 1.2.1). Входами в процесс, как правило, выступают выходы других процессов [11].

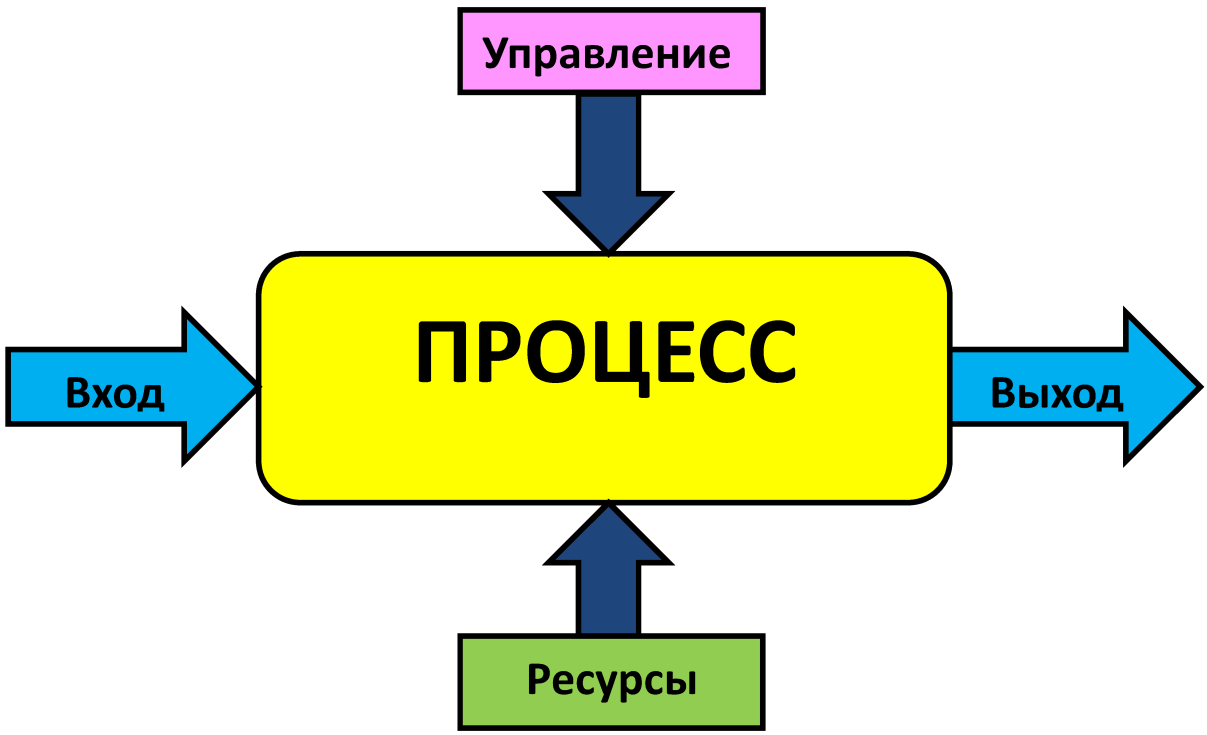


Рис. 1.2.1. Иллюстрация понятия «процесс»

Входами могут быть, например, множество активов организации при осуществлении их защиты от кибератак. На выходе формируется непосредственный результат процесса.

Входы и выходы процесса управления кибербезопасностью могут быть осязаемыми (используемое оборудование для защиты, характеристики информационных атак, защищаемая информация на различных носителях и т.п.) и неосязаемыми (характеристики «спящих» угроз, планируемые требования и услуги по защите информации и т.п.).

Любой процесс управления кибербезопасностью имеет заинтересованные стороны, например, потребителя защиты информации, внутреннего или внешнего относительно организации, и действует в соответствии с установленными целями.

Процессы, происходящие в организации и требующие для своего осуществления управления их кибербезопасностью, можно разделить на четыре группы [10]:

1. Основные процессы жизненного цикла, обеспечивающие базовый результат деятельности организации. Назначение таких процессов – создание конечных продуктов; результат – конечный продукт.

2. Обеспечивающие, предназначенные для нормального функционирования основных и других процессов необходимыми ресурсами; они обеспечивают сервисное обслуживание оборудования, энергоресурсное снабжение, обеспечение информацией, PR-деятельность и связь с общественностью и т.д. Результат указанных процессов – ресурсы, сервисы, услуги для основных процессов. Очевидно, что в этом смысле обеспечение компьютерной безопасности (ОКБ) относится к вспомогательной деятельности.

3. Процессы управления, относящиеся к постановке целей, стратегическому планированию, установлению политик, созданию инфокоммуникаций. Назначение процессов – управление деятельностью организации; результат – деятельность организации с той или иной эффективностью. По своей природе управленческие задачи являются информационными.

4. Процессы измерения, анализа и совершенствования направлены на усовершенствование всей деятельности организации. Чем более совершенна эта деятельность, тем лучше отлажены процессы указанной группы.

Их эффективность отражает способность достижения желаемых результатов, оцениваемых посредством внутренних и внешних процессов контроля.

Процессный подход – это определение применяемых организацией процессов и управления ими, особенно – их взаимодействием [11]. В основе подхода – взгляд на организацию как на совокупность ключевых процессов, а не функциональных подразделений. Главное внимание при

этом уделяется процессам, объединяющим отдельные функции в общие потоки и в целом направленным на достижение конечного результата всей организацией, а не отдельного подразделения.

Таким образом, основное преимущество процессного подхода заключается в управлении и контроле взаимодействия между различными процессами и связующими звеньями в контексте функциональной иерархии (организационно-штатной структуры) организации.

В ГОСТ Р ИСО 9000-2001 «Системы менеджмента качества. Основные положения и словарь» [11] содержится ряд требований к реализации процессного подхода в организации, главными из которых являются следующие:

- определение процессов, необходимых для реализации;
- выявление входов и выходов каждого процесса для установления их последовательности и взаимодействия;
- планирование и обеспечение ресурсами (включая информацию), необходимыми для реализации процессов и управления ими;
- установление необходимой степени реализации и документирование процессов;
- планирование процессов;
- наличие критериев и методов оценки управления процессами;
- осуществление мониторинга, оценки и анализа процессов;
- проведение корректирующих и превентивных действий по результатам анализа процессов, включая их совершенствование;
- определение методов и осуществление управления процессами, результаты которых сложно проверить посредством измерения.

Управление – вид деятельности, появившийся с возникновением совместной активности людей и регулирующий их отношения в этом процессе. Оно представляет целенаправленную деятельность человека, с помощью которой он упорядочивает и подчиняет своим интересам элементы среды существования общества [12].

Это процесс, состоящий из серии непрерывных взаимосвязанных действий (как отражение управленческих функций). Управление суммирует все управленческие функции, состав которых впервые предложен Анри Файолем: «Управлять – это значит предвидеть, организовывать, распоряжаться, координировать и контролировать» [13].

С позиции системного подхода управление представляет собой совокупность непрерывных взаимосвязанных воздействий на объект (управляемую систему) для достижения заданной цели. Оно направлено либо на сохранение ее основного качества (совокупности свойств, утеря которых приводит к разрушению системы), либо на выполнение некоторой программы, обеспечивающей устойчивость функционирования и достижение цели.

Системой управления (СУ) называют систему, реализующую функции управления. Главные вопросы, стоящие перед СУ, – чем и как управлять.

Основной элемент управляющей системы (УС) – *субъект управления*. Это лицо, группа лиц или специально созданный орган, являющийся источником управленческого воздействия на объект – *управляемую систему*, осуществляющие деятельность, направленную на обеспечение его нормального функционирования и успешное достижение заданной цели.

Объект управления – это система (организация, коллектив, конкретное лицо), на которую направлены управленческие воздействия с целью ее совершенствования, повышения качества реализации функций и решения задач, успешного достижения цели (целей).

Управление всегда связано с решением проблем, возникших в процессе функционирования объекта управления. При этом субъект управления, применяя системный подход, выявляет всю совокупность условий, причин и факторов, приведших к возникновению проблем, и определяет возможные пути и средства их разрешения.

Субъект управления реализует задачи целеполагания, достижения оптимального выполнения программы, обеспечивая удержание выходных характеристик системы в требуемых пределах при изменении характеристик внешней среды.

Метод управления – это совокупность последовательно применяемых способов воздействия субъекта управления на объект управления для достижения поставленной цели.

Программное управление – это выполнение последовательности действий (операций) в строгом соответствии с предписанной программой (законами, правилами, распоряжениями и т.п.).

Управление учитывает обратные связи, отражающие отклонения от намеченного пути, предполагает понимание объектом управления своего состояния в каждый момент времени на траектории следования к намеченной цели. При отклонении текущих параметров от требуемых включается программа коррекции траектории, что позволяет компенсировать ошибки и учесть внешние возмущения.

В теории управления существует три основных подхода: системный, процессный и ситуационный. О первых двух сказано выше. Ситуационный подход предполагает их сочетание в зависимости от конкретной ситуации функционирования организации для достижения ею своих целей, в частности, связанной с обеспечением кибербезопасности.

Для полноты раскрытия термина «управление» необходимо отметить, что в английском языке имеется несколько слов, которые переводятся на русский как «управление»:

- *control* – исторически первый из применяемых в информационных

технологиях (ИТ) терминов, отражающий самые простейшие операции в области управления, в большей степени с точки зрения технического аспекта деятельности;

- *management* – термин, который первоначально употреблялся в отношении управления человеческими ресурсами; в настоящее время встречается в сочетании с множеством понятий из области ИТ и имеет смысл регулирования (администрирования) какой-либо деятельности;
- *governance* – термин, который стал активно использоваться применительно к ИТ в последнем десятилетии; под ним понимается руководство по организации и контролю за какой-либо деятельностью. Переводится на русский как «власть, руководство, управление».

Институт под названием IT Governance Institute (ITGI, http://www.itgi.org) определяет руководство ИТ как структуру взаимоотношений и процессов по управлению и контролю для достижения организацией поставленных целей посредством снижения рисков и повышения дохода от использования ИТ и связанных с ними процессов. Руководство ИТ концентрируется на том, что необходимо делать для удовлетворения нынешних и будущих потребностей бизнеса и клиентов организации.

В основе такого руководства лежит концепция, согласно которой управление должно быть хорошо организованной деятельностью, осуществляемой специалистами, осознающими полную ответственность и подотчетность своих действий. Руководство является формальным средством исполнения своих обязанностей представителями исполнительной власти в государственных, коммерческих, образовательных и иных организациях. Оно обусловлено необходимостью управления рисками и защитой самой организации и по своей сути связано с двумя функциями: производством продукции и снижением рисков.

В организации должна быть создана система руководства, применяемая ко всем видам деятельности и процессам: планированию, проектированию, закупкам, разработке, внедрению и мониторингу. Система руководства включает в себя управление различными областями деятельности и строится на определенных принципах: понятные показатели, четкие политики и стандарты, сильные связи, ясная стратегия; понятное выполнение операций с установленной ответственностью компетентные организационные структуры, четко определенные роли и обязанности, упорядоченные процессы и процедуры, эффективное использование технологий, ответственное управление активами; активное управление изменениями; независимый анализ и постоянное совершенствование.

Руководство осуществляется в следующих условиях и обстоятельствах:

- федеральные и государственные законы, директивы и руководящие указания;
- миссия и стратегия организации;
- допустимые для организации риски;
- этика, культура и ценности организации;
- подход к управлению – централизованный или децентрализованный;
- политики, стандарты, процессы и процедуры, принятые в организации;
- роли и ответственность в организации;
- планы и отчетность организации;
- контроль практики управления.

Возможные области руководства: стратегическое планирование и регулирование – прогноз и возможности, необходимые для поставки продуктов организации; поставка продукции – создание прибыли в рамках бюджета; управление рисками КБ – непрерывный процесс, начинающийся с идентификации рисков КБ (угроз и уязвимостей КБ) и оценки их воздействия на активы, снижение рисков КБ посредством контрмер и формальное принятие руководством остаточных рисков КБ; управление ресурсами – правильное использование возможностей (люди, оборудование, ПО и т.д.) для удовлетворения потребностей организации; измерение производительности обеспечивает обратную связь с потребностями организации, чтобы она оставалась дееспособной или вовремя принимались корректирующие меры.

В начале XX века начала развиваться наука управления, которую стали называть менеджмент (от англ. *manage* – управлять, руководить).

В современной литературе имеются разные определения менеджмента, раскрывающие это понятие с различных точек зрения:

- способ (манера) обращения с людьми, власть и искусство управления, особого рода административные навыки, орган управления (Оксфордский словарь английского языка);
- совокупность принципов, форм, методов, приемов и средств управления производством и производственным персоналом с использованием достижений науки управления;
- искусство управления интеллектуальными, финансовыми, материальными ресурсами [8];
- эффективное и результативное достижение целей организации посредством планирования, организации и контроля над организационными ресурсами [9];
- скоординированная деятельность по управлению организацией [11].

В других источниках менеджмент определяется:

- как особый вид профессионально осуществляемой деятельности, направленной на достижение целей путем рационального использования материальных и трудовых ресурсов с применением научных подходов, принципов, функций и методов;
- объединение управленческой деятельности с кадровой политикой;
- процесс оптимизации человеческих, материальных и финансовых ресурсов для достижения организационных целей;
- теория и практика научного и хозяйственного управления организацией в условиях рынка;
- система научных знаний, составляющих теоретическую базу практического опыта в области управления и имеющих междисциплинарный характер.

Менеджмент включает основные функции управления (прогнозирование, целеполагание, планирование, организация деятельности, мотивирование персонала, лидерство, контроль, учет и анализ, корректировка деятельности и т.д.) и определяет эффективное достижение целей организации при оптимальном использовании ресурсов. Ограниченность ресурсов при выполнении функций управления требует их эффективного распределения и использования с учетом взаимозависимости, и взаимосвязанности этих функций. Менеджмент применяет и реализует специальные технологии и инструменты управления: организацию и организационные отношения (формальные и неформальные), организационную культуру, мотивирование, стимулирование и др. Таким образом, менеджмент является наиболее эффективным способом управления.

Подчеркнем, что часто слова «менеджмент» и «управление» используются как синонимы, хотя их научная трактовка, что видно из приведенных выше объяснений, совпадает не полностью.

Согласно Рекомендациям по стандартизации Р 50.1.053-2005 «Информационные технологии. Основные термины и определения в области технической защиты информации» и ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», безопасность информации (данных) – это состояние защищенности информации, при котором обеспечивается ее (их) конфиденциальность, доступность и целостность [15, 16].

Согласно Р 50.1.053-2005, безопасность информации (при применении информационных технологий – это состояние защищенности ИТ, обеспечивающее безопасность информации, для обработки которой она применяется, и ИБ автоматизированной ИС, в которой она реализована.

В ГОСТ Р 50922-2006 под защитой информации понимается деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на

защищаемую информацию.

Словосочетание «информационная безопасность» в разных контекстах имеет разный смысл. Например, в Доктрине информационной безопасности Российской Федерации этот термин определяется как состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В Стандарте Банка России СТО БР ИББС 1.0 ИБ – это безопасность, связанная с угрозами в информационной сфере. При этом защищенность достигается обеспечением совокупности свойств ИБ: доступности, целостности, конфиденциальности информационных активов, а информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений [17].

Обобщая, можно сказать, что под ИБ понимается:

- защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры [18];
- механизм защиты, обеспечивающий конфиденциальность, целостность и доступность информации [19];
- свойство информации сохранять конфиденциальность, целостность и доступность [20].

Согласно ГОСТ Р 53113.1-2008 «Информационная технология.Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения», информационная безопасность – это аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и надежности информации или средства ее обработки [21].

Кроме того, данное понятие в современных условиях включает в себя еще четыре свойства:

- аутентичность, или подлинность (свойство, гарантирующее правдивость) применяется к пользователям, процессам, системам, информации;
- учет (однозначное отслеживание всех действий, влияющих на ИБ);
- неоспоримость (причастность к совершению операций с информацией);
- надежность (соответствие запланированному поведению и результатам).

ИБ должна стать неотъемлемой частью производственной и деловой

культуры организации. Для достижения целей ИБ организации перечисленные свойства информации поддерживаются комплексом мероприятий, осуществляемых на основе соответствующих нормативных актов, политики ИБ и организационных структур за счет реализации установленных мер, методов, процедур и программно-аппаратных средств защиты информации (СЗИ), которыми необходимо постоянно управлять [20].

Итак, ИБ и, соответсвенно, КБ представляют, главным образом, проблему управления по поддержанию состояния защищенности активов организации, которое должно осуществляться постоянно. Этапы этого процесса составляют основу комплексной системой обеспечения КБ организации, включающей организационную (подготовленный персонал и нормативные документы), техническую (СЗИ) и другие составляющие (рис. 1.2.2).

Рис. 1.2.2. Этапы обеспечения КБ организации

1.3. Общая концепция управления рисками кибербезопасности

Под киберриском будем понимать потенциальную возможность причинения ущерба организации в процессе реализации конкретной угрозы при использовании уязвимостей ее активов. Тогда *величиной киберриска является произведение вероятности негативного события и размера ущерба.*

Условно это можно выразить следующей формулой: *Величина риска = Вероятность события * Размер ущерба.*

Существуют классификации рисков: по источнику риска (например, атаки хакеров или инсайдеров, финансовые ошибки, воздействие государственных регуляторов, юридические претензии контрагентов, негативное информационное воздействие конкурентов); по цели (информационные активы, физические активы, репутация, бизнес-процессы); по продолжительности влияния (операционные, тактические, стратегические).

Этапы и цели анализа рисков таковы:

1. Идентифицировать активы и оценить их ценность.
2. Идентифицировать угрозы активам и уязвимости в системе защиты.
3. Рассчитать вероятность реализации угроз и их влияние на деятельность организации.
4. Соблюсти баланс между стоимостью возможных негативных последствий и стоимостью мер защиты, дать рекомендации руководству организации по обработке выявленных рисков.

Этапы с 1-го по 3-й являются процедурами оценки риска (англ. risk assessment), отражая сбор имеющейся информации и частично – ее обработку.

Этап 4 представляет полноценный анализ рисков (англ. risk analysis), т.е. изучение собранных данных и выдачу результатов/указаний для дальнейших действий. При этом важно понимать уровень корректности и точности проведенной оценки.

На этапе 4 предлагаются методы обработки для каждого из актуальных рисков: передача (например, путем страхования), избегание (например, отказ от внедрения той или иной технологии или сервиса), принятие (сознательная готовность понести ущерб в случае реализации риска), минимизация (применение мер для снижения вероятности негативного события, приводящего к реализации риска).

После завершения всех этапов анализа рисков следует выбрать приемлемый для организации уровень рисков (англ. acceptable risk level), установить минимально возможный уровень безопасности (англ. baselines of performance), затем внедрить контрмеры и в дальнейшем оценивать их с точки зрения достижимости установленного минимально возможного уровня безопасности. Ущерб от реализации атаки может

быть прямым или непрямым.

Прямой ущерб – это непосредственные очевидные и легко прогнозируемые потери организации, такие как утеря прав интеллектуальной собственности, разглашение секретов деятельности, снижение стоимости активов или их частичная или полная ликвидация, судебные издержки и выплаты штрафов и компенсаций и т.д.

Непрямой ущерб может включать качественные или косвенные потери.

Качественными потери отражают приостановку или снижение эффективности деятельности компании, потерю клиентов, снижение качества производимых товаров или оказываемых услуг.

Косвенные потери – это недополученная прибыль, потеря деловой репутации, дополнительно понесенные расходы.

В зарубежной литературе встречаются также такие понятия, как *тотальный риск* (англ. total risk), когда вообще никакие меры защиты не внедряются, а также *остаточный риск* (англ. residual risk), если угрозы реализовались, несмотря на внедренные меры защиты.

Анализ рисков может быть как количественным, так и качественным.

Рассмотрим один из способов *количественного* анализа рисков. Основными показателями являются величины:

ALE – annual loss expectancy, ожидаемые годовые потери, т.е. «стоимость» всех инцидентов за год.

SLE – single loss expectancy, ожидаемые разовые потери, т.е. «стоимость» одного инцидента.

EF – exposure factor, фактор открытости перед угрозой, отражающий, какая доля актива будет ликвидирована при успешной реализации угрозы.

ARO – annualized rate of occurrence, среднее количество инцидентов в год.

Значение SLE вычисляется как произведение расчётной стоимости актива и значения EF, т.е. *SLE=AssetValue*EF*. При этом в стоимость актива следует включать и штрафные санкции за его недостаточную защиту.

Значение ALE вычисляется как произведение SLE и ARO, т.е. *ALE=SLE*ARO*. Значение ALE позволяет проранжировать риски – риск с самым высоким ALE является самым критичным. Рассчитанное значение ALE можно использовать для определения максимальной стоимости реализуемых мер защиты, учитывая, что стоимость защитных мер не должна превышать стоимость актива или величину прогнозируемого ущерба, а расчетные затраты на атаку для злоумышленника должны быть меньше, чем ожидаемая им прибыль от реализации этой атаки. Ценность мер защиты также можно определить, вычтя из расчётного значения ALE до внедрения мер защиты значение расчётного значения ALE после их внедрения, а также вычтя ежегодные затраты на реализацию этих мер.

Условно это выражение записывается следующим образом:

Ценность мер защиты = ALE до внедрения мер защиты - ALE после внедрения мер защиты - Ежегодные затраты на реализацию мер защиты.

Примерами *качественного* анализа рисков являются метод Дельфи, в котором проводится анонимный опрос экспертов в несколько итераций до достижения консенсуса, а также мозговой штурм и прочие примеры оценки так называемым «экспертным методом».

Приведем кратко методологии риск-менеджмента, самые распространенные из них рассмотрим далее.

1. Фреймворк «NIST Risk Management Framework» на базе NIST (National Institute of Standards and Technology – Национального института стандартов и технологий, США) включает в себя набор взаимосвязанных «специальных публикаций» (англ. Special Publication – SP, назовем их стандартами):

1.1. Стандарт NIST SP 800-39 «Managing Information Security Risk» («Управление рисками информационной безопасности») предлагает трехуровневый подход к управлению рисками: организация, бизнес-процессы, информационные системы. Данный стандарт описывает методологию процесса управления рисками: определение, оценка, реагирование и мониторинг рисков.

1.2. Стандарт NIST SP 800-37 «Risk Management Framework for Information Systems and Organizations» («Фреймворк управления рисками для информационных систем и организаций») предлагает для обеспечения безопасности и конфиденциальности использовать подход управления жизненным циклом систем.

1.3. Стандарт NIST SP 800-30 «Guide for Conducting Risk Assessments» («Руководство по проведению оценки рисков») сфокусирован на ИТ, ИБ и операционных рисках. Он описывает подход к процессам подготовки и проведения оценки рисков.

1.4. Стандарт NIST SP 800-137 «Information Security Continuous Monitoring» («Непрерывный мониторинг информационной безопасности») описывает мониторинг информационных систем и ИТ–сред в целях контроля примененных мер обработки рисков ИБ и определения их пересмотра.

2. Стандарты Международной организации по системе ISO (International Organization for Standardization):

2.1. Стандарт ISO/IEC 27005:2018 «Information technology – Security techniques – Information security risk management» («Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности») входит в серию стандартов ISO 27000 и является логически взаимосвязанным с другими стандартами по ИБ из этой серии. Данный стандарт отличается фокусировкой на ИБ при рассмотрении процессов управления рисками.

2.2. Стандарт ISO/IEC 27102:2019 «Information security management – Guidelines for cyber-insurance» («Управление информационной безопасностью. Руководство по киберстрахованию») предлагает подходы к оценке киберстраховки как меры обработки рисков, а также к оценке и взаимодействию со страховщиком.

2.3. Серия стандартов ISO/IEC 31000:2018 описывает подход к риск-менеджменту без привязки к ИТ/ИБ. В этой серии стоит отметить стандарт ISO/IEC 31010:2019 «Risk management – Risk assessment techniques», а также данный стандарт в его отечественном варианте ГОСТ Р ИСО/МЭК 31010-2011 «Менеджмент риска. Методы оценки риска».

3. Методология FRAP (Facilitated Risk Analysis Process) является относительно упрощенным способом оценки рисков, с акцентированием только на самых критических активах. Качественный анализ при этом проводится с помощью экспертной оценки.

4. Методология OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) сфокусирована на самостоятельной работе членов производственных подразделений. Она используется для масштабной оценки всех информационных систем и производственных процессов организации.

5. Австралийский и новозеландский стандарт AS/NZS ISO 31000-2009 фокусируется не только на ИТ-системах, но и на производственной деятельности организации, предлагая более широкий подход к управлению рисками.

6. Методология FMEA (Failure Modes and Effect Analysis) предлагает проведение оценки системы для поиска ненадежных элементов.

7. Методология CRAMM (Central Computing and Telecommunications Agency Risk Analysis and Management Method) предлагает использование автоматизированных средств для управления рисками.

8. Методология FAIR (Factor Analysis of Information Risk) предназначена для количественного анализа рисков, предлагая модель управления рисками на основе экономически эффективного подхода, принятия риск-решений, сравнения мер управления рисками и финансовых показателей.

9. Концепция COSO ERM (Enterprise Risk Management) описывает пути интеграции риск-менеджмента со стратегией и финансовой эффективностью деятельности организации и акцентирует внимание на важности их взаимосвязи. В документе описаны такие компоненты управления рисками, как стратегия и постановка целей, экономическая эффективность деятельности организации, анализ и пересмотр рисков, корпоративное управление, культура и отчетность.

NIST Risk Management Framework

Рассмотрим первый набор документов – программную платформу

управления рисками (Risk Management Framework) американского национального института стандартов и технологий (NIST). Данный институт выпускает документы по ИБ в рамках серии стандартов FIPS (Federal Information Processing Standards, Федеральные стандарты обработки информации) и рекомендаций SP (Special Publications, Специальные публикации) 800-й серии.

Данная серия отличается логической взаимосвязанностью, детальностью, единой терминологической базой. Среди документов, касающихся управления рисками ИБ, следует отметить публикации NIST SP 800-39, 800-37, 800-30, 800-137 и 800-53/53a.

Создание данного набора документов явилось следствием принятия Федерального закона США об управлении информационной безопасностью (FISMA, Federal Information Security Management Act, 2002 г.) и Федерального закона США о модернизации информационной безопасности (FISMA, Federal Information Security Modernization Act, 2014 г.). Несмотря на декларируемую «привязку» стандартов и публикаций NIST к законодательству США и обязательность их исполнения для американских государственных органов, эти документы вполне можно рассматривать и как подходящие для любой организации, стремящейся улучшить управление ИБ, вне зависимости от юрисдикции и формы собственности.

NIST SP 800-39

Итак, документ **NIST SP 800-39 «Managing Information Security Risk: Organization, Mission, and Information System View»** предлагает гибкий подход к управлению рисками в контексте деятельности организации, ее активов и контрагентов. При этом риск-менеджмент является целостным процессом, затрагивающим всю организацию, в которой практикуется риск-ориентированное принятие решений на всех уровнях. Управление риском определяется в данном документе как процесс, включающий в себя этапы определения (frame), оценки (assess), обработки (respond) и мониторинга (monitor) рисков. Рассмотрим указанные этапы подробнее.

1. На этапе определения рисков организации следует выявить:

- предположения о рисках, т.е. идентифицировать актуальные угрозы, уязвимости, последствия, вероятность возникновения рисков;
- ограничения рисков, возможности осуществления оценки, реагирования и мониторинга;
- риск-толерантность, т.е. терпимость к рискам – приемлемые типы и уровни рисков, а также допустимый уровень неопределенности в вопросах управления рисками;
- приоритеты и возможные компромиссы, т.е. нужно изучить компромиссы, на которые может пойти организация при обработке рисков,

а также ограничения и факторы неопределенности, сопровождающие этот процесс.

2. На этапе оценки рисков организации следует выявить:

- угрозы КБ, т.е. конкретные действия, которые могут являться угрозами для самой организации или могут быть направлены на другие организации;
- внутренние и внешние уязвимости, включая организационные уязвимости в производственных процессах, управлении организацией, архитектуре ИТ-систем и т.д.;
- ущерб организации с учетом вероятности реализации угроз;
- вероятность возникновения ущерба.

В итоге в организации формируется понимание детерминант риска, включая уровень ущерба и его вероятность для каждого риска.

Для обеспечения процесса оценки рисков организация определяет:

- инструменты, техники и методологии, используемые для оценки риска;
- допущения и ограничения, которые влияют на оценки рисков;
- роли и ответственность;
- способы проведения оценки;
- способы сбора, обработки и передачи информации об оценке рисков в пределах организации;
- частоту проведения оценки;
- способы получения информации об угрозах.

3. На этапе реагирования на риск организация выполняет:

- разработку планов реагирования;
- оценку планов реагирования;
- определение планов реагирования, допустимых с точки зрения риск-толерантности организации;
- реализацию принятых планов реагирования на риск.

Для обеспечения реагирования на риски организация определяет типы возможной обработки рисков (принятие, избегание, минимизация, разделение или передача риска), а также инструменты, технологии и методологии для разработки планов реагирования, способы оценки планов реагирования и методы оповещения о предпринятых мерах реагирования в рамках самой организации и/или сторонних организационных структур.

На этапе мониторинга рисков решаются задачи:

- проверки реализации планов реагирования на риск и выполнения нормативных требований КБ;
- определения эффективности мер реагирования на риски;

- оценки значимых для риск-менеджмента изменений в ИТ-системах и средах, включая спектр угроз, уязвимости, производственные функции и процессы, ИТ–инфраструктуру, взаимоотношения с другими организациями, риск-толерантность организации и т.д.

Организации описывают методы оценки нормативного соответствия и эффективности мер реагирования на риски, а также контроль изменений, способных повлиять на эффективность реагирования на риски.

Управление рисками ведется на уровнях организации, производственных процессов и информационных систем, при этом следует обеспечивать взаимосвязь и обмен информацией между указанными уровнями в целях непрерывного повышения эффективности осуществляемых действий.

На верхнем уровне организации осуществляется принятие решений по определению рисков, что напрямую влияет на процессы нижних уровней (производственных процессов и информационных систем), а также на финансирование этих процессов.

На уровне организации осуществляются выработка и внедрение функций управления, согласующихся с ее целями и нормативными требованиями: создание функции риск-менеджмента, назначение ответственных, внедрение стратегии управления рисками и определение риск-толерантности, разработка и реализация инвестиционных стратегий в ИТ и КБ.

На уровне производственных процессов происходит определение и создание риск-ориентированных производственных процессов и организационной архитектуры. Кроме того, на данном уровне осуществляется разработка архитектуры КБ, которая обеспечит эффективное выполнение требований КБ и внедрение всех необходимых мер и средств защиты.

На уровне информационных систем обеспечивается выполнение решений, принятых на более высоких уровнях применительно к управлению рисками КБ на всех этапах жизненного цикла систем: инициализация, разработка, внедрение, использование и вывод из эксплуатации.

Отметим, что в описании каждого из способов обработки рисков нужно указать, что в организации должна существовать как общая стратегия обработки риска в той или иной ситуации, так и отдельные стратегии для каждого из способов обработки рисков. Детализируем основные принципы обработки рисков:

- принятие (acceptance) риска не должно противоречить стратегии риск-толерантности организации и её возможности отвечать за возможные последствия этого;

- избегание (avoidance) риска – зачастую самый надежный способ обработки рисков, но он может идти вразрез с необходимостью применения нужных организациям ИТ-систем и технологий;
- разделение (share) и передача (transfer) рисков – это частичное или полное разделение ответственности за последствия реализованного риска с внешними партнерами в соответствии с принятой стратегией, конечная цель которой – успешность функционирования организации;
- смягчение (mitigation) рисков подразумевает применение стратегии минимизации рисков ИБ на всех трех уровнях. Организации следует выстраивать производственные процессы в соответствии с принципами защиты информации, архитектурные решения, политики, процессы и средства КБ должны быть достаточно универсальными и гибкими для применения их в динамичной и разнородной среде организации с учетом непрерывно меняющегося спектра угроз ИБ.

NIST SP 800-37 «Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy» («Фреймворк управления рисками для информационных систем и организаций: жизненный цикл систем обеспечения безопасности и конфиденциальности») обновлен в 2018 году с тем, чтобы учесть современный спектр угроз и акцентировать внимание на важности управления рисками на уровне руководителей организации, подчеркнуть связь между программой управления рисками (Risk Management Framework, RMF) и программой кибербезопасности (Cybersecurity Framework, CSF), указать на важность интеграции процессов управления конфиденциальностью и управления рисками поставок (англ. supply chain risk management, SCRM), а также логически увязать список предлагаемых мер защиты с документом NIST SP 800-53. Выполнение положений NIST SP 800-37 можно использовать при проведении взаимной оценки процедур риск-менеджмента организаций в случаях, когда им требуется обмен данными или ресурсами. По аналогии с NIST SP 800-39 рассматривается управление рисками на уровнях организации, производственных процессов, информационных систем.

В NIST SP 800-37 указывается на важность разработки и внедрения возможностей по обеспечению безопасности и конфиденциальности в ИТ-системах на протяжении всего жизненного цикла (англ. system development life cycle, SDLC), непрерывной поддержки ситуационной осведомленности о состоянии защиты ИТ-систем с применением процессов непрерывного мониторинга (continuous monitoring, CM) и предоставления информации руководителям для принятия взвешенных риск-ориентированных решений. В RMF выделены следующие типы рисков: программный риск, риск несоответствия законодательству, финансовый риск, правовой риск, бизнес-риск, политический риск, риск безопасности и

конфиденциальности, проектный риск, репутационный риск, риск безопасности жизнедеятельности, риск стратегического планирования.

Кроме этого, RMF:

- предоставляет повторяемый процесс для риск-ориентированной защиты информации и информационных систем;
- подчеркивает важность подготовительных мероприятий для управления безопасностью и конфиденциальностью;
- обеспечивает категоризацию информации и информационных систем, а также выбора, внедрения, оценки и мониторинга средств защиты;
- предлагает использовать средства автоматизации для управления рисками и мерами защиты в режиме реального времени, а также актуальные варианты предоставления информации для принятия решений;
- связывает процессы риск-менеджмента на различных уровнях и указывает на важность выбора ответственных за принятие защитных мер.

В вышеназванном документе указаны семь этапов применения RMF:

1. Определение целей и их приоритезация с точки зрения организации и ИТ-систем.
2. Категоризация систем и информации на основе анализа возможного негативного влияния в результате её потери. NIST SP 800-30 также указывает три фактора при проведении оценки риска: угрозы, уязвимости, вероятность события.
3. Выбор базовых мер защиты и их уточнение для снижения риска до приемлемого уровня;
4. Внедрение мер защиты и описание процедур их применения.
5. Оценка внедренных мер защиты для определения их корректности, работоспособности и результативности, удовлетворяющих требованиям безопасности и конфиденциальности.
6. Авторизация систем или мер защиты на основе заключения о приемлемости рисков.
7. Непрерывный мониторинг систем и примененных мер защиты для оценки их эффективности, изменений, проведения оценки рисков и анализа негативного их влияния, создания отчетов по состоянию безопасности и конфиденциальности.

Далее в NIST SP 800-37 рассматриваются задачи, решаемые на каждом из этапов применения RMF. Для каждой из задач указывается ее название, перечисляются входные и выходные данные процесса, приводится перечень ответственных и вспомогательных ролей, даются ссылки на документы NIST.

Задачи этапа «**Подготовка**» на уровне *организации* включают:

- определение ролей для управления рисками;
- формулирование стратегии управления рисками с учетом риск-толерантности организации;

- проведение оценки рисков;
- выбор целевых значений мер защиты из Cybersecurity Framework;
- приоритезацию ИТ-систем;
- определение для ИТ-систем общих мер защиты, которые могут быть унаследованы с более высоких уровней (например, с уровня организации или производственных процессов);
- разработку и внедрение непрерывного мониторинга эффективности мер защиты.

Задачи этапа «**Подготовка**» на *уровне ИТ-систем* включают:

- определение производственных функций и процессов, которые поддерживает каждая ИТ-система;
- идентификацию лиц, заинтересованных в создании, внедрении, оценке, функционировании, поддержке, выводе систем из эксплуатации;
- определение активов, требующих защиты;
- определение границы авторизации для системы;
- выявление типов информации, обрабатываемых, передаваемых, хранимых в системе;
- идентификацию и анализ жизненного цикла всех типов информации, обрабатываемых/передаваемых/хранимых в системе;
- проведение оценки рисков на уровне ИТ-систем и обновление результатов оценки;
- определение требований по безопасности и конфиденциальности для систем и сред функционирования;
- определение местоположения систем в общей архитектуре организации.
- формальную регистрацию ИТ-систем в соответствующих департаментах и документах.

Задачи этапа «**Категоризация**» включают:

- документирование характеристик системы;
- категоризацию системы и документирование результатов категоризации по требованиям безопасности;
- пересмотр и согласование результатов и решений по категоризации по требованиям безопасности.

Задачи этапа «**Выбор набора мер защиты**» включают:

- выбор мер защиты для системы и среды её функционирования;
- уточнение (адаптация) выбранных мер защиты для системы и среды её функционирования;
- распределение точек применения мер обеспечения безопасности и конфиденциальности к системе и среде её функционирования;

- документирование мер обеспечения безопасности и конфиденциальности системы и среды её функционирования в соответствующих планах;
- создание и внедрение мониторинга эффективности применяемых мер защиты, которая логически связана с общей организационной стратегией мониторинга и дополняет ее;
- пересмотр и согласование планов обеспечения безопасности и конфиденциальности системы и среды её функционирования.

Задачи этапа «**Внедрение мер защиты**» включают:

- внедрение мер защиты в соответствии с планами обеспечения безопасности и конфиденциальности;
- документирование изменений в запланированные меры защиты на основании реальных результатов.

Задачи этапа «**Оценка внедренных мер защиты**» включают:

- выбор действий, соответствующих типу проводимой оценки;
- разработку, пересмотр и согласование планов по оценке мер защиты;
- проведение оценки мер защиты в соответствии с процедурами, описанными в планах;
- подготовку отчетности, содержащей найденные недостатки и рекомендации по их устранению;
- выполнение корректирующих действий по мерам защиты и переоценку скорректированных мер;
- подготовку плана действий на основании найденных недостатков и рекомендации из отчетов.

Задачи этапа «**Авторизация**» включают:

- сбор пакета документов и отправку его на авторизацию;
- анализ и определение риска использования системы или применения мер защиты;
- определение и внедрение плана действий при реагировании на выявленный риск;
- определение приемлемости риска при использовании системы и применения мер защиты;
- сообщение о результатах авторизации и о недостатках мер защиты, представляющих значительный риск для безопасности или конфиденциальности.

Задачи этапа «**Непрерывный мониторинг**» включают:

- мониторинг информационной системы и среды её функционирования на наличие изменений, влияющих на состояние безопасности и конфиденциальности системы;

- оценку мер защиты в соответствии со стратегией непрерывного мониторинга;
- реагирование на риск на основе результатов непрерывного мониторинга, оценок риска, плана действий;
- обновление планов, отчетов по оценке планов действий на основании результатов непрерывного мониторинга;
- сообщение о состоянии безопасности и конфиденциальности соответствующему должностному лицу в соответствии со стратегией непрерывного мониторинга системы;
- пересмотр состояния безопасности и конфиденциальности системы для определения приемлемости риска;
- разработку стратегии вывода системы из эксплуатации и выполнение соответствующих действий при окончании срока её службы.

NIST SP 800-30 «Guide for Conducting Risk Assessments» («Руководство по проведению оценок риска») посвящено процедуре оценки риска, которая является важнейшим компонентом процесса управления в организации в соответствии с NIST SP 800-39, наряду с определением, обработкой и мониторингом.

Процедуры оценки рисков используются для идентификации, оценки и приоритезации рисков, порождаемых использованием информационных систем, для деятельности организации, её активов и работников.

Целями оценки рисков являются информирование лиц, принимающих решения, и поддержка процесса реагирования на риск путем идентификации:

- актуальных угроз самой организации и опосредованно – другим организациям;
- внутренних и внешних уязвимостей;
- потенциального ущерба организации с учетом возможностей использования уязвимостей;
- вероятности возникновения ущерба.

Конечным результатом является вычисление значения риска от его вероятности и размера ущерба. Оценка производится на всех трех уровнях управления рисками (организации, производственных процессов, информационных систем) по аналогии с подходом, применяемым в NIST SP 800-39 и NIST SP 800-37.

Оценка рисков – это непрерывный процесс, затрагивающий все уровни управления рисками в организации, проводимый с частотой, соответствующей целям и объему оценки.

Процесс оценки рисков включает:

- подготовку к оценке;
- проведение оценки;

- передачу информации об оценке внутри организации;
- поддержание и развитие достигнутых результатов.

В указанном документе говорится о важности формирования методологии оценки рисков. Указано, что организация может выбрать одну или несколько методологий оценки в зависимости от имеющихся ресурсов, сложности и зрелости производственных процессов, критичности/важности обрабатываемой информации. Создание корректной методологии повышает качество и воспроизводимость реализуемых оценок риска. Методология оценки риска включает:

- описание процесса оценки;
- модель, описывающую факторы риска и взаимосвязи между ними;
- способ оценки (например, качественный или количественный), описывающий значения, которые могут принимать факторы риска;
- способ учета комбинации факторов риска.

Модель рисков описывает их оцениваемые факторы и взаимосвязи между ними.

Факторы риска – это характеристики, используемые в моделях риска в качестве входных данных для определения уровней рисков при проведении их оценки. Кроме того, факторы риска используются для выделения тех из них, которые значимо влияют на уровни рисков в определенных ситуациях и контекстах.

При этом некоторые факторы риска могут быть декомпозированы до более детальных характеристик, например, угрозы можно декомпозировать до источников угроз (англ. threat sources) и событий угроз (англ. threat events).

Угроза – *это любое обстоятельство или событие, имеющее потенциал негативного влияния на производственные процессы или активы организации, сотрудников, организации-партнеры путем осуществления несанкционированного доступа, разрушения, разглашения или модификации информации и/или отказа в обслуживании.*

Источником угроз может быть преднамеренное действие, направленное на использование уязвимости, или ненамеренное действие, в результате которого уязвимость использована случайно.

Среди источников можно назвать:

- враждебные кибератаки или физические атаки;
- человеческие ошибки;
- структурные ошибки в активах, подконтрольных организации;
- природные, антропогенные и техногенные аварии или катастрофы.

Детальность определения угроз зависит от глубины построения модели рисков. В случае детального рассмотрения модели рисков можно строить сценарии угроз, которые являются набором из нескольких

событий, приводящих к негативным эффектам, привязанным к определенному источнику (источникам) угроз и упорядоченным по времени; при этом рассматривается потенциальная вероятность последовательной эксплуатации нескольких уязвимостей, приводящей к успешной реализации атаки. События угроз в кибер- или физических атаках характеризуются набором тактик, техник и процедур (англ. tactics, techniques, and procedures, TTPs), о которых говорилось ранее.

Рассматриваемый документ также говорит о таком понятии, как «**смещение угрозы**» (англ. threat shifting), под которым понимается изменение атакующими своих TTPs в зависимости от мер защиты, предпринятых организацией и выявленных атакующими. Смещение угрозы может быть осуществлено во временн***о***м аспекте (например, попытки атаковать в другое время или растянуть (сжать) атаку во времени), в целевом отношении (например, выбор менее защищенной цели), ресурсном плане (например, использование дополнительных ресурсов для взлома цели), методах планирования или атаки (например, использование другого хакерского инструментария или попытки атаковать иными методами).

Кроме этого, нужно учитывать, что атакующие зачастую для достижения своих целей выбирают самое слабое звено в цепи защиты.

Уязвимость – *это слабость в информационной системе, процедурах обеспечения безопасности, внутренних способах защиты или в особенностях конкретной реализации/внедрения той или иной технологии или системы.*

Уязвимость характеризуется возможностью её устранения; при этом опасность уязвимости может быть определена в зависимости от ожидаемого негативного эффекта от ее использования.

Большинство уязвимостей в информационных системах организации возникают или из-за непримененных (случайно или умышленно) мер КБ, или примененных некорректно. Важно помнить и об эволюции угроз и самих защищаемых систем – и в тех, и в других со временем происходят изменения, которые следует учитывать при проведении переоценки рисков. Кроме уязвимостей технического характера в ИТ-системах, следует учитывать и ошибки в управлении организацией и в архитектуре систем.

Предварительное условие (англ. predisposing condition) в контексте оценки рисков – это *условие, существующее в бизнес-процессе, архитектуре или ИТ-системе, снижающее или увеличивающее вероятность причинения ущерба.*

Логическими синонимами являются термины «подверженность» (англ. susceptibility) или «открытость» (англ. exposure) риску, означающие, что уязвимость может быть использована для нанесения ущерба. Например, SQL-сервер потенциально подвержен уязвимости SQL-

инъекции.

Кроме технических предварительных условий следует учитывать и организационные: так, местоположение офиса в низине увеличивает риск подтопления, а отсутствие коммуникации между сотрудниками при разработке ИТ-системы увеличивает риск её взлома.

Вероятность возникновения угрозы (англ. likelihood of occurrence) – *показатель того, что определенная уязвимость (или группа уязвимостей) может быть использована для причинения реального ущерба.*

Для намеренных угроз оценка вероятности возникновения обычно оценивается на основании возможностей и целей злоумышленника. Для ненамеренных угроз оценка вероятности возникновения, как правило, зависит от эмпирических и исторических данных.

При этом вероятность возникновения оценивается на определенную временну**ю** перспективу – например, на следующий год или на отчетный период.

При оценке вероятности возникновения угрозы следует учитывать состояние управления и процессы, характеризующие организацию, предварительные условия, наличие и эффективность мер защиты. Вероятность негативного влияния означает возможность того, что при реализации угрозы будет нанесен какой-либо ущерб. При определении общей вероятности возникновения угроз используют три этапа:

1. Оценка вероятности того, что угроза будет кем-либо инициирована (в случае намеренной угрозы) или реализуется случайно сама.
2. Оценка вероятности того, что возникшая угроза приведет к ущербу или нанесет вред организации, активам, сотрудникам.
3. Общая вероятность рассчитывается в результате комбинации первых двух полученных оценок.

В документе дается рекомендация не искать абсолютно все взаимосвязанные угрозы и уязвимости, а сконцентрироваться на тех из них, которые действительно могут быть использованы в атаках, а также на процессах организации и функциях с недостаточными мерами защиты.

Уровень негативного влияния (англ. impact) события угрозы – это величина ущерба, который ожидается от несанкционированного разглашения, доступа, изменения, утери информации или недоступности информационных систем. Организация явным образом определяет:

1. Процесс, используемый для определения негативного влияния.
2. Предположения и обоснования, используемые для определения негативного влияния.
3. Источники и методы получения информации о негативном влиянии.

Кроме этого, при расчете негативного влияния организации должны учитывать ценность активов и информации: можно использовать принятую в организации систему категорирования информации по

уровням значимости или результаты оценок негативного влияния на конфиденциальность.

При оценке рисков важным фактором является **степень неопределённости** (англ. uncertainty), которая возникает из-за ограничений: невозможности точно спрогнозировать будущие события; недостаточности сведений об угрозах; неизвестных уязвимостях; нераспознанных взаимозависимостях.

С учетом вышесказанного **модель риска** можно описать как такую логическую структуру: *источник угрозы* с определенной *вероятностью* инициирует *угрозу*, которая использует *уязвимость* (несущую определенную опасность с учетом успешного обхода защитных мер), вследствие чего создается *негативное влияние* (зависящее от вероятности возникновения ущерба), которое порождает *риск*.

Документ дает рекомендации по использованию процесса **агрегирования рисков** (англ. risk aggregation) в целях объединения нескольких разобщенных или низкоуровневых рисков в один более общий: например, риски отдельных ИТ- систем могут быть агрегированы в общий риск для всей поддерживаемой ими организационной системы.

При таком объединении следует учитывать, что некоторые риски могут реализовываться одновременно или чаще, чем это прогнозировалось. Также следует учитывать взаимосвязи между разобщенными рисками и либо объединять их, либо разъединять.

В NIST SP 800-30 также описаны основные **способы оценки рисков**: количественный (англ. quantitative), качественный (англ. qualitative) и полуколичественный (англ. semi-quantitative).

Количественный анализ оперирует конкретными цифрами (стоимостью, временем простоя, затратами и т.д.) и лучше всего подходит для проведения анализа выгод и затрат (англ. cost-benefit analysis), являясь достаточно ресурсоёмким.

Качественный анализ применяет описательные характеристики (например, высокий, средний, низкий), что может привести к некорректным выводам ввиду субъективности выставления оценок.

Полуколичественный способ является промежуточным вариантом, предлагающим использовать больший диапазон возможных оценок (например, по шкале от 1 до 10) для более точной оценки и анализа результатов сравнения. Применение конкретного способа оценки рисков зависит как от сферы деятельности организации (например, в банковской сфере может применяться более строгий количественный анализ), так и от стадии жизненного цикла системы (например, на начальных этапах цикла может проводиться только качественная оценка рисков, а на более поздних – количественная).

Наконец, в документе описаны три основных **способа анализа** факторов рисков: угрозоцентричный (англ. threat-oriented),

ориентированный на активы (англ. asset/impact-oriented) или уязвимости (англ. vulnerability-oriented).

Угрозоцентричный способ сфокусирован на создании сценариев угроз и начинается с определения источников угроз и событий угроз; далее уязвимости идентифицируются в контексте угроз, а негативное влияние связывается с намерениями злоумышленника.

Способ, **ориентированный на активы**, подразумевает выявление событий угроз и источников угроз, способных оказать негативное влияние на активы; при этом во главу угла ставится потенциальный ущерб активам.

Применение способа, **ориентированного на уязвимости**, начинается с анализа предварительных условий и недостатков/слабостей, которые могут быть использованы; далее определяются возможные события угроз и последствия использования найденных уязвимостей.

Документ содержит рекомендации по комбинированию описанных способов анализа для получения более объективной картины угроз при оценке рисков.

Итак, по NIST SP 800-30 процесс оценки рисков разбивается на 4 шага:

- подготовка к оценке рисков;
- проведение оценки рисков;
- коммуницирование результатов оценки и передача информации внутри организации;
- поддержание достигнутых результатов.

Рассмотрим подробнее задачи, выполняемые на каждом из этапов.

1. **Подготовка к оценке рисков.** В рамках подготовки к оценке рисков решаются следующие подзадачи:

1.1. Идентификация цели оценки: какая информация ожидается в результате, какие решения будут являться результатом оценки.

1.2. Идентификация области оценки в контексте применимости к конкретной организации, временному интервалу, архитектуре и используемым технологиям.

1.3. Идентификация ограничений оценки рисков. В рамках этой подзадачи определяются ограничения в таких элементах, как источники угроз, события угроз, уязвимости, предварительные условия, вероятность возникновения, негативное влияние, риск-толерантность и уровень неопределенности, а также выбранный способ анализа.

1.4. Идентификация источников информации об источниках угроз и уязвимостей. В этом процессе источники информации могут быть как внутренними (ими служат отчеты по инцидентам и аудитам, журналы безопасности и результаты мониторинга), так и внешними (отчеты CERT, результаты исследований и прочая релевантная общедоступная информация).

1.5. Идентификация модели рисков, способов оценки рисков и

методов анализа, которые используются при оценке.

2. Проведение оценки рисков. В рамках оценки рисков выполняются подзадачи:

2.1. Идентификация и описание актуальных источников угроз, включая возможности, намерения и цели намеренных угроз, а также возможные эффекты от ненамеренных угроз.

2.2. Идентификация потенциальных событий угроз, их релевантности, а также источников угроз, которые могут инициировать указанные события.

2.3. Идентификация уязвимостей и условий, которые влияют на вероятность того, что события угроз приведут к негативному влиянию. Целью является определение того, насколько рассматриваемые процессы и информационные системы уязвимы перед идентифицированными ранее источниками угроз и насколько идентифицированные события угроз действительно могут быть инициированы этими источниками угроз.

2.4. Определение вероятности того, что угрозы приведут к негативному событию, с учетом характеристик их источников, уязвимостей и условий, а также подверженности организации этим угрозам, принимая во внимание внедренные меры защиты.

2.5. Определение негативного влияния, порожденного реализацией угроз, с учетом характеристик их источников, уязвимостей и условий, а также подверженности организации этим угрозам с учетом внедренных мер защиты.

2.6. Определение риска при реализации угроз, принимая во внимание вероятность наступления негативных событий.

3. Передача информации при оценке рисков. При передаче информации решаются задачи:

3.1. Ознакомления с результатами оценки лицами, принимающими решения при реагировании на риски.

3.2. Информирования заинтересованных лиц результатами оценки.

4. Поддержание достигнутых результатов. В рамках поддержания достигнутых результатов решаются подзадачи:

4.1. Проведения мониторинга факторов, определяющих риски деятельности организации, их влияния на активы, сотрудников, организации-партнеры. Данной подзадаче посвящен стандарт NIST SP 800-137.

4.2. Актуализация оценки рисков с использованием результатов мониторинга факторов риска.

Документ NIST SP 800-30 предлагает детальный подход к моделированию угроз и расчету рисков. Важными являются приложения к стандарту, содержащие примеры расчетов по каждой из подзадач оценки рисков, а также перечни возможных источников угроз, событий угроз, уязвимостей и предварительных условий.

NIST SP 800-137

Перейдем к обзору документа NIST SP 800-137 «Information Security Continuous Monitoring for Federal information Systems and Organizations» («Непрерывный мониторинг информационной безопасности для федеральных информационных систем и организаций»).

Задачей непрерывного мониторинга информационной безопасности является оценка эффективности мер защиты и статуса безопасности систем с целью реагирования на вызовы в сфере информационной безопасности.

Система непрерывного мониторинга КБ помогает предоставлять данные о состоянии безопасности информационных систем, собранные из различных ресурсов (активы, процессы, технологии, сотрудники). Данная система является одной из тактик в общей стратегии управления рисками.

В документе приведен рекомендуемый процессный подход к выстраиванию системы мониторинга КБ, состоящий из:

- определения стратегии мониторинга КБ (включает выстраивание стратегии на уровне организации, производственных процессов и информационных систем); назначения ролей и ответственных; выбор процедур сбора данных;
- разработки программы мониторинга КБ (включает определение процедур оценки и контроля; регулярности проведения мониторинга и оценки; разработку архитектуры системы мониторинга);
- внедрения программы мониторинга КБ;
- анализа найденных недостатков и отчета о них (включает анализ данных; отчетность по оценке мер защиты);
- реагирования на выявленные недостатки;
- модернизации стратегии и программы мониторинга КБ.

В документе даются рекомендации по выбору инструментов обеспечения мониторинга КБ:

- поддержка большого количества источников данных;
- использование открытых и общедоступных спецификаций;
- интеграция с другим ПО, системами управления инвентаризацией и конфигурациями, а также системами реагирования на инциденты;
- поддержка соответствия законодательным нормам;
- процесс создания отчетов с возможностью усиления глубины рассматриваемых данных;
- поддержка систем Security Information and Event Management (SIEM) и систем визуализации данных.

Систему всемирной стандартизации формируют Международная организация по стандартизации ISO (ИСО) и Международная электротехническая комиссия (МЭК).

В соответствии с разработанными стандартами обеспечение КБ в любой организации заключается в выполнении следующих действий:

- определение целей КБ;

- создание эффективной СУКБ;
- расчет совокупности детализированных не только качественных, но и количественных показателей для оценки соответствия уровня КБ заявленным целям;
- применение инструментария обеспечения КБ и оценки текущего состояния, использование методик (с системой критериев и защитных мер) в процессе анализа и управления рисками, позволяющих объективно оценить текущее состояние дел в организации.

Основополагающей в подобной стандартизации стала серия стандартов ISO 9000, предъявляющих требования к системам менеджмента качества, соблюдение которых позволяет контролировать качество выпускаемой продукции или предоставляемых услуг.

При разработке стандартов на системы управления КБ многое взято именно из стандартов серии ISO 9000. Например, процессный подход и использование циклической модели PDCA для совершенствования как самой системы, так и отдельных ее процессов.

Помимо этого, отличительной особенностью стандартов ISO 9000, является то, что они устанавливают степень ответственности руководства организации за качество продукции или услуг. Причем руководство предприятия отвечает как за разработку политики в области качества, так и за внедрение и поддержание в рабочем состоянии системы менеджмента качества.

1.4. Функционирование информационных систем МВД России в условиях деструктивных кибервоздействий

Основные усилия по развитию информационных систем МВД России и обеспечению их взаимодействия направлены на перевод от технологий построения автономных вычислительных комплексов к технологиям построения единой инфокоммуникационной системы (ЕИКС) в рамках реализации концепции единого информационного пространства.

ЕИКС представляет собой совокупность баз данных специальных систем, защищенных технологий их ведения и санкционированного использования, инфокоммуникационных систем и сетей, функционирующих на основе правил, обеспечивающих безопасное устойчивое информационное взаимодействие подразделений МВД России, а также полное удовлетворение их информационных потребностей [22, 23].

Становление и развитие инфокоммуникационных систем ведомственного назначения происходит в условиях эволюции как информационных потребностей должностных лиц, так и внешних факторов, включая санкционные. Оно сопровождается стремительным сокращением жизненного цикла технических решений, составляющих основу инфраструктуры, интеграцией процессов телекоммуникационных

сетей, устройств и служб, а также резко увеличившимися возможностями по проведению компьютерных атак.

Повышение эффективности решения задач управления в МВД России в рамках единого информационного пространства невозможно без широкого применения современных вычислительных средств, новых информационных технологий. Что, как правило, приводит к возрастанию угроз защищенности как самих объектов КИИ, так и обрабатываемой информации. Очевидно, что для компенсации данных угроз необходимо внедрение в соответствующую систему сбора, обработки и передачи данных единой системы управления.

Рассмотрение устойчивости функционирования КИИ МВД России целесообразно проводить в рамках государственной информационной инфраструктуры, которая включает:

- физическую инфраструктуру, развернутую на базе ведомственных ИТКС, интегрированных в ИТКС общего пользования России и тем самым являющихся неотъемлемой частью государственных информационных систем, функционирующих в киберпространстве;
- информационную инфраструктуру как совокупность взаимосвязанных ведомственных ИС, подключенных через сегменты ведомственной ИТКС, и взаимодействующих с ней информационных систем правоохранительных структур, других силовых ведомств и государственных корпораций;
- инфраструктуру управления, представляющую собой системы управления ИТКС, отдельные сервисы и службы, информационно связанные между собой

Процесс внедрения перспективных информационных технологий при создании ЕИКС МВД России осложняется большим количеством различных источников и потребителей информации, их организационной и территориальной распределенностью, обработкой информации, характеризующейся различной степенью конфиденциальности, и, как следствие, повышением рисков нарушения устойчивости функционирования таких систем.

Таким образом, рассмотрение устойчивого функционирования КИИ правоохранительных структур в целом и МВД России в частности затруднено вследствие ее масштабности, сложности связей, нахождения на различных уровнях инфраструктуры и к тому же в зонах ответственности разных подразделений. Кроме того, КИИ как объект управления обладает рядом специфических особенностей:

- многоуровневой иерархией подсистем и элементов внутри системы;
- разнородностью и сложностью процессов взаимодействия подсистем КИИ;
- многофункциональностью внутренней структуры КИИ;
- многофакторностью описания состояний КИИ;

• высокой динамикой изменения состояний КИИ;

• большими объемами разнородной информации, характеризующей состояния КИИ;

• нахождением объектов КИИ в зоне ответственности нескольких органов управления;

• эмерджентностью;

• сложностью формализации процедур принятия и реализации решений.

Применительно к указанным особенностям, когда разнородные системы управления, имеющие подчас антагонистические цели, используют ресурсы единого киберпространства, ситуация усугубляется наличием неопределенностей в:

• знаниях о внешней среде и действующих факторах;

• несогласованности, противоречивости целей и динамики их изменения;

• поведении взаимодействующих систем;

• текущем состоянии КИИ в режиме реального времени, вследствие неполноты и неточности информации.

Всё вышесказанное требует адекватных решений по построению системы обеспечения устойчивого функционирования КИИ правоохранительных структур, которая должна быть адаптируемой к потоку решаемых задач и текущим целям, а также к структуре ИТКС и к воздействию дестабилизирующих факторов, учитывать условия ограниченности ресурсов, необходимых для реализации данных процессов [24].

В настоящее время в МВД России существует большая номенклатура разобщенных информационных систем, в которых осуществляется обработка информации специального назначения в различных структурах и звеньях управления, различающихся задачами обработки исходной информации, алгоритмами и техническими средствами выработки управляющих воздействий и способов организации информационного обмена. При анализе каждого объекта КИИ необходимо их рассматривать как композицию взаимосвязанных функций, сетей и технологий, что существенно усложняет описание процесса их функционирования [22].

Таким образом, в элементном составе КИИ находятся несколько сотен взаимосвязанных объектов, которые с точки зрения науки управления являются подсистемами, а количество и род взаимосвязей с другими объектами определяется, исходя из принятых технических решений по их построению, а также решений по построению системы управления. При проектировании объектов КИИ закладываются контуры управления, позволяющие осуществлять его за счет изменения характеристик: технических средств обработки информации и программного обеспечения, а также сетей передачи данных и используемого в них сетевого

оборудования и средств защиты информации [25].

Для решения вопросов предотвращения информационной уязвимости сложных организационно-технических систем управления, используемых для специальных целей, Указом Президента создана ГосСОПКА [26]. ГосСОПКА представляет собой единый централизованный, территориально распределенный комплекс, включающий силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак (рис. 1.4.1).

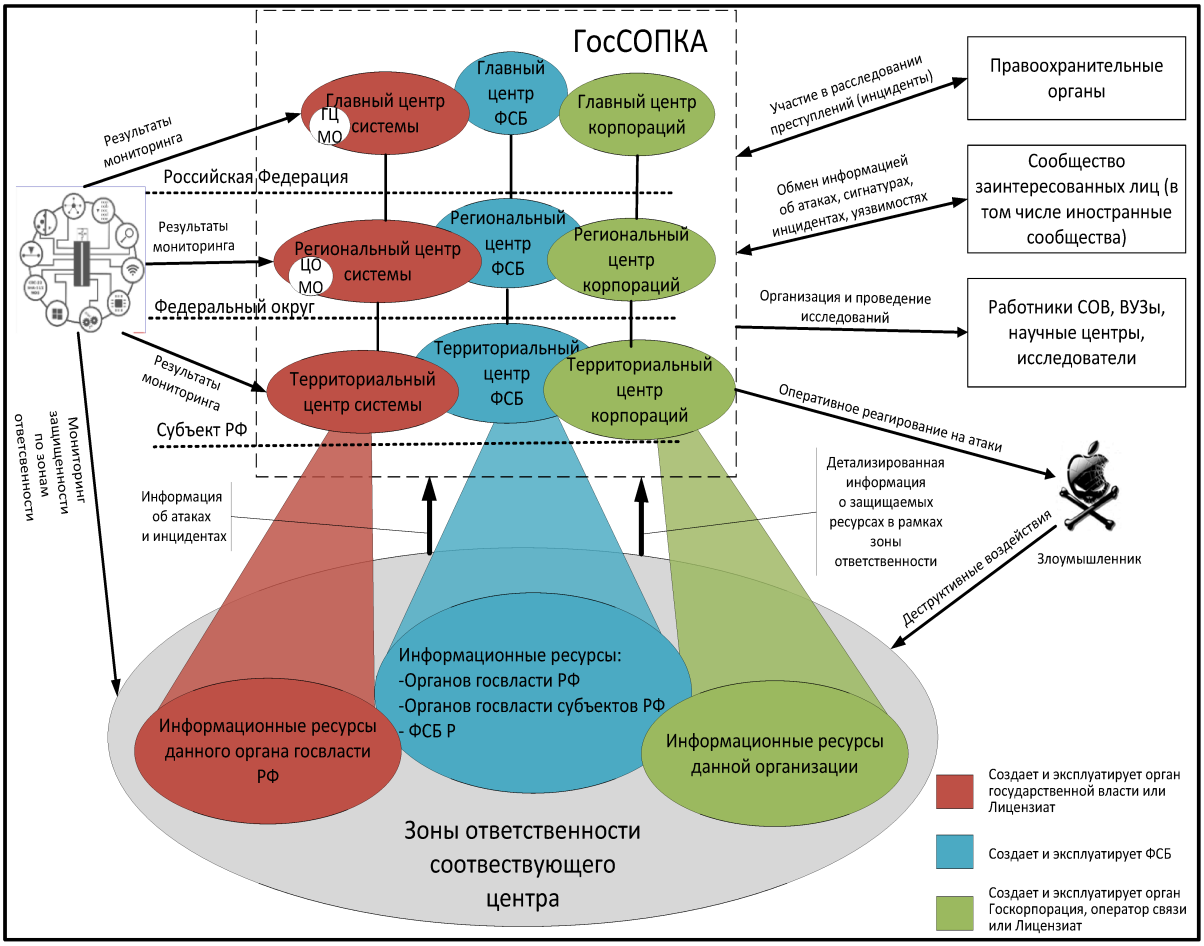


Рис. 1.4.1. Обобщенная структурная схема ГосСОПКА

Основными задачами ГосСОПКА выступают:

- выявление признаков проведения компьютерных атак (КА), определения их источников, методов, способов и средств осуществления и направленности, а также разработка методов и средств обнаружения, предупреждения и ликвидации последствий КА;
- прогнозирование ситуации в области обеспечения кибербезопасности Российской Федерации, включая выявленные и прогнозируемые угрозы, их оценку;
- сбор и анализ информации о КА и вызванных ими компьютерных

инцидентах в отношении информационных ресурсов Российской Федерации;

• обеспечение взаимодействия владельцев информационных ресурсов Российской Федерации, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий КА;

• осуществление контроля степени защищенности критической информационной инфраструктуры Российской Федерации от КА.

Основой организационно-технической составляющей ГосСОПКА являются центры обнаружения, предупреждения и ликвидации последствий КА, организованные по ведомственному и территориальному принципам. Центры подразделяются на главный центр, региональные центры, ведомственные центры (центры органов государственной власти и органов государственной власти субъектов) и корпоративные центры. Зоной ответственности ведомственных центров являются принадлежащие органам государственной власти информационные ресурсы.

В рамках выполнения задач, возложенных на ГосСОПКА, сформулированы основные функции ведомственного центра:

• принятие решений по обеспечению информационной безопасности информационных ресурсов;

• выявление, сбор и анализ сведений об уязвимостях, а также проведение мероприятий по оценке защищённости информационных ресурсов от КА;

• информирование ЛПР и субъектов ГосСОПКА по вопросам обнаружения, предупреждения и ликвидации последствий КА;

• обеспечение защиты данных, передаваемых между ведомственным центром и Главным центром по каналам, защищённым с использованием сертифицированных средств защиты информации;

• предоставление дополнительной информации о компьютерных инцидентах в информационно-телекоммуникационных сетях, находящихся в зоне ответственности ведомственного центра.

Техническое оснащение ГосСОПКА включает средства:

• доверенного резервного канала управления (межсетевые экраны, криптомаршрутизаторы);

• сбора, хранения и корреляции событий КБ;

• обнаружения и предотвращения вторжений;

• ложных сетевых информационных объектов;

• управления инцидентами КБ.

Проведенный в [27] анализ показал, что существующие технические решения не позволяют в полной мере реализовать вышеуказанные функции в соответствии с [26]. В целях обеспечения необходимого уровня защищенности критической информационной инфраструктуры

целесообразно осуществить внедрение системы управления информационной безопасностью (СУИБ), обеспечивающей на основе интеллектуальных процедур ее устойчивое функционирование при проведении в отношении ее КА. В таких процедурах должны быть реализованы принципы не только априорной защиты, которые обеспечиваются межсетевыми экранами, антивирусными средствам и т.д., но и принципы апостериорной защиты, связанной со сбором информации о состоянии КИИ, воздействующих факторах, доступных ресурсах и другой информации и выработкой контрмер на основе ее анализа.

Основные типы деструктивных воздействий можно классифицировать следующим образом, таблица 1.4.1:

Таблица 1.4.1
Классификация деструктивных воздействий на КИИ ФОИВ

Вид ДВ	Проявление угрозы	Последствия реализации угроз	Объект воздействия
Стихийные	- пожары, молнии, землетрясения, ураганы, наводнения; - другие форс-мажорные обстоятельства; - различные необъяснимые явления	1. Уничтожение	- ТСОИ; - носители информации; - ПО, ОС, СУБД; - помещения; - персонал.
Техногенные	- несовершенство ТСОИ и ПО; - несовершенство вспомогательных средств; - средства передачи информации, опасные производства; - сети коммуникаций (энерго-, тепло-водоснабжения и др.); - транспорт.	1. Нарушение режима работы	- АС; - СПД; - старение ТСОИ
		2. Уничтожение	- ТСОИ; - ПО; - носители информации; - помещения; - персонал.
		3. Модификация	- ПО; - состояния ТСОИ; - информация.

Вид ДВ	Проявление угрозы	Последствия реализации угроз	Объект воздействия
Антропо-генные	умышленные и случайные. - технический персонал и должностные лица ИС; - технический персонал и должностные лица взаимодействую-щих ИС; -недобросовестные партнеры; - криминальные структуры.	1. Кража	- ТСОИ; - носители информации; - информация (копирование или передача); - средства доступа (ключи, пароли)
		2. Подмена, модификация	- ПО (ОС, приложения); - информации (отрицание факта передачи сообщения); - пароли и правила доступа.
		3. Уничтожение	- ТСОИ; - ПО; - информация; - пароли и ключевая информация.
		4. Нарушение режима работы	- снижение скорости передачи информации; - уменьшение объема свободной оперативной памяти; - уменьшение объема свободного дискового пространства; - нарушение электропитания, охлаждения и т.п.
		5. Ошибочные действия	- при установке и эксплуатации ПО; - при эксплуатации ТСОИ
		6. Несанкциони-	- за счет ПЭМИН от

Вид ДВ	Проявление угрозы	Последствия реализации угроз	Объект воздействия
		рованный перехват информации	ТСОИ; - за счет ПЭМИН от линий электропитания, передачи и т.д. - по акустическим и визуальным каналам от средств ввода-вывода; - при подключении к каналам передачи информации; - за счет нарушения правил доступа

• антропогенные – воздействия со стороны субъектов, т.е. воздействия, приводящие к ущербу безопасности ИС, связанные с человеческим фактором;

• техногенные – воздействия, связанные с несовершенством технической компоненты ИС (в том числе и программного обеспечения);

• природные – воздействия, связанные с природными явлениями (пожарами, землетрясениями, наводнениями и другими непредсказуемыми или трудно предсказуемыми событиями).

В качестве показателей воздействий могут выступать различные вероятностно-временные характеристики системы, такие как вероятность отказа в обслуживании, интенсивность воздействия, мощность воздействия, величина вероятного ущерба, коэффициент снижения производительности системы из-за влияния воздействий, коэффициент неготовности и т.д. Таким образом, вследствие того, что в условиях информационного конфликта в киберпространстве наиболее вероятными и результативными будут являться целенаправленные комплексные ИТВ [28], ограничим рамки данного исследования только одним классом деструктивных воздействий – ИТВ [29]. Оценка влияния ИТВ на процесс обеспечения устойчивости функционирования КИИ ФОИВ существенно затруднена вследствие особенной КИИ, а также целенаправленности и комплексности ИТВ, а формализация процесса воздействия ИТВ связана с разработкой соответствующей модели.

1.5. Информационно-психологическое обеспечение кибербезопасности

Как показано в [30], гибридные войны в решении современных геополитических проблем сегодня все чаще проявляются в виде своей системообразующей составляющей – психологической войны, войны ментальной, смысловой, поведенческой. Об этом наглядно свидетельствуют драматические события на Украине. Массовые манипулятивные технологии, в том числе – в киберпространстве, которые использованы для информационно-психологического воздействия на массовое общественное сознание с учетом этнопсихологических, гендерных, психолого-возрастных и других особенностей населения, позволили породить информационный, социальный и экономический хаос на Украине. Достаточно эффективно были героизированы и внедрены в массовое сознание деструктивные образы С. Бандеры, Р. Шухевича и других укронацистов. В этих условиях, по сути, была подменена когнитивная карта сознания значительной части населения. В результате в украинском общественном сознании произошла эрозия этнополитического кода и окрепло архаичное сознание, породившие массовое деструктивное поведение [31]. Так, Украина, вопреки своим национальным интересам, из-за успешно проведенных информационно-психологических операций стала объектом геополитической экспансии Запада.

В России также заметно расширились масштабы использования западными спецслужбами средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической ситуации в различных регионах страны, подрыв ее суверенитета и территориальной целостности. Активно наращивается информационное воздействие, в первую очередь, на молодежь для размывания традиционных российских духовно-нравственных ценностей, исторических основ и патриотических традиций.

На Западе все более усиливается предвзятая оценка государственной политики Российской Федерации в средствах массовой информации. В то же время попытки объективного анализа зарубежными или российскими СМИ подвергаются откровенной дискриминации [30].

Не случайно в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5.12.2016 № 646, в качестве одной из стратегических целей и основных направлений обеспечения информационной безопасности отмечается нейтрализация информационно-психологического воздействия на население страны. В связи с этим Л.Г. Ивашов, президент Академии геополитических проблем, напоминает, что мы еще в советское время как-то слабо среагировали на то, что еще в 1963 г. в США издано наставление

по информационно-психологическим операциям американских вооруженных сил. И с тех пор американцы планомерно осваивают фронт новой борьбы. Так, несколько лет назад в Пентагоне создано главное киберкомандование, в настоящее время насчитывающее более 40 тысяч специалистов. Эти силы способны с помощью кибератак полностью выводить из строя систему государственного, финансового и военного управления той или иной страны [32]. В настоящее время имеются специальные органы по ведению психологической войны у целого ряда стран [30]. Они носят наименования подразделений «психологических операций» (Великобритания, Южная Корея), «информационных операций» (Канада), «оперативной информации» (ФРГ), «психологического обеспечения» (Израиль), «психологической обороны» (Швеция), «психологических действий» (Польша), «психологической войны» (Турция) и т.д. Более того, в 2014 г. в Латвии начал функционировать Центр стратегических коммуникаций НАТО (NATO Strategic Communications Centre of Excellence), среди задач которого наиболее значимыми является ведения «гибридных войн» [33].

Информационно-психологическое воздействие на людей не является изобретением сегодняшнего дня, а имеет давнюю историю, описанную в целом ряде историко-философских трактатов восточных, древнекитайских, а также более поздних европейских авторов [33].

Но систематизировать и научно объяснять информационно-психологическое воздействие в широких масштабах на людей стало возможным только в начале XX века [30]. Начиная со Второй мировой войны, пропагандистская работа стала проводиться в форме информационно-психологических операций и других мероприятий информационно-психологического воздействия [34].

В современных условиях глобального внедрения информационных технологий в жизнедеятельность общества американские военные специалисты одними из первых отметили повышение роли информационно-психологических операций в мире и стали изучать возможности их использования для достижения своих геополитических целей [35]. По мнению специалистов Пентагона, перед службами специального назначения в первую очередь стоит задача искажения взглядов, ценностей, мировоззрения людей и внедрение ложных целей общественно-политического развития в сознание населения государств, являющихся геополитическими конкурентами. Для большинства западных стран сегодня использование информационно-психологических операций стало неотъемлемой частью их геополитики, во-многом благодаря отсутствию у большинства граждан понимания той угрозы, которую представляют современные информационно-психологические технологии при их латентном использовании для достижения геополитических и других целей [30].

Информационно-психологические операции в настоящее время представляют собой осуществление на практике совокупности различных видов информационно-психологического воздействия, скоординированных и взаимоувязанных по целям, объектам, месту и времени, представляющих в итоге настоящую психологическую войну. Объектами воздействия информационно-психологических операций являются психика отдельных людей, общественное сознание, мнение и настроение больших социальных групп, населения всего государства. При этом информационно-психологические операции представляют одну из форм геополитического противоборства – достижение и удержание информационно-психологического превосходства. В результате информационно-психологического воздействия у граждан, подвергающихся геополитическому воздействию, формируется положительный стереотип по отношению к государству, осуществляющему геополитическую экспансию. Опираясь на поддержку обманутого населения, такое государство сможет реализовывать необходимую ему политическую линию. Информационно-психологические операции, использующие технологии массовой манипуляции для явного и скрытого управления психикой, поведением человека, разных социальных групп путем формирования у них искаженных представлений, ценностей, потребностей, оказывают деструктивное воздействие на социум, порождая хаос и развивая постоянные конфликты в обществе. При этом с помощью явного и скрытого управления психикой, действиями и поведением человека эти операции делают ставку не на сознание, а на подсознательные и бессознательные пласты психики, порождающие эмоционально неконтролируемое поведение. Так осуществляется политическое манипулирование, скрытое управление политическим сознанием и поведением людей для принуждения их действовать вопреки собственным интересам [30].

Манипуляция представляет собой вид скрытого, неявного психологического воздействия на людей с целью управления их поведением. Манипуляцией являются все формы воздействия, как сознательно организованные, так и бессознательные. Мишенью манипуляции являются эмоции людей, чтобы, вызвав чувство вины или страха, зависти или эйфории, изменить их поведение в соответствии с желанием и целью манипулирующего геополитического оппонента. Все многообразие манипулирования общественным сознанием направлено на замену мировоззренческих основ общества, его политических, нравственных, эстетических и других ценностей. Достигается это с помощью манипулятивной подачи информации, с использованием развитых речевых психотехник.

Исследователи выделяют [30] целый ряд часто встречающихся

манипуляций:

- провоцирование защитных реакций;
- провоцирование замешательства;
- дезориентация личности;
- формирование впечатления, что партнер настроен на сотрудничество;
- игра на нетерпимости – «висящая морковка»;
- игра на чувстве безысходности;
- игра на чувстве жадности;
- использование запланированных «трудных» уступок;
- намеренное затягивание времени обсуждения;
- провоцирование интереса к партнеру – «убаюкивание», чтобы «убить» позднее.

В современных условиях существует большое количество манипулятивных приемов, которые хорошо описаны. Среди них можно выделить [36]:

- «навешивание ярлыков»: оскорбительные названия, имена, эпитеты, метафоры, вызывающие эмоционально негативное отношение к конкретным людям, всему государству – объекту геополитической экспансии;
- «трансфер» («перенос»): ненавязчиво и незаметно переносится общепризнанный авторитет на нужную при геополитической экспансии фигуру, явление, процесс для формирования между ними ассоциативных связей, имеющих ценность и значимость для окружающих;
- «ссылка на авторитет»: установление доверительных отношений с манипулируемой аудиторией или конкретными людьми;
- «перетасовка» («подтасовка карт»): односторонняя подача только положительных или только отрицательных фактов, свидетельств, доводов, при одновременном замалчивании противоположных;
- «общий вагон»: подбор суждений, высказываний, фраз, требующих единообразия в поведении для создания впечатления, будто так делают все;
- «обратный эффект»: большое количество негативной информации вызывает прямо противоположный эффект;
- «принцип контраста»: одна информация подается на фоне другой;
- «правда – наполовину»: аудитории преподносится только часть достоверной информации;
- «осмеяние» конкретных лиц, взглядов, идей, программ, организаций для усиления информационно-психологического воздействия на целевые аудитории;
- слухи: пропагандистское воздействие в условиях дефицита информации;

- провокации: как целенаправленное создание событий в качестве информационного повода;
- «захват» медиапространства: люди получают информацию только от одной организации как единственно верную;
- «утвердительные заявления»: распространение различных утверждений как самоочевидных и не требующих доказательств;
- «принуждающая пропаганда»: использование слов и выражений принуждающего характера, типа «голосуй или проиграешь»;
- «общественное неодобрение»: создание негативного образа политика путем тенденциозного подбора различных высказываний «групп влияния», «представителей» различных слоев населения;
- «прямое опровержение» всех элементов пропаганды другой стороны;
- «игнорирование»: преднамеренное умолчание нежелательных элементов и тем другой стороны;
- «нарушение логических и временных связей между событиями» для создания иллюзии тех или иных тенденций и ситуаций;
- «замена источника сообщения» для увеличения или уменьшения доверия к сообщению за счет манипулирования источниками;
- «формирование информационного окружения» вокруг какого-то события для снижения или увеличения его значения;
- «рейтинги» для манипулирования общественным мнением в других странах. В ходе различных информационно-психологических операций в пределах «окна возможностей» продвигать совершенно чуждые обществу идеи [30].

Такая опасная технология позволяет легализовать самые низменные людские пороки, убивая в людях остатки человечности [30]. Изучение феномена информационно-психологических войн имеет междисциплинарный характер, является результатом исследований широкого круга историков, политологов, философов, правоведов [30].

Эти исследования показывают, что информационно-психологические операции следует трактовать как совокупность методов и приемов трансформации информационного пространства и поведения населения геополитическим противником. При этом базовым элементом таких операций является навязывание населению определенной картины мира, в которой заложены желаемые типы социального поведения.

В настоящее время разработан целый ряд информационно-психологических операций, показавших свою эффективность манипулирования людьми в разных странах. Эти операции становятся все более масштабными и результативными.

Традиционными политическими технологиями, используемыми для достижения эффективного результата в создании у населения

определенных политических убеждений и ориентаций, являются:

1. Политическая мифологизация – процесс формирования у населения государства (геополитического конкурента) установок, стереотипов, групповых норм, массовых политических настроений, общественного мнения для развития некритического мышления, неустойчивого, импульсивно воспринимающего состояния в целях управления поведением людей в нужном направлении. При конструировании политического мифа и для эффективного его внедрения в массовое сознание решающее значение имеет героизация того или иного образа политического лидера. Такая героизация опирается на социальную востребованность в герое на базе несоответствия желаемого и действительного в политической жизни страны. Положительный образ героя играет значительную роль для оправдания, легитимизации тех или иных деструктивных действий в стране для ее внешнего геополитического субъекта.

2. Политическое имиджирование, при котором распространенными политическими имиджформирующими приемами являются [30]:

- внедрение образа-посредника для отождествления политического лидера с образом другого известного человека на основе позитивного его восприятия в массовом сознании;
- систематическая публикация результатов рейтингов, социологических опросов, которые, как достоверные источники, ориентируют население с помощью использования того или иного образа на соответствующие политические нормы, ценности;
- сравнение с зарубежными политиками, при котором на фоне негативного, ироничного характера информации, например, об отечественных политиках, в массовом сознании в определенном позитивном ракурсе представляются те или иные политические лидеры геополитического субъекта, которые становятся все ближе к народу, понимают его и живут его чаяниями и проблемами. При этом о своих политиках допускается дозированная негативная информация, чтобы не допустить их идеализации;
- политические скандалы, «грязные» политические истории, которые целенаправленно предлагаются массовому сознанию для определенного восприятия той или иной политической фигуры данной страны, нежелательной для внешнего геополитического субъекта. Для создания у граждан негативной оценки о политике СМИ преподносят в нужный момент различные политические скандалы в виде таких «грязных» историй, имеющих разоблачительный и резонансный характер, как громкие некорректные высказывания политиков, нелепые истории, коррупционный скандал, шпионаж за политическими оппонентами, компромат на аудиовидеозаписях, фальшивые дипломы, плагиат в диссертациях, алкогольные истории, любовные романы. Многие такие скандалы, как правило, носят достаточно спорный характер из-за

отсутствия официальных доказательств причастности политика к тем или иным событиям.

3. Деструкции дискурса, понимаемые как «нарушения кодирования (декодирования) информации, влияющие на процесс восприятия и интерпретации мировых событий и обусловленные культурными различиями, этноцентризмом, стереотипами, свойственными участникам коммуникации» [30, 37].

Деструкция дискурса имеет свои характерные черты и в пространстве современных СМИ проявляется в различных приемах и методах, таких как:

- изменение аксиологических приоритетов и установок;
- замена идеологической парадигмы;
- цензура на высказывания в СМИ;
- идеологическое преследование людей, имеющих собственную точку зрения на происходящие события [30, 39].

4. Хоррор-менеджмент, который предполагает выполнение следующих задач:

- целенаправленное внедрение негативной информации как истинной в массовое сознание для решения геополитических задач;
- формирование чувства собственной незащищенности посредством поддержания обстановки постоянной ненависти, агрессии, страха, тревоги;
- реализация замыслов, достижение которых связывается с поддержкой общественного мнения.

Постоянная негативная информация в СМИ заставляет население чувствовать себя беззащитной, неполноценной, разобщенной нацией и нуждаться в другой, более сильной политической власти, которая смогла бы объединить граждан, решить социальные проблемы, взять на себя ответственность за судьбу страны. В политические технологии информационно-психологического противоборства внедряются элементы деструктивной инновационности табуированного характера, выраженной в сокрытии манипулирования массовым сознанием. Так, одной из табуированных целей политических технологий цветных революций является деформация общества. Для достижения этой цели активно привлекаются СМИ, одной из главных задач которых становится смена ценностной ориентации граждан, особенно молодежи, разрушение «культурного ядра» и дестабилизация общества. Это необходимо реформаторам для установления культурной диктатуры ради дальнейшего перехвата управления государством [30, 39].

5. Когнитивное моделирование, направленное на переформатирование сознания. Наглядным примером такого моделирования сегодня является фальсификация истории Великой Отечественной войны, ядра сакральной исторической матрицы России. Она осуществляется в несколько этапов. Сначала внедряются в сознание людей такие установки, как «советские

войска, а не гитлеровские, были оккупационными». Далее на базе подобных закреплённых образов и представлений происходит пересмотр отношения ко всем советскому, а далее – к русскому [30]. На следующем этапе уже следуют конкретные действия – начинается уничтожение военных памятников и всего того, что связано с Великой Победой. Главной целью фальсификации истории становится не только пересмотр важнейших геополитических итогов Второй мировой войны, но и реабилитация преступных идеологий, их институциональное возрождение и легализация. Основным ее направлением является концептуальная фальсификация, предполагающая на первом этапе постановку знака равенства между гитлеровской Германией и Советским Союзом, как представляющими тоталитарные режимы, и возложение на них равной ответственности за развязывание Второй мировой войны [30,40]. Из этого следует, если советский режим подобен фашистскому, то, по этой логике, СССР к победе не причастен и его нахождение в числе государств-победителей и празднование Дня Победы 9 Мая являются нелегитимными. Советский Союз должен быть не среди триумфаторов, а среди тех, кто был осужден за преступления против человечества. На роль победителей утверждаются страны англо-саксонского мира.

На следующем этапе выдвигается тезис о преимущественной виновности СССР в развязывании Второй мировой войны. Так, активно муссируется тезис о том, что Сталин якобы готовил нападение на Германию и Гитлер вынужден был опередить его. Сегодня уже идут дальше – оказывается, наша страна развязала и Первую мировую войну [30, 41]. И отсюда вывод: раз Россия вчера развязала Первую и Вторую мировые войны, то сегодня она развязывает Третью мировую войну. Так из процесса десоветизации вытекает процесс дерусификации, осуждения России как цивилизации [30, 41]. При таком подходе происходит реабилитация позиции Запада, который поощрял нацистов в предвоенные годы и снисходителен к ним в настоящее время. Поэтому общественному мнению предлагается сознательное искажение фактов. Следующим направлением фальсификации итогов Второй мировой войны является искажение, умолчание и сокрытие неприглядных для Запада исторических фактов. Так, умалчивая о битвах на советско-германском фронте, на Западе исключительно ведется речь о сражениях в Западной Европе, Африке и Тихом океане [30].

Например, с первых дней Великой Отечественной войны Германия имела в составе своих войск десятки дивизий своих союзников из Западной Европы, которые в целях усиления вермахта мобилизовали свыше 1 млн 800 тыс. чел. для борьбы против Советского Союза. Из них было сформировано 59 дивизий, 23 бригады и ряд отдельных полков, легионов и батальонов. В войсках СС было создано 26 добровольческих дивизий, в которых служили албанцы, голландцы, датчане, венгры,

бельгийцы, французы, латыши, литовцы, эстонцы, украинцы и др. В составе военнопленных в СССР были и венгры, румыны, австрийцы, чехи, словаки, поляки, итальянцы, французы, хорваты и т.д. [30].

В фальсификации исторических фактов важное место отводится кампании дегероизации участников Великой Отечественной войны. В этой кампании можно выделить несколько подходов. Первый подход заключается в утверждении, что подвига не было, он оказывается вымыслом, развенчиваемым дегероизаторами. Отсюда вытекают, например, попытки отрицания существования «Молодой гвардии». Другой подход предполагает, что подвиг был совершен, но героями являются неизвестные никому люди, не те, кто официально почитался. Этот подход иллюстрируют попытки лишения подвига Николая Гастелло [30]. Третий подход состоит в маргинализации героев, не достойных подражания. Примером тому является муссирование криминального прошлого Александра Матросова. Четвертый подход состоит в утверждении, что совершенные подвиги являлись преступлениями. Например, Зоя Космодемьянская определяется в качестве террористки. Пятый подход в дегероизации состоит в «замещении героев», вытеснении образов настоящих героев преступниками, такими как С. Бандера или Р. Шухевич [30, 41]. Фальсификации исторических фактов приводят к чудовищным результатам. Так, сегодня более 30% японских школьников считают, что атомные бомбы на Хиросиму и Нагасаки сбросили советские, а не американские самолеты [30].

В фальсификации истории Великой Отечественной войны геополитические противники важное место отводят внутрироссийской пропаганде. Фальсификация, ревизия итогов Второй мировой войны имеет четкую геополитическую цель: снижение геополитической субъектности России и оттеснение ее на периферию мировой политики.

5. Среди информационно-психологических операций активно применяется технология воздействия через сетевые структуры. В современном информационном обществе сетевые структуры оказывают непосредственное влияние на политику, экономику, духовную культуру, а также на систему государственного управления, финансово-кредитную, информационно-аналитическую деятельность [30]. Под воздействием сетевых структур делается попытка деформирования общественной психологии и культуры в постсоветском пространстве, что уже привело к ряду нарушений устоявшихся культурно-этических представлений в обществе и разрушению единого советского геополитического пространства.

В настоящее время миллиарды людей не могут жить без контактов в социальных сетях. Для них количество получаемых смайликов стало более референтным, чем нравоучения родителей, учителей или других окружающих их людей. Именно такие сети легко формируют, особенно

среди молодежи, деструктивное, делинквентное поведение. Одним из эффективных методов формирования такого поведения является игра в сетях. В опытных руках игра превращается в очень грозное оружие, принимая во внимание высокую скорость распространения информационных технологий, их привлекательность и способность смешивать мир виртуальной игры с миром реальным. Так, игры в поиск монстров-покемонов могут стать сравнительно безобидной прелюдией безумного тотального совмещения компьютерной интерактивной игры и реального мира, воли конкретного человека и приказов неведомого ему программиста [30].

7. Одно из ведущих мест среди информационно-психологических операций занимает такой популярный вид манипулирования людьми, как флешмоб [30]. Его популярность основана на возможностях быстрого обмена информацией друг с другом участниками флешмоба через социальные и мобильные сети. Флешмоб позволяет участникам в большой организованной толпе в сети почувствовать свою силу, свою возможность для самоутверждения и эмоциональной подзарядки, ощутить чувство свободы от общественных стереотипов поведения, свою причастность к общему делу. Основным участником флешмоба, как правило, является молодежь, как основной пользователь мобильной связи. Кроме этого, активными пользователями этих сетей являются образованные люди с активной жизненной позицией, критически настроенные к власти и, соответственно, находящиеся в состоянии постоянной готовности к активным действиям. Используя нервозность людей, даже далеких от центра событий, можно привлечь их к протестным действиям. Так, можно за короткое время вывести на улицы тысячи недовольных и успешно обострить и дестабилизировать общественно-политическую ситуацию в целой стране. С этим явлением, как показывают события на мировой арене, справиться достаточно сложно. Огромную роль флешмоб сыграл в ряде североафриканских государств, на постсоветской территории и, конечно же, на Украине. Эта технология собирает огромные толпы, создает революционную ситуацию, вырабатывает четкую политическую позицию и умело скоординированные действия. Свою роль флэш-мобу еще предстоит сыграть в геополитическом противоборстве в Европе, Азии и на других континентах [30].

8. Одним из видов технологий информационно-психологического воздействия является нейролингвистическое программирование (НЛП), подбор «ключа» к подсознанию человека [30]. В качестве такого «ключа» используется специально подобранный нейросемантический гипертекст с наиболее значимыми словами и фразами для суггестируемого лица. Областью применения НЛП являются средства массовой информации, система образования, медицина, торговля, реклама. С помощью нейролингвистического программирования осуществляется воздействие

на эмоции человека для искусственного формирования представлений, побуждений, установок посредством образов и воображения. Манипулирование такими образами позволяет произвести в сфере подсознания человека локальные операции, направленные на изменение его представлений, взглядов, привычек и, в конечном итоге, – трансформацию сознания [30].

9. К числу информационно-психологических операций относится и психотронное (парапсихологическое, экстрасенсорное) воздействие, предполагающее коррекцию поведения людей путем передачи информации через неосознаваемое восприятие [30]. Так, известны факты применения акустического воздействия на психофизическое состояние человека, вызывающего головокружение, слуховые галлюцинации, под влиянием которых он совершает неконтролируемые поступки. Появились факты о манипулировании с психикой с помощью медицинских препаратов, химических, биологических веществ. Они способны контролировать, усиливать или подавлять агрессивное поведение человека, разрушать его психику. При этом могут быть использованы различные цвета, запахи, оказывающие сильное воздействие на психику человека. Современные методы и средства информационно-психологического воздействия взаимосвязаны и рассчитаны на формирование новых мотивов, ценностей, стереотипов, на модификацию психических процессов и состояний.

С помощью информационно-психологических операций достигается цель интенсивного воздействия на различные процессы, протекающие на уровне общественно-государственного устройства в любой стране, любом регионе мира. Политическая элита любой страны, не осознающая смысла ведущихся против нее информационно-психологических операций в киберпространстве, обречена на поражение. Поэтому сегодня важнейшая задача – дать достойный ответ на эти вызовы и угрозы. Не случайно Л. Г. Ивашов подчеркивает: «Для того чтобы проводить мирную политику, нужно иметь силу, в том числе и мощные информационные «войска» [30].

Контрольные вопросы:

1. Как определяется понятие системы?
2. Каковы основные свойства системы?
3. В чем заключается системный подход к исследованию объектов компьютерной безопасности?
4. Каковы особенности рассмотрения системного подхода применительно к управлению компьютерной безопасностью?
5. Какие виды деятельности в организации можно назвать процессом?
6. Какую роль играют процессы в организации?

7. Какие элементы процесса могут быть исключены из определения: входные данные процесса, выходные данные процесса, управляющее воздействие, ресурсы?

8. Что понимается под ресурсами в рамках определения понятия процесса?

9. Кто в организации может и должен определять цели процессов?

10. Что понимается под управляющим воздействием в рамках определения процесса?

11. В чем заключается процессный подход?

12. Дайте определение понятия «управление» с позиций системного подхода.

13. Что такое метод управления?

14. Дайте определение системы управления.

15. Что представляет собой система управления, основанная на процессном подходе?

16. Каковы особенности рассмотрения процессного подхода применительно к управлению?

17. К каким процессам организации может быть применена циклическая модель PDCA?

18. В чем состоят основные преимущества использования циклической модели PDCA?

19. Чем различаются термины «кибербезопасность» и «информационная безопасность»?

20. Какие свойства кибербезопасности в современных условиях должны приниматься во внимание, что понимается под каждым из ее свойств?

Литература к главе 1

1. Марков, А. С. Кибербезопасность и информационная безопасность как бифуркация номенклатуры научных специальностей / А. С. Марков. – Текст : непосредственный // Вопросы кибербезопасности. – 2022. – № 1(47). – С. 1–9.

2. Алпеев, А.С. Терминология безопасности: кибербезопасность, информационная безопасность / А.С. Алпеев. – Текст : непосредственный // Вопросы кибербезопасности. – 2014. – № 4 (38). – С. 39–42.

3. Харрис, Ш. Кибер войн@. Пятый театр военных действий / Ш. Харрис. Москва: Альпина нон-фикшн, 2016. – 390 с. – Текст: непосредственный.

4. Möller D. P. F. Cybersecurity in Digital Transformation. Scope and Applications. URL: https://link.springer.com/book/10.1007/978-3-030-60570-4 (дата обращения 29.06.2022). – Текст : электронный.

5. Международная информационная безопасность: теория и практика : Учебник для вузов: в 3-х томах. /А. В. Крутских, А. В. Бирюков, С. М. Бойко [и др]; – Том 1. Под общ. ред. А. В. Крутских. 2-е изд., доп.– Москва: МГИМО, 2021. – 384 с. – Текст : непосредственный.

6. Wilson, D. C. Cybersecurity / D.C. Wilson. – MIT, 2021. – 160 p. – Текст : непосредственный.

7. Леонов, Г. А. Теория управления / Г. А. Леонов. – Санкт-Петербург : СПбГУ, 2006. – Текст : непосредственный.

8. Репин, В. Процессный подход к управлению. Моделирование бизнес-процессов / В. Репин, В. Елиферов. Москва: Стандарты и качество, 2004. – Текст : непосредственный.

9. Акофф, Р. Планирование будущего корпорации / Р. Акофф. – Москва: Сирин, 2002. – Текст : непосредственный.

10. Аудит информационной безопасности / под ред. А. П. Курило. – Москва: БДЦПресс, 2006. – Текст : непосредственный.

11. ГОСТ Р ИСО 9000-2001. Системы менеджмента качества. Основные положения и словарь. – Москва: Госстандарт России, 2001. – 32 с. – Текст : непосредственный.

12. Лигинчук, Г. Г. Основы менеджмента. Ч. 1. / Г. Г. Лигинчук. – Москва: Московский институт экономики, менеджмента и права, 2009. – Текст : непосредственный.

13. Нив, Г. Пространство доктора Деминга / Г. Нив. – М.: Альпина Бизнес Букс, 2007. – Текст : непосредственный.

14. Гостехкомиссия России. Защита от несанкционированного доступа к информации. Термины и определения. – Москва, 1992. – Текст : непосредственный.

15. Рекомендации по стандартизации Р 50.1.053-2005. Информациионные технологии. Основные термины и определения в области технической защиты информации: Утв. Приказом Ростехрегулирования от 06.04.2005 № 77-ст. – Москва: Стандартинформ, 2005.

16. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Москва: Стандартинформ, 2008. – Текст : непосредственный.

17. Стандарт Банка России СТО БР ИББС-1.0. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. – Москва: Банк России, 2001. – Текст : непосредственный.

18. Галатенко, В.А. Основы информационной безопасности / В. А. Галатенко. – Москва: Бином, Лаборатория знаний Интуит, 2008. – Текст : непосредственный.

19. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью. – Москва: Стандартинформ,

2006. – Текст : непосредственный.

20. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – Москва: Стандартинформ, 2008. – Текст : непосредственный.

21. ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Ч. 1. Общие положения. – Москва: Стандартинформ, 2009. – Текст : непосредственный.

22. Кузнецов, С. Д. Направления исследований в области управления базами данных: краткий обзор / С. Д. Кузнецов // СУБД. –1995. – С. 23 – 32. – Текст : непосредственный.

23. Теория систем и системный анализ в управлении организациями: Справочник / под ред. В. Н. Волковой и А. А. Емельянова. – Москва: Финансы и статистика, 2006. – 848 с. – Текст : непосредственный.

24. Захарченко, Р. И. Модель функционирования автоматизированной информационной системы в киберпространстве / Р. И. Захарченко, И. Д. Королев. – Текст : непосредственный // Вопросы кибербезопасности. – 2019. – № 6(34). – С. 69–78. – ISSN 2311 – 3456.

25. Новиков, Б.А. Основы технологий баз данных / Б. А. Новиков, Е. А. Горшкова. – Москва: – ДМК Пресс, 2019. – 240 с. – Текст : непосредственный.

26. Ульман, Д. Д. Системы баз данных. Полный курс / Д. Д. Ульман, Д. Уидом. – Вильямс, 2014. – 1088 с.

27. Патент на изобретение № RU 2313125 C1 Российская Федерация. Генератор случайной последовательности / В. С. Авраменко, И. В. Безродный, Я. М. Копчак, И. Б. Паращук, А. Ю. Харитонов; заявл. 05.06.2006. – Текст : непосредственный.

28. Толковый словарь по вычислительным системам /под ред. В. Иллингуорта; пер. с англ. – Москва : Машиностроение, 1991. – 560 с. – Текст : непосредственный.

29. Норткатт, Стивен. Анализ типовых нарушений безопасности в сетях. – Москва: Вильяме, 2001. – 464 с. – Текст : непосредственный.

30. Информационно-психологическая и когнитивная безопасность : монография / под ред. И. Ф. Кефели, Р. М. Юсупова. Санкт-Петербург, Петрополис, 2017. – 300 с. – Текст : непосредственный.

31. Собольников, В. В. Место и роль психологического воздействия в стратегии ведения «гибридных» войн НАТО / В В. Собольников. – Текст: непосредственный.// Гуманитарные проблемы военного дела. – 2015. – № 3(4). – С. 25–31.

32. Ивашов, Л. Доктрина информационной безопасности. – URL: http://www.news-front. info/2016/12/0/doktrina-informacionnoj-bezopasnosti-

leonid-ivashov. – Текст : электронный.

33. 10 древних тактик ведения психологической войны. – URL: http: //www. ucmopuockon.livejournal.com/12502591.html. – Текст: электронный.

34. Баришполец, В. А. Области применения информационно-психологического воздействия. – URL: https://www.docviewer.yandex.ru – Текст : электронный.

35. Лайнбарджер, П. Психологическая война. Теория и практика обработки массового сознания / П. Лайнбарджер. – Москва: 2013. – 445 с. – Текст : непосредственный.

36. Кара-Мурза, С. Г. Манипуляция сознанием. / С. Г. Кара-Мурза. – Москва : Эксмо, – 2009. – 528 с. – Текст : непосредственный.

37. Кошкарова, Н. Н. Лингвистические подходы к изучению конфликтного дискурса / Н. Н. Кошкарова. – Текст : непосредственный // Вестник Новосибирского гос. ун-та. Серия: История, филология. – 2015. – Т. 14. – № 2. – С. 143.

38. Кошкарова, Н. Н. «Как слово наше отзовется»: Почему информационная политика может перерасти в информационно-психологическую войну / Н. Н. Кошкарова. – Текст : непосредственный // Теоретические и прикладные аспекты изучения речевой деятельности. – Нижний Новгород: НГЛУ им. Н.А. Добролюбова, 2015. – С. 88.

39. Нестерчук, О. А. Традиционные и инновационные политические технологии в информационно-психологическом противоборстве / О. А. Нестерчук. – Текст : непосредственный // PolitBook. – 2015. – № 2. – С. 96–97.

40. Пономарева, Е. Фальсификация истории Великой Отечественной войны – технология трансформации сознания / Е. Пономарева. – Текст : непосредственный // ОБОЗРЕВАТЕЛЬ – OBSERVER. – 2016.

41. Багдасарян, В. Э. Великая Отечественная война в фокусе информационно-психологической войны против России / В. Э. Багдасарян. – Текст : непосредственный // Вестник Московского гос. обл. ун-та. Серия: История и политические науки. – 2015. – № 2. – С. 27.

42. Минкин, А. Чья победа? // Московский комсомолец. –2005. – 22 июня. – URL: http://www.mk.ru/editions/daily/ article/2005/06/22/194712-chya-pobeda.html. – Текст : электронный.

Глава 2. Нормативно-правовое обеспечение кибербезопасности

2.1. Основные положения государственной информационной политики

Изучение основных положений государственной политики в информационной сфере позволяет выявить качественные признаки этого самостоятельного и весьма важного явления в жизни общества, определить некоторые закономерности в содержании и форме данной политики.

В литературе термин «*государственная политика в информационной сфере*» в научном его понимании не имеет широкого распространения. Для государственной же политики имеет значение не столько область знаний, сколько часть сферы практической человеческой деятельности, связанной с информацией. Относительно обособленная и самостоятельная деятельность государства в этой сфере обычно определяется как государственная информационная политика.

Термин «государственная информационная политика» применим именно в качестве определения новой области деятельности государства в XXI веке. Учитывая это обстоятельство, необходимо рассматривать данный термин не только в качестве рабочего, но и на уровне понятия, объединяющего крупные институты информационных знаний в области государственной деятельности [1].

В учебнике под редакцией профессора В. Д. Попова *государственная информационная политика* представляется как комплекс политических, правовых, экономических, социально-культурных и организационных мероприятий государства, направленный на обеспечение конституционного права граждан на доступ к информации. Государственная информационная политика – это «особая сфера жизнедеятельности людей, связанная с воспроизводством и распространением информации, удовлетворяющей интересы государства и гражданского общества, и направленная на обеспечение творческого, конструктивного диалога между ними и их представителями» [2].

В настоящее время осуществляется повсеместное внедрение информационных технологий в деятельность органов государственной власти. Почти во всех органах государственной власти созданы основы информационно-технологической инфраструктуры, формируется организационно-методическое, финансовое и кадровое обеспечение эффективного использования информационных технологий.

Увеличивается численность сотрудников органов государственной власти, обеспеченных персональными компьютерами, отвечающими современным требованиям. В большинстве органов государственной власти созданы территориально распределенные компьютерные сети, в том числе имеющие доступ в сеть Интернет.

Развитие информационных систем и технологий в органах государственной власти подтверждается также тем, что увеличивается доля затрат на программное обеспечение и услуги системной интеграции в структуре бюджетных расходов на использование информационных технологий в деятельности федеральных органов государственной власти.

Функционируют органы государственной власти, ответственные за реализацию государственной политики в сфере использования информационных технологий. Так, Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации определено государственным заказчиком и оператором единой системы межведомственного электронного взаимодействия. Министерство осуществляет координацию деятельности по подключению к единой системе межведомственного электронного взаимодействия, а также обеспечивает эксплуатацию единой системы межведомственного электронного взаимодействия и устанавливает технические требования к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия [1].

Основной целью государственной политики в области использования информационных технологий в деятельности органов государственной власти является повышение эффективности государственного управления на основе общей информационно-технологической инфраструктуры, обеспечивающей их функционирование, взаимодействие между собой, населением и организациями в рамках предоставления государственных услуг.

Повышение эффективности государственного управления проявляется во многих направлениях:

- в оптимизации государственных функций;
- в повышении уровня прозрачности органов исполнительной власти;
- в противодействии коррупции;
- в формировании эффективной системы предоставления государственных услуг;
- в снижении административных барьеров, т.е. ограничении вмешательства государства в экономическую деятельность субъектов предпринимательства, в том числе – избыточного государственного регулирования.

Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации определены Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

- свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
- установление ограничений доступа к информации только федеральными законами;
- открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
- равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
- обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
- достоверность информации и своевременность ее предоставления;
- неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами [3].

В Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203, определены цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов.

Основными принципами Стратегии являются:

- обеспечение прав граждан на доступ к информации;
- обеспечение свободы выбора средств получения знаний при работе с информацией;
- сохранение традиционных и привычных для граждан (отличных от цифровых) форм получения товаров и услуг;
- приоритет традиционных российских духовно-нравственных ценностей и соблюдение основанных на этих ценностях норм поведения при использовании информационных и коммуникационных технологий;
- обеспечение законности и разумной достаточности при сборе, накоплении и распространении информации о гражданах и организациях;

- обеспечение государственной защиты интересов российских граждан в информационной сфере [4].

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

Согласно Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, национальными интересами в информационной сфере являются:

- обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечения информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применения информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации;
- обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь, критической информационной инфраструктуры Российской Федерации и единой сети электросвязи Российской Федерации в мирное время, в период непосредственной угрозы агрессии – в военное время;
- развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности;
- доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения национальной безопасности Российской Федерации в области культуры;
- содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве.

Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия

информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации [5].

С учетом определенных целей и приоритетов сформированы следующие направления деятельности в сфере реализации государственной программы Российской Федерации «Информационное общество», утвержденной Постановлением Правительства Российской Федерации от 15 апреля 2014 г. № 313:

- формирование современной информационно-телекоммуникационной инфраструктуры, предоставление на ее основе качественных услуг в сфере информационных технологий и обеспечение высокого уровня доступности информации и технологий для населения;
- совершенствование системы государственных гарантий конституционных прав и свобод человека и гражданина в информационной сфере;
- повышение качества образования, медицинского обслуживания, социальной защиты населения на основе развития и использования информационных технологий;
- формирование новой технологической основы для развития экономики и социальной сферы;
- повышение эффективности государственного управления и местного самоуправления, взаимодействия гражданского общества и коммерческих организаций с органами государственной власти, качества и оперативности предоставления государственных услуг;
- развитие науки, технологий и техники, а также подготовка квалифицированных кадров в сфере информационных технологий;
- сохранение культуры многонационального народа Российской Федерации, укрепление нравственных и патриотических принципов в общественном сознании, а также развитие системы культурного и гуманитарного просвещения;
- противодействие использованию потенциала информационных технологий в целях предотвращения угрозы национальным интересам России;
- создание и применение российских информационных и коммуникационных технологий, обеспечение их конкурентоспособности на международном уровне.

Кроме того, к сфере реализации программы «Информационное общество» относятся следующие направления экономической модернизации страны:

- совершенствование российскими специалистами информационных технологий, которые позволят добиться серьезного влияния на процессы

развития глобальных общедоступных информационных сетей с использованием суперкомпьютеров и другой необходимой материальной базы;

- создание собственной наземной и космической инфраструктуры передачи всех видов информации;
- обеспечение национальных интересов в области цифровой экономики.

Повышается значение информационных технологий для реализации таких фундаментальных политических свобод, как свобода слова и собраний, а также выявление и ликвидация очагов коррупции, непосредственный обмен мнениями и знаниями [6].

В рамках реализации Указов Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» и от 21 июля 2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года», в том числе – с целью решения задачи по обеспечению ускоренного внедрения цифровых технологий в экономике и социальной сфере, Правительством Российской Федерации сформирована национальная программа «Цифровая экономика Российской Федерации», утвержденная протоколом заседания президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7.

В состав Национальной программы «Цифровая экономика Российской Федерации» входят следующие федеральные проекты:

- «Нормативное регулирование цифровой среды»;
- «Кадры для цифровой экономики»;
- «Информационная инфраструктура»;
- «Информационная безопасность»;
- «Цифровые технологии»;
- «Цифровое государственное управление»;
- «Искусственный интеллект»;
- «Обеспечение доступа в Интернет за счет развития спутниковой связи»;
- «Развитие кадрового потенциала ИТ-отрасли»;
- «Цифровые услуги и сервисы онлайн».

Федеральный проект «*Нормативное регулирование цифровой среды*» предусматривает поэтапную разработку и реализацию законодательных инициатив, направленных на снятие первоочередных барьеров, препятствующих развитию цифровой экономики и созданию благоприятного правового поля для реализации в российской юрисдикции проектов цифровизации.

Будет создана гибкая система правового регулирования цифровой

экономики, сняты первоочередные барьеры для развития современных технологий и ведения бизнеса в таких сферах, как гражданский оборот, финансовые технологии, интеллектуальная собственность, телекоммуникации, судопроизводство и нотариат, стандартизация. Будут урегулированы вопросы идентификации субъектов правоотношений, электронного документооборота, сбора, хранения и обработки данных.

Новые экономические и технологические условия требуют создания и реализации подходов по содействию гражданам в освоении ключевых компетенций цифровой экономики, обеспечении массовой цифровой грамотности и персонализации образования. В этих целях реализуется федеральный проект «*Кадры для цифровой экономики*» национальной программы «Цифровая экономика Российской Федерации».

В результате к 2024 году будет выстроена преемственная на всех уровнях система образования, включающая выявление и поддержку талантов в областях математики и информатики, подготовку высококвалифицированных кадров, отвечающих новым требованиям к ключевым компетенциям цифровой экономики, реализацию программ переподготовки по востребованным профессиям в условиях цифровой экономики, а также перспективных образовательных проектов.

Основная цель федерального проекта – обеспечение подготовки высококвалифицированных кадров для цифровой экономики.

Она достигается выполнением следующих задач обеспечения:

- доступности для населения обучения по программам дополнительного образования для получения новых востребованных на рынке труда цифровых компетенций;
- потребности рынка труда в специалистах в сфере ИТ и информационной безопасности, а также в специалистах, владеющих цифровыми компетенциями, прошедших обучение по соответствующим программам высшего и среднего профессионального образования;
- онлайн-сервисами образовательных организаций, реализующих программы начального, основного общего, среднего общего и профессионального образования.

Проект «*Цифровые профессии*» предлагает россиянам получить дополнительное ИТ-образование за половину стоимости. Проект предлагает 24 направления образовательных программ от популярных ИТ-организаций и образовательных учреждений.

Проект «*Готов к цифре*» – агрегатор сервисов по тестированию уровня цифровой грамотности, обучению безопасной и эффективной работе с цифровыми технологиями. Посетители сайта могут оценить уровень своей цифровой грамотности, узнать о возможностях онлайн-среды и сформировать необходимые ИТ-навыки.

Проект «*CDO*» – это образовательная программа, позволяющая получить новые цифровые компетенции. Целевая аудитория –

представители федеральных и региональных органов власти, которые отвечают за реализацию национальной программы «Цифровая экономика», а также руководители и менеджеры российских компаний, представители высших учебных заведений, отраслевых и научных организаций, заинтересованных в цифровом развитии.

Основной задачей федерального проекта «*Информационная инфраструктура*» является создание конкурентоспособной, устойчивой и безопасной инфраструктуры высокоскоростной передачи данных, доступной для всех граждан, бизнеса и органов власти. Реализация мероприятий проекта не только обеспечит полномасштабное подключение к сети Интернет ключевых социально значимых объектов инфраструктуры, но и позволит населению пользоваться качественными современными цифровыми услугами даже в самых удаленных уголках нашей страны.

Так, одним из приоритетных направлений в рамках федерального проекта является создание инфраструктуры для подключения к сети Интернет социально значимых организаций на всей территории Российской Федерации, а также эффективного и безопасного использования ими онлайн-сервисов.

В рамках проекта проводится активная работа по подключению государственных (муниципальных) образовательных организаций, центральных избирательных комиссий к Единой сети передачи данных (ЕСПД) в целях обеспечения не только защищенного доступа к государственным и муниципальным информационным системам, но и безопасного интернет-пространства.

Вместе с тем в рамках федерального проекта предусмотрено оснащение учебных классов государственных (муниципальных) образовательных организаций внутренней ИТ-инфраструктурой – как для обеспечения безопасного доступа к сети Интернет по технологии Wi-Fi, так и для использования защищенного доступа к государственным и муниципальным информационным системам, что, в свою очередь, является гарантом обеспечения базовой безопасности образовательного процесса.

Важным мероприятием проекта является оказание универсальных услуг связи (УУС) в малонаселенных пунктах. Они включают установку точек доступа беспроводного интернета (Wi Fi) и организацию сотовой связи в населенных пунктах от 100 до 500 человек.

Одновременно с этим в рамках проекта заложены мероприятия, направленные на создание условий для поэтапного внедрения современных стандартов связи 5G/IMT-2020. 5G будет работать на базе отечественного оборудования.

Также федеральным проектом предусмотрено создание космических аппаратов для системы «Экспресс-РВ» в период 2022–2024 гг. Система спутниковой связи и вещания с использованием четырех космических

аппаратов обеспечит качественное покрытие услугами связи как стационарных, так и подвижных объектов на всей территории страны, в том числе – на территориях Арктической зоны и Дальнего Востока, а также на всей протяженности Северного морского пути.

Вызовами и угрозами для реализации целей развития цифровой экономики в сфере кибербезопасности являются рост масштабов компьютерной преступности, в том числе международной, отставание Российской Федерации в разработке и использовании отечественного программного обеспечения, недостаточный уровень кадрового обеспечения в области кибербезопасности.

В результате реализации направления «*Информационная безопасность*» будут обеспечены устойчивость и безопасность информационной инфраструктуры, конкурентоспособность отечественных разработок и технологий информационной безопасности и выстроена эффективная система защиты прав и законных интересов личности, бизнеса и государства от угроз информационной безопасности.

Ключевая цель проекта «*Цифровые технологии*» – обеспечение технологической независимости государства, возможности коммерциализации отечественных исследований и разработок, а также ускорение технологического развития российских компаний и обеспечение конкурентоспособности разрабатываемых ими продуктов и решений на рынке.

Задачи федерального проекта заключаются в создании благоприятных условий для развития стартапов, разрабатывающих решения в сфере информационных технологий, поддержке отечественных компаний – лидеров рынка ИТ и стимулировании спроса на их решения, а также развитии перспективных высокотехнологичных направлений, таких как квантовые коммуникации, квантовые вычисления, квантовая криптография, мобильные сети связи пятого поколения (5G).

Решение данных задач предусматривает осуществление комплекса мероприятий по грантовой поддержке проектов малых и крупных компаний, разрабатывающих российские ИТ-решения, грантовой поддержке внедрения на предприятиях отечественных ИТ-решений, венчурному финансированию проектов, льготному кредитованию компаний с целью стимулирования процессов цифровой трансформации бизнеса, льготному лизингу для поддержки внедрения цифровых технологий и платформенных решений на основе отечественных программно-аппаратных комплексов, методическому сопровождению разработки и реализации компаниями стратегий цифровой трансформации на основе отечественных ИТ-решений и акселерации российских технологических стартапов.

Данная система мер обеспечивает поддержку проектов на любой стадии технологической готовности – от идеи, разработки прототипа,

акселерации стартапов до полноценного внедрения разработок и тиражирования лучших отечественных решений.

Развитие высокотехнологичных направлений, требующих централизованных прикладных исследований, разработок и создания отечественного оборудования, осуществляется с привлечением ресурсов и компетенций крупнейших российских технологических госкомпаний, заключивших соглашения с Правительством Российской Федерации.

Федеральный проект «*Цифровое государственное управление*» национальной программы «Цифровая экономика Российской Федерации» реализуется в рамках государственной программы «Информационное общество». Проект направлен на достижение национальной цели «Цифровая трансформация», которая определена Указом Президента Российской Федерации от 21 июля 2021 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года».

Ключевой целевой показатель, характеризующий достижение национальной цели, – увеличение доли массовых социально значимых услуг, доступных в электронном виде, до 95% к 2030 году.

Федеральный проект включает мероприятия цифровой трансформации системы государственного управления, которые обеспечивают новый уровень предоставления услуг, необходимых для повышения качества жизни граждан и развития бизнеса.

Мероприятия федерального проекта направлены на реализацию трех ключевых направлений:

- обеспечение удовлетворенности граждан качеством предоставления массовых социально значимых государственных и муниципальных услуг в электронном виде с использованием Единого портала государственных и муниципальных услуг;
- цифровизация процессов предоставления государственных услуг и исполнения государственных функций государственными органами власти;
- стимулирование граждан к получению государственных и муниципальных услуг в электронном виде с использованием Единого портала государственных и муниципальных услуг.

Задача федерального проекта «*Искусственный интеллект*» – создать условия для того, чтобы предприятия и граждане использовали продукты и услуги, основанные преимущественно на отечественных технологиях искусственного интеллекта, обеспечивающих качественно новый уровень эффективности деятельности.

Реализация федерального проекта осуществляется по следующим направлениям:

- поддержка научных исследований и разработок;
- разработка и развитие программного обеспечения, в том числе – за счет поддержки стартапов и пилотных внедрений технологий ИИ;

- создание комплексной системы правового регулирования в сфере искусственного интеллекта;
- повышение доступности и качества данных;
- повышение доступности аппаратного обеспечения;
- повышение уровня обеспечения российского рынка технологий ИИ квалифицированными кадрами и уровня информированности населения о возможных сферах использования ИИ.

Федеральный проект «*Цифровое государственное управление*» национальной программы «Цифровая экономика Российской Федерации» включает три инициативы социально-экономического развития Российской Федерации до 2030 года, утверждённые распоряжением Правительства Российской Федерации от 6 октября 2021 г. № 2816-р:

- Цифровой профиль гражданина;
- Госуслуги онлайн;
- Электронный документооборот.

Проект направлен на оптимизацию взаимодействия граждан и бизнеса с органами власти с использованием цифровых сервисов.

Реализация инициативы «Цифровой профиль гражданина» обеспечит удобство и новое качество получения государственных услуг онлайн, сократит время на идентификацию граждан и снизит количество визитов в учреждения для получения государственных услуг.

Инициатива «Госуслуги онлайн» подразумевает фундаментальное изменение формата предоставления и получения госуслуг, что обеспечивает повышение цифровой зрелости государственного управления.

Инициатива «Электронный документооборот» решает проблемы нормативных и технологических ограничений применения цифровых инструментов и сервисов для всех типов взаимодействия. Инициатива также предоставляет гражданам возможность использовать облачную подпись при подписании электронных документов без необходимости личных визитов.

Реализация инициатив направлена на достижение двух показателей национальной цели развития Российской Федерации «Цифровая трансформация» – снизить издержки бизнеса и повысить эффективность за счет проекта по цифровой идентификации, переход на онлайн-формат взаимодействия обеспечивает достижение показателя «цифровой зрелости» ключевых отраслей экономики и социальной сферы, в том числе – здравоохранения и образования, а также государственного управления.

Федеральный проект «*Развитие кадрового потенциала ИТ-отрасли*» национальной программы «Цифровая экономика Российской Федерации» реализуется в рамках перечня инициатив социально-экономического развития Российской Федерации до 2030 года, утвержденных распоряжением Правительства Российской Федерации от 6 октября 2021

года № 2816-р, и направлен на создание возможностей для формирования востребованных рынком труда цифровых компетенций.

Цель федерального проекта – создание возможностей для формирования востребованных рынком труда цифровых компетенций.

Федеральный проект способствует формированию у молодого поколения цифровых компетенций, начиная со старших классов, а в перспективе минимизирует разрыв между требованиями работодателей и уровнем кандидатов в области ИТ.

Проект направлен на достижение «*цифровой зрелости*» ключевых отраслей экономики и социальной сферы, в т.ч. здравоохранения и образования, а также государственного управления, в рамках национальной цели «Цифровая трансформация» путем увеличения количества квалифицированных ИТ-кадров и на поддержание баланса спроса и предложения на рынке труда в ИТ-отрасли.

Федеральный проект «*Обеспечение доступа в Интернет за счет развития спутниковой связи*» национальной программы «Цифровая экономика Российской Федерации» реализуется в рамках перечня инициатив социально-экономического развития Российской Федерации до 2030 года, утверждённых распоряжением Правительства Российской Федерации от 6 октября 2021 года № 2816-р.

Цель федерального проекта – создать равные возможности доступа к современным телекоммуникационным сервисам всем жителям и компаниям в нашей стране.

Реализация инициативы «Доступ в Интернет» обеспечит россиян возможностью воспользоваться современными телекоммуникационными сервисами, в том числе – в удаленных и труднодоступных местностях, где строительство волоконно-оптических линий связи затратно или невозможно. Для этих целей в рамках федерального проекта создаются спутниковые системы связи «Экспресс» на геостационарной орбите и «Экспресс-РВ» на высокоэллиптических орбитах.

К 2030 году вся территория Российской Федерации, в том числе – Арктическая зона и Дальний Восток, будет обеспечена современными услугами связи.

Федеральный проект «Обеспечение доступа в Интернет за счет развития спутниковой связи» направлен на достижение показателя «рост доли домохозяйств, которым обеспечена возможность широкополосного доступа к информационно-телекоммуникационной сети Интернет до 97%» [7].

В заключение еще раз отметим Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», в рамках которого создается ГосСОПКА.

Государственная система обнаружения, предупреждения и

ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации представляет собой единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Согласно этому федеральному закону, субъектами критической информационной инфраструктуры являются государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей [8].

На основании изложенного можно сделать вывод, что исключительно масштабная и глубокая цифровизация жизни страны требует крайне продуманной и надежной защиты информационного пространства России от возрастающих киберугроз. Рассмотрим в этой связи внутренние и внешние угрозы кибербезопасности.

2.2. Внутренние и внешние источники угроз кибербезопасности

Как говорилось в первой главе учебника, кибербезопасность следует рассматривать как составную часть информационной безопасности. В теории информационной безопасности и методологии защиты информации виды угроз имеют устоявшуюся классификацию. Традиционно источники угроз информационной безопасности принято делить на внешние и внутренние. Спектр угроз информационной безопасности, вызванных внешними факторами, чрезвычайно широк и может меняться. Внешние угрозы представляют собой наибольшую опасность, в качестве них, как правило, рассматриваются разведывательная деятельность иностранных специальных служб и преступных сообществ, а также деятельность иностранных государственных и частных коммерческих структур. К внешним угрозам кибербезопасности относятся целенаправленные методы воздействия, доступ в операционную среду компьютерных систем с целью нарушения, прекращения функционирования, создания угрозы безопасности обрабатываемой информации.

В то же время значительное число инцидентов информационной

безопасности связано с воздействием внутренних угроз. В классификации внутренних угроз, в первую очередь, можно выделить две большие группы – совершаемые из корыстных или других злонамеренных соображений и совершаемые без злого умысла, по неосторожности или технической некомпетентности.

Кибербезопасность – это совокупность методов и практик защиты от атак злоумышленников компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных. Кибербезопасность находит применение в самых разных областях – от бизнес-сферы до мобильных технологий. В этом направлении можно выделить несколько основных категорий.

Безопасность сетей – действия по защите компьютерных сетей от различных угроз, например, целевых атак или вредоносных программ.

Безопасность приложений – защита устройств от угроз, которые злоумышленики могут скрыть в программах. Зараженное приложение может открыть им доступ к данным, которые оно должно защищать. Безопасность приложения обеспечивается еще на стадии разработки, задолго до его появления в открытых источниках.

Безопасность информации – обеспечение целостности и приватности данных как во время хранения, так и при передаче.

Операционная безопасность – обращение с информационными активами и их защита. К этой категории относится, например, управление разрешениями для доступа к сети или правилами, которые определяют, где и каким образом данные могут храниться и передаваться.

Аварийное восстановление и непрерывность бизнеса – реагирование на инцидент безопасности (действия злоумышленников) и любое другое событие, которое может нарушить работу систем или привести к потере данных. Аварийное восстановление – набор правил, описывающих то, как необходимо бороться с последствиями атаки и восстанавливать рабочие процессы. Непрерывность бизнеса – план действий на случай, если организация теряет доступ к определенным ресурсам из-за атаки злоумышленников.

Повышение осведомленности – обучение пользователей. Это направление помогает снизить влияние самого непредсказуемого фактора в области кибербезопасности – человеческого. Даже самая защищенная система может подвергнуться атаке из-за чьей-то ошибки или незнания. Поэтому каждая организация должна проводить тренинги для сотрудников и рассказывать им о главных правилах: например, почему не нужно открывать подозрительные вложения в электронной почте или подключать сомнительные USB-устройства [9].

Актуальные угрозы кибербезопасности ежегодно публикуются крупными IT-компаниями в виде аналитических отчетов (обзоров).

Согласно аналитическому обзору компании Positive Technologies

можно выделились следующие киберугрозы:

- *нарушения регламентов информационной безопасности*. Использование программного обеспечения для удаленного доступа и использование незащищенных сетевых протоколов (LLRNM, NetBios). Наиболее часто среди выявляемых нарушений регламентов информационной безопасности выступает использование программного обеспечения для удаленного доступа, например, TeamViewer, Ammyy Admin, LightManager, Remote Manipulator System (RMS), Dameware Remote Control (DWRC), AnyDesk и другие;
- *подозрительная сетевая активность*. К ней относятся сокрытие трафика, запуск инструментов сканирования сети, попытки удаленного запуска процессов, множественные неудачные попытки аутентификации и т.д.;
- *активность вредоносного программного обеспечения* – наиболее распространенная угроза. Её создают вредоносное программное обеспечение для удалённого управления, майнеры, шифровальщики, рекламное программное обеспечение, банковские трояны, шпионское программное обеспечение;
- *эксплуатация уязвимостей в программном обеспечении*. Это как попытки атак внутри сети, так и успешные атаки на периферийные системы.
- *подбор паролей*. Это доступ к базе данных веб-сайта, в том числе – к учетным данным пользователей [10].

2.3. Структура и функциональные особенности системы обеспечения кибербезопасности

Система кибербезопасности является областью активных исследований и разработок. При этом кибербезопасность с законодательной точки зрения не выделена в самостоятельное направление, рассматриваясь сегодня в контексте информационной безопасности.

Система обеспечения информационной безопасности (СОИБ) – совокупность ресурсов (сил и средств) безопасности для осуществления скоординированной и спланированной деятельности по обеспечению информационной безопасности. Состав СОИБ представлен на рис. 2.3.1.

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

В то же время СОИБ строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере с учетом предметов ведения федеральных органов государственной власти, органов государственной власти субъектов РФ, а также органов местного самоуправления, определяемых законодательством РФ в области обеспечения безопасности (рис. 2.3.2).

Рис. 2.3.1. Состав системы обеспечения информационной безопасности Российской Федерации

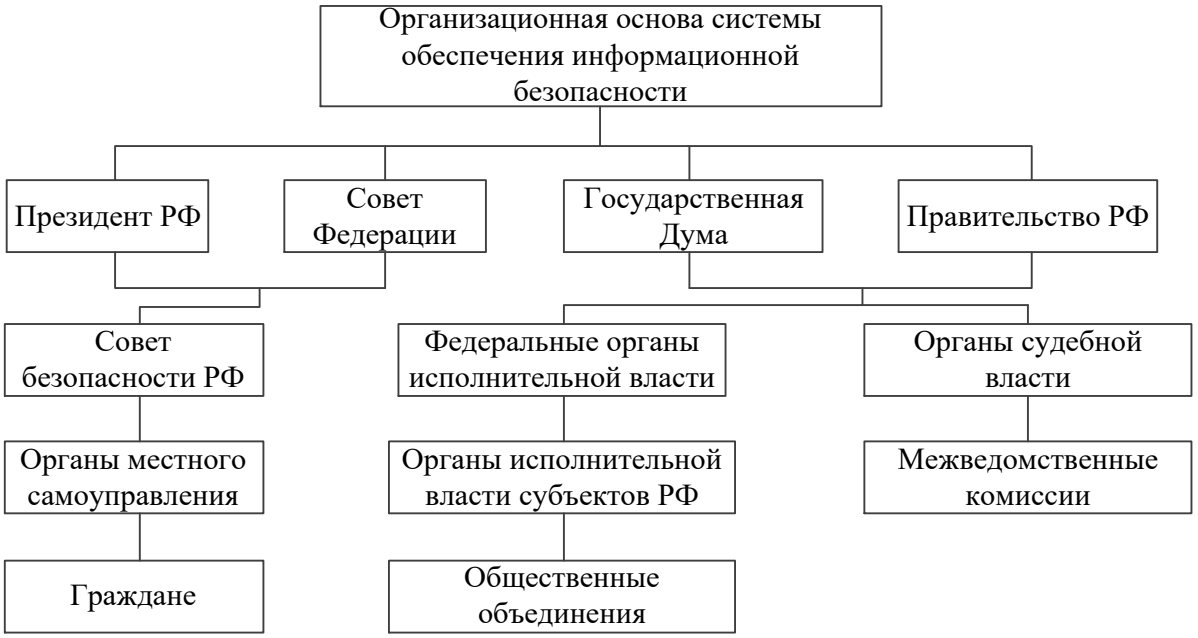


Рис. 2.3.2. Организационная основа системы обеспечения информационной безопасности Российской Федерации

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

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

Органы управления и обеспечения информационной безопасности РФ составляют организационную основу СОИБ.

Президент РФ руководит в пределах своих конституционных полномочий органами и силами по обеспечению информационной безопасности; санкционирует действия по обеспечению информационной безопасности РФ; в соответствии с законодательством РФ формирует, реорганизует и упраздняет подчиненные ему органы и силы по обеспечению информационной безопасности РФ; определяет в своих ежегодных посланиях Федеральному Собранию приоритетные направления государственной политики в области обеспечения информационной безопасности РФ, а также меры по реализации Доктрины информационной безопасности РФ.

Палаты Федерального Собрания РФ на основе Конституции РФ по представлению Президента РФ и Правительства РФ формируют законодательную базу в области обеспечения информационной безопасности РФ.

Правительство РФ в пределах своих полномочий и с учетом сформулированных в ежегодных посланиях Президента РФ Федеральному

Собранию приоритетных направлений в области обеспечения информационной безопасности РФ координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов РФ; при формировании в установленном порядке проектов федерального бюджета на соответствующие годы предусматривает выделение средств, необходимых для реализации федеральных программ в этой области.

Совет Безопасности РФ проводит работу по выявлению и оценке угроз информационной безопасности Российской Федерации, оперативно готовит проекты решений Президента Российской Федерации по предотвращению таких угроз, разрабатывает предложения в области обеспечения информационной безопасности Российской Федерации, а также предложения по уточнению отдельных положений Доктрины, координирует деятельность органов и сил по обеспечению информационной безопасности, контролирует реализацию федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации решений Президента Российской Федерации в этой области.

Федеральные органы исполнительной власти обеспечивают исполнение законодательства Российской Федерации, решений Президента Российской Федерации и Правительства Российской Федерации в пределах своей компетенции, разрабатывают НПА в этой области и представляют их в установленном порядке Президенту Российской Федерации и Правительству Российской Федерации.

Межведомственные и государственные комиссии, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, решают в соответствии с предоставленными им полномочиями задачи обеспечения информационной безопасности Российской Федерации.

Органы исполнительной власти субъектов Российской Федерации взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения законодательства Российской Федерации, решений Президента Российской Федерации и Правительства Российской Федерации в области обеспечения информационной безопасности Российской Федерации, а также по вопросам реализации федеральных программ в этой области; совместно с органами местного самоуправления осуществляют мероприятия по привлечению граждан, организаций и общественных объединений к оказанию содействия в решении проблем обеспечения информационной безопасности Российской Федерации; вносят в федеральные органы исполнительной власти предложения по совершенствованию СОИБ Российской Федерации.

Федеральные органы, осуществляющие функции по обеспечению информационной безопасности Российской Федерации, представлены на

рис. 2.3.3.

Органы государственной власти обеспечивают соблюдение законодательства Российской Федерации в области обеспечения информационной безопасности России.

Органы судебной власти осуществляют правосудие по делам о преступлениях, связанных с посягательствами на законные интересы личности, общества и государства в информационной сфере, и обеспечивают судебную защиту граждан и общественных объединений, чьи права были нарушены в связи с деятельностью по обеспечению информационной безопасности Российской Федерации [11].

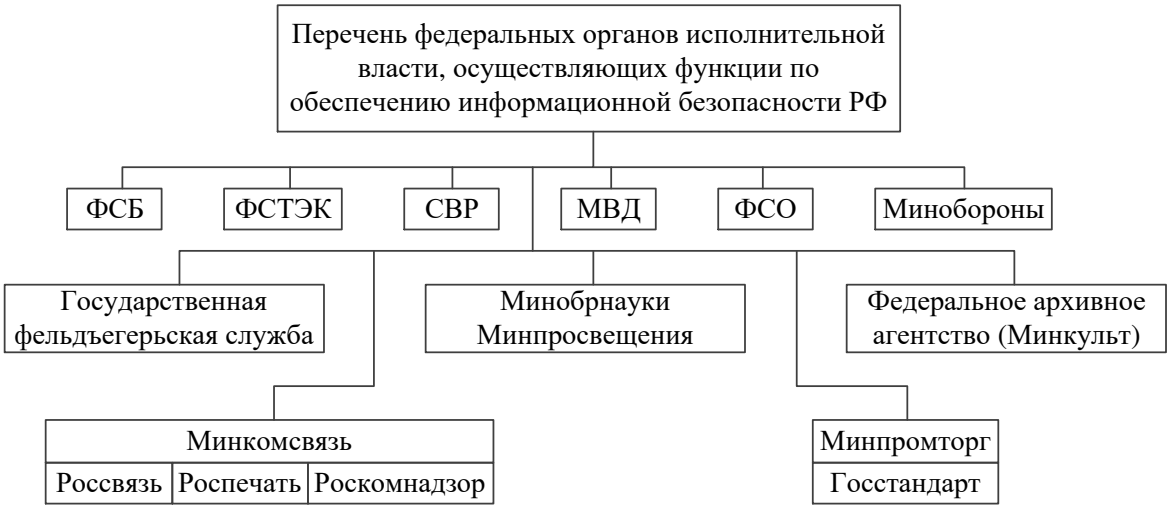


Рис. 2.3.3. Федеральные органы, осуществляющие функции по обеспечению информационной безопасности РФ

Согласно Указу Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», на Федеральную службу безопасности Российской Федерации возложены полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Согласно Указу, Федеральная служба безопасности Российской Федерации выполняет следующие функции:

- организует и проводит работы по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, осуществляет контроль за исполнением этих работ, а также обеспечивает во взаимодействии с государственными органами функционирование ее элементов;

- разрабатывает методику обнаружения компьютерных атак на информационные системы и информационно-телекоммуникационные сети государственных органов и по согласованию с их владельцами – на иные информационные системы и информационно-телекоммуникационные сети;
- определяет порядок обмена информацией между федеральными органами исполнительной власти о компьютерных инцидентах, связанных с функционированием информационных ресурсов Российской Федерации;
- организует и проводит в соответствии с законодательством Российской Федерации мероприятия по оценке степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;
- разрабатывает методические рекомендации по организации защиты критической информационной инфраструктуры Российской Федерации от компьютерных атак;
- определяет порядок обмена информацией между федеральными органами исполнительной власти и уполномоченными органами иностранных государств (международными организациями) о компьютерных инцидентах, связанных с функционированием информационных ресурсов, и организует обмен такой информацией [12].

В системе обеспечения кибербезопасности в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, функции ведения банка данных угроз безопасности информации и уязвимостей программного обеспечения возложены на ФСТЭК России.

Кроме того, основными задачами ФСТЭК России являются:

- реализация в пределах своей компетенции государственной политики в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации;
- осуществление государственной научно-технической политики в области защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;
- обеспечение проведения единой государственной политики в области засекречивания сведений при подготовке развернутых перечней сведений, подлежащих засекречиванию;
- организация деятельности государственной системы противодействия техническим разведкам и технической защиты информации на федеральном, межрегиональном, региональном, отраслевом и объектовом уровнях, а также руководство указанной государственной системой;

- осуществление самостоятельного нормативно-правового регулирования вопросов;
- обеспечение безопасности значимых объектов критической информационной инфраструктуры (в редакции Указа Президента Российской Федерации от 25.11.2017 № 569, вступил в силу с 1 января 2018 г.);
- противодействия техническим разведкам;
- технической защиты информации;
- размещение и использование иностранных технических средств наблюдения и контроля в ходе реализации международных договоров Российской Федерации, иных программ и проектов на территории Российской Федерации, на континентальном шельфе и в исключительной экономической зоне Российской Федерации;
- координация деятельности государственных органов и организаций по подготовке развернутых перечней сведений, подлежащих засекречиванию, а также методическое руководство этой деятельностью (в редакции Указа Президента Российской Федерации от 08.12.2021 № 698);
- осуществление экспортного контроля;
- обеспечение в пределах своей компетенции безопасности значимых объектов критической информационной инфраструктуры, противодействие техническим разведкам и технической защиты информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации, органах местного самоуправления и организациях;
- прогнозирование развития сил, средств и возможностей технических разведок, выявление угроз безопасности информации;
- противодействие добыванию информации техническими средствами разведки, техническая защита информации;
- осуществление координации деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации и организаций по государственному регулированию размещения и использования иностранных технических средств наблюдения и контроля в ходе реализации международных договоров Российской Федерации, иных программ и проектов на территории Российской Федерации, на континентальном шельфе и в исключительной экономической зоне Российской Федерации;
- осуществление в пределах своей компетенции контроля деятельности по противодействию техническим разведкам и по технической защите информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, в федеральных органах исполнительной власти, органах исполнительной

власти субъектов Российской Федерации, органах местного самоуправления и организациях;

- осуществление государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры;
- реализация государственной политики и организация межведомственного взаимодействия в области экспортного контроля;
- осуществление контроля за соблюдением российскими участниками внешнеэкономической деятельности законодательных и иных нормативных правовых актов Российской Федерации в области экспортного контроля;
- осуществление центральным аппаратом ФСТЭК России организационно-технического обеспечения деятельности Межведомственной комиссии по защите государственной тайны и Комиссии по экспортному контролю Российской Федерации [13].

2.4. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы

Как указывалось выше, в январе 2013 года вступил в силу Указ Президента Российской Федерации «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». Документ определил основные задачи ГосСОПКА, а также орган исполнительной власти, на который были возложены полномочия по созданию и обеспечению функционирования ГосСОПКА (ФСБ России).

В декабре 2014 года Президентом РФ утверждена Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (утверждена Президентом РФ 12 декабря 2014 г. № К 1274), в которой уточнялось назначение, принципы создания и функционирования ГосСОПКА.

В 2015 году ФСБ России в рамках развития ГосСОПКА создает Национальный координационный центр по компьютерным инцидентам (НКЦКИ), который согласно закону РФ от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры» обеспечивает координацию деятельности субъектов критической информационной инфраструктуры по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

НКЦКИ разработал методические рекомендации по созданию ведомственных и корпоративных центров ГосСОПКА, в которых освещены общие вопросы создания центров ГосСОПКА и их основные

функции [14].

Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации представляет ГосСОПКА как единый централизованный, территориально распределенный комплекс, включающий силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

Система осуществляет реализацию следующих функций:

- выявление признаков проведения компьютерных атак, определение их источников, методов, способов и средств осуществления и направленности, а также разработка методов и средств обнаружения, предупреждения и ликвидации последствий компьютерных атак;
- формирование и поддержание в актуальном состоянии детализированной информации об информационных ресурсах Российской Федерации, находящихся в зоне ответственности субъектов Системы;
- прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации, включая выявленные и прогнозируемые угрозы и их оценку;
- организация и осуществление взаимодействия с правоохранительными органами и другими государственными органами, владельцами информационных ресурсов Российской Федерации, операторами связи, интернет-провайдерами и иными заинтересованными организациями на национальном и международном уровнях в области обнаружения компьютерных атак и установления их источников, включая обмен информацией о выявленных компьютерных атаках и вызванных ими компьютерных инцидентах, а также обмен опытом в сфере выявления и устранения уязвимостей программного обеспечения и оборудования и реагирования на компьютерные инциденты;
- организация и проведение научных исследований в сфере разработки и применения средств и методов обнаружения, предупреждения и ликвидации последствий компьютерных атак;
- осуществление мероприятий по обеспечению подготовки и повышения квалификации кадров, требующихся для создания и функционирования Системы;
- сбор и анализ информации о компьютерных атаках и вызванных ими компьютерных инцидентах в отношении информационных ресурсов Российской Федерации, а также о компьютерных инцидентах в информационных системах и информационно-телекоммуникационных сетях других стран, с которыми взаимодействуют владельцы информационных ресурсов Российской Федерации;

- осуществление мероприятий по оперативному реагированию на компьютерные атаки и вызванные ими компьютерные инциденты, а также по ликвидации последствий данных компьютерных инцидентов в информационных ресурсах Российской Федерации;
- выявление, сбор и анализ сведений об уязвимостях программного обеспечения и оборудования;
- мониторинг степени защищенности информационных систем и информационно-телекоммуникационных сетей на всех этапах создания, функционирования и модернизации информационных ресурсов Российской Федерации, а также разработка методических рекомендаций по организации защиты информационных ресурсов Российской Федерации от компьютерных атак;
- организация и осуществление антивирусной защиты;
- совершенствование оперативно-тактического взаимодействия сил и средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Создание и функционирование государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак осуществляется на основе следующих принципов:

- территориальная распределенность;
- отраслевая и территориальная организация;
- единство государственного планирования, а также координации и контроля реализации комплекса технических и организационных мер;
- обеспечение функционирования Системы на основе единой научно-технической и организационно-методической политики;
- достаточность и рациональное использование сил и средств обнаружения, предупреждения и ликвидации последствий компьютерных атак;
- разделение полномочий и ответственности между субъектами Системы на основе нормативно-правовой базы Российской Федерации.

Основной организационно-технической составляющей ГосСОПКА являются *центры обнаружения, предупреждения и ликвидации последствий компьютерных атак*, организованные по ведомственному и территориальному принципам.

К основным задачам центров относятся:

- обнаружение, предупреждение и ликвидация последствий компьютерных атак, направленных на контролируемые информационные ресурсы;
- проведение мероприятий по оценке степени защищенности контролируемых информационных ресурсов;

- проведение мероприятий по установлению причин компьютерных инцидентов, вызванных компьютерными атаками на контролируемые информационные ресурсы;
- сбор и анализ данных о состоянии информационной безопасности в контролируемых информационных ресурсах;
- осуществление взаимодействия между центрами;
- информирование заинтересованных лиц и субъектов Системы по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Центры подразделяются на главный центр Системы, региональные центры, территориальные центры, центры органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации (ведомственные центры) и корпоративные центры (рис. 2.4.1).

Главный центр Системы, региональные и территориальные центры Системы создаются силами федерального органа исполнительной власти, уполномоченного в области создания и обеспечения функционирования Системы. Зоной ответственности данных центров являются информационные ресурсы органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации (органы государственной власти), а также информационные ресурсы указанного федерального органа исполнительной власти.

Рис. 2.4.1. Организационная структура ГосСОПКА

Данные центры организуют и проводят в соответствии с

законодательством Российской Федерации мероприятия по оценке степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак.

Ведомственные центры создаются заинтересованными органами государственной власти. Зоной ответственности таких центров являются принадлежащие органам государственной власти информационные ресурсы. Также ведомственные центры могут создаваться и эксплуатироваться в интересах органов государственной власти организациями, осуществляющими лицензируемую деятельность в области защиты информации.

Функционирование ведомственного центра обеспечивается органом государственной власти, создавшим этот центр.

Корпоративные центры могут создаваться государственными корпорациями, операторами связи и другими организациями, осуществляющими лицензируемую деятельность в области защиты информации.

Функционирование корпоративного центра обеспечивается организацией, создавшей такой центр.

Включение ведомственного (корпоративного) центра в состав Системы осуществляется на основе соглашения органа государственной власти (организации), создавшего (создавшей) указанный центр, с федеральным органом исполнительной власти, уполномоченным в области создания и обеспечения функционирования Системы.

В составе Системы функционирует созданный в Федеральной службе безопасности Российской Федерации Национальный координационный центр по компьютерным инцидентам, который организует и осуществляет обмен информацией о компьютерных инцидентах с юридическими лицами, владеющими на праве собственности или ином законном основании объектами критической информационной инфраструктуры Российской Федерации, операторами связи, обеспечивающими взаимодействие объектов критической информационной инфраструктуры Российской Федерации между собой, уполномоченными органами иностранных государств, международными и неправительственными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты.

Федеральный орган исполнительной власти, уполномоченный в области создания и обеспечения функционирования Системы, осуществляет доведение до субъектов Системы информации об угрозах информационным ресурсам Российской Федерации и о необходимых мерах по нейтрализации данных угроз, а также обеспечивает реализацию мероприятий по совершенствованию оперативно-тактического взаимодействия субъектов Системы [15].

В дополнение, в соответствии с Указом Президента Российской

Федерации от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», задачами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации являются:

- прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации;
- обеспечение взаимодействия владельцев информационных ресурсов Российской Федерации, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак;
- осуществление контроля степени защищенности информационных ресурсов Российской Федерации от компьютерных атак;
- установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации [16].

Построение центра ГосСОПКА – комплексное решение для создания ведомственного (корпоративного) центра и взаимодействия с ГосСОПКА. В качестве примера рассмотрим решение на основе продуктов Positive Technologies и услуги экспертного центра безопасности PT Expert Security Center (PT ESC).

С помощью продуктов подразделение информационной безопасности самостоятельно реализует функции центра ГосСОПКА, а специалисты PT ESC дополняют команду ИБ недостающей экспертизой и берут на себя сопровождение работы подразделения, в том числе часть функций центра ГосСОПКА.

Создание центра – длительный и трудоемкий процесс, реализуемый в несколько этапов. На первом этапе необходимо создать систему защиты от типовых атак на периметр, на втором – от типовых внутренних атак и на третьем – от нетиповых, новых угроз. Такой подход помогает организациям постепенно развивать внутреннюю экспертизу в области ИБ, выстраивать процессы в подразделении ИБ и успешно отражать все виды атак (рис. 2.4.2).

Представленное решение позволяет иметь следующие характеристики.

Быстрый старт выполнения требований. Постепенное построение центра позволяет спланировать бюджет и уже на первом этапе начать выполнять требования законодательства и взаимодействовать с НКЦКИ.

Соответствие требованиям регуляторов «на лету». Продукты Positive Technologies регулярно обновляются с учетом актуальных угроз и требований новых нормативных правовых актов.

Единая система. Все продукты являются частью универсальной платформы средств безопасности Positive Technologies, что обеспечивает совместимость компонентов и простоту интеграции.

Высокий уровень практической безопасности IT-систем. Продукты Positive Technologies защищают критические IT-инфраструктуры крупнейших российских банков и промышленных предприятий, федеральных органов власти, госкорпораций.

Оперативное противодействие актуальным угрозам. Эксперты PT ESC непрерывно анализируют актуальные угрозы и передают данные об уязвимостях, способах выявления и реагирования на новые типы атак в единую базу знаний Positive Technologies Knowledge Base, которая входит в MaxPatrol SIEM [17].

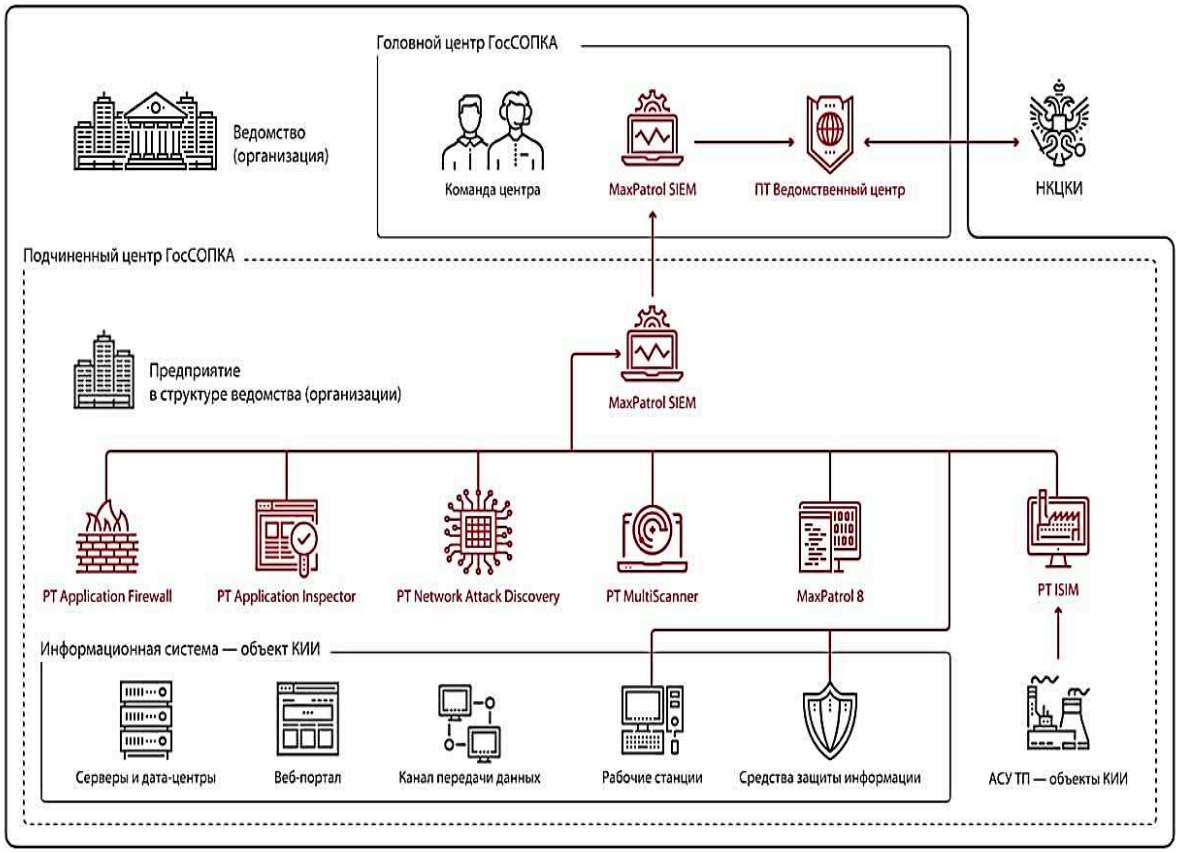


Рис. 2.4.2. Решение на основе продуктов Positive Technologies

2.5. Государственная международная политика Российской Федерации в сфере обеспечения кибербезопасности

Международное сотрудничество в области обеспечения информационной безопасности и как ее элемента – кибербезопасности – неотъемлемая составляющая политического, военного, экономического, культурного и других видов взаимодействия стран, входящих в мировое

сообщество. Такое сотрудничество должно способствовать повышению информационной безопасности всех членов мирового сообщества.

Указом Президента РФ от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» определено, что *государственная политика в области международной информационной безопасности* представляет собой совокупность скоординированных мер, направленных на формирование с учетом национальных интересов Российской Федерации системы обеспечения международной информационной безопасности [18].

Нормативную правовую базу по обеспечению международной информационной безопасности составляют Конституция Российской Федерации, международные договоры Российской Федерации о сотрудничестве в области обеспечения международной информационной безопасности, федеральные законы и иные нормативные правовые акты Российской Федерации.

В целом система документов в области международной информационной безопасности направлена на:

- продвижение на международной арене российских подходов к формированию системы обеспечения международной информационной безопасности и российских инициатив в области международной информационной безопасности;
- содействие созданию международно-правовых механизмов предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве;
- организацию межведомственного взаимодействия при реализации государственной политики в области международной информационной безопасности.

Система обеспечения международной информационной безопасности представляет собой совокупность международных и национальных институтов, регулирующих деятельность в глобальном информационном пространстве в целях предотвращения (минимизации) угроз международной информационной безопасности.

Обозначенными в Указе угрозами международной информационной безопасности являются:

- использование информационно-коммуникационных технологий в военно-политической и иных сферах в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности государств, осуществления в глобальном информационном пространстве иных действий, препятствующих поддержанию международного мира, безопасности и стабильности;

- использование информационно-коммуникационных технологий в террористических целях, в том числе – для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;
- использование информационно-коммуникационных технологий в экстремистских целях, а также для вмешательства во внутренние дела суверенных государств;
- использование информационно-коммуникационных технологий в преступных целях, в том числе – для совершения преступлений в сфере компьютерной информации, а также для совершения различных видов мошенничества;
- использование информационно-коммуникационных технологий для проведения компьютерных атак на информационные ресурсы государств, в том числе – на критическую информационную инфраструктуру;
- использование отдельными государствами технологического доминирования в глобальном информационном пространстве для монополизации рынка информационно-коммуникационных технологий, ограничения доступа других государств к передовым информационно-коммуникационным технологиям, а также для усиления их технологической зависимости от доминирующих в сфере информатизации государств и информационного неравенства.

Достижение цели государственной политики в области международной информационной безопасности осуществляется путем решения задач по развитию на глобальном, региональном, многостороннем и двустороннем уровнях сотрудничества Российской Федерации с иностранными государствами по вопросам формирования системы обеспечения международной информационной безопасности, а также противодействия основным угрозам международной информационной безопасности.

Основными направлениями реализации государственной политики в области международной информационной безопасности *по развитию на глобальном, региональном, многостороннем и двустороннем уровнях сотрудничества Российской Федерации с иностранными государствами* по вопросам формирования системы обеспечения международной информационной безопасности являются:

- создание условий для принятия государствами – членами Организации Объединенных Наций (ООН) Конвенции об обеспечении международной информационной безопасности;
- содействие организации под эгидой ООН регулярного институционального диалога с участием всех государств – членов ООН для обеспечения демократического, инклюзивного и транспарентного переговорного процесса по вопросам безопасности в сфере использования информационно-коммуникационных технологий;

- содействие выработке с учетом специфики информационно-коммуникационных технологий новых принципов и норм международного права, регулирующих деятельность государств в глобальном информационном пространстве;
- достижение и выполнение двусторонних и многосторонних договоренностей международно-правового и иного характера между Российской Федерацией и иностранными государствами о сотрудничестве в области обеспечения международной информационной безопасности;
- проведение на регулярной основе двусторонних и многосторонних экспертных консультаций, согласование позиций и основных направлений сотрудничества в области обеспечения международной информационной безопасности с государствами – участниками Содружества Независимых Государств (СНГ), объединения БРИКС, государствами – членами Организации Договора о коллективной безопасности (ОДКБ), Шанхайской организации сотрудничества (ШОС), Ассоциации государств Юго-Восточной Азии (АСЕАН), «Группы двадцати», другими государствами и международными организациями;
- организация международных конференций и семинаров по вопросам международной информационной безопасности;
- проведение организационно-штатных мероприятий, направленных на создание (укрепление) структурных подразделений федеральных органов исполнительной власти, участвующих в реализации государственной политики в области международной информационной безопасности, а также совершенствование координации деятельности и взаимодействия федеральных органов исполнительной власти в данной области;
- совершенствование механизма участия представителей российского научного и экспертного сообщества в научно-исследовательском, аналитическом и научно-методическом обеспечении продвижения инициатив Российской Федерации по формированию системы обеспечения международной информационной безопасности;
- продвижение национальных стандартов Российской Федерации в области информационной безопасности при осуществлении международного и регионального сотрудничества в сфере стандартизации, содействие их принятию в качестве международных, региональных и межгосударственных стандартов.

Основными направлениями реализации государственной политики в области международной информационной безопасности *по противодействию угрозе использования информационно-коммуникационных технологий в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности государств*, осуществления в глобальном информационном пространстве иных действий, препятствующих поддержанию международного мира,

безопасности и стабильности, являются:

- развитие сотрудничества с иностранными государствами в целях предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве;
- содействие развитию региональных систем обеспечения международной информационной безопасности и формированию соответствующей глобальной системы на основе общепризнанных принципов и норм международного права с учетом специфики информационно-коммуникационных технологий, а также на основе новых принципов и норм международного права, разработанных в целях предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве;
- выработка на глобальном, региональном, многостороннем и двустороннем уровнях мер укрепления доверия в области противодействия использованию информационно-коммуникационных технологий для осуществления в глобальном информационном пространстве действий, представляющих угрозу международному миру, безопасности и стабильности;
- развитие переговорного процесса и повышение эффективности взаимодействия с иностранными государствами в интересах совместного противодействия вызовам и угрозам, возникающим в связи с масштабным использованием информационно-коммуникационных технологий в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности государств, а также в целях осуществления в глобальном информационном пространстве других действий, представляющих угрозу международному миру, безопасности и стабильности;
- содействие совершенствованию под эгидой ООН принципов и норм международного гуманитарного права применительно к сфере использования информационно-коммуникационных технологий с учетом специфики данных технологий.

Основными направлениями реализации государственной политики в области международной информационной безопасности *по формированию механизмов международного сотрудничества в сфере противодействия угрозе использования информационно-коммуникационных технологий в террористических целях* являются:

- развитие сотрудничества с иностранными государствами, их правоохранительными органами и специальными службами, международными организациями по вопросам противодействия использованию информационно-коммуникационных технологий в террористических целях, использованию информационно-телекоммуникационной сети Интернет и других информационно-телекоммуникационных сетей для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

- содействие разработке на межгосударственном уровне комплекса мер, направленных на противодействие угрозе использования информационно-коммуникационных технологий в террористических целях;
- совершенствование на глобальном, региональном, многостороннем и двустороннем уровнях механизма обмена информацией о фактах использования информационно-коммуникационных технологий в террористических целях, повышение эффективности взаимодействия уполномоченных государственных органов.

Основными направлениями реализации государственной политики в области международной информационной безопасности *по созданию условий для противодействия угрозе использования информационно-коммуникационных технологий в экстремистских целях*, а также в целях вмешательства во внутренние дела суверенных государств являются:

- содействие разработке и реализации на глобальном, региональном, многостороннем и двустороннем уровнях комплекса мер, направленных на противодействие угрозе использования информационно-коммуникационных технологий в экстремистских целях;
- развитие сотрудничества с иностранными государствами, их правоохранительными органами и специальными службами, а также с международными организациями, осуществляющими борьбу с экстремизмом, по вопросам противодействия угрозе использования информационно-коммуникационных технологий в экстремистских целях;
- содействие созданию эффективного международного механизма контроля за использованием информационно-коммуникационных технологий для предотвращения их использования в экстремистских целях, а также в целях вмешательства во внутренние дела суверенных государств;
- содействие выработке порядка межгосударственного обмена информацией о распространении материалов запрещенных экстремистских организаций, а равно иной информационной продукции, содержащей материалы данных организаций.

Основными направлениями реализации государственной политики в области международной информационной безопасности *по повышению эффективности международного сотрудничества, направленного на противодействие угрозе использования информационно-коммуникационных технологий в преступных целях*, и по созданию необходимого для этого международно-правового режима являются:

- содействие разработке специальным межправительственным комитетом экспертов открытого состава всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, а также создание

условий для последующего принятия государствами – членами ООН данной конвенции;

- развитие сотрудничества с государствами – участниками СНГ, объединения БРИКС, государствами – членами ОДКБ, ШОС, АСЕАН, «Группы двадцати», другими государствами и международными организациями по вопросам противодействия угрозе использования информационно-коммуникационных технологий в преступных целях;
- повышение эффективности информационного обмена между правоохранительными органами государств в ходе расследования преступлений в сфере компьютерной информации, а также случаев мошенничества с использованием информационно-коммуникационных технологий;
- совершенствование механизма обмена информацией о методиках расследования преступлений в сфере компьютерной информации, случаев мошенничества с использованием информационно-коммуникационных технологий, а также о судебной практике рассмотрения уголовных дел о таких преступлениях;
- организация международных конференций и семинаров по вопросам противодействия использованию информационно-коммуникационных технологий в преступных целях.

Основными направлениями реализации государственной политики в области международной информационной безопасности *по совершенствованию межгосударственного взаимодействия, направленного на противодействие угрозе использования информационно-коммуникационных технологий для проведения компьютерных атак* на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру, а также межгосударственного взаимодействия в области реагирования на компьютерные инциденты являются:

- развитие сотрудничества с иностранными государствами, международными, международными неправительственными организациями и организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, в целях выработки механизма обмена информацией о таких инцидентах и повышения эффективности взаимодействия уполномоченных органов;
- развитие сотрудничества с государствами – участниками СНГ, объединения БРИКС, государствами – членами ОДКБ и ШОС, другими государствами и международными организациями по вопросам реагирования на компьютерные инциденты обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру;

- содействие созданию на глобальном, региональном, многостороннем и двустороннем уровнях эффективного механизма межгосударственного взаимодействия, направленного на предотвращение компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру;
- содействие выработке на глобальном, региональном, многостороннем и двустороннем уровнях порядка обмена информацией о передовых практиках обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру, а также реагирования на компьютерные инциденты;
- совершенствование взаимодействия между Национальным координационным центром по компьютерным инцидентам и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также реагирования на компьютерные инциденты.

Основными направлениями реализации государственной политики в области международной информационной безопасности *по созданию условий для обеспечения технологического суверенитета государств в области информационно-коммуникационных технологий* и преодоления информационного неравенства между развитыми и развивающимися странами являются:

- создание условий для противодействия использованию отдельными государствами технологического доминирования и монополизации ими различных сегментов рынка информационно-коммуникационных технологий, включая основные информационные ресурсы, критическую информационную инфраструктуру, ключевые технологии, продукты и услуги;
- содействие обеспечению безопасного и стабильного функционирования и развития информационно-телекоммуникационной сети Интернет на основе равноправного участия государств – членов мирового сообщества в управлении данной сетью и повышению роли Международного союза электросвязи в таком управлении;
- содействие обеспечению равного доступа государств к новейшим информационно-коммуникационным технологиям и предотвращению технологической зависимости в сфере информатизации и информационного неравенства;
- содействие разработке и реализации на глобальном, региональном, многостороннем и двустороннем уровнях международных программ,

направленных на преодоление информационного неравенства между развитыми и развивающимися государствами;

- содействие развитию национальных информационных инфраструктур и равноправному участию государств в создании и использовании современных глобальных информационных сетей и систем, в том числе на основе реформирования протоколов функционирования глобальной сети связи;
- содействие обеспечению равных прав национальных коммерческих организаций – производителей товаров и услуг в сфере информационно-коммуникационных технологий и информационной безопасности;
- повышение эффективности государственно-частного партнерства в сфере информационной безопасности, содействие участию национальных коммерческих организаций – производителей товаров и услуг в указанной сфере в международном сотрудничестве в интересах укрепления информационной безопасности Российской Федерации и формирования системы обеспечения международной информационной безопасности [18].

Огромным шагом является выход проблемы кибербезопасности на международный уровень. Принята резолюция Генеральной Ассамблеи ООН 57/239 «Создание глобальной культуры кибербезопасности» от 2002 года, а также резолюция Генеральной Ассамблеи ООН 72/200 «Использование информационно-коммуникационных технологий в целях устойчивого развития» от 2017 года.

В рамках Организации Договора о коллективной безопасности между странами – участниками также ведется работа по обеспечению кибербезопасности. В 2017 году странами подписано Соглашение о сотрудничестве государств – членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности, которое вступило в силу в 2019 году.

В Соглашении определены основные угрозы информационной безопасности:

- осуществление деструктивного информационного воздействия на государства – члены ОДКБ и Организацию в целом;
- использование информационно-коммуникационных технологий террористическими и экстремистскими организациями, организованными преступными группами (сообществами);
- осуществление противоправной деятельности с использованием информационно-коммуникационных технологий.

Сотрудничество в области обеспечения информационной безопасности по следующим основным направлениям:

- взаимодействие в разработке и продвижении правовых основ сотрудничества, содействие совершенствованию международной правовой базы;
- формирование практических механизмов совместного реагирования на угрозы информационной безопасности;
- развитие мер укрепления доверия в сфере обеспечения информационной безопасности;
- совершенствование технологической основы обеспечения информационной безопасности;
- создание условий для взаимодействия компетентных органов Сторон в целях реализации настоящего Соглашения.

В целом Россией подписан ряд документов в области обеспечения международной информационной безопасности в рамках региональных международных организаций ШОС, ОДКБ, СНГ и БРИКС, а также двусторонние соглашения в области обеспечения международной информационной безопасности с Республикой Беларусь, Бразилией, КНР, Кубой, Индией и рядом арабских стран. Документы содержат общие вопросы государственной политики по обеспечению кибербезопасности.

2.6. Деятельность Министерства внутренних дел России в области обеспечения кибербезопасности

На разных этапах развития органов государственной власти ведомственными учеными учитывались мировые научно-технические тренды.

Долгое время приоритетом в развитии органов внутренних дел выступала широкая информатизация. В 2005 году положено начало информационного развития ведомства созданием ЕИТКС.

Приказом от 20 мая 2008 г. № 435 «Об утверждении новой редакции Программы МВД России «Создание единой информационно-телекоммуникационной системы органов внутренних дел» определены этапы и период развития ЕИТКС. Своевременно принятое решение позволило значимо оптимизировать работу служб Министерства, но уже очень скоро потребовались новые модернизации его информационной сферы.

В 2012 году Министерство утвердило концепцию создания единой системы информационно-аналитического обеспечения деятельности ИСОД МВД России. Новая система стала продолжением развития ЕИТКС с акцентом на интеграцию информационных систем. Создание ИСОД МВД России в основном связано с объединением информационной инфраструктуры Министерства внутренних дел.

Сегодня ИСОД МВД России – достаточно сложная мультисервисная система, имеющая необходимые подключения через межсетевые экраны к

сети Интернет. Сегодня практически у каждого сотрудника имеются возможности доступа к системе.

Интернет сделал информационную структуру Министерства уязвимой для компьютерных атак, осуществляемых извне спецслужбами иностранных государств, профессиональными и любительскими хакерскими группировками, в том числе – курируемыми криминалитетом.

Кроме того, усилилась проблема внутреннего нарушителя. А именно, сотрудники, имеющие низкую компьютерную грамотность или намеренно игнорирующие требования по безопасности информации, стали создавать повышенную угрозу ведомственной информационной структуре. Все это поставило на передний план задачи обеспечения кибербезопасности.

На сегодняшний день прямое определение *кибербезопасности* приводится в ГОСТ Р 56205-2014 – это *действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли, повреждения критических систем или информационных объектов* [22].

Для понимания роли и места Министерства в обеспечении кибербезопасности классифицируем ее на три направления: государственная; корпоративная (ведомственная); личная.

Начнем с анализа личной кибербезопасности. Использующий современные информационные технологии сотрудник создает на основе интернет-возможностей свое цифровое пространство – своеобразную экосистему.

Часто создание личной цифровой экосистемы обусловлено использованием технических и программных средств одного производителя, например, пользователи Apple могут открывать ссылки в браузерах одновременно на всех устройствах общей системы, использовать единую систему электронных платежей, синхронизацию файлов и многое другое. Более того, современные облачные сервисы позволяют объединять устройства разных производителей в одну цифровую экосистему, где пользователи хранят в облаке копии документов, фотографии, пароли и т.д. Удобство, с одной стороны. Но оно становится киберугрозой – с другой. А для того, чтобы провести эффективную работу по расследованию реализованной киберугрозы, необходимо участие следователей и оперативных работников с профессиональным знанием основ кибербезопасности.

Движемся далее. Цифровая экосистема формируется как для отдельной личности, так и для корпорации. Одной из основных причин является переход к цифровым услугам и ориентация на современного пользователя. Кроме того, в условиях коронавирусной пандемии большинству организаций пришлось организовать многофункциональные удаленные рабочие места. Обеспечение корпоративной кибербезопасности, как и личной, осуществлялось собственными силами

владельцев цифровой экосистемы. Базовый набор средств для этого – межсетевые экраны, системы предотвращения компьютерных атак, системы обнаружения вторжений, антивирусы и пр. Если указанные средства не сработали или были атакованы с фатальным исходом, то в большинстве случаев все также сведется к расследованию преступления.

В государственном масштабе кибербезопасность – важнейшая часть обеспечения информационной безопасности. И здесь основополагающим документом является Доктрина информационной безопасности Российской Федерации. В структуре основных информационных угроз, указанных в Доктрине, к сфере деятельности органов внутренних дел относятся незаконный трансграничный обмен информацией и информационно-психологическое воздействие на общество, отдельные группы социума, конкретного индивида.

Нарушение кибербезопасности осуществляется путем реализации компьютерных атак, под которыми в нашем случае будем понимать целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой информации [8]. В действующем правовом поле деятельность органов внутренних дел по обеспечению кибербезопасности в масштабах страны пока не определена. Информационная структура органов внутренних дел к объектам критической информационной инфраструктуры на данный момент *не относится*.

По своей уголовно-правовой и административной направленности, а также в соответствии с Федеральным законом от 07.02.2011 № 3-ФЗ «О полиции» прямое обеспечение кибербезопасности – не функциональная обязанность полиции, и рассматривать ее можно только с позиции собственной безопасности [23]. Реализацию функций ведомственного центра обнаружения, предупреждения и ликвидации последствий компьютерных атак осуществляет департамент информационных технологий, связи и защиты информации МВД России [21]. Обеспечение же кибербезопасности государства возложено на Федеральную службу безопасности России [12].

Ведомственная подследственность при расследовании преступлений в области информационно-телекоммуникационных технологий определяется статьей 151 УПК РФ. В соответсвии с пунктом 3 части 2 статьи 151 УПК РФ расследование киберпреступлений преимущественно осуществляют следственные органы МВД России [24]. Преступления, предусмотренные статьей 274.1 УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации», расследуют следователи органов ФСБ России. Таким образом, кибербезопасность в

части противодействия киберпреступности МВД России обеспечивает только для юридических и физических лиц, а противодействие киберпреступности в сфере государства – область деятельности ФСБ России.

2.7. Субъекты информационных отношений в деятельности подразделений МВД России и обеспечение их кибербезопасности

Информационные правоотношения, рассмотренные как система, представляют собой сложное явление, состоящее из различных элементов и структурных связей между ними. В общей теории правоотношений в качестве его элементов выделяют участников (субъектов), объект и содержание правоотношения. К основным субъектам информационного права относятся лица, участвующие в создании, преобразовании, передаче и распространении, получении и потреблении информации. Это прежде всего создатели или производители информации, обладатели информации, потребители информации.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать по каким-либо признакам доступ к информации [3].

Согласно статье 11 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции» органы внутренних дел могут в своей деятельности использовать достижения науки и техники, современных технологий и информационных систем, а именно:

- полиция в своей деятельности использует достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру;
- полиция в порядке, установленном законодательством Российской Федерации, применяет электронные формы приема и регистрации документов, уведомления о ходе предоставления государственных услуг, взаимодействия с другими правоохранительными органами, государственными и муниципальными органами, общественными объединениями и организациями;
- полиция использует технические средства, включая средства аудио-, фото- и видеофиксации, при документировании обстоятельств совершения преступлений, административных правонарушений, обстоятельств происшествий, в том числе – в общественных местах, а также для фиксирования действий сотрудников полиции, выполняющих возложенные на них обязанности;
- федеральный орган исполнительной власти в сфере внутренних дел обеспечивает полиции возможность использования информационно-

телекоммуникационной сети Интернет, автоматизированных информационных систем, интегрированных банков данных [23].

Также стоит отметить, что органы внутренних дел являются субъектами оперативно-розыскной деятельности. Согласно Федеральному закону от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» органы, осуществляющие оперативно-розыскную деятельность, для решения задач, возложенных на них настоящим Законом, могут создавать и использовать информационные системы, а также заводить дела оперативного учета.

Обозначенные направления деятельности подчеркивают важнейшую роль информационных подразделений в системе МВД России. Основой функционирования информационного подразделения МВД России является распоряжение Правительства РФ от 19 августа 2011 г. № 1474-р «О создании федерального казенного учреждения «Главный информационно-аналитический центр Министерства внутренних дел Российской Федерации».

Предметом и целями деятельности Главного информационно-аналитического центра Министерства внутренних дел Российской Федерации являются:

- централизованное информационное обеспечение в установленном порядке подразделений МВД России, органов государственной власти Российской Федерации, органов местного самоуправления, компетентных органов иных государств оперативно-справочными, оперативными, розыскными, криминалистическими, дактилоскопическими, статистическими, архивными сведениями, сведениями, содержащимися в информационных системах и банках данных в сфере миграции;
- формирование и ведение централизованных учетов, баз данных оперативно-справочной, розыскной, криминалистической, дактилоскопической, статистической и иной информации;
- формирование архивных фондов, осуществление учета, хранения, экспертизы научной и практической ценности, научно-технической обработки архивных документов, образовавшихся в деятельности служб центрального аппарата МВД (МООП) СССР, МВД (МООП) РСФСР, МВД СССР, МВД России и территориальных органов внутренних дел Российской Федерации;
- оказание услуг в целях обеспечения реализации предусмотренных законодательством Российской Федерации полномочий МВД России;
- обеспечение эксплуатации единой системы информационно-аналитического обеспечения деятельности МВД России;
- обеспечение эксплуатации и технической поддержки информационных систем и банков данных в сфере миграции [25].

Функции по обеспечению информационной безопасности и кибербезопасности как ее элемента обозначены в Уставе федерального

казенного учреждения «Главный информационно-аналитический центр МВД России».

Учреждение проводит работы, связанные с использованием сведений, составляющих государственную и служебную тайну, а также с защитой государственной и служебной тайны в соответствии с законодательными и иными нормативными правовыми актами Российской Федерации, нормативными правовыми актами МВД России, лицензиями, полученными в установленном порядке. Допуск учреждения к проведению работ, связанных с использованием сведений, составляющих государственную тайну, эксплуатацией средств защиты информации, а также реализацией мероприятий по защите государственной тайны, осуществляется путем получения им в порядке, установленном Правительством Российской Федерации, лицензии на проведение работ со сведениями, составляющими государственную тайну.

Обеспечение защиты персональных данных, содержащихся в информационных системах и базах данных ФКУ «ГИАЦ МВД России», осуществляется в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Кроме того, ГИАЦ МВД России обязано осуществлять обеспечение режима секретности, защиту сведений, составляющих государственную и иную охраняемую законом тайну, в том числе – с использованием криптографических средств, ведение шифровальной работы.

Выработка и реализация государственной политики по нормативному правовому регулированию в области совершенствования информационных и телекоммуникационных технологий, автоматизированных информационных систем, систем и средств связи, обеспечения электромагнитной совместимости радиоэлектронных средств, противодействия иностранным техническим разведкам, технической и криптографической защиты информации, использования электронной подписи, организации применения и эксплуатации робототехнических комплексов и беспилотных воздушных судов, формирования и ведения информационных ресурсов, межведомственного информационного взаимодействия, реализации государственных программ Российской Федерации, федеральных целевых программ и ведомственных целевых программ (ведомственных проектов), а также программ (мероприятий и проектов) Союзного государства, национальных проектов (программ) и федеральных проектов в области информатизации и навигационно-информационных систем органов внутренних дел, организаций и подразделений, созданных для выполнения задач и осуществления полномочий, возложенных на МВД России, осуществляет Департамент информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации (ДИТСиЗИ МВД России) [21].

2.8. Нормативное правовое регулирование, кадровое и организационное обеспечение органов внутренних дел в сфере кибербезопасности

Ведомственная регламентация кибербезопасности в органах внутренних дел на данный момент не имеет прямых документов, однако если рассматривать ее как элемент информационной безопасности, то сегодня сложилась определенная нормативно-правовая архитектура. Нормативные правовые акты МВД России в области защиты информации и особенностей эксплуатации собственных информационных систем условно делятся на открытые и ограниченного доступа (распространения). В данном разделе рассмотрены документы, не содержащие охраняемую законом информацию.

Обеспечение кибербезопасности строится на основе безопасности информационных ресурсов МВД России. В данный момент в органах внутренних дел можно выделить обобщенный информационный ресурс ИСОД МВД России и 470 отдельных информационных систем, разрешенных к эксплуатации в территориальных органах, организациях и подразделениях системы МВД России (письмо ДИТСиЗИ МВД России от 19.01.22 № 9/383).

ИСОД МВД России представляет собой совокупность используемых в Министерстве автоматизированных систем обработки информации, программно-аппаратных комплексов и программно-технических средств, а также систем связи и передачи данных, необходимых для обеспечения деятельности МВД России. Основу защиты информации ИСОД МВД России составляет сервис управления доступом к информационным ресурсам и системам (далее – СУДИС).

Нормативно-правовая основа эксплуатации и обеспечения защиты информации ИСОД МВД России – это приказ МВД России от 10 апреля 2015 г. № 016 «Вопросы организации эксплуатации единой системы информационно-аналитического обеспечения деятельности МВД России».

Стоит отметить, что ИСОД МВД России и отдельные информационные системы предназначены для обработки персональных данных и отдельными своими элементами являются государственной информационной системой. Соответственно, в вопросах защиты информации и, в частности, обеспечения кибербезопасности необходимо руководствоваться следующими основными документами:

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

Постановление Правительства РФ от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Приказ ФСТЭК России от 11 февраля 2013 г. № 17 (ред. от 28.05.2019)

«Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

Приказ ФСТЭК России от 18 февраля 2013 г. № 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

В органах внутренних дел значительное количество нормативных правовых актов посвящено обеспечению безопасности информации в автоматизированных системах.

Основной перечень этих документов представлен ниже:

Приказ МВД России от 2 сентября 2021 г. № 656 «Вопросы организации эксплуатации сервиса по использованию централизованных оперативно-справочных, криминалистических и розыскных учетов органов внутренних дел Российской Федерации при предоставлении государственных услуг, в том числе в электронной форме»;

Приказ МВД России от 15 июня 2021 г. № 444 «Об утверждении Положения о Департаменте информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации»;

Распоряжение МВД России от 29 декабря 2020 г. № 1/15065 (ред. от 08.09.2021) «Об утверждении Ведомственной программы цифровой трансформации МВД России на 2021 – 2023 годы»;

Приказ МВД России от 13 января 2020 г. № 3 «О некоторых вопросах обработки персональных данных в МВД России»;

Приказ МВД России от 26 февраля 2018 г. № 109 «О порядке подготовки и размещения информации о деятельности Министерства внутренних дел Российской Федерации в информационно-телекоммуникационной сети Интернет»;

Приказ МВД России от 9 ноября 2018 г. № 755 «О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе МВД России (вместе с Инструкцией по организации деятельности по обращению со служебной информацией ограниченного распространения в системе МВД России);

Приказ МВД России от 5 февраля 2016 года № 60 «О порядке эксплуатации специального программного обеспечения федеральной информационной системы Госавтоинспекции»;

Приказ МВД России от 29 декабря 2016 г. № 925 «О некоторых вопросах обработки персональных данных в МВД России»;

Приказ МВД России от 24 декабря 2015 г. № 1228 «Об утверждении правил организации доступа к информационно-телекоммуникационной сети Интернет в органах внутренних дел Российской Федерации»;

Приказ МВД России от 16 января 2012 г. № 25 «Об утверждении Комплекса мер по обеспечению информационной безопасности и защиты данных информационных систем МВД России с учетом реализации «облачной архитектуры»;

Приказ МВД России от 14 марта 2012 г. № 169 «Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года»;

Приказ МВД России от 6 июля 2012 г. № 678 «Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации»;

Распоряжение Правительства РФ от 19 августа 2011 г. № 1474-р «О создании федерального казенного учреждения “Главный информационно-аналитический центр Министерства внутренних дел Российской Федерации”»

Приказ МВД России от 16 июня 2010 года № 437 «Об утверждении Устава федерального государственного казенного учреждения “Экспертно-криминалистический центр Министерства внутренних дел Российской Федерации”».

Министерство внутренних дел Российской Федерации осуществляет деятельность по обеспечению кибербезопасности государства, общества, личности, заключающуюся в борьбе с преступностью в информационном пространстве (криминальные угрозы, экстремизм и терроризм).

Важным направлением работы ОВД является обеспечение кибербезопасности страны, противодействие совершению преступлений в сфере компьютерной информации и международное сотрудничество в области борьбы с преступлениями, совершаемыми с использованием информационных и компьютерных технологий. В МВД России данной сферой занимается управление «К».

Управление «К» МВД России в пределах своей компетенции осуществляет выявление, предупреждение, пресечение и раскрытие следующих преступлений.

1. *Преступления в сфере компьютерной информации*:

- неправомерный доступ к охраняемой законом компьютерной информации;
- создание, использование и распространение вредоносных компьютерных программ;
- нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации либо информационно-телекоммуникационных сетей;
- мошенничество в сфере компьютерной информации.

2. *Преступления, совершаемые с использованием информационно-телекоммуникационных сетей* (включая сеть Интернет) *и направленные против здоровья несовершеннолетних и общественной нравственности:*

- изготовление и распространение материалов или предметов с порнографическими изображениями несовершеннолетних;
- использование несовершеннолетнего в целях изготовления порнографических материалов или предметов.

3. *Преступления, связанные с незаконным оборотом специальных*

технических средств, *предназначенных для негласного получения информации.*

4. *Преступления, связанные с незаконным использованием объектов авторского права или смежных прав* [20].

Департамент информационных технологий, связи и защиты информации, а также центры информационных технологий, связи и защиты информации в субъектах Российской Федерации осуществляют организацию и координацию межведомственного информационного взаимодействия, в том числе участвуют в организации межгосударственного информационного взаимодействия по вопросам деятельности ДИТСиЗИ; осуществляют контроль за созданием государственных информационных систем; координацию работ по использованию средств обеспечения информационной безопасности и информационных технологий, применяемых в органах, организациях и подразделениях системы МВД России.

Департамент выполняет функции головного подразделения министерства в области:

- совершенствования информационных и телекоммуникационных технологий, разработки и развития автоматизированных информационных систем, систем и средств связи;
- радио- и радиотехнического контроля, радиоэлектронной борьбы;
- шифрованной связи;
- противодействия иностранным техническим разведкам, технической и криптографической защиты информации, использования электронной подписи;
- организации применения и эксплуатации робототехнических комплексов и беспилотных воздушных судов;
- межведомственного информационного взаимодействия;
- координации и контроля деятельности по защите персональных данных при их автоматизированной обработке в системе МВД России;
- реализации функций центрального шифровального органа министерства и ведомственного центра обнаружения, предупреждения и ликвидации последствий компьютерных атак;
- реализации государственных программ Российской Федерации, федеральных целевых программ и ведомственных проектов, а также программ (мероприятий и проектов) Союзного государства, национальных проектов (программ) и федеральных проектов в области информатизации и навигационно-информационных систем;
- реализации государственной политики в сфере международной информационной безопасности, в работе по нормативному правовому регулированию указанной сферы в пределах компетенции [21].

Главное управление по противодействию экстремизму Министерства внутренних дел Российской Федерации является самостоятельным структурным подразделением, входящим в центральный аппарат Министерства внутренних дел Российской Федерации. В пределах своей

компетенции оно осуществляет функции по выработке и реализации государственной политики и нормативному правовому регулированию, а также правоприменительные полномочия в области противодействия экстремистской деятельности и терроризму.

Главное управление является головным оперативным подразделением Министерства в сфере противодействия экстремистской деятельности и терроризму, в том числе и в информационно-телекоммуникационных сетях.

Помимо перечисленного можно выделить иные подразделения и службы МВД России, занимающиеся некоторыми вопросами обеспечения информационной безопасности при межгосударственном взаимодействии, однако данные функции для них не являются приоритетными и выполняются только в части, их касающейся, например, ГУРЛС, Управление по взаимодействию с институтами гражданского общества и средствами массовой информации (УОС), НЦБ Интерпола, Научно-производственное объединение «Спецтехника и Связь» (ФКУ НПО «СТиС») и др.

Согласно Доктрине информационной безопасности Российской Федерации, компьютерные преступления являются угрозой информационной безопасности РФ. В Доктрине отмечен рост масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере, повышение числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий [6].

Следует отметить, что на расширенном заседании коллегии Министерства внутренних дел Российской Федерации министр МВД России обозначил, что подготовка специалистов для IT-подразделений системы МВД России осуществляется в ведомственных образовательных организациях, в том числе – во взаимодействии с профильными вузами страны [27].

Ведущим вузом здесь выступает Московский университет МВД России имени В. Я. Кикотя. На протяжении нескольких лет в рамках специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере в университете готовят сотрудников по направлению специализации «Компьютерная экспертиза» и узкой специализации «Оперативно-техническое обеспечение раскрытия и расследования киберпреступлений».

Специфика противодействия киберпреступности требует углубленных знаний для правоохранительной деятельности участников процессуальных действий и оперативно-розыскной деятельности. Так, с 2021 года Московский университет МВД России имени В. Я. Кикотя организует набор курсантов по специальности 40.05.01 уголовно-правовой специализации по профилю образовательной программы

«Предварительное следствие в органах внутренних дел по уголовным делам в отношении лиц, совершивших преступления с использованием информационно-телекоммуникационных технологий». Также осуществляется набор по специальности 40.05.02 с последующей специализацией «Оперативно-розыскная деятельность» и профилем образовательной программы «Деятельность оперуполномоченного уголовного розыска, осуществляющего выявление, предупреждение, пресечение и раскрытие преступлений, совершаемых с использованием информационно-телекоммуникационных технологий». Следователи и оперуполномоченные с таким образованием позволят повысить качество процессуальных действий по киберпреступлениям.

Многолетний опыт подготовки технических специалистов имеет Воронежский институт МВД России. Традиционно образовательной организацией готовятся выпускники по специальности 10.05.02 Информационная безопасность телекоммуникационных систем. В период с 2003 по 2020 год институтом выпущено более 800 квалифицированных специалистов этого направления. Стоит отметить, что с 2020 года в институте действует кафедра компьютерной безопасности и технической экспертизы, являющаяся выпускающей по специальности 10.05.01 Компьютерная безопасность.

В ряду образовательных организаций, реализующих образовательные программы по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере, находятся также Краснодарский и Санкт-Петербургский университеты МВД России.

Академия управления МВД России на постоянной основе проводит обучающие семинары, встречи со специалистами и повышение квалификации по вопросам выявления, раскрытия и расследования преступлений, совершенных с использованием информационно-коммуникационных технологий.

Важное место в системе подготовки кадров в области борьбы с киберпреступностью занимает дополнительное профессиональное образование. В ВИПК МВД России и его филиалах ежегодно проходят повышение квалификации, профессиональную переподготовку, профессиональную подготовку порядка 9000 сотрудников органов внутренних дел Российской Федерации и Росгвардии по более чем 180 образовательным программам; иностранные специалисты по таким ключевым международно-значимым направлениям, как борьба с терроризмом и экстремизмом, обеспечение транспортной безопасности, борьба с незаконным оборотом наркотиков, противодействие незаконной (нелегальной) миграции, участие в миротворческих миссиях.

Обеспечение кибербезопасности в современных условиях базируется на основе сложной архитектуры информационно-телекоммуникационного оборудования, которое требует дополнительных мер защиты. В предыдущих разделах определено, что кибербезопасность в структуре нормативных правовых актов Российской Федерации на данный момент

является составной частью информационной безопасности.

Законодательная база информационной безопасности Российской Федерации сегодня имеет сложную иерархию по разным направлениям, подведомственности, масштабам, виду информации ограниченного доступа и т.д.

По последним оценкам, существует более 100 различных нормативных правовых актов и иной официальной правовой информации (международные стандарты и акты, государственные стандарты, нормативная методическая документация и т.п.) в области информационной безопасности и защиты информации.

Почти все государственные организации Российской Федерации входят в правовую систему информационной безопасности. В разные периоды формирования правовой системы информационной безопасности существовали так называемые регуляторы, среди которых Федеральное агентство правительственной связи и информации при Президенте Российской Федерации, Гостехкомиссия России, которые на данный момент уже не существуют, однако отдельные документы в области информационной безопасности этих организаций используются. Принято считать, что направление криптографической защиты информации – это область регулирования ФСБ России, а техническая защита информации (без использования криптографии) – область ФСТЭК России.

Стратегическим документом в России, несомненно, является Доктрина информационной безопасности. В 2000 году Президентом России утверждена первая Доктрина информационной безопасности, которая после достаточно долгих обсуждений в конце 2016 г. была заменена Указом Президента РФ от 5 декабря 2016 г. № 646.

В новой Доктрине на основе анализа основных информационных угроз и оценки состояния информационной безопасности определены стратегические цели и ключевые направления обеспечения информационной безопасности с учетом стратегических национальных приоритетов Российской Федерации. Обозначенный нормативный правовой акт является основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения информационной безопасности.

Основные документы, регламентирующие сферу информационной безопасности в Российской Федерации в целом и кибербезопасности, в частности, приведены в приложении 1.

Контрольные вопросы:

1. Назовите основные принципы стратегии развития информационного общества в Российской Федерации.
2. Охарактеризуйте направления деятельности по реализации государственной программы Российской Федерации «Информационное общество»
3. Какие федеральные проекты входят в состав Национальной программы «Цифровая экономика Российской Федерации»?
4. Назовите основные киберугрозы.
5. Определите состав системы обеспечения информационной безопасности Российской Федерации.
6. Какова организационная основа системы обеспечения информационной безопасности Российской Федерации?
7. Представьте структуру федеральных органов, осуществляющих функции обеспечения информационной безопасности Российской Федерации.
8. Каковы основные функции ГосСОПКА?
9. Назовите основные угрозы международной информационной безопасности.
10. Дайте общее представление деятельности МВД России в области обеспечения кибербезопасности.
11. Дайте характеристику субъектов информационных отношений в МВД России.
12. Дайте общую характеристику нормативного правового регулирования в органах внутренних дел по обеспечению кибербезопасности.
13. Назовите функции и органы МВД России по обеспечению кибербезопасности.
14. Охарактеризуйте систему подготовки кадров в МВД России в области борьбы с киберпреступностью.

Литература к главе 2

1. Боброва, Ю. М. Государственная политика в области информатизации и использования информационных технологий в органах государственной власти: конспект лекции / Ю. М. Боброва. – Санкт-Петербург: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2020. – 32 с. – Текст: непосредственный.

2. Попов, В. Д. Информационная политика: учебник / В. Д. Попов. – М.: Издательство РАГС, 2003. – 467 с. – ISBN 5-7729-0148-6. – EDN SUEVQZ. – Текст: непосредственный.

3. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ // Собрание

законодательства Российской Федерации. – 2006. – № 31, ч. 1. – Ст. 3448. 4. – Текст: непосредственный.

4. О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы: Указ Президента Российской Федерации от 9 мая 2017 года № 203. – Москва, 2017. – 2, 27 листов. – Текст: непосредственный.

5. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 5 декабря 2016 № 646. – Москва, 2016. – 1, 16 листов. – Текст: непосредственный.

6. Об утверждении государственной программы Российской Федерации «Информационное общество» // Постановление Правительства РФ от 15 апреля 2014 г. № 313

7. Сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: https://digital.gov.ru/ru/activity/directions/858/.

8. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ.

9. Что такое кибербезопасность? URL: https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security.

10. Топ угроз ИБ в корпоративных сетях, 2021 URL: https://www.ptsecurity.com/ru-ru/research/analytics/top-ugroz-ib-v-korporativnyh-setyah-2021/.

11. Основы информационной безопасности в органах внутренних дел: учебное пособие / А. Б. Сизоненко, С. Г. Клюев, В. Н. Цимбал. – Краснодар: Краснодарский университет МВД России, 2018. – 222 с.

12. Указ Президента РФ от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

13. Указ Президента РФ от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

14. Развертывание центра мониторинга ГосСОПКА в Республике Крым URL: https://cyberseclab.ru/gossopka/.

15. Выписка из «Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (Утв. Президентом РФ 12.12.2014 N К 1274).

16. Указ Президента Российской Федерации от 22.12.2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

17. Построение центра ГосСОПКА Комплексное решение для создания центра ГосСОПКА и взаимодействия с НКЦКИ URL:

https://www.ptsecurity.com/ru-ru/solutions/center-gossopka/.

18. Указ Президента РФ от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности».

19. Соглашение о сотрудничестве государств - членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности от 30 ноября 2017 года (вступило в силу для Российской Федерации 17 апреля 2019 года).

20. Сайт Управления «К» МВД России URL: https://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii/Pamjatka_Upravlenie_K_preduprezhdaet.

21. Приказ МВД России от 15.06.2021 № 444 (ред. от 28.12.2021) «Об утверждении Положения о Департаменте информационных технологий, связи и защиты информации Министерства внутренних дел Российской Федерации».

22. ГОСТ Р 56205-2014 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели».

23. Федеральный закон «О полиции» от 07.02.2011 № 3-ФЗ.

24. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ.

25. Распоряжение Правительства РФ от 19 августа 2011 г. N 1474-р “О создании федерального казенного учреждения «Главный информационно-аналитический центр Министерства внутренних дел Российской Федерации».

26. Устав федерального казенного учреждения «Главный информационно-аналитический центр МВД России».

27. Выступление Министра внутренних дел Российской Федерации генерала полиции Российской Федерации Владимира Колокольцева на расширенном заседании коллегии Министерства внутренних дел Российской Федерации. URL: https://xn--b1aew.xn--p1ai/news/item/23305248/.

Глава 3. Принципы обеспечения компьютерной безопасности

3.1. Принципы обеспечения безопасности устройств на базе операционных систем семейства Windows

3.1.1. Версии операционных систем

Первые компьютеры не имели современных запоминающих устройств, таких как жесткие диски, оптические накопители или флэш-накопители. Первые методы хранения данных использовали перфокарты, бумажную ленту, магнитную ленту и аудиокассеты [1].

Предшественником операционной системы Windows была операционная система DOS. Компания Microsoft выкупила DOS и разработала MS-DOS. В MS-DOS в качестве интерфейса для создания программ и работы с файлами данных использовалась командная строка [2]. Некоторые команды приведены в таблице 3.1.1.

Ранние версии Windows состояли из графического интерфейса пользователя (GUI), который работал под управлением MS-DOS, а первой была Windows 1.0, в 1985 году.

Сегодня многие задачи, которые раньше выполнялись через интерфейс командной строки MS-DOS (рис. 3.1.1), могут быть выполнены в графическом интерфейсе пользователя Windows [3, 4].

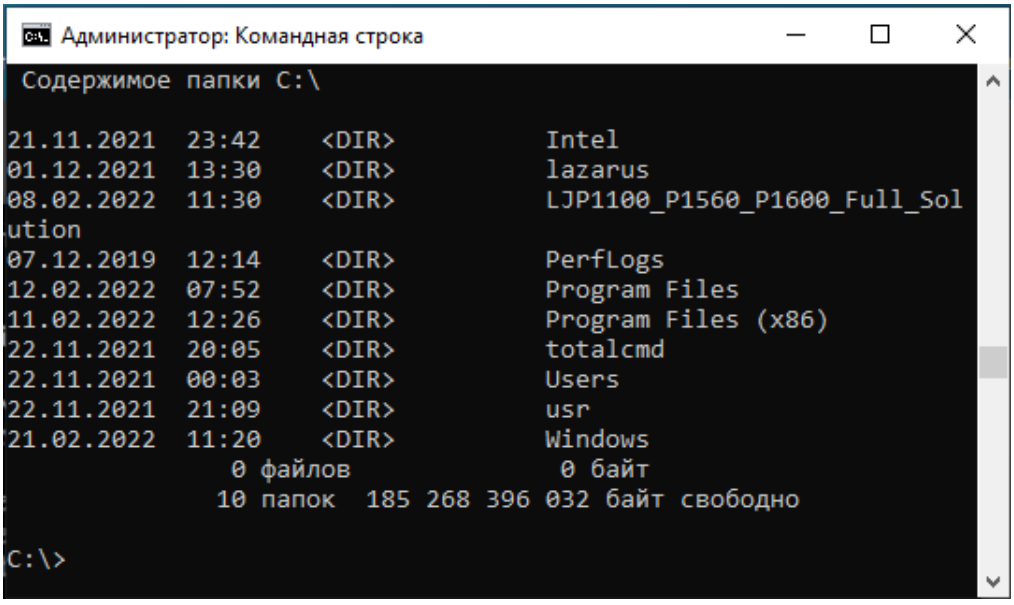


Рис. 3.1.1. Вид командной строки Windows

Ниже перечислены некоторые команды, которые можно использовать.

Таблица 3.1.1
Некоторые команды режима командной строки ОС Windows

Команда	Описание
dir	отображение списков всех файлов в текущем каталоге
cd каталог	изменение текущего каталога на указанный каталог
cd..	изменение текущего каталога на каталог уровнем выше текущего
cd	изменение текущего каталога на корневой (часто C:)
copy	копирование файлов в другое местоположение
del	удаление одного или нескольких файлов
find	поиск текста в файлах
mkdir	создание нового каталога
ren	переименование файла

С 1993 года было выпущено более 20 версий Windows на основе операционной системы NT.

Начиная с Windows XP стали доступы 64-разрядные версии ОС. 64-разрядная операционная система имела совершенно новую архитектуру. У нее было 64-разрядное адресное пространство вместо 32-разрядного. Это не просто вдвое больше места (поскольку эти биты представляют двоичные числа). В то время как 32-разрядная Windows может использовать чуть меньше 4 ГБ ОЗУ, 64-разрядная Windows теоретически может использовать 16,8 миллиона терабайт.

В Windows 7 было шесть различных версий, в Windows 8 – пять, а в Windows 10 – восемь. Каждая версия не только предлагает разные возможности, но и стоит по-разному.

Достаточно полный перечень операционных систем семейства Windows, выпускавшихся в период 1993–2021 гг. показан в таблице 3.1.2.

Таблица 3.1.2
Версии ОС Windows

ОС	Версии
Windows 7	Starter, Home Basic, Home Premium, Professional, Enterprise, Ultimate
Windows Server 2008 R2	Foundation, Standard, Enterprise, Datacenter, Web Server, HPC Server, системы на основе Itanium
Windows Home Server 2011	None
Windows 8	Windows 8, Windows 8 Pro,

ОС	Версии
	Windows 8 Enterprise, Windows RT
Windows Server 2012	Foundation, Essentials, Standard, Datacenter
Windows 8.1	Windows 8.1, Windows 8.1 Pro, Windows 8.1 Enterprise, Windows RT 8.1
Windows Server 2012 R2	R2 Foundation, Essentials, Standard, Datacenter
Windows 10	Home, Pro, Pro Education, Enterprise, Education, loT Core; Mobile, Mobile Enterprise
Windows Server 2016	Essentials, Standard, Datacenter, Multipoint Premium Server, Storage Server, Hyper-V Server
Windows 11	Home, Pro, Pro Education, Enterprise, Education, loT Core; Mobile, Mobile Enterprise
Windows Server 2019	Essentials, Standard, Datacenter, Multipoint Premium Server, Storage Server, Hyper-V Server

Графический интерфейс (GUI) пользователя Windows

В Windows для работы с файлами данных и программным обеспечением предусмотрен графический интерфейс пользователя (GUI). Основная область графического интерфейса называется «Рабочий стол» (рис. 3.1.2).

В нижней части рабочего стола находится панель задач. На панели задач имеются три области, которые используются для разных целей. Слева – меню «Пуск». Оно используется для доступа ко всем установленным программам, параметрам конфигурации и функции поиска. В центральной части панели задач пользователи размещают значки быстрого запуска, которые запускают определенные программы или открывают определенные папки при нажатии. Наконец, в правой части панели задач находится область уведомлений. В области уведомлений представлен краткий обзор функциональных возможностей множества различных программ и функций. Например, мигающая пиктограмма конверта может указывать на новое электронное сообщение, а пиктограмма сети с красным значком x может указывать на проблему с сетью.

Часто щелчок правой кнопкой мыши по какому-либо значку вызывает дополнительные функции, которые можно использовать. Этот

список называется «Контекстное меню». Существуют контекстные меню для значков в области уведомлений, а также для значков быстрого запуска, значков конфигурации системы, а также для файлов и папок.

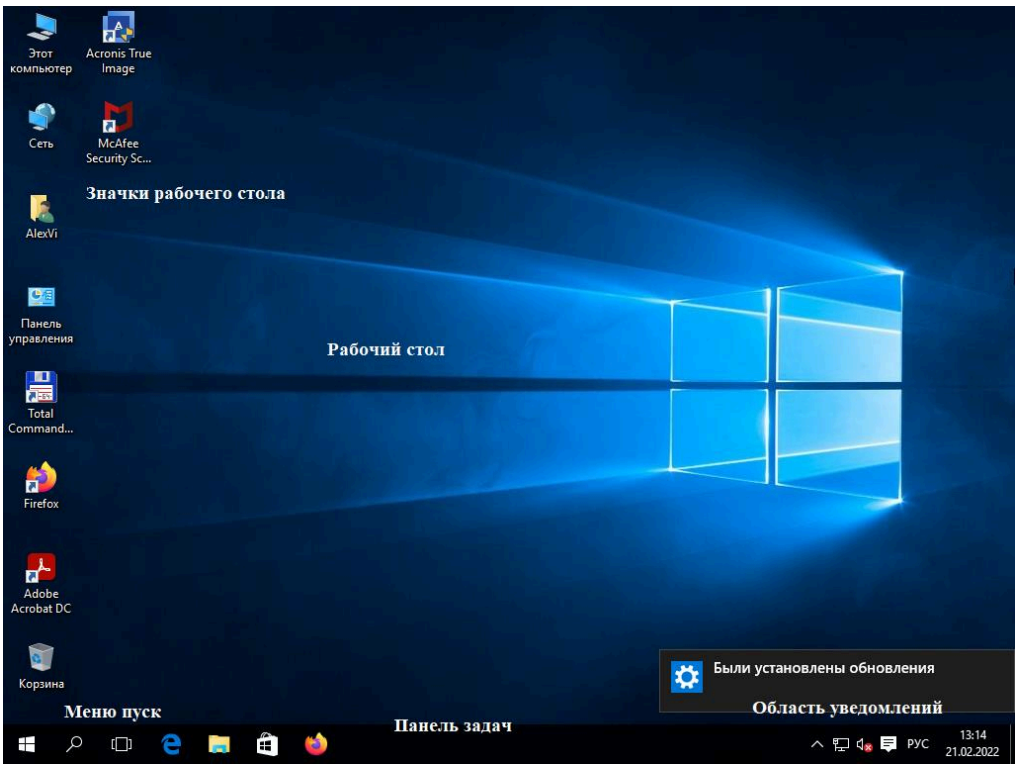


Рис. 3.1.2. Вид рабочего стола ОС Windows

Проводник Windows, показанный на рис. 3.1.3, представляет собой инструмент, используемый для навигации по всей файловой системе компьютера.

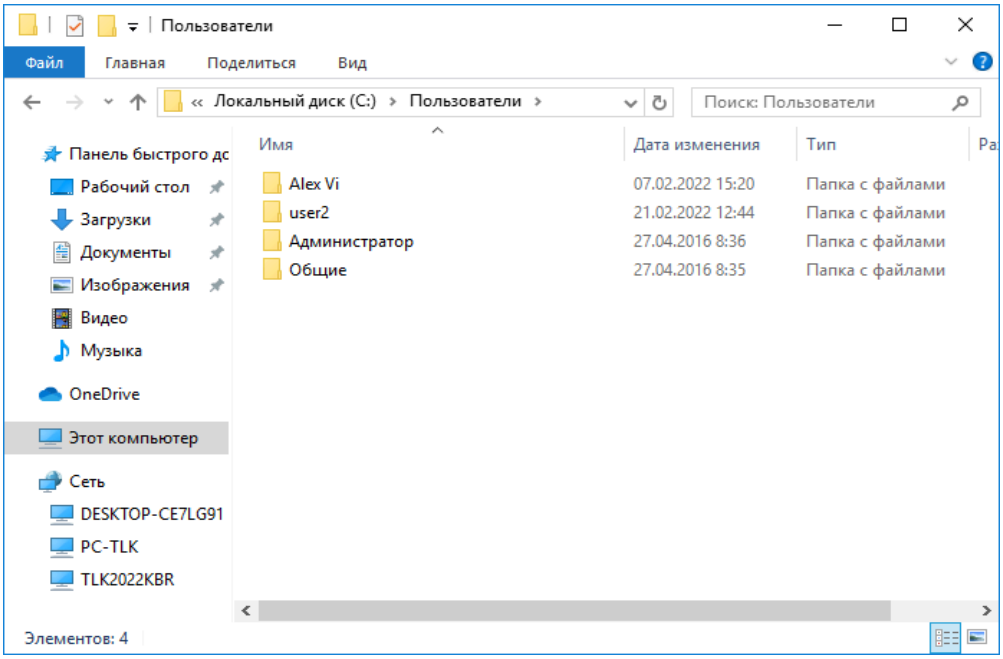


Рис. 3.1.3. Вид проводника ОС Windows

3.1.2. Базовая архитектура

Компьютеры Windows используют множество разных типов аппаратного обеспечения. Когда операционная система устанавливается, она не должна зависеть от возможных различий в аппаратном обеспечении. Базовая архитектура Windows показана на рис. 3.1.4. Уровень абстракции аппаратного обеспечения (HAL) – это код, который обрабатывает весь обмен данными между аппаратным обеспечением и ядром. Ядро лежит в основе операционной системы и контролирует компьютер в целом.

Существует два различных режима работы ЦП компьютера с установленной ОС Windows: пользовательский режим и режим ядра. Установленные приложения выполняются в пользовательском режиме, а код операционной системы – в режиме ядра (рис. 3.1.5).

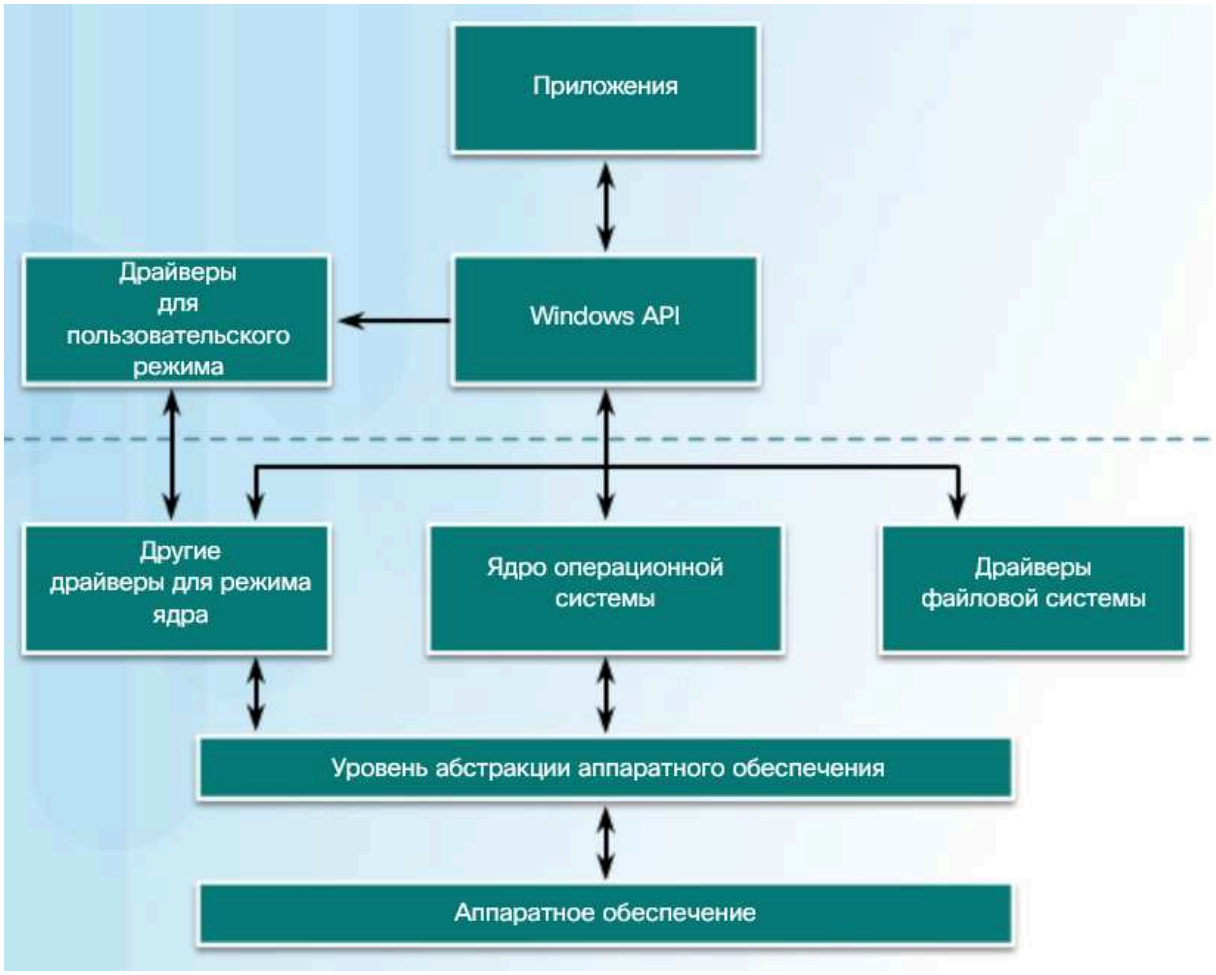


Рис. 3.1.4. Базовая архитектура ОС Windows

Код, который выполняется в режиме ядра, имеет неограниченный доступ к базовому аппаратному обеспечению и способен выполнять любые инструкции CPU. Код режима ядра также может ссылаться на любой адрес памяти напрямую. Для наиболее критичных функций ОС в коде,

работающем в режиме ядра, предусмотрена возможность сбоя, останавливающего работу всего компьютера. И наоборот, такие программы, как пользовательские приложения, работают в пользовательском режиме и не имеют прямого доступа к аппаратному обеспечению или ячейкам памяти.

Весь код, который выполняется в режиме ядра, использует одно и то же адресное пространство. Драйверы режима ядра не изолируются от операционной системы. В случае ошибки драйвера, работающего в режиме ядра, которая привела к записи данных в неправильное адресное пространство, может быть нарушена работа операционной системы или другого драйвера режима ядра. В этом случае может произойти сбой драйвера, что приведет к сбою всей операционной системы.

Когда выполняется код в пользовательском режиме, ядро предоставляет ему отдельное ограниченное адресное пространство, а также процесс, созданный специально для этого приложения. Это делается для того, чтобы приложения не могли изменить код операционной системы, который выполняется параллельно. Благодаря собственному процессу приложение получает свое собственное закрытое адресное пространство, что не позволяет другим приложениям изменять данные в нем. Это также помогает предотвратить сбой операционной системы и других приложений в случае сбоя данного приложения.

3.1.3. Файловые системы и риски безопасности

Одной из основных составляющих операционных систем семейства Windows является файловая система. Файловая система указывает, каким образом информация организована на носителе. Некоторые файловые системы могут быть удобнее по сравнению с другими в зависимости от типа носителя, который будет использоваться. Ниже перечислены файловые системы, поддерживаемые Windows.

- **Таблица размещения файлов (File Allocation Table, FAT)** –FAT имеет ограничения по количеству разделов, размерам разделов и размерам файлов, которые она может адресовать, поэтому она обычно не используется для жестких дисков (HD) и твердотельных накопителей (SSD).
- **exFAT** – это расширенная версия FAT, которая имеет еще меньше ограничений, чем FAT32, но редко поддерживается за пределами Windows.
- **Иерархическая файловая система Plus (Hierarchical File System Plus, HFS+)** – эта файловая система используется на компьютерах с MAC OC X, она позволяет использовать гораздо более длинные имена файлов, Windows может считывать данные с разделов HFS+.
- **Расширенная файловая система (Extended File System, EXT)** – эта файловая система используется с компьютерами на базе Linux. Хотя

она не поддерживается Windows, Windows может считывать данные из разделов EXT с помощью специального программного обеспечения.

- **Файловая система новой технологии (New Technology File System, NTFS)** – это наиболее часто используемая файловая система в Windows. NTFS является наиболее широко используемой файловой системой для Windows по множеству причин. NTFS поддерживает большие файлы и разделы, а также хорошо совместима с другими операционными системами. NTFS также очень надежна и поддерживает функции восстановления. Разграничение доступа к данным осуществляется через дескрипторы безопасности. Эти дескрипторы безопасности содержат информацию о владельце файла и разрешениях вплоть до уровня файла. NTFS также отслеживает метки времени различных событий, позволяя контролировать операции с файлом. Метки времени MACE (Modify, Access, Create, Entry Modified) часто используются при расследованиях для определения истории файла или папки. NTFS также поддерживает шифрование файловой системы, позволяя защитить носитель целиком.

NTFS хранит файлы в виде ряда атрибутов, таких как имя файла или метка времени. Данные, содержащиеся в файле, хранятся в атрибуте $DATA и называются потоком данных. С помощью NTFS можно подключить альтернативные потоки данных (ADS) к файлу. Это иногда используется приложениями, которые хранят дополнительную информацию о файле. ADS является важным фактором при обсуждении вредоносных программ. Это связано с тем, что данные весьма просто скрыть в ADS. Злоумышленник может сохранить вредоносный код в ADS, а затем вызвать его из другого файла.

Форматирование NTFS создает важные структуры на диске для хранения файлов и таблицы для записи расположения файлов.

- **Загрузочный сектор** – это первые 16 секторов диска. Он содержит местоположение основной таблицы файлов (MFT). Последние 16 секторов содержат копию загрузочного сектора.
- **MFT** – эта таблица содержит местоположение всех файлов и каталогов в разделе, включая такие атрибуты файлов, как информация о безопасности и метки времени.
- **Системные файлы** – это скрытые файлы, в которых хранится информация о других томах и атрибутах файлов.
- **Область файлов** – это основная область раздела, где хранятся файлы и каталоги.

Нередко при форматировании раздела существовавшие данные по-прежнему можно восстановить, поскольку не все данные полностью удаляются. Существует принципиальная возможность просмотреть свободное пространство и считать файлы, которые могут скомпрометировать безопасность. В этой связи для повторного

использования диска рекомендуется выполнить его безопасную очистку. Безопасная очистка должна будет перезаписывать данные на весь диск несколько раз, чтобы гарантировать отсутствие оставшихся данных.

3.1.4. Основные этапы работы операционной системы и уязвимости управления безопасностью

Между моментом нажатия кнопки питания компьютера и полной загрузкой Windows выполняется много операций, как показано на рис. 3.1.5.

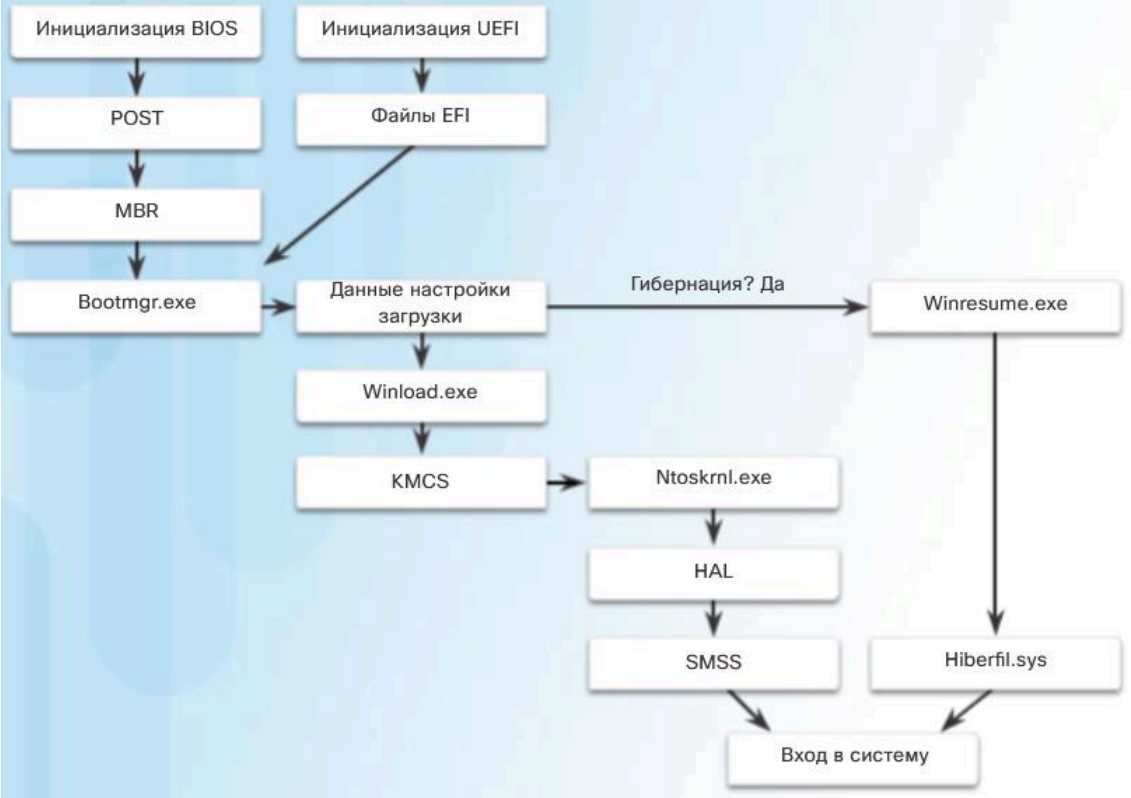


Рис. 3.1.5. Процесс загрузки ОС Windows

Существуют два типа микропрограммного обеспечения компьютера: базовая система ввода-вывода (BIOS) и единый расширяемый микропрограммный интерфейс (UEFI). Микропрограммное обеспечение BIOS было создано в начале 1980-х годов, и с той поры его работа не изменилась. UEFI был разработан для замены BIOS и поддерживает новые функции.

В микропрограммном обеспечении BIOS процесс начинается с этапа инициализации BIOS [5]. Это происходит, когда аппаратные устройства инициализируются и выполняется самотестирование при включении питания (POST), чтобы убедиться, что все эти устройства могут обмениваться данными. При обнаружении системного диска фаза POST заканчивается. Последняя инструкция в POST – поиск основной

загрузочной записи (MBR).

В отличие от микропрограммного обеспечения BIOS микропрограммное обеспечение UEFI позволяет точнее контролировать процесс загрузки. UEFI загружается путем загрузки программных файлов EFI, хранящихся в виде файлов .efi в специальном разделе диска, известном как системный раздел EFI (ESP).

На компьютере, использующем UEFI, загрузочный код хранится в микропрограммном обеспечении. Это позволяет повысить безопасность компьютера во время загрузки, так как компьютер переходит непосредственно в защищенный режим.

Какое бы микропрограммное обеспечение ни использовалось, BIOS или UEFI, после обнаружения правильно установленной версии Windows запускается файл Bootmgr.exe. Bootmgr.exe переключает систему из реального режима в защищенный, чтобы могла использоваться вся системная память.

Запуск и завершение работы Windows

Существует два важных элемента реестра, которые используются для автоматического запуска приложений и служб: **HKEY_LOCAL_MACHINE**: в этом разделе хранятся некоторые аспекты конфигурации Windows, в том числе информация о службах, которые запускаются при каждой загрузке; **HKEY_CURRENT_USER**: в этом разделе хранятся некоторые аспекты, касающиеся вошедшего в систему пользователя, в том числе информация о службах, которые запускаются, только когда этот пользователь входит в систему.

Одна из вкладок инструмента Msconfig.exe с параметрами конфигурации показана на рис. 3.1.6.

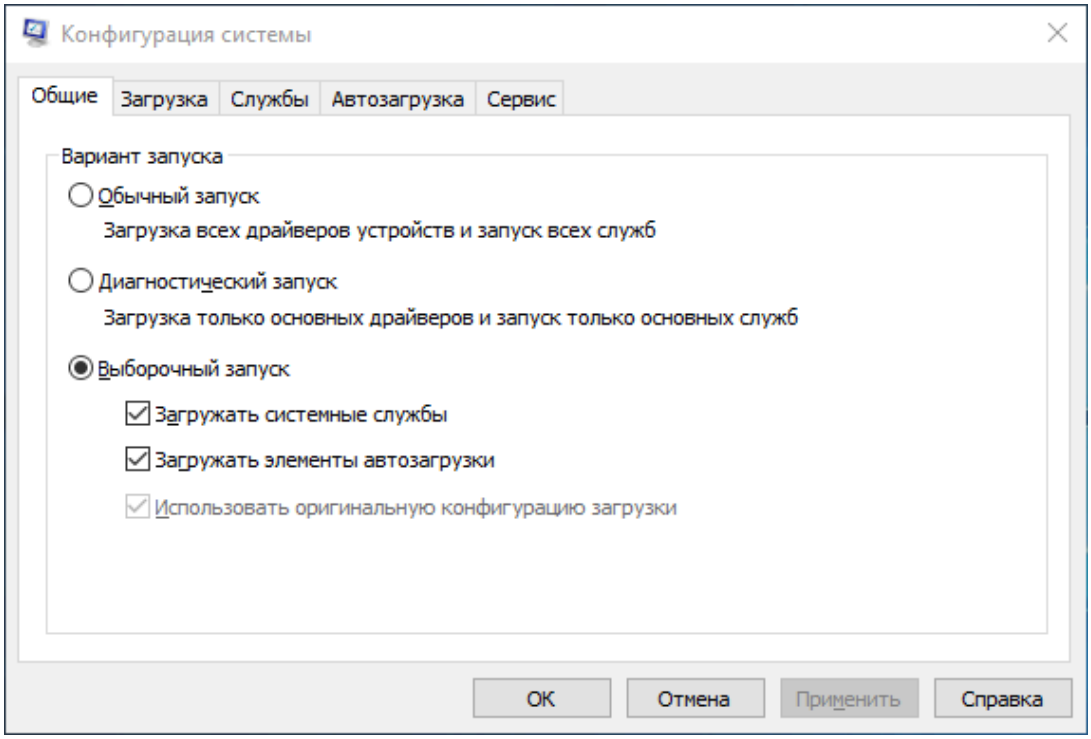


Рис. 3.1.6. Конфигурация системы. Вкладка «Общие»

3.1.5. Назначение и риски применения ключей реестра

Работа приложений Windows опирается на выполнение процессов [6]. Приложению может быть выделен один или несколько процессов. Процесс – это любая программа, исполняемая в данный момент. Каждый работающий процесс состоит хотя бы из одного потока. Процессор выполняет вычислительные операции с потоком. Для того чтобы настроить процессы Windows, следует использовать диспетчер задач.

Все потоки, выделенные для процесса, содержатся в одном адресном пространстве. Таким образом, эти потоки не имеют доступа к адресному пространству любых других процессов. Это позволяет предотвратить повреждение других процессов. Поскольку Windows является многозадачной операционной системой, несколько потоков могут выполняться одновременно. Количество потоков, которые могут выполняться одновременно, зависит от количества процессоров в компьютере.

Некоторые процессы, выполняемые ОС Windows, являются службами. Их можно настроить для автоматического запуска при загрузке Windows или запускать вручную. Их также можно останавливать, перезапускать или отключать. Приложение панели управления службами Windows показано на рис. 3.1.7.

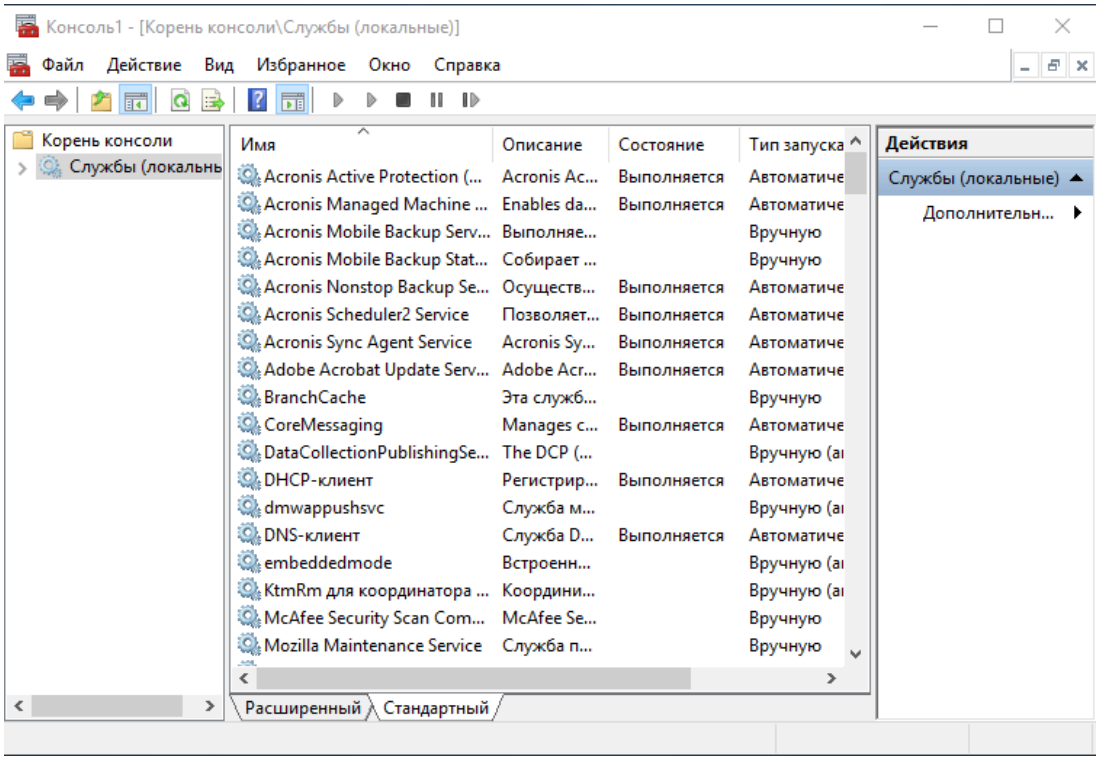


Рис. 3.1.7. Управление службами ОС Windows через универсальную консоль mmc

Windows хранит всю информацию о параметрах аппаратного обеспечения, приложений, пользователей и системы в большой базе данных, которая называется реестром. Записываются также способы взаимодействия этих объектов, например, какие файлы открывает приложение, и все сведения о свойствах папок и приложений. Реестр – это иерархическая база данных, верхний уровень которой называется кустом, под которым расположены разделы, а еще ниже – подразделы (рис. 3.1.8). Значения, в которых хранятся данные, находятся в разделах и подразделах. В разделе реестра может быть до 512 уровней.

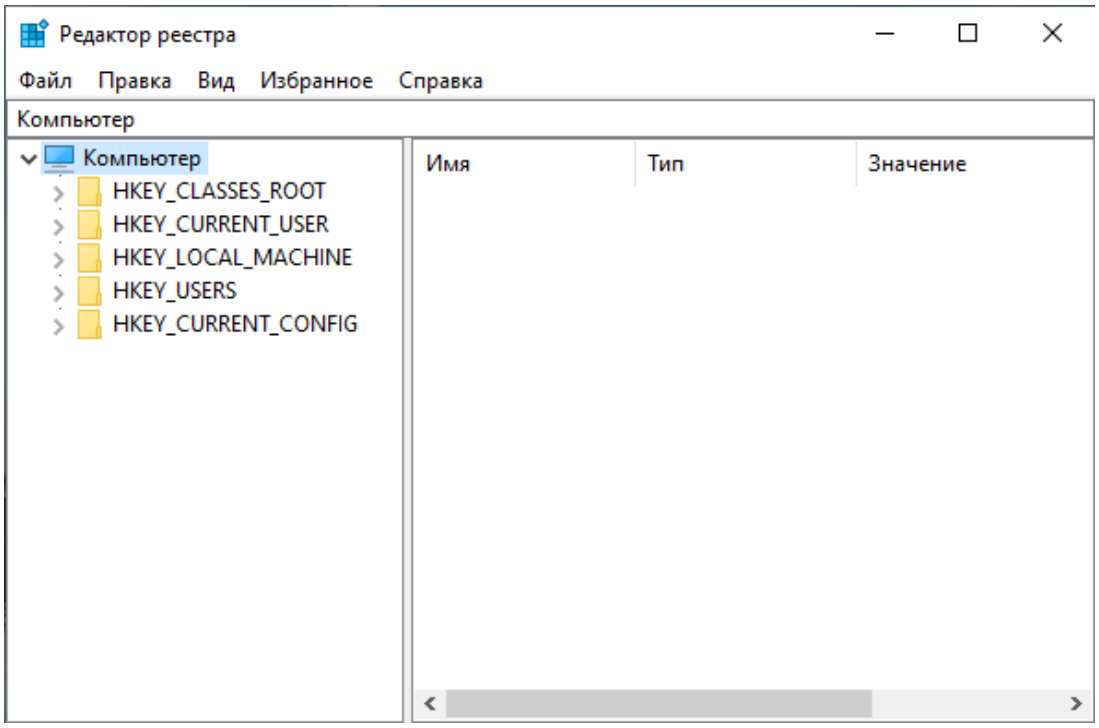


Рис. 3.1.8. Просмотр реестра ОС Windows с помощью программы regedit.exe

Реестр Windows состоит из пяти следующих кустов.

- **HKEY_CURRENT_USER (HKCU)** содержит данные, относящиеся к пользователю, который в данный момент находится в системе.
- **HKEY_USERS (HKU)** содержит данные, касающиеся всех учетных записей пользователей на хосте.
- **HKEY_CLASSES_ROOT (HKCR)** содержит данные о регистрациях связывания и внедрения объектов (OLE).
- **HKEY_LOCAL_MACHINE (HKLM)** содержит данные, относящиеся к системе.
- **HKEY_CURRENT_CONFIG (HKCC)** содержит данные о текущем профиле аппаратного обеспечения.

Новые кусты создавать нельзя. Разделы и значения реестра в кустах можно создавать, изменять или удалять, используя учетную запись с правами администратора. Небольшие изменения в реестре могут привести к очень серьезным последствиям, работать с реестром необходимо осторожно.

Навигация в реестре очень похожа на навигацию в проводнике Windows.

В разделе реестра может находиться подраздел или значение. Ниже перечислены различные значения, которые могут содержаться в разделах.

- **REG_BINARY** – числа или логические значения.
- **REG_DWORD** – числа больше 32 бит или необработанные данные.
- **REG_SZ** – строковые значения.

Так как в реестре содержится практически вся информация об операционной системе и пользователях, важно защитить его от несанкционированного доступа. Реестр также содержит действия, которые пользователь выполняет при обычном повседневном использовании компьютера. Сюда входит журнал аппаратных устройств, содержащий информацию обо всех устройствах, подключавшихся к компьютеру, включая название, производителя и серийный номер. В реестре хранится и другая информация, например: какие документы открывались пользователем или программой, где они находятся и когда к ним обращались. Это весьма полезная информация, когда требуется выполнить техническую экспертизу [7–10].

3.1.6. Безопасность работы локальных пользователей и доменов

При первом запуске нового компьютера или установке Windows система предлагает создать учетную запись пользователя, которая называется локальным пользователем.

В целях безопасности рекомендуется не включать учетную запись администратора и не предоставлять стандартным пользователям права администратора. Необходимость ввода пароля администратора защищает компьютер от установки или выполнения любого неразрешенного программного обеспечения или несанкционированного доступа к файлам.

Для упрощения администрирования пользователей в Windows используются группы. У каждой группы есть имя и определенный набор полномочий. Когда пользователь помещается в группу, ему предоставляются полномочия этой группы. Для того чтобы предоставить пользователю много разных полномочий, его можно поместить в несколько групп. Управление локальными пользователями и группами осуществляется с помощью приложения панели управления lusrmgr.msc, как показано на рис. 3.1.9.

Помимо групп для установки полномочий, в Windows можно также использовать домены [13]. Домен – это тип сетевой службы, в котором база данных хранит всех пользователей, группы, компьютеры, периферийные устройства и настройки безопасности, а также управляет ими. Эта база данных хранится на специальных компьютерах или в группах компьютеров, которые называются контроллерами домена. Контроллер домена должен выполнить аутентификацию каждого пользователя и компьютера в домене для входа и доступа к сетевым ресурсам.

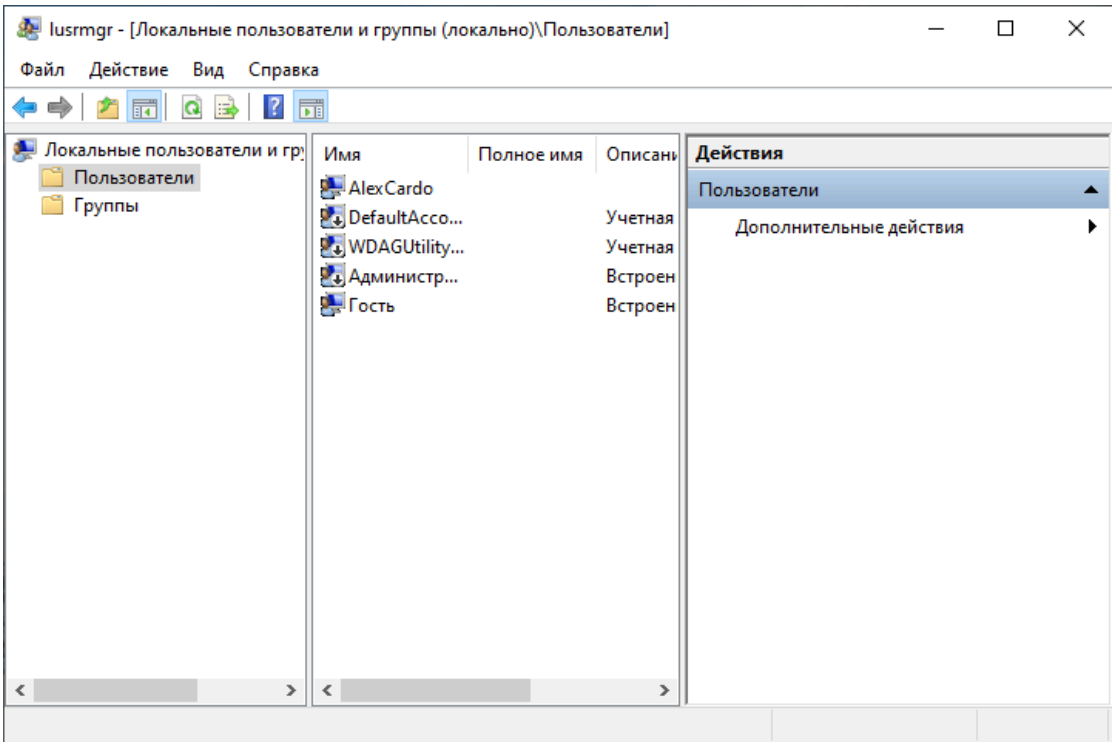


Рис. 3.1.9. Управление пользователями ОС Windows

3.1.7. Основные команды консольного интерфейса

В Windows есть множество команд, которые можно ввести в командной строке. Одной из наиболее важных является команда **net**, которая используется при администрировании и обслуживании операционной системы. Команда **net** поддерживает множество других команд, которые вводятся после **net** и могут дополняться различными параметрами для получения определенного результата.

Для того чтобы просмотреть список команд группы **net**, нужно ввести в командной строке **net help**. На рис. 3.1.10 показаны команды, которые могут использоваться с командой **net**. Для просмотра подробной справки о какой-либо команде группы net введите команду **net help:**

- **net accounts** устанавливает требования к паролю и входу в систему для пользователей;

- **net session** выводит список сеансов между компьютером и другими компьютерами в сети или закрывает эти сеансы;
- **net share** создает, удаляет общие ресурсы или управляет ими;
- **net start** запускает сетевую службу или выводит список запущенных сетевых служб;
- **net stop** останавливает сетевую службу;
- **net use** подключает, отключает общие сетевые ресурсы или выводит информацию о них;
- **net view** отображает список компьютеров и сетевых устройств в сети.

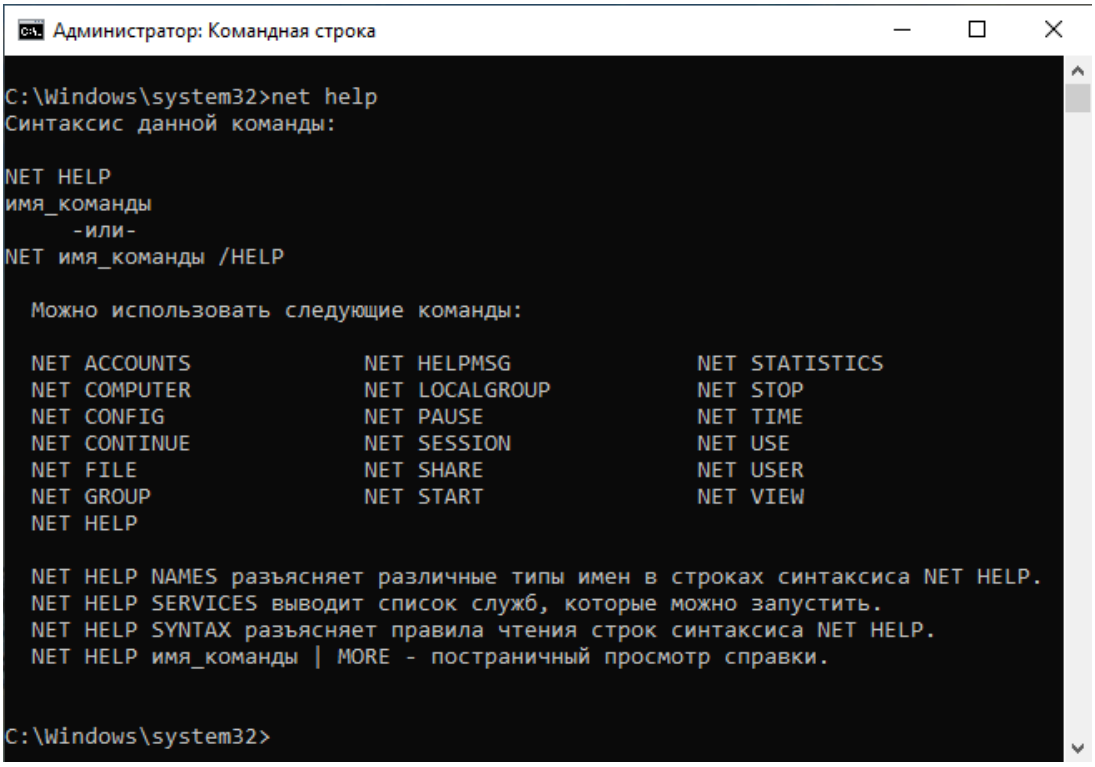


Рис. 3.1.10. Варианты команды **net**

- **netstat** отображает все активные доступные подключения TCP. Когда на компьютере присутствует вредоносное ПО, оно часто открывает порты связи на хосте для отправки и получения данных. С помощью команды netstat можно находить несанкционированные входящие и исходящие подключения.

Изучив эти подключения, можно определить, какие из программ прослушивают несанкционированные подключения.

3.1.8. Просмотр событий

Средство «Просмотр событий» Windows ведет журналы событий, относящихся к приложениям, безопасности и системе.

В ОС Windows есть две категории журналов событий: журналы Windows и журналы приложений и служб. В каждой из этих категорий имеется несколько типов журналов (рис. 3.1.11).

Можно также настроить нестандартное представление. Это удобно при поиске событий определенных типов или событий, произошедших за определенный период времени, при отображении событий определенного уровня и во многих других случаях.

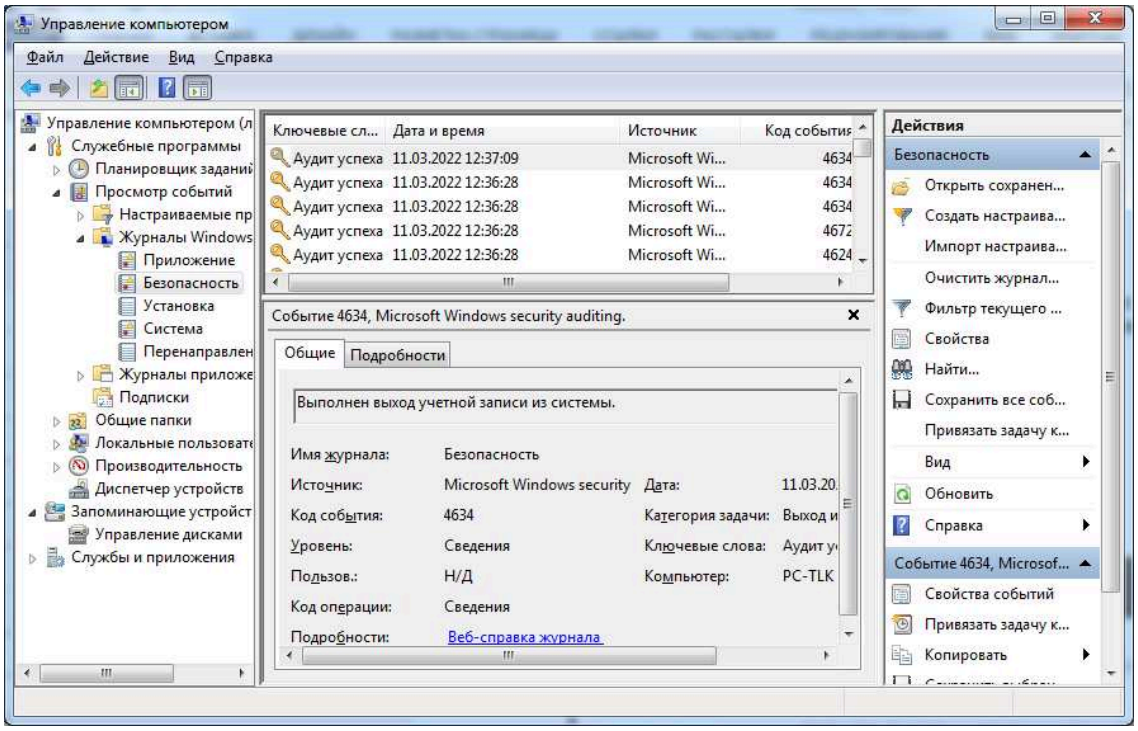


Рис. 3.1.11. Просмотр событий ОС Windows

3.1.9. Межсетевой экран

В составе Windows имеется брандмауэр (межсетевой экран) – программа, которая контролирует обмен данными между компьютером и внешними сетями, блокируя несанкционированный доступ к компьютеру.

Существует возможность полностью отключить брандмауэр. Для этого используют ссылку Включение и отключение брандмауэра Windows и устанавливают соответствующий переключатель в положение «Отключить брандмауэр Windows». Если контроль брандмауэра не требуется для какого-то одного из имеющихся на компьютере подключений, то в том же окне снимают флажки возле подключения, защита которого не требуется. Отключение брандмауэра даже для одного сетевого подключения Центр поддержки расценит как недопустимое снижение уровня защиты: всплывающие сообщения в области уведомлений будут напоминать вам о необходимости вернуться к прежним настройкам.

3.1.10. Основные меры по усилению защиты устройств под управлением Windows

Для защиты персонального компьютера на базе операционной системы Windows рекомендуется применять следующие меры защиты:

1. Обновлять Windows и установленные программы. Один из важнейших шагов, которые следует предпринять для обеспечения безопасности устройства и данных – поддержание Windows и установленного программного обеспечения в актуальном состоянии. Компании-разработчики программных продуктов постоянно выпускают обновления для устранения известных уязвимостей, которые могут эксплуатироваться киберпреступниками.

2. Обеспечить наличие актуального многокомпонентного антивируса. Антивирус является обязательным компонентом на каждом компьютере – он служит для обнаружения и удаления вредоносных программ, прежде чем они смогут скомпрометировать прикладные и системные файлы, повлиять на производительность или нарушить работоспособность устройства.

В качестве альтернативы системной защите существует возможность выбрать сторонний инструмент, например, Kaspersky Anti-Ransomware Tool. Бесплатное решение от «Лаборатории Касперского» предназначено для защиты компьютеров от известных вредоносных объектов, включая шифровальщики, программы-вымогатели и криптомайнеры.

3. Использовать брандмауэр Windows. Брандмауэр или межсетевой экран – это программный или аппаратный инструмент, который служит для блокировки вредоносных атак хакеров, червей, шифровальщиков, вирусов и других типов угроз, которые пытаются получить доступ к компьютеру из интернета или локальной сети для последующей кражи информации.

4. Использовать надежные проверенные приложения. Microsoft рекомендует избегать загрузки и установки приложений из неизвестных источников и предписывает использовать программное обеспечение с официальных сайтов, по возможности загружать приложения из Магазина Microsoft в Windows. Программы на этой площадке проверены Microsoft и не содержат вредоносный код.

5. Работать в системе под учетной записью обычного пользователя. Рекомендуется использовать стандартную учетную запись пользователя вместо учетной записи администратора, чтобы предотвратить установку вредоносных программ с использованием повышенных привилегий.

6. Создавать и поддерживать нескольких резервных копий системной и прикладной информации (стека резервных копий). Одним из лучших способов защиты компьютера и файлов от вредоносных атак

является регулярное создание резервных копий. Рекомендуется создавать стеки резервных копий (недельный, месячный, годовой) и обеспечивать их локальное и облачное хранение.

Стратегия резервного копирования должна предусматривать создание полной резервной копии системы и данных, которую можно хранить в локальном местоположении – например, на локальном сетевом носителе (хранилище NAS) или на внешнем жестком диске. Данный тип резервной копии позволит восстановить данные после вредоносного заражения, повреждения основного носителя, отказов оборудования или других несчастных случаев.

После создания резервной копии следует отключить диск от основной системы и сохранить его в надежном месте или отключить от сети сетевое хранилище, на котором хранятся копии.

7. Периодически производить полную проверку системы на наличие вредоносного программного обеспечения.

Если вирус, интернет-червь, шифровальщик или другой тип вредоносного программного обеспечения все же смог обойти механизмы безопасности компьютера, необходимо:

- отключить компьютер от интернета и локальной сети. Это можно сделать, выдернув кабель Ethernet, отключив Wi-Fi адаптер или отключив питание ближайшего сетевого устройства – таким способом будет заблокировано распространение угрозы на другие устройства;

- произвести очистку вредоносного заражения. Для этого следует, например, открыть Защитник Windows и использовать функцию автономного сканирования. Если результатом действия вредоносного программного обеспечения стала потеря контроля над компьютером, следует использовать другое устройство для записи загрузочного носителя с копией Windows Defender Offline. Существует, кроме того, возможность использования антивирусных программ, которые поддерживают возможность автономного сканирования с помощью антивирусных загрузочных дисков;

- если ни один из шагов не помог удалить вредоносное программное обеспечение, следует восстановить систему с использованием последней доступной резервной копии, предварительно сняв образ зараженного системного диска (для обеспечения дальнейшего изучения и расследования). В случае если имеется только резервная копия прикладных файлов, следует произвести чистую установку Windows. После установки нужно будет переустановить приложения, повторно применить настройки и восстановить файлы, используя резервные копии.

3.2. Обеспечение безопасности операционных систем семейства Linux

3.2.1. История и особенности операционных систем

Предшественниками современных операционных систем можно назвать системы пакетной обработки, когда выполняемые задания вводились для выполнения поочередно. Сначала это исполнялось вручную, затем появились средства автоматизации операций. Так возникли предпосылки разработки программных средств управления набором (пакетом) заданий. Важной вехой в этом развитии стал 1964 год, когда IBM анонсировала, а затем и выпустила OS/360. Естественным развитием идей более эффективного использования возможностей вычислительных машин стало появление систем разделения времени. Одними из первых, обеспечивших реализацию систем разделения времени, стали операционные системы семейства UNIX [11].

Версия Linux, поддерживающая графический интерфейс (рис. 3.2.1), была разработана в 1992 году.

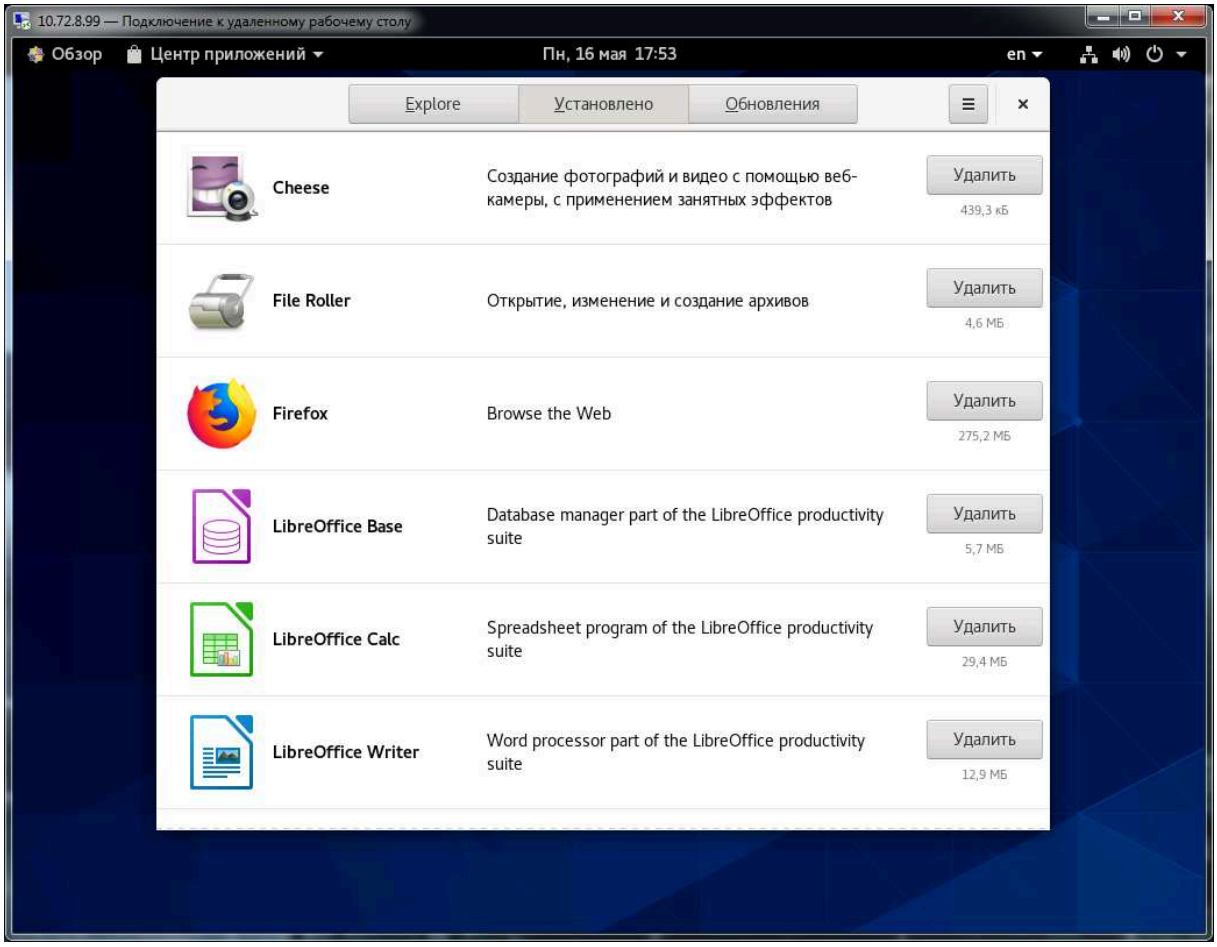


Рис. 3.2.1. Графический интерфейс ОС Linux

Базовые команды консольного интерфейса Linux

Команды Linux – это программы, разработанные для выполнения определенной задачи. Для получения документации по командам можно использовать команду man (сокращение от слова manual – руководство). Например, команда man ls открывает сведения по команде ls из руководства пользователя.

Для вызова команды с помощью оболочки просто вводят имя команды. Оболочка будет пытаться найти эту команду в пути системы и выполнить ее.

Несмотря на возможность установки в современных версиях Linux графического интерфейса, значительная часть команд по-прежнему может выполняться из командной строки (рис. 3.2.2). Основная часть базовых команд ОС Linux, выполняющихся в режиме командной строки, показана в таблице 3.2.1.

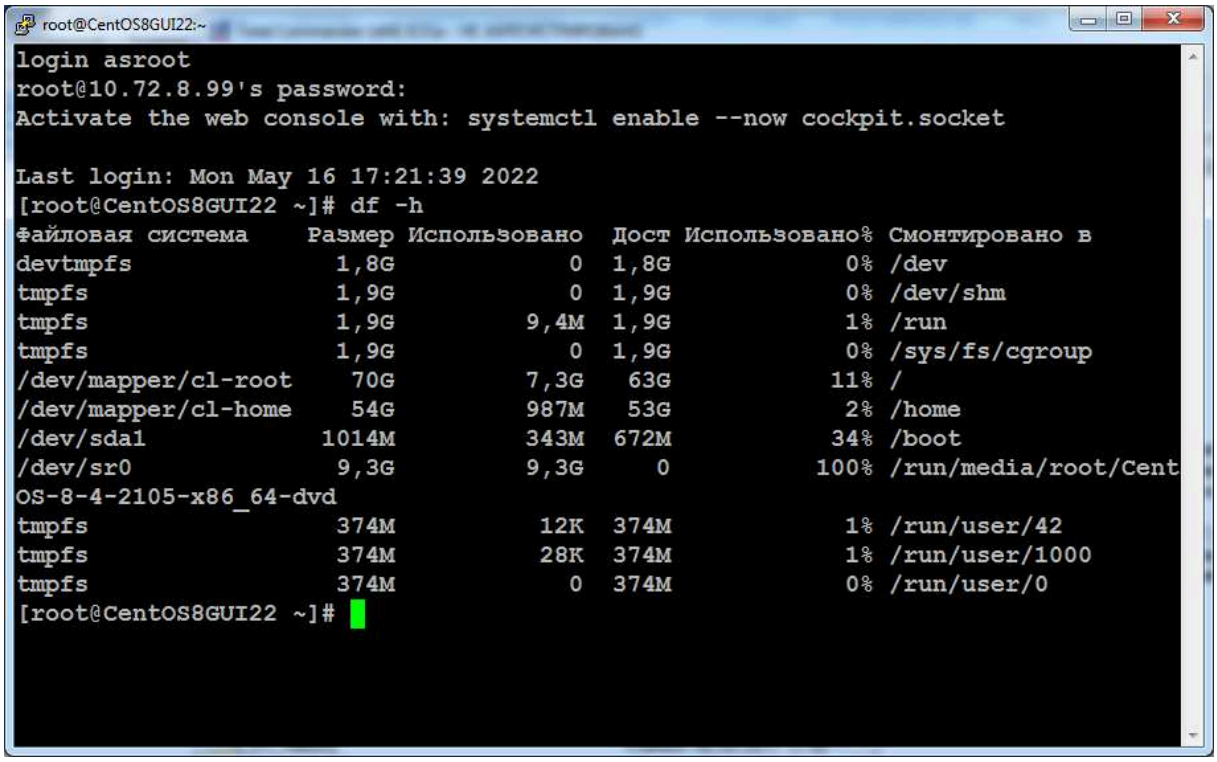


Рис. 3.2.2. Пример выполнения одной из базовых команд Linux в командной строке

Предполагается, что пользователь имеет соответствующие разрешения для выполнения этой команды. Разрешения для файлов в Linux рассматриваются далее в данной главе.

Таблица 3.2.1
Некоторые команды режима командной строки Linux

Команда	Описание
mv	Перемещение или переименование файлов и каталогов
chmod	Изменение разрешений для файла
chown	Изменение владельца файла
dd	Копирование данных из ввода в вывод
pwd	Отображение имени текущего каталога
ps	Отображение списка выполняющихся процессов в системе
su	Эмуляция входа в качестве другого пользователя или получение полномочий суперпользователя
sudo	Выполнение команды от имени другого пользователя
grep	Используется для поиска определенных строк или символов в файле или результатах выполнения других команд. Реализуется добавлением команды grep в конце команды, результаты которой необходимо отфильтровать
ifconfig	Служит для отображения сведений о сетевой плате и настройке ее параметров. При вызове без параметров отображает информацию о сетевых платах системы.
apt-get	Используется для установки, настройки и удаления пакетов в Debian. Комбинация dpkg и apt-get – это система управления пакетами по умолчанию во всех производных Debian, включая Raspbian
iwconfig	Служит для отображения сведений о плате беспроводной сети и настройки ее параметров
shutdown	Выключение системы. Команда shutdown может выполнить ряд задач, связанных с завершением работы, перезапуском и остановом системы
passwd	Используется для изменения пароля. Если параметры не указаны, команда passwd меняет пароль текущего пользователя
cat	Служит для вывода содержимого файла, обычно используется для вывода содержимого текстовых файлов
man	Отображает документацию по определенной команде
ls	Отображение списка файлов в текущем каталоге
cd	Переход к другому каталогу
mkdir	Создание каталога в текущем каталоге
cp	Копирование файлов из исходной папки в целевую
rm	Удаление файлов

Конфигурационные файлы сервисов и служб

В Linux службы управляются с помощью файлов конфигурации. После изменения файла конфигурации чаще всего требуется перезапустить службу, чтобы изменения вступили в силу.

Так как для запуска служб часто требуются права суперпользователя, для редактирования файлов конфигурации служб тоже часто требуются права суперпользователя.

Конфигурационные файлы можно редактировать с помощью текстовых редакторов, большинство из которых запускаются из командной строки. К числу таких редакторов следует отнести vim, nano, mcedit. На рис. 3.2.3 приведен вид конфигурационного файла межсетевого экрана-маршрутизатора iptables, открытого в редакторе nano.

На рис. 3.2.4 показан вид консольного окна с запущенным файловым менеджером, используя встроенный редактор, которого mcedit, также существует возможность редактировать конфигурационные файлы.

Типовой сценарий настройки какой-либо службы в Linux после ее установки, заключается в следующем:

1. Осмотр и редактирование файла конфигурации службы, в данном случае по адресу /etc/dnsmasq.conf. Это можно сделать с помощью команды # nano /etc/dnsmasq.conf

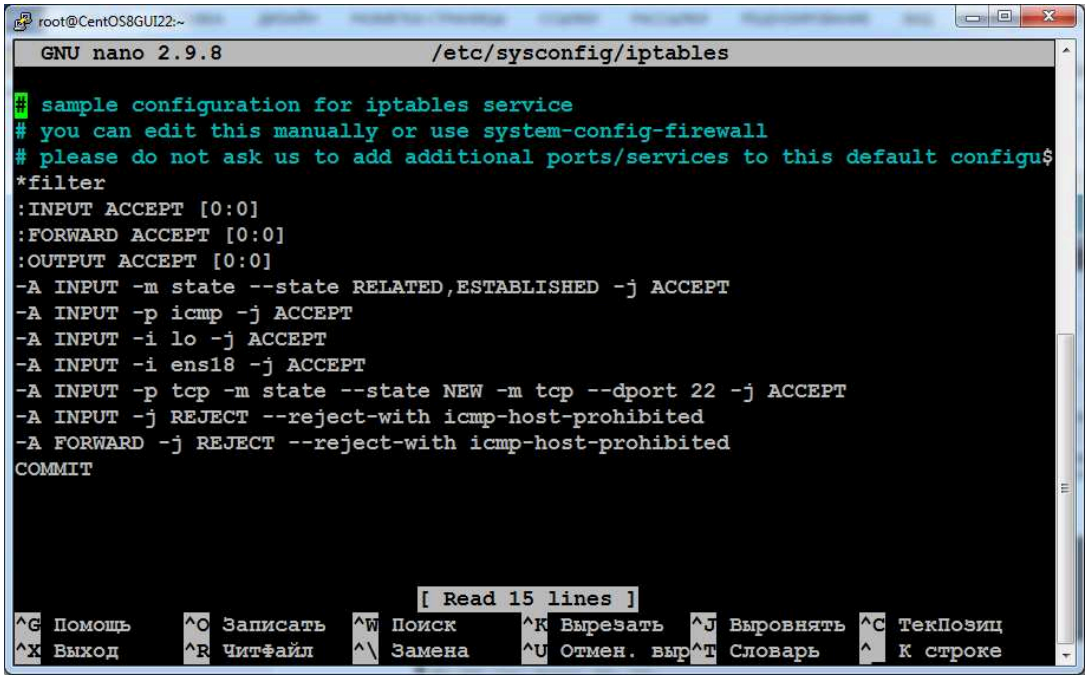


Рис. 3.2.3. Вид конфигурационного файла межсетевого экрана-маршрутизатора iptables в ОС CentOS8

2. Запуск службы в текущий момент времени. Это делается с помощью команды # systemctl start dnsmasq.

3. Осмотр состояния работающей службы после запуска. Это делается с помощью команды # systemctl status dnsmasq. С момента запуска должен начаться отсчет времени ее работы. Статус службы должен быть в состоянии «работает», «active». Количество информации, выдаваемой данной командой, сильно зависит от типа службы и обычно составляет от нескольких единиц до нескольких десятков строк.

4. Планирование службы в автозапуск с помощью команды # systemctl enable dnsmasq, при условии что пункты 1..3 данного сценария выполнены успешно.

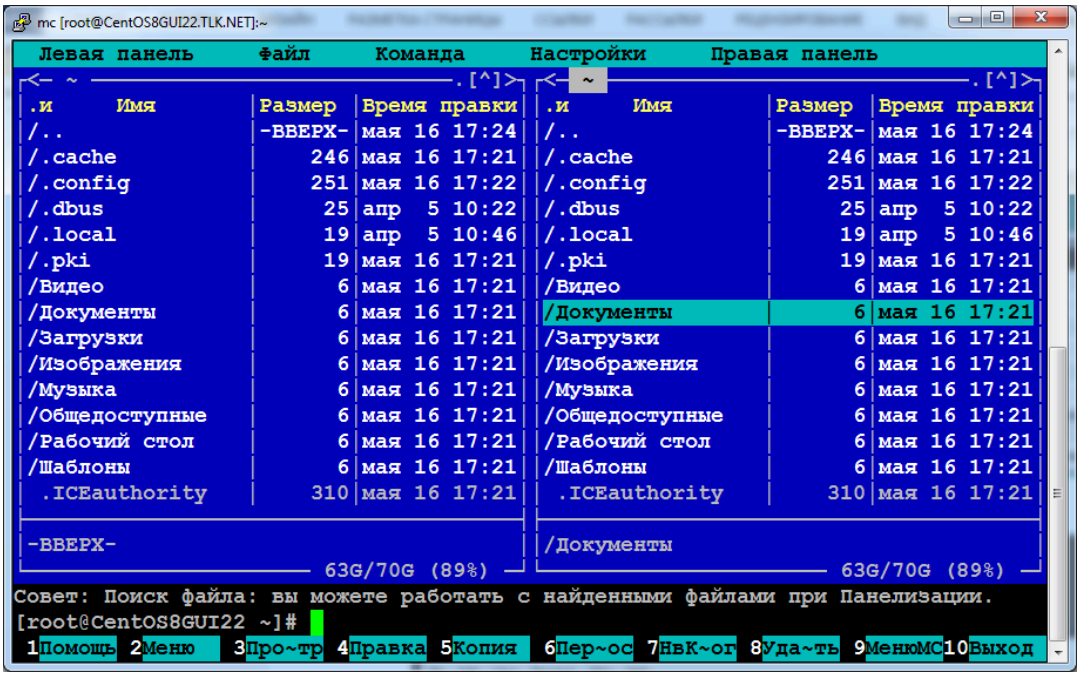


Рис. 3.2.4. Вид консольного окна с mc

Контроль журналов и служб

Файлы журналов представляют собой записи, которые сохраняются компьютером для отслеживания важных событий. В файлы журналов записываются события ядра, служб и приложений.

В Linux файлы журналов могут быть отнесены к следующим категориям: журналы приложений; журналы событий; журналы служб; системные журналы.

Ниже перечислены некоторые распространенные файлы журналов Linux и их функции:

- /var/log/messages – в этом каталоге содержатся общие журналы операций компьютера. В основном он используется для хранения информационных и некритических системных сообщений. На компьютерах Debian эту функцию выполняет каталог /var/log/syslog;

• /var/log/auth.log – в этом файле содержатся все связанные с аутентификацией события на компьютерах Debian и Ubuntu. В нем можно найти все, что связано с механизмом авторизации пользователей;

• /var/log/secure – этот каталог используется на компьютерах RedHat и CentOS вместо файла /var/log/auth.log. В нем также отслеживаются входы sudo, входы SSH и другие ошибки, регистрируемые SSSD;

• /var/log/boot.log – в этом файле содержится информация, связанная с загрузкой, и сообщения, зарегистрированные во время процесса запуска компьютера;

• /var/log/dmesg – в этом каталоге содержатся сообщения кольцевого буфера ядра. Сюда записывается информация в отношении аппаратных устройств и их драйверов. Это очень важно, так как низкоуровневые события и системы ведения журналов, такие как системный журнал, еще не работают во время возникновения таких событий, поэтому они часто недоступны для администратора в реальном времени;

• /var/log/kern.log – в этом файле содержится информация, зарегистрированная ядром;

• /var/log/cron – в этом каталоге хранятся события службы Cron, которая используется в Linux для планирования автоматических задач. При каждом запуске запланированной задачи (также называемой заданием cron) здесь сохраняется вся соответствующая информация, включая сообщения о состоянии выполнения и об ошибках;

• /var/log/mysqld.log или /var/log/mysql.log – это файл журнала MySQL. В нем регистрируются все сообщения отладки, а также сообщения о сбоях и об успешном выполнении, связанные с процессом mysqld и демоном mysqld_safe. На компьютерах RedHat, CentOS и Fedora журналы MySQL хранятся в файле /var/log/mysqld.log, а на компьютерах Debian и Ubuntu – в файле /var/log/mysql.log.

На рис. 3.2.5 показан пример команды, позволяющей отфильтровывать информацию о фактах входа учетных записей в систему из содержимого журнала /var/log/auth.log. На рис. 3.2.6 показан пример команды, позволяющей отфильтровывать информацию о фактах неудачных попыток входа учетных записей.

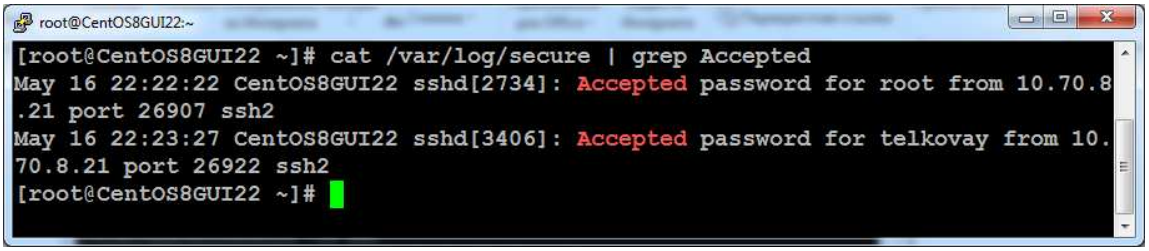


Рис. 3.2.5. Результат фильтрации попыток успешного входа на хост с операционной системой CentOS8 Linux по протоколу ssh

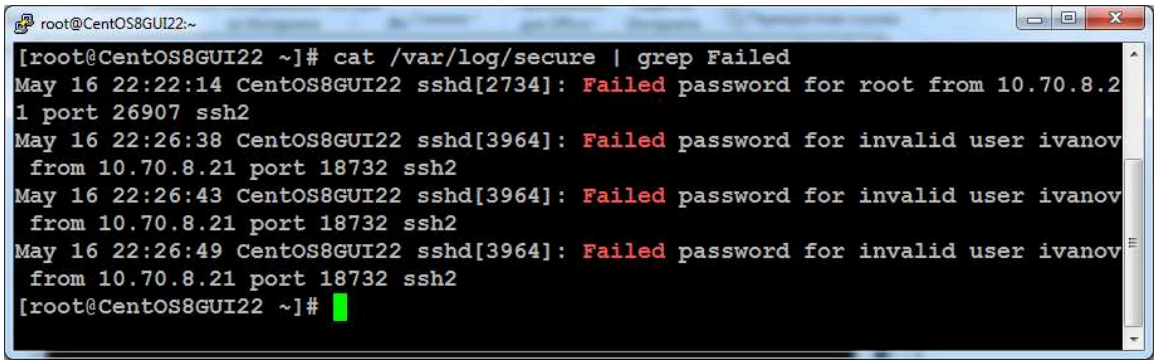


Рис. 3.2.6. Результат фильтрации попыток безуспешного доступа на хост с операционной системой CentOS8 Linux по протоколу ssh

Информация о подключавшихся в системе USB устройствах в процессе ее работы может быть выдана с помощью команды dmesg – см. рис. 3.2.7.

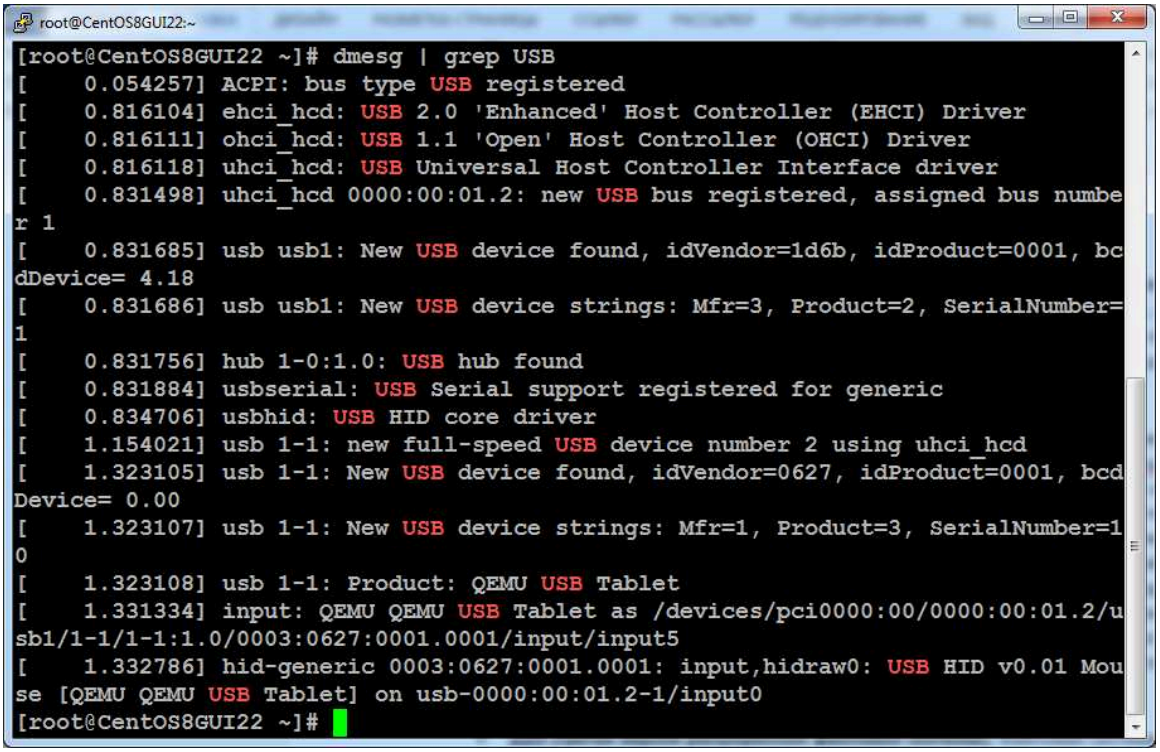


Рис. 3.2.7. Вывод информации об устройствах USB

Типы файловых систем в Linux

Ниже приведено несколько наиболее распространенных типов файловых систем, поддерживаемых Linux:

- ext2 (вторая версия расширенной файловой системы). Файловая система ext2 использовалась по умолчанию в нескольких основных дистрибутивах Linux, пока не была заменена на ext3.
- ext3 (третья версия расширенной файловой системы). Файловая система с протоколированием ext3 разрабатывалась с целью улучшения

существующей файловой системы ext2. Журнал (главный компонент, добавленный в ext3) представляет метод, используемый для максимального снижения риска повреждения файловой системы в случае внезапного отключения питания. Максимальный размер файла в файловой системе ext3 – 32 ТБ.

- ext4 (четвертая версия расширенной файловой системы). Файловая система ext4, разрабатывавшаяся как преемник ext3, была создана на основе ряда расширений ext3.
- NFS (сетевая файловая система). NFS – это файловая система на базе сети, обеспечивающая доступ к файлам по сети. NFS является открытым стандартом.
- Система файлов подкачки. Система файлов подкачки используется Linux, когда вся оперативная память оказывается занятой. В этом случае ядро перемещает неактивное содержимое оперативной памяти в раздел подкачки на диске.
- HFS Plus или HFS+ (иерархическая файловая система плюс). Эта файловая система используется Apple в их компьютерах Macintosh. В ядре Linux предусмотрен модуль для подключения HFS+ для операций чтения и записи.
- Главная загрузочная запись (MBR). MBR располагается в первом секторе секционированного компьютера и хранит всю информацию о способе организации файловой системы. Главная загрузочная запись быстро передает управление функции загрузки, которая загружает операционную систему.

Подключение – термин, используемый для обозначения процесса назначения каталога разделу.

На рис. 3.2.8 показаны выходные данные команд blkid, lsblk выданные с виртуальной машины CentOS8. Приведенная информация позволяет оценить размеры элементов файловых разделов, их идентификаторы и места монтирования.

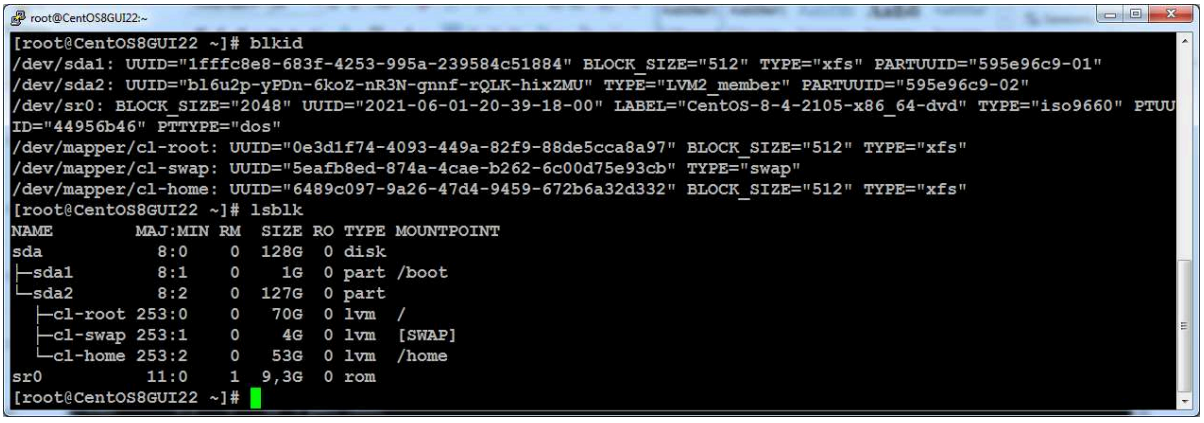


Рис. 3.2.8. Результаты выполнения команд blkid, lsblk в ОС CentOS8

Роли и разрешения на объекты файловой системы Linux

В Linux большинство системных объектов рассматриваются как файлы. Каждый файл в Linux имеет свои разрешения, определяющие действия, которые владелец файла, группа и другие пользователи могут выполнять с этим файлом. Применяются разрешения на чтение, запись и выполнение. Команда ls с параметром -l выводит дополнительную информацию о файле. Рассмотрим результат выполнения команды ls -l, приведенный на рис. 3.2.9.

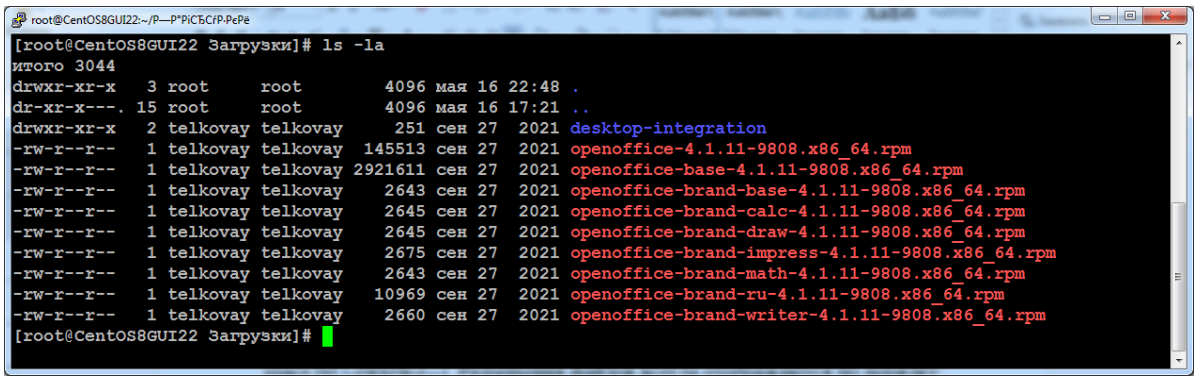


Рис. 3.2.9. Результаты осмотра содержимого каталога Linux с детализацией разрешений на файловые объекты

В этих выходных данных содержится много информации о файле space.txt.

В первом поле отображаются разрешения, назначенные файлу space.txt (-rwxrw-r--). Разрешения файлов всегда отображаются по порядку: сначала для пользователя, далее для группы, а затем для других пользователей.

Файл openoffice-4.1.11-9808.x86_64.rpm, показанный на рис. 3.2.9, имеет следующие разрешения. - Тире (-) означает, что это файл. Для каталогов первым символом была бы буква d. Первый набор символов указывает разрешения пользователя (rw-). Пользователь telkovay, которому принадлежит файл, имеет разрешения на чтение (r), запись (w) этого файла. Второй набор символов указывает разрешения группы (r--). Группа telkovay, которой принадлежит этот файл, имеет разрешения на чтение файла (r). Третий набор символов указывает разрешения всех остальных пользователей и групп (r--). Все остальные пользователи и группы на компьютере могут только читать (r) этот файл. Второе поле определяет количество жестких ссылок на этот файл (число 1 после разрешений). Жесткая ссылка создает другой файл с другим именем, привязанный к тому же месту в файловой системе (называемому индексным дескриптором, или inode). В этом заключается отличие от символических ссылок. В третьем и четвертом полях указываются соответственно

пользователь (telkovay) и группа (telkovay), которым принадлежит этот файл. В пятом поле указан размер файла в байтах, openoffice-4.1.11-9808.x86_64.rpm имеет размер 145 513 байт. В шестом поле указывается дата и время последнего изменения. В седьмом поле указано имя файла.

В таблицах 3.2.2, 3.2.3 показаны значения, формирующие разрешения для файлов. Разрешения файлов являются основополагающей частью Linux и не могут быть нарушены. Пользователь имеет столько прав на файл, сколько задано в разрешениях для этого файла. Единственный, кто может переопределять разрешения файлов на компьютере Linux, – это привилегированный пользователь. Так как привилегированный пользователь может переопределять разрешения файлов, он может выполнять запись в любой файл. Поскольку все элементы в Linux рассматриваются как файлы, привилегированный пользователь имеет полный контроль над компьютером Linux. Для обслуживания системы и ее администрирования зачастую требуются права root.

Таблица 3.2.2
Принципы формирования разрешений для файлов
(- указывает на файл, d указывает на каталог)

Бит файла	Пользователь			Группа			Другое		
- или d	r	w	x	r	w	x	r	w	x

Таблица 3.2.3
Определение разрешений через восьмеричные значения

Двоичные	Восьмеричные	Разрешение	Описание
000	0	---	Нет доступа
001	1	--x	Только выполнение
010	2	-w-	Только запись
011	3	-wx	Запись и выполнение
100	4	r--	Только чтение
101	5	r-x	Чтение и выполнение
110	6	rw-	Чтение и запись
111	7	rwx	Чтение, запись, выполнение

Система X Window

Графический интерфейс на большинстве компьютеров Linux построен на основе оконной системы X Window. Система X Window, также называемая X или X11, представляет собой систему управления окнами, разработанную в целях обеспечения базовой архитектуры для графического интерфейса пользователя. Система X имеет функции рисования и перемещения окон на устройстве отображения, а также

взаимодействия с мышью и клавиатурой (рис. 3.2.1).

Графический интерфейс X работает как сервер и, таким образом, предоставляет удаленному пользователю возможность использования сети для подключения, запуска графического приложения и получения открытого графического окна на удаленном терминале. Хотя само приложение работает на сервере, его графический аспект отправляется системой X по сети и отображается на удаленном компьютере.

Установка и запуск приложений на хосте Linux

Многие пользовательские приложения – это сложные программы, написанные на компилируемых языках. Для упрощения процесса установки в Linux часто имеются программы, называемые диспетчерами пакетов. При установке пакета с помощью диспетчера пакетов все необходимые файлы помещаются в правильное место в файловой системе (рис 3.2.10).

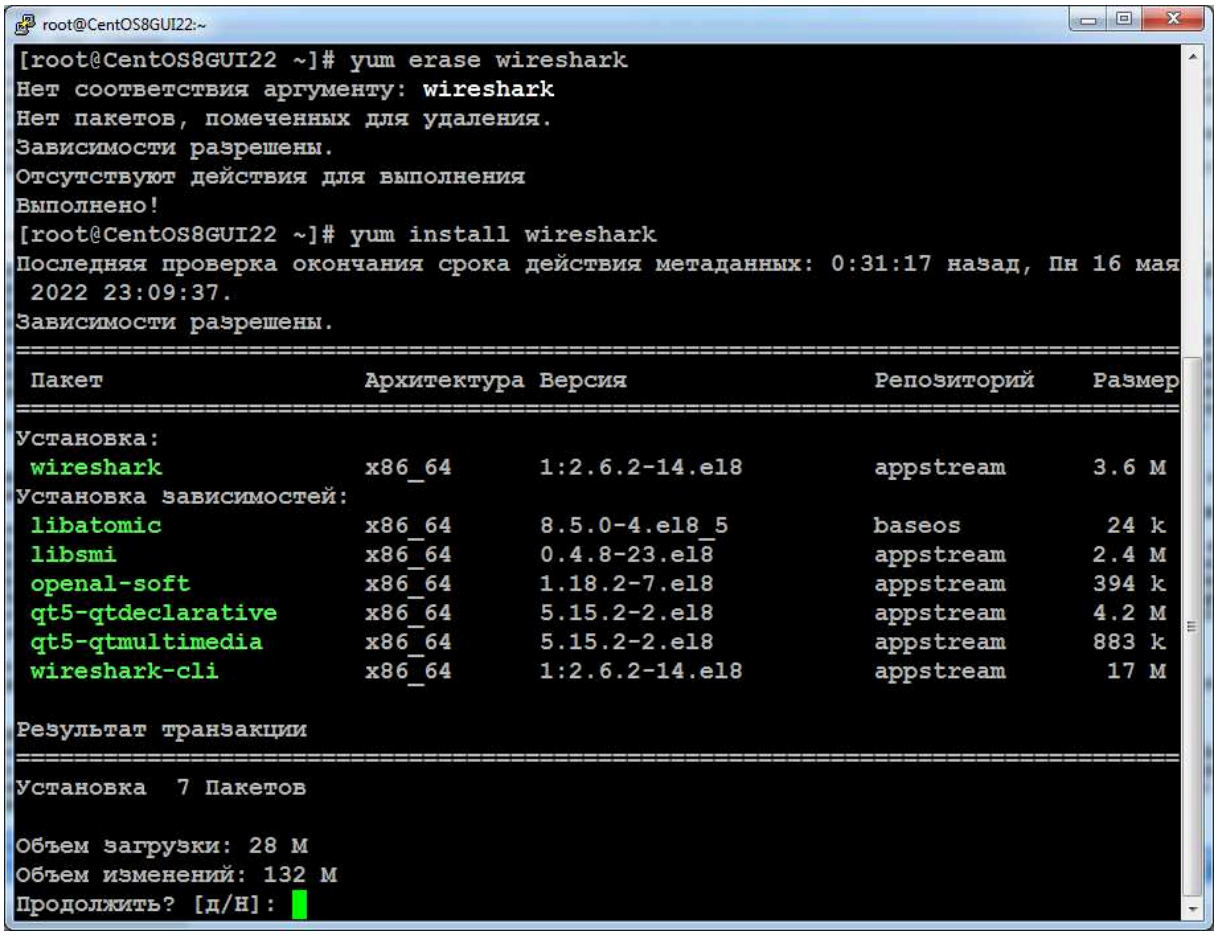


Рис. 3.2.10. Пример установки и удаления пакетов в CentOS8 Linux через пакетный менеджер

В операционных системах, основанных на ядре Debian, используют диспетчер пакетов Advanced Packaging Tool (apt). Команда apt-get update используется для получения списка пакетов из репозитория пакетов и обновления локальной базы данных пакетов. В операционных системах на

ядре Red Hat используют пакетные менеджеры yum и dnf.

3.2.2. Основные элементы, угрозы и риски безопасности Linux

Большинство вредоносных воздействий на операционные системы семейства Linux происходит путем получения несанкционированного доступа к хосту и повышения привилегий пользователя до уровня root. Комплекс мер по усилению защиты устройств на базе Linux будет рассмотрен позднее. Если несанкционированный доступ к операционной системе произошел и повышение привилегий состоялось, этот факт может быть обнаружен с помощью программы поиска руткитов.

Наличие аномальной загрузки системы может быть обнаружено с помощью утилит top, htop, а наличие сетевых соединений неизвестного происхождения – с помощью команды conntrack –L из набора утилит conntrack-tools (рис. 3.2.11, 3.2.12).

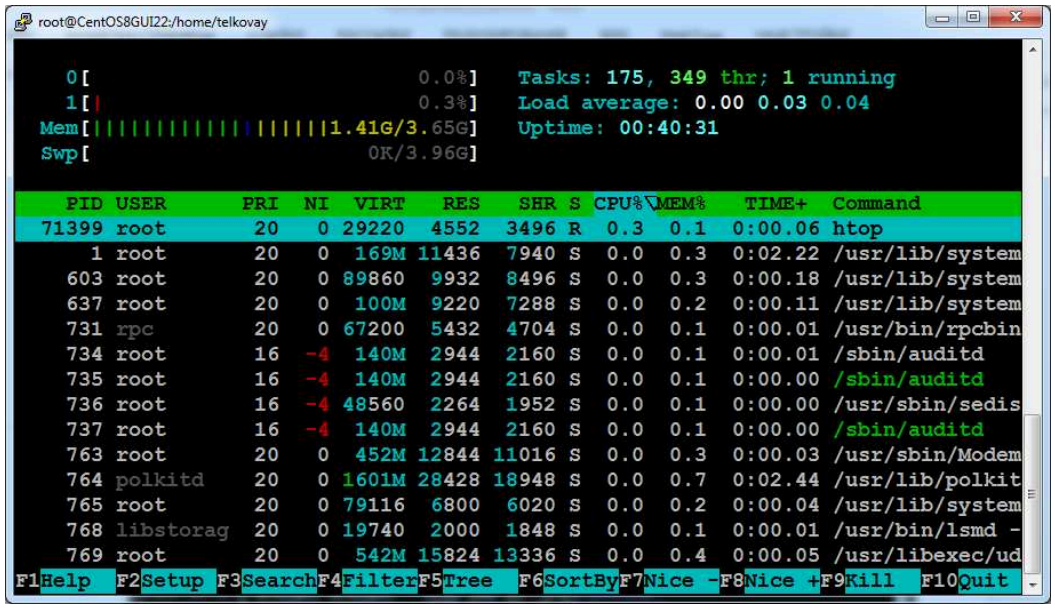


Рис. 3.2.11. Тестирование ОС CentOS8 Linux с htop (фрагмент)

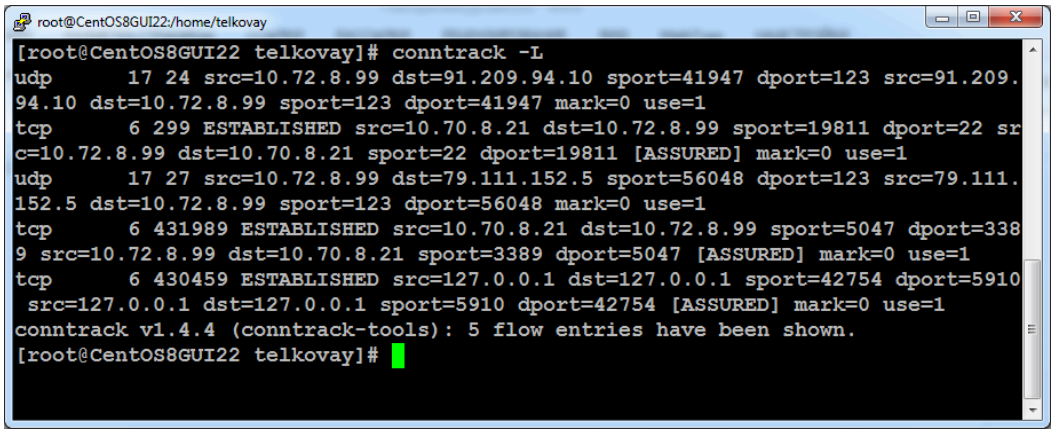


Рис. 3.2.12. Тестирование ОС CentOS8 Linux с conntrack –L

В приведенных примерах аномальная загрузка ресурсов отсутствует, сетевых соединений неизвестного происхождения не обнаруживается.

3.2.3. Основные меры по защите устройств на базе операционной системы Linux

Основные меры по защите подразумевают реализацию политики минимизации привилегий пользователей системы, отключение неиспользуемых локальных и сетевых служб и некоторые другие меры.

Базовая роль в этой задаче отводится правильному определению разрешений использования объектов файловой структуры, решению вопроса о том, какие пользователи или группы имеют доступ к определенным файлам.

Кроме задач правильного управления доступом к файловым объектам, базовые задачи обеспечения безопасности на хосте Linux включают:

- минимизацию пользовательских привилегий, в том числе путем недопущения включения учетных записей пользователей в группу root;
- установку и запуск приложений из командной строки;
- поддержание актуальности системы с помощью функций apt-get update и apt-get upgrade, yum update, yum check-update, dnf update и т.п.;
- просмотр текущих процессов и ветвлений, выполняющихся в памяти с помощью утилит top, htop;
- поиск подозрительной сетевой активности на хосте с помощью команд iftop, conntack –L;
- поиск подозрительных сетевых интерфейсов в системе с помощью команд ifconfig –a, ip a;
- использование chkrootkit, rkhunter для проверки компьютера на наличие известных руткитов;
- использование конвейеризации для создания цепочки команд и передачи выходных данных одной команды в качестве входных данных для другой команды;
- правильную настройку межсетевого экрана и маршрутизатора iptables или межсетевого экрана firewalld для реализации минималистичных политик сетевого доступа к узлу;
- использование встроенного средства безопасности SELINUX для контроля действий процессов и служб в системе;
- регулярный осмотр журналов безопасности, приложений и служб на наличие аномальной активности.

3.3. Защищенные операционные системы семейства Linux

3.3.1. Современные требования и основные подходы к созданию защищенных операционных систем

Существует два основных подхода к созданию защищенных операционных систем. Первый подход подразумевает, что защищённость операционной системы обеспечивается при реализации некоторых заданных изначально требований по безопасности, включая наличие некоторого набора механизмов защиты, проверку отсутствия предопределённого перечня уязвимостей и т.п. При втором подходе рассматривается возможность использования операционной системы в составе автоматизированных систем, которые считаются их владельцами (пользователями) критическими, в связи с чем в операционной системе должен обеспечиваться комплекс средств защиты, адекватный угрозам безопасности именно этих систем.

Таким образом, защищённой (доверенной) целесообразно считать операционную систему, которая не только реализует заданные априорно требования по безопасности, но и адекватна угрозам безопасности, специфичным для отечественных автоматизированных систем, в том числе для которой отсутствует возможность несанкционированного влияния на её работу извне, при этом владелец (пользователь) защищённой ОС должен иметь однозначное представление об алгоритме функционирования её защитных механизмов во всех режимах работы.

Это требование становится все более актуальным в последние годы. Автоматическое обновление, автоматическое оповещение разработчиков о программных ошибках, разнообразные онлайн-сервисы существенно повышают потребительские качества прикладного и системного программного обеспечения операционных систем, но, с другой стороны, создают все больше возможностей для производителей программного обеспечения контролировать действия пользователей. Для целого ряда применений защищённых операционных систем вопрос доверия к её разработчику оказывается более значимым, чем вопрос об объёме и качестве реализации в данной операционной системе стандартных механизмов обеспечения безопасности.

Именно этими соображениями можно объяснить рост интереса к отечественным защищённым операционным системам, отмечающийся в последнее время в Российской Федерации со стороны органов государственной власти и предприятий промышленности. Дополнительным стимулом по данному направлению стало принятое Правительством Российской Федерации решение об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд.

В современных условиях перспективная отечественная защищённая операционная система должна отвечать следующим требованиям:

- соответствовать требованиям обеспечения технологической независимости (импортозамещения) Российской Федерации в важнейших областях информатизации, телекоммуникации и связи;
- быть пригодной к функционированию в компьютерных сетях – как изолированных, так и подключённых к сети Интернет (или иным телекоммуникационным сетям), в том числе ориентированных на обработку информации, отнесённой к государственной тайне, или персональных данных;
- реализовывать современные механизмы обеспечения информационной безопасности, учитывающие возможность обработки в данной операционной системе информации, отнесённой к государственной тайне, как с точки зрения удовлетворения формальных требований соответствующих нормативных документов и стандартов, так и с точки зрения обеспечения реальной защиты от актуальных угроз безопасности.

Разработчик такой операционной системы должен обладать развитой инфраструктурой разработки и сопровождения её прикладного и системного программного обеспечения. Должны быть реализованы механизмы, обеспечивающие доверие к разработчику операционной системы, возможность научного обоснования безопасности реализуемых в ней программно-технических решений.

3.3.2. Базовые средства безопасности

Базовые средства безопасности операционных систем семейства Linux унаследованы от ранних версий ОС семейства UNIX, разрабатывавшихся в начале 70-х годов прошлого столетия. Исходя из требований обратной совместимости со старыми версиями, операционные системы семейства Linux продолжают поддерживать целый ряд устаревших защитных механизмов и концепций.

В частности, в подсистемах защиты большинства этих операционных систем присутствуют следующие качества:

- все объекты (сущности) доступа должны интерпретироваться как файловые объекты, атрибуты защиты других типов объектов не могут корректно описываться штатными средствами операционной системы;
- набор прав доступа субъектов (процессов) к сущностям (файлам, каталогам) сильно ограничен, поддерживаются только три права доступа: чтение, запись и выполнение, а также задаётся владелец каждой сущности;
- полномочия суперпользователя root практически не ограничены;

- отсутствуют механизмы автоматического назначения атрибутов защиты вновь создаваемым сущностей на основе атрибутов защиты контейнеров (каталогов), где эти сущности создаются;
- для динамического изменения полномочий субъектов доступа применяется неудобный и потенциально опасный механизм SUID/SGID;
- не поддерживаются механизмы олицетворения субъектов доступа, осуществляющих клиентский доступ к процессу-серверу;
- не поддерживается автоматическая генерация сообщений аудита при обращениях определённых субъектов к определенным сущностям;
- поддерживаемые средства минимизации полномочий пользователей крайне примитивны;
- не поддерживается мандатный контроль целостности;
- не поддерживается изолированная программная среда, даже частично.

Отдельно стоит отметить проблемы безопасности графического интерфейса X Window System, используемого в современных версиях операционных систем семейства Linux для взаимодействия с процессами пользователей. Еще в 1994 г. Р. Браатен в нашумевшем в свое время сообщении в ходе конференции comp.security. Unix сформулировал угрозу похищения графическим приложением X Window System конфиденциальной информации, адресованной другому графическому приложению. В ОС семейства Microsoft Windows, начиная с ОС Windows Vista, введён мандатный контроль целостности графических сущностей, значительно повысивший защищённость графической подсистемы, однако в X Window System ничего подобного не произошло.

3.3.3. Отечественные и зарубежные защищенные операционные системы, построенные на базе Linux

Попытки построить на базе операционных систем семейства Linux защищённую операционную систему неоднократно предпринимались как в России, так и за рубежом.

Исторически можно считать, что первым проектом в данном направлении является операционная система Linux-Mandrake Russian Edition, разрабатывавшаяся группой энтузиастов в 1999 – 2000 гг., в дальнейшем трансформировавшимся в проект операционной системы ALT Linux, поддерживаемый компанией «Альт Линукс». Начиная с 2005 г. дистрибутив операционной системы ALT Linux является полностью самостоятельным. Подсистема безопасности операционной системы ALT Linux имеет несколько интересных нововведений (раздельное хранение аутентификационных данных разных пользователей, минимизация количества SUID- и SGID-программ), которые, однако, не оказывают существенного влияния на общую защищённость операционной системы. Исходя из этого, можно предположить, что разработчики операционной

системы ALT Linux ориентируются на применение данной операционной системы главным образом в тех организациях, где к безопасности хранимой и обрабатываемой информации не предъявляется высоких требований (например, в школах, университетах и т.д.).

Следующей попыткой построить на базе операционной системы семейства Linux высокозащищённую операционную систему, по всей видимости, стала операционная система «Феникс», разрабатывавшаяся в Санкт-Петербургском государственном политехническом университете начиная с 2001 г. Данная операционная система ограниченно применялась в ЗАО «Инфосистемы Джет».

Далее некоторое время самой защищённой российской операционной системой семейства Linux являлась Мобильная система Вооружённых Сил (МСВС), разработанная по заказу Минобороны России Всероссийским научно-исследовательским институтом автоматизации управления в непромышленной сфере (ВНИИНС) на основе ОС Red Hat Enterprise Linux. ОС МСВС была принята на снабжение Вооружённых Сил в 2002 г. На протяжении многих лет она широко применялась в самых различных компьютерных системах военного и двойного назначения, существуют её настольные и серверные версии, предназначенные для функционирования на обычных бытовых компьютерах.

В 2006 г. в Китае начались поставки в военные и государственные учреждения операционной системы Kylin, разработанной китайским Национальным университетом оборонных технологий на базе ОС FreeBSD. Дистрибутив операционной системы Kylin некоторое время был доступен для скачивания. По мнению экспертов, данная операционная система не содержит каких-либо выдающихся защитных механизмов, никто не упоминает о поддержке в ней мандатного управления доступом, мандатного контроля целостности, изолированной программной среды и т.п.

Семейство отечественных операционных систем «РОСА» производится с 2009 г. группой компаний «РОСА» на основе операционной системы Mandriva Linux, являясь в настоящее время последней поддерживаемой её ветвью. Семейство операционных систем «РОСА» включает в себя сертифицированные защищённые ОС «РОСА Хром» и «РОСА Никель» (заявлена поддержка мандатного управления доступом), «РОСА Кобальт», а также несколько свободно распространяемых дистрибутивов, потребительские качества которых оцениваются пользователями довольно высоко. Весной 2015 г. «НТЦ ИТ РОСА» вошла в число пяти российских компаний, подавших заявку на государственную поддержку отечественных программных продуктов.

Операционная система «Заря» разработана АО «Центральный научно-исследовательский институт экономики информатики и систем управления» (ЦНИИ ЭИСУ) по заказу Минобороны России в 2013 г.

Данная операционная система основана на операционной системе CentOS Linux, доступные в сети Интернет схемы её архитектуры не содержат каких-либо уникальных особенностей, существенно отличающих её от других операционных систем семейства Linux. Некоторые источники позиционируют операционную систему «Заря» как следующее поколение ОС МСВС. Операционная система «Заря» совместима с пакетами программного обеспечения Libre Office, GIMP и Chromium, существуют версии ОС для настольных, серверных и встраиваемых систем.

В 2013–2014 гг. компанией «Ред Софт» по заказу Федеральной службы судебных приставов (ФССП) России разработана ОС «ГосЛинукс», также основанная на операционной системе CentOS, которая позиционируется как защищённая операционная система с функциями, позволяющими «приставу обрабатывать персональные данные должников и взыскателей без дополнительных средств защиты информации, а также применять электронную подпись для издания документов в электронном виде». На официальном сайте ФССП России утверждается, что «основные доработки, выполненные подрядчиком, касались криптографической подсистемы и предконфигурации встроенных средств защиты информации».

В целом, несмотря на очевидные недостатки безопасности операционных систем семейства Linux, широкий спектр не всегда удачных разработок защищённых операционных систем на их основе, в настоящее время операционные системы этого семейства по-прежнему являются удобной платформой для создания на их основе отечественной защищённой операционной системы.

3.3.4. Архитектура, назначение и области применения операционной системы специального назначения Astra Linux Special Edition

При построении перспективных и модернизации существующих автоматизированных систем актуальной задачей является использование типовых решений, стандартизация и унификация аппаратно-программных платформ, включая операционные системы, среды разработки программного обеспечения, комплексов системного и прикладного программного обеспечения для поддержки функционирования актуальных информационных сервисов автоматизированной системы. Подобный подход в первую очередь связан со снижением затрат на развёртывание и администрирование компонентов автоматизированных систем, сокращением сроков разработки и/или переноса требуемого для их функционирования программного обеспечения, повышением эффективности процесса обучения персонала, администрирующего и эксплуатирующего их информационную инфраструктуру.

Дополнительным аспектом, актуальным для современных условий,

являются вопросы ограничения применения в рамках автоматизированных систем (в первую очередь функционирующих в интересах органов государственной власти) продукции иностранного производства, для которой существуют отечественные аналоги. В частности, изменения, внесённые в Федеральные законы «Об информации, информационных технологиях и о защите информации» и «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», имеют прямое отношение к курсу на импортозамещение, базирующемуся на тенденциях развития рынка российского программного обеспечения.

При этом в ходе решения этой задачи важным фактором является строгое соответствие подобных разработок национальным стандартам в области информационной безопасности, например, для АСЗИ – это ГОСТ 51583–2014 «Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения», и требованиям отечественных систем сертификации средств защиты информации по требованиям безопасности информации.

В этом смысле операционная система специального назначения в достаточной степени учитывает большинство из рассмотренных выше аспектов. Согласно технической документации, базовым назначением операционной системы специального назначения является построение на её основе автоматизированных систем в защищенном исполнении, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну с грифом не выше «совершенно секретно».

В общем же случае, наряду с защитой такой информации, автоматизированные системы, реализованные с использованием операционной системы специального назначения, могут обеспечивать защиту следующих видов информации:

- конфиденциальная информация;
- коммерческая тайна;
- персональные данные.

Указанные возможности операционной системы специального назначения подтверждаются сертификатом соответствия № 2557 от 27 января 2012 г. в системе сертификации ФСТЭК России. Проведенные испытательной лабораторией ЗАО «НПО Эшелон» сертификационные испытания подтвердили соответствие операционной системы требованиям руководящих документов ФСТЭК России по 3-му классу защищенности средств вычислительной техники и 2-му уровню контроля отсутствия недекларированных возможностей. Операционная система может использоваться при создании автоматизированных систем до класса защищенности 1Б включительно.

Архитектурной основой операционной системы специального назначения является проект Debian GNU/ Linux – ассоциация

разработчиков свободного ПО, основой которого являются ОС семейства GNU/Linux на базе ядра Linux Kernel.

В связи с этим, в общем случае, архитектура ОССН соответствует архитектурным решениям GNU/Linux.

При этом особенности реализации соответствуют особенностям реализации ОС проекта Debian GNU/Linux.

Существующие релизы дистрибутива операционной системы специального назначения базируются на указанных версиях. Редакция релиза дистрибутива определяет специфику дистрибутива: поддерживаемый перенос (аппаратная платформа) и область применения. Номер версии – две или три цифры, определяющие версию дистрибутива операционной системы специального назначения. Текущий релиз – 1.7.

Релиз «Смоленск» операционной системы специального назначения Astra Linux Special Edition предназначен для функционирования на средствах вычислительной техники с процессорной архитектурой x86-64.

Релиз «Новороссийск» предназначен для функционирования на мобильных и встраиваемых компьютерах с процессорной архитектурой ARM.

Релиз «Мурманск» разработан для функционирования на мэйнфреймах IBM System Z. IBM System z (более раннее название – IBM eServer zSeries) – бренд, созданный компанией IBM для обозначения линейки мейнфреймов. Буква Z происходит от «zero down time», которое означает «ноль времени недоступности», позволяющее непрерывно поддерживать работу сервера 24 часа в сутки, 7 дней в неделю 365 дней в году.

Релиз «Севастополь» – дистрибутив Astra Linux Special Edition, предназначенный для функционирования на настольных, мобильных и встраиваемых компьютерах с процессорной архитектурой MIPS.

Релиз «Керчь» – дистрибутив Astra Linux Special Edition, предназначенный для функционирования на высокопроизводительных серверах, базирующихся на платформах с процессорной архитектурой POWER.

Базовые компоненты, библиотеки и средства разработки в составе дистрибутива операционной системы специального назначения реализуют следующие базовые функции:

- запуск программ, их загрузка в оперативную память и управление их выполнением;
- поддержка вытесняющей многозадачности;
- диспетчеризация аппаратных ресурсов компьютера между выполняющимися программами;
- межпроцессное взаимодействие;
- организация механизма виртуальной памяти;

- поддержка операций ввода/вывода и логической организации запоминающих устройства (жёсткие диски, SSD-диски, оптические диски, USB-диски);
- поддержка файловых систем;
- поддержка ввода/вывода к периферийным устройствам;
- поддержка стеков сетевых протоколов;
- обеспечение многопользовательского режима работы;
- обеспечение CLI (Command Line Interface) пользовательского интерфейса командной строки;
- обеспечение GUI (Graphical User Interface) пользовательского графического интерфейса, в том числе и для компьютеров, оборудованных сенсорными экранами, поддерживающими многоточечный ввод;
- поддержка разработки и отладки прикладного программного обеспечения с CLI и GUI пользовательским интерфейсом.

Для организации доменной сетевой инфраструктуры, развёрнутой на базе операционной системы специального назначения, в состав её дистрибутива входит OpenLDAP – реализация протокола LDAP с открытым исходным кодом. Для формирования ключей шифрования, сертификатов открытых ключей и выполнения шифрования данных SSL/TLS соединений в состав дистрибутива операционной системы специального назначения входит криптографический пакет OpenSSL.

Поддержка OpenLDAP и OpenSSL обеспечивает реализацию функции единого пространства пользователей (ЕПП) в рамках доменной инфраструктуры Astra Linux Directory (ALD) с поддержкой резервирования контроллеров домена и установления между ними отношений доверия.

Кроме базовых компонентов, библиотек и средств разработки в состав дистрибутива ОССН входит общее ПО, реализующее следующие функции:

- обработка документальной информации (текстовые, табличные редакторы и средства создания презентационных материалов и доступа к реляционным базам данных);
- сканирование, печать и передача документальной информации;
- доступ к информации, хранящейся в реляционных базах данных, включая поддержку программного обеспечения «1С» и программного обеспечения для работы с географическими объектами PostGIS.

Перечень основных компонентов программного обеспечения показан в таблице 3.3.1.

Ключевой особенностью дистрибутива ОССН является то, что в его состав входят СЗИ, обеспечивающие реализацию следующих функций:

- аутентификация пользователей с использованием инфраструктуры PAM (Pluggable Authentication Modules) локально и в рамках единого пространства пользователей, двухфакторная аутентификация на основе

цифровой подписи и инфраструктуры открытых ключей, поддерживаемых внешним носителем аутентификационной информации «Рутокен»;

Таблица 3.3.1

Перечень основных компонентов программного обеспечения Astra Linux

Защищенная система управления базами данных (СУБД)	PostgreSQL
Работа с документами. Пакет офисных программ	LibreOffice (текстовый редактор, табличный редактор, программа подготовки презентаций, механизм подключения к внешним СУБД, векторный графический редактор, редактор формул)
Защищенный комплекс программ гипертекстовой обработки данных	Web-сервер Apache Браузер Firefox
Защищенные средства передачи электронной почты	Сервер электронной почты Exim Сервер электронной почты Dovecot Почтовый клиент Thunderbird
Редактор растровой графики	GIMP

- идентификация пользователей с использованием модульного окружения NSS (Name Service Switch) локально и в рамках единого пространства пользователей;
- дискреционное управление доступом процессов (субъект-сессий) к ресурсам (сущностям) с поддержкой стандартов Minimal ACL и Extended ACL (в последующих версиях ОССН дискреционное управление доступом будет заменено ролевым управлением доступом в сочетании с мандатным управлением доступом и контролем целостности, реализованными на основе мандатной сущностно-ролевой ДП - модели – МРОСЛ ДП-модели, базовые элементы которой будут рассмотрены в следующих параграфах);
- вместо системы принудительного контроля доступа SELinux в Astra Linux Special Edition используется запатентованная мандатная сущностно-ролевая ДП-модель управления доступом и информационными потокам (МРОСЛ ДП-модель);
- основанное на МРОСЛ ДП-модели мандатное управление доступом процессов к ресурсам, реализация которого в ОССН осуществляется на уровнях механизма межпроцессного взаимодействия, включая файловые системы ртос и tmpfs, стек протоколов TCP/IP (IPv4), на уровне виртуальной файловой системы (VFS) и в файловых системах семейства extfs (Ext2, Ext3, Ext4);
- изоляция адресных пространств процессов;

- регистрация (протоколирование) и аудит событий, реализованные в виде централизованной системы с функцией оповещения администратора безопасности о попытках НСД;
- очистка оперативной памяти и освобождаемых областей данных на носителях с файловыми системами Ext2, Ext3, Ext4:
- регламентный контроль целостности сущностей файловой системы, в том числе неизменности исполняемых файлов и соответствия эталонному дистрибутиву ОССН, на основе библиотеки libgost, в которой реализована функция хэширования в соответствии с ГОСТ Р 34.11-94 [3], и мандатный контроль целостности, препятствующий доступу к защищаемой информации скомпрометированными субъектами после перехвата управления и повышения привилегий (элементы мандатного контроля целостности также заданы в рамках МРОСЛ ДП-модели и рассмотрены в главе 2);
- базирующаяся на мандатном контроле целостности замкнутая программная среда, позволяющая определить для каждой учётной записи пользователя индивидуальный перечень ПО, разрешённого для использования, с возможностью загрузки иерархических цепочек ключей для проверки цифровой подписи исполняемых файлов формата ELF (Executable and Linkable Format), реализованной в соответствии с ГОСТ Р 34.10-2001 [2];
- маркировка документов уровнями конфиденциальности при выводе их на печать;
- обеспечение надёжного восстановления ОССН после сбоев;
- реализация правил управления доступом к внешним носителям (для этого в рамках МРОСЛ ДП-модели заданы сущности с косвенными метками);
- обеспечение доступа к реляционным базам данных в соответствии с требованиями для управления доступом к информации, содержащей сведения, составляющие государственную тайну с грифом не выше «совершенно секретно», совместимого с реализованными в ОССН мандатным управлением доступом и мандатным контролем целостности (с этой целью МРОСЛ ДП-модель была расширена для использования с штатной для ОССН СУБД PostgreSQL);
- обеспечение доступа к информации через сервер гипертекстовой обработки данных, обмена сообщениями электронной почты в соответствии с требованиями для управления доступом к информации, содержащей сведения, составляющие государственную тайну с грифом не выше «совершенно секретно». Дополнительно в состав ядра дистрибутива ОССН добавлен пакет дополнений модуля PaX (средство ограничения прав доступа к страницам памяти), обеспечивающий выполнение программного обеспечения в режиме наименьших привилегий и защиту от эксплуатации в нём различных уязвимостей путём:

- запрета записи в область памяти, помеченную как исполняемая;
- запрета создания исполняемых областей памяти;
- запрета перемещения сегмента кода;
- запрета создания исполняемого стека;
- случайного распределения адресного пространства процесса.

Важным компонентом ОССН является подсистема обеспечения безопасности PARSEC, расширяющая стандартную для ОС семейства Linux систему привилегий, предназначенную для передачи пользователям прав выполнения функций администратора ОССН с поддержкой мандатного управления доступом и мандатного контроля целостности.

Подсистема PARSEC поддерживает следующие расширенные привилегии:

- посылать сигналы процессам, игнорируя дискреционные и мандатные правила управления доступом;
- изменять уровни доступа (мандатные метки) учётных записей пользователей и устанавливать другие привилегии;
- менять уровни конфиденциальности (мандатные метки) конфиденциальности файлов;
- управлять политикой аудита;
- игнорировать правила мандатного управления доступом при чтении и поиске файлов (исключая функцию записи);
- создавать привилегированный сокет и менять его уровень конфиденциальности;
- изменять время доступа к файлу;
- игнорировать мандатное управление доступом по уровням конфиденциальности и неиерархическим категориям;
- устанавливать привилегии на файлы;
- устанавливать любой непротиворечивый набор привилегий для выбранного процесса;
- менять уровень конфиденциальности точки сетевого соединения.

Подсистема безопасности PARSEC реализует указанные расширенные привилегии с использованием механизма перехвата системных вызовов (hook), который перехватывает и анализирует аргументы запросов процессов и в соответствии с установленными правилами мандатного управления доступом разрешает или запрещает их. Таким образом, в ОССН мандатный контекст (используемые в запросе уровни конфиденциальности, доступа и целостности) считывается при выполнении каждого запроса локально или удалённо (в рамках единого пространства пользователей) запущенного процесса.

Уникальной особенностью подсистемы обеспечения безопасности PARSEC является её реализация в качестве модуля XPARSEC, расширяющего функциональность сервера X.Org и менеджера окон Fly-wm. Благодаря этому модулю сервер X.Org получает возможность

определения привилегий X.Org клиента (программы с GUI интерфейсом) и передачи их с использованием модифицированного X-протокола менеджеру окон Fly-wm, который и выполняет привилегированные операции в ходе запуска X.Org клиента с различными мандатными контекстами.

При этом на рабочем столе Fly выполняется отображение:

- мандатного контекста пользовательской сессии в области уведомлений на панели задач;
- мандатного уровня конфиденциальности и целостности каждого окна;
- уровня конфиденциальности окна для локально и удалённо запущенного приложения (цветовое обрамление – рамка окна приложения);
- мандатного уровня и целостности всех приложений, размещённых на рабочем столе Fly.

3.4. Обеспечение безопасности сетевой инфраструктуры

3.4.1. Общее описание сетевой инфраструктуры

Сетевая инфраструктура определяет способ подключения устройств друг к другу для обеспечения сквозной связи. Для определения принципов сетевого взаимодействия при работе сети рассматривают модель взаимодействия открытых систем (OSI), а также модель стека TCP/IP, как показано на рис. 3.4.1.

Возможность сетевого взаимодействия обеспечивается согласованной работой стека коммуникационных протоколов. При этом на каждом узле происходит непосредственное взаимодействие протоколов конкретного слоя стека TCP/IP с соседним слоем (слоя сетевого доступа со слоем интернета, слоя интернета с транспортным слоем и т.д.), а опосредованное взаимодействие между участниками происходит на соответствующих уровнях стека протоколов (между уровнями сетевого доступа, между уровнями интернета, между транспортными уровнями и т.д.). Каждый слой стека обеспечивает работу своей группы протоколов, как показано на рис. 3.4.2.

В процессе сетевого взаимодействия используется несколько видов адресов: на уровне сетевого доступа – MAC адреса, на межсетевом уровне – IP-адреса, на транспортном уровне – номера портов. Точкой входа в конкретную сетевую программу (Web-обозреватель, клиент обмена мгновенными сообщениями, сервер FTP и т.п.) у каждого из участников сетевого взаимодействия является номер порта. Совокупность IP адреса, типа протокола транспортного уровня и номера транспортного порта называется сокетом. Как правило, для сетевого взаимодействия требуется две пары сокетов: серверный сокет и клиентский сокет.

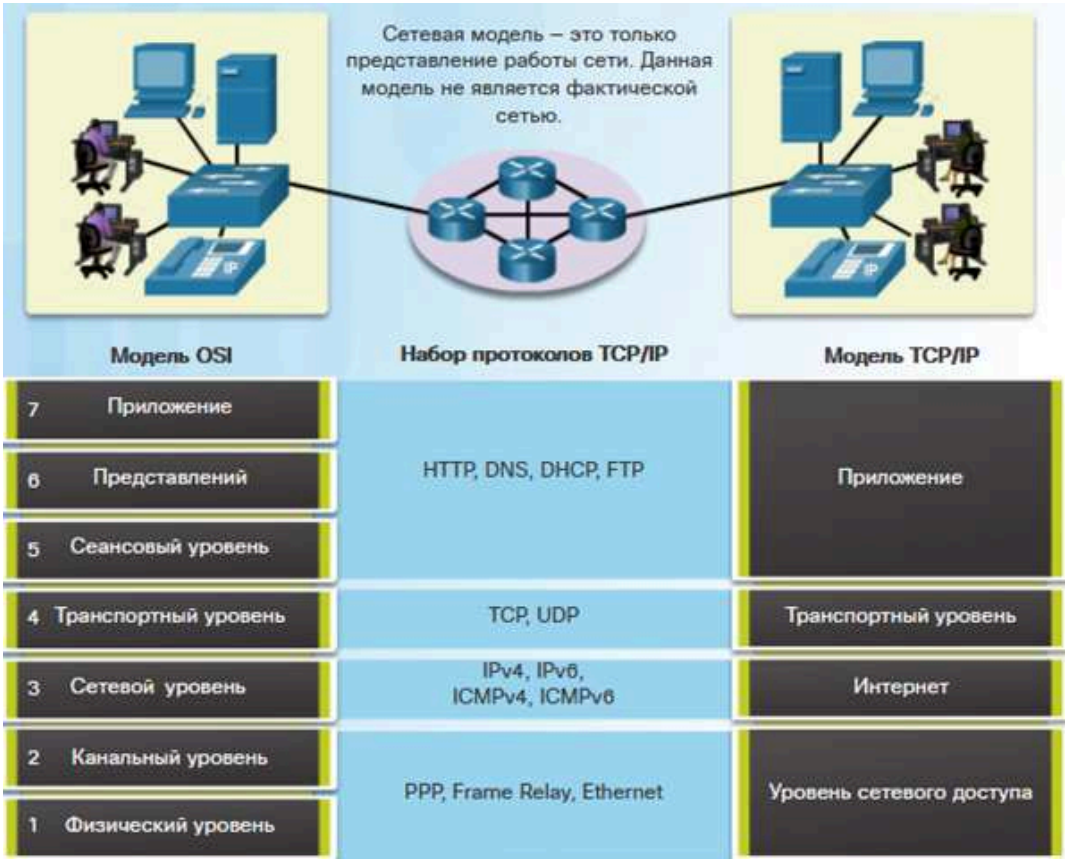


Рис. 3.4.1. К пояснению принципов сетевого взаимодействия между участниками

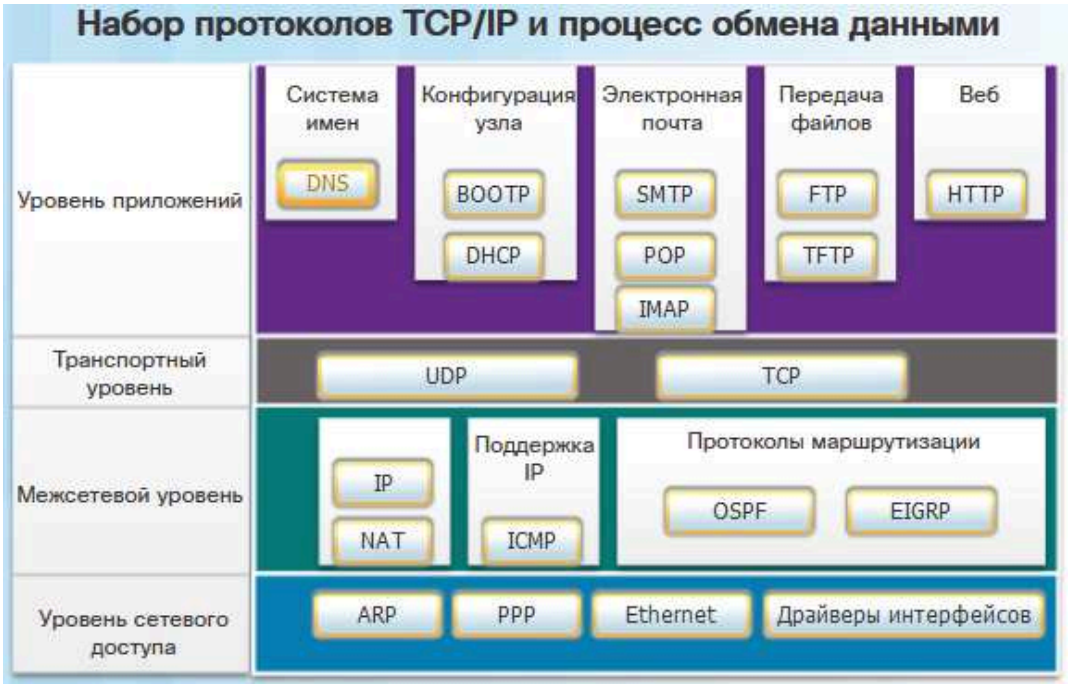


Рис. 3.4.2. К пояснению состава сетевых протоколов

При передаче информации от прикладной программы-клиента некоторого сетевого сервиса происходит ее движение по стеку протоколов сверху вниз. На уровне самой программы информация представляет собой прикладные данные, на транспортном уровне – сегменты, на межсетевом уровне – пакеты и на уровне доступа к сети – кадры. Процесс включения модуля данных протокола предыдущего уровня в модуль данных протокола текущего уровня с одновременным добавлением заголовков и концевиков текущего уровня называется инкапсуляцией (рис. 3.4.3). При поступлении информации на узел назначения происходит аналогичный процесс в обратном направлении – обратная инкапсуляция, иногда называемая декапсуляцией. На рис. 3.4.4 приведен состав кадра Ethernet в процессе взаимодействия клиента с ftp и web сервером.

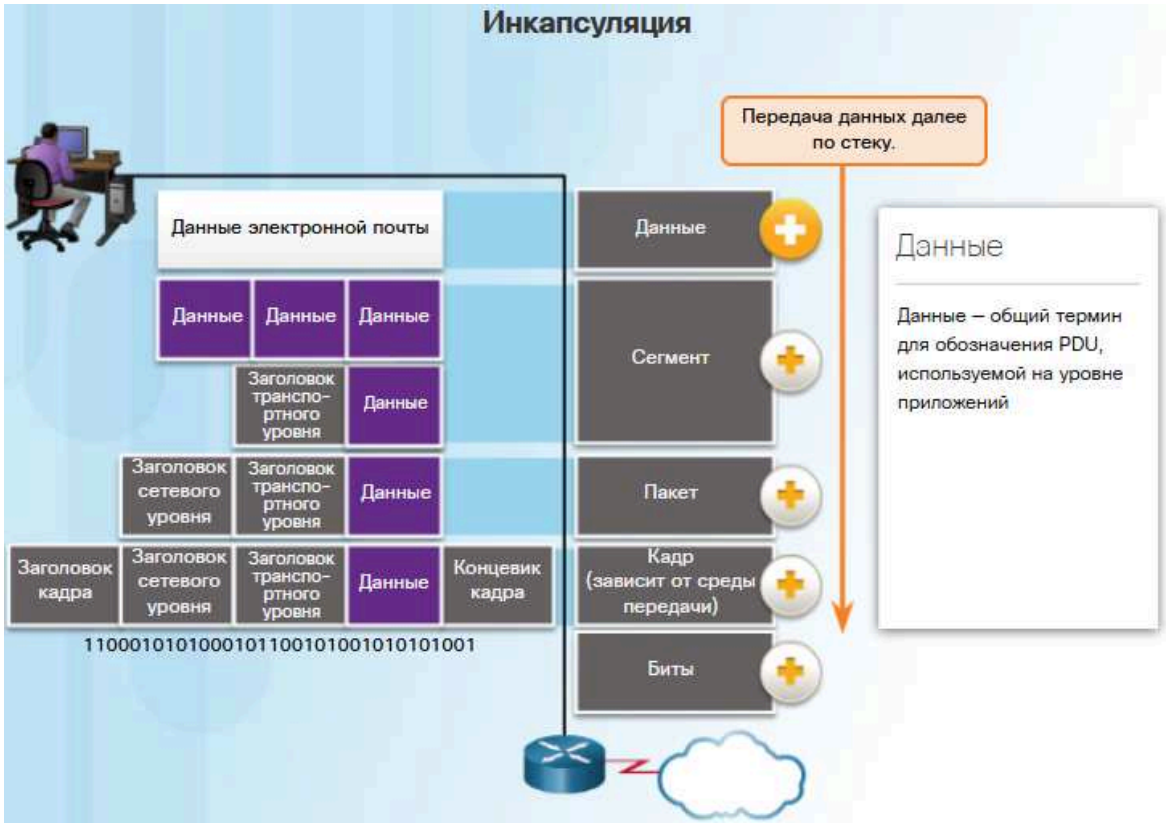


Рис. 3.4.3. К пояснению процесса инкапсуляции

Ethernet работает на уровне 2 модели OSI. Ethernet отвечает за инкапсуляцию данных верхнего уровня в кадре, включающих MAC-адреса источника и назначения. MAC-адреса используются в локальной сети для поиска назначения или шлюза по умолчанию.

IP работает на уровне 3 модели OSI. IP имеет две версии: IPv4 и IPv6. Хотя идет процесс замены IPv4 на IPv6, IPv4 по-прежнему широко распространен в современных сетях. В IPv4 используется 32-разрядное адресное пространство, указываемое в формате десятичного представления с точками, например 192.168.1.1. В IPv6 используется 128-битовое

адресное пространство, указываемое в шестнадцатеричном формате. В IPv6 можно исключать нулевые разряды в каждом хекстете, а также исключить один сегмент со всеми нулями.

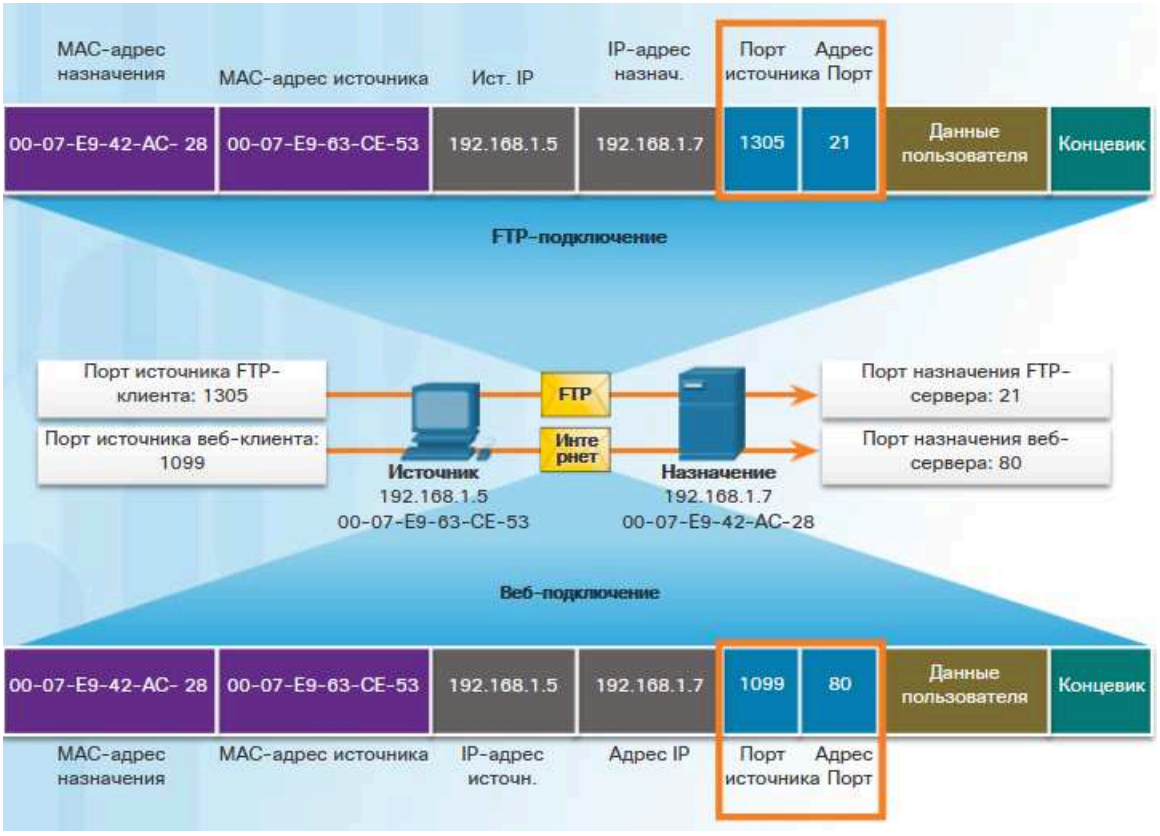


Рис. 3.4.4. Состав кадра Ethernet в процессе взаимодействия клиента с ftp и web сервером

Например, IPv6 адрес 2001:0DB8:0000:1111:0000:0000:0000:0200 можно представить в виде 2001:DB8:0:1111::200.

ICMP в основном используется для тестирования сквозного подключения от источника до места назначения. ICMP для IPv4 отличается от ICMP для IPv6. В ICMP для IPv6 имеется запрос маршрутизаторов, объявления маршрутизаторов и обнаружение дублирующихся адресов. Утилиты ping и traceroute используют функцию ICMP. Команда ping используется для проверки соединения между двумя узлами, но не позволяет получить информацию об устройствах, находящихся между ними. Команда traceroute (tracert) – это утилита, позволяющая составить список переходов, по которым успешно проходит эхозапрос на пути к узлу назначения.

ARP работает между уровнями 2 и 3, сопоставляя MAC-адреса с IP-адресами. Прежде чем хост сможет отправить трафик в удаленную сеть, он должен узнать MAC-адрес шлюза по умолчанию. Хост уже знает IP-адрес шлюза по умолчанию. Например, на хосте с IP-адресом 192.168.1.10 может быть задан шлюз по умолчанию 192.168.1.1. Хост использует ARP-

запрос, чтобы спросить, кому принадлежит конкретный IP-адрес (Who is 192.168.1.1?). Шлюз по умолчанию ответит, указав свой собственный MAC-адрес. На этом этапе хост сопоставил IP-адрес с MAC-адресом шлюза по умолчанию и теперь может формировать кадр для отправки данных в удаленную сеть.

Транспортный уровень отвечает за разделение данных уровня приложения на сегменты, которые могут быть отправлены на сетевой уровень. TCP – это протокол транспортного уровня, используемый когда все данные должны поступать на хост назначения в правильном порядке. UDP – протокол транспортного уровня, используемый когда приложение может допустить потерю некоторых данных при передаче.

На уровне приложения существует ряд важных сетевых служб, о которых должны знать аналитики по кибербезопасности:

- DHCP автоматизирует назначение адресов IPv4, масок подсети, шлюза и других параметров сети IPv4;
- DNS обеспечивает надежные средства управления и предоставления доменных имен и связанных с ними IP-адресов;
- NAT выполняет преобразование между частными и общедоступными адресами IPv4;
- передача файлов. Такие приложения, как FTP, TFTP и SMB, можно использовать для передачи файлов от одного хоста к другому;
- электронная почта требует наличия ряда приложений и служб, включая POP3, IMAP и SMTP;
- HTTP – протокол, используемый для отправки и получения веб-страниц.

3.4.2. Межсетевое экранирование при обеспечении сетевой безопасности

Для обеспечения функций передачи и продвижения информации в IP-сетях используются сетевые устройства различных видов. Основные виды сетевых устройств с описанием их функций сведены в таблицу 3.4.1

Таблица 3.4.1
Виды и функции сетевых устройств

№ п/п	Название устройства	Функция, особенности
1.	Коммутатор	Предназначен для обеспечения сетевого взаимодействия в локальных сетях. Создает и обслуживает таблицы коммутации (сопоставление MAC-адресов и портов). Работают на втором уровне стека TCP/IP. Некоторые модели имеют возможность использовать для работы IP-адреса и называются «коммутаторами третьего уровня». В последнем случае говорят о решении задач

№ п/п	Название устройства	Функция, особенности
		маршрутизации в локальной сети на скорости коммутации (это работает быстрее чем программная маршрутизация)
2.	Оконечные устройства	Устройства, являющиеся источниками трафика или точками приема трафика (компьютеры, ноутбуки, IP телефоны, сетевые принтеры, смартфоны и т.п.). Представляют собой интерфейсы сетевого взаимодействия для конечных пользователей
3.	Точка беспроводного доступа	Обеспечивает подключение беспроводных клиентов к сети
4.	Контроллер беспроводной локальной сети	Управляет беспроводными точками доступа. Позволяет решать задачи безопасности, управления, мониторинга, создания «бесшовной» WiFi сети
5.	Маршрутизатор	Представляет собой устройство сетевого уровня. Предназначен для продвижения и маршрутизации пакетов между сетевыми сегментами по наилучшему пути. Поддерживает в процессе своей работы таблицу маршрутизации. В случае использования динамических протоколов маршрутизации оперирует со специфичными базами данных, обеспечивающими их функционирование и быструю сходимость сети

Различные типы межсетевых экранов позволяют обеспечить безопасность сети:

- межсетевой экран с фильтрацией пакетов (без контроля состояния) обеспечивает фильтрацию уровня 3 и иногда уровня 4;
- межсетевой экран с контролем состояния разрешает или блокирует трафик на основе состояния, порта и протокола;
- межсетевой экран шлюза приложений (межсетевой экран на прокси-сервере) фильтрует информацию на уровнях 3, 4, 5 и 7.

Сервисы сетевой безопасности улучшают защиту сети с помощью следующих средств:

- списки контроля доступа (ACL) – ряд команд, определяющих, должно устройство пересылать или отбрасывать пакеты, исходя из информации, приведенной в заголовке пакета;
- SNMP – эта служба позволяет администраторам осуществлять мониторинг и контролировать производительность сети, находить и устранять проблемы, а также планировать рост сети;
- NetFlow – эта технология предоставляет статистические данные о пакетах, проходящих через маршрутизатор или многоуровневый коммутатор;

- зеркалирование портов – это функция, позволяющая коммутатору создавать копии трафика, проходящего через коммутатор, а затем отправлять их через порт, к которому подключен сетевой монитор;
- сервер системных журналов используется для доступа к системным сообщениям, создаваемым сетевыми устройствами;
- NTP синхронизирует время на всех устройствах в сети, чтобы обеспечить точность и согласованность меток времени системных сообщений;
- AAA – архитектура для настройки служб пользовательской аутентификации, авторизации и учета;
- VPN – частная сеть, создаваемая между двумя оконечными устройствами в общедоступной сети.

Сетевые топологии обычно представлены в виде физических и логических сетей. Топология физической сети относится к физическим соединениям и определяет, как соединены оконечные устройства. Логическая топология относится к стандартам и протоколам, которые используются при взаимодействии устройств. Большинство топологий представляют собой сочетание логической и физической топологий и показывают, как устройства соединяются логически и физически.

Рассматривая топологию, имеющую доступ к внешним или общедоступным сетям, следует определить архитектуру безопасности. Самый простой вариант – назначение внешней сети и внутренней сети, которые определяются двумя интерфейсами на межсетевом экране. Сети, для которых требуется общедоступный доступ к службам, часто имеют демилитаризованную зону DMZ с открытым доступом, при этом доступ к внутренней сети строго блокируется. Межсетевые экраны на основе зональных политик (ZPF) используют концепцию зон, которая обеспечивает дополнительную гибкость. Зона — это группа, состоящая из одного или нескольких интерфейсов со сходными функциями и назначением.

Отдельное место в системе защиты сетевой инфраструктуры принадлежит системам обнаружения вторжений (СОВ или IDS Intrusion Detection System) и (СПВ или IPS Intrusion Prevention System). Ключевые особенности этих систем сведены в таблицу. Функции этих систем, которые могут быть реализованы на транзитных сетевых устройства или серверах или конечных хостах, непосредственно следуют из их названия.

Таблица 3.4.2

Характеристика	IDS	IPS
Более уязвима к методам обхода системы сетевой безопасности, обеспечиваемым различными методами сетевых атак	+	
Может быть источником задержки и джиттера, вызывающих		+

Характеристика	IDS	IPS
снижение производительности в сети		
Должна быть реализована таким образом, чтобы не оказывать негативного влияния на работу чувствительных к задержкам приложений		+
Не может остановить вызвавший тревогу пакет и не гарантирует разрыва подключения	+	
Может использовать методы нормализации потока, чтобы сократить или устранить многие из существующих возможностей обхода системы сетевой безопасности		+
Существует возможность настроить на отбрасывание пакетов		+
В основном предназначен для определения возможных инцидентов, внесения в журнал информации об инцидентах и передачи сообщений об инцидентах	+	
Требует поточной реализации и необходимо прохождение трафика через него		+
Не обладает высокой эффективностью для остановки почтовых вирусов и автоматических атак, таких как интернет-черви	+	

3.5. Характеристики кибератак на сетевые ресурсы

Для того чтобы лучше понимать любые сведения о сетевой безопасности, важно знать следующие термины:

- угроза – потенциальная опасность для ресурсов, таких как данные или сама сеть;
- уязвимость и поверхность атаки. Уязвимости – слабые места в системе или ее архитектуре, которые могут быть использованы злоумышленниками. Поверхность уязвимости к атакам – это сумма всех уязвимостей в конкретной системе, доступных хакерам. Поверхность уязвимости к атакам описывает различные точки, через которые хакеры могут проникнуть в систему и где они могут получить данные из системы. Например, вашей операционной системе и веб-обозревателю могут требоваться исправления системы безопасности, так как они уязвимы для атак. Вместе они образуют поверхность атаки, которой может воспользоваться злоумышленник;
- эксплойт – механизм для использования уязвимости в целях взлома ресурса. Эксплойты могут быть локальными или удаленными. Удаленный эксплойт работает по сети без предварительного получения доступа к целевой системе. Хакеру не требуется учетная запись в конечной системе для эксплуатации уязвимости. В локальном эксплойте хакер имеет некоторый вид пользовательского или административного доступа к конечной системе. Локальный эксплойт не обязательно означает, что хакер имеет физический доступ к конечной системе;

- риск – вероятность того, что определенная угроза выразится в использовании определенной уязвимости ресурса и приведет к нежелательным последствиям;
- управление рисками – это процесс, который балансирует эксплуатационные расходы по обеспечению защитных мер с преимуществами, достигнутыми за счет защиты ресурса. Существует четыре основных метода управления рисками;
- принятие риска – когда стоимость вариантов управления рисками перевешивает стоимость самого риска. Риск принимается без действий.
- предотвращение риска – действие, которое позволяет исключить любую подверженность риску. Обычно это самый дорогой вариант мер по снижению рисков;
- ограничение рисков – ограничение подверженности компании риску за счет принятия определенных мер. Это стратегия, в которой часть рисков принимается и часть рисков предотвращается. Это самая распространенная стратегия снижения рисков;
- передача риска – риск передается заинтересованной третьей стороне, например страховой компании.

Ниже приводятся другие часто используемые термины из области сетевой безопасности:

- контрмеры – защитное решение, устраняющее угрозу или риск;
- влияние – ущерб, который был причинен организацией данной угрозой.

Для локального эксплойта необходим доступ к сети изнутри, например пользователь с учетной записью в сети. При удаленном эксплойте для использования уязвимости сети учетная запись в этой сети не нужна.

Основные категории атак составляют:

- разведывательные атаки;
- атаки доступа;
- атаки типа «отказ в обслуживании» (DoS-атаки).

3.5.1. Разведывательные атаки

Разведкой называется сбор информации. Такие атаки аналогичны вору, который осматривает окрестности, переходя от двери к двери и притворяясь, будто что-то продает. Вор фактически ищет уязвимые дома для взлома, например: незанятые дома, дома с легко открывающимися окнами и дверьми и дома без систем безопасности или камер видеонаблюдения.

Злоумышленники используют разведывательные атаки для несанкционированного обнаружения и сопоставления систем, служб или уязвимостей. Разведывательные атаки, нацеленные на оконечные

устройства в сети, такие как компьютеры и серверы, также называются профилированием хостов. Это связано с тем, что хакер может получить профиль системы, включая тип и версию операционной системы. Если в системе установлены не все обновления и исправления, хакер затем ищет известные уязвимости, которыми можно воспользоваться.

Разведывательные атаки предшествуют атакам доступа или DoS-атакам и часто используют свободно доступные инструменты.

Ниже перечислены некоторые методы, используемые хакерами в ходе разведывательных атак.

– Информационный запрос к целевому объекту. Хакер ищет исходную информацию о целевом объекте. Для этого используются общедоступные инструменты, включая поиск веб-сайта организации в Google. Общедоступную информацию о целевой сети можно получить из реестров DNS с помощью служебных программ dig, nslookup и whois.

– Запуск ping-тестирования адресов целевых сетей. Злоумышленник запускает ping-тестирование адресов целевых сетей, обнаруженных предыдущими DNS-запросами, для определения адресов в целевой сети. Ping-тестирование выявляет активные IP-адреса. Это позволяет создать логическую топологию целевой сети.

– Запуск сканирования портов активных IP-адресов. Хакер запускает сканирование портов на хостах, найденных в ходе эхотестирования, чтобы определить доступные порты или службы. Инструменты сканирования портов, такие как Nmap, SuperScan, Angry IP Scanner и NetScanTools, инициируют подключения к целевым хостам, выполняя поиск портов, открытых на целевых компьютерах.

– Запуск сканеров уязвимостей. Злоумышленник отправляет запросы на выявленные порты с помощью таких инструментов сканирования уязвимостей, как Nipper, Secunia PSI, Core Impact, Nessus, SAINT или Open VAS. Целью является поиск потенциальных уязвимостей на целевых хостах.

– Запуск инструментов использования уязвимостей. Теперь хакер пытается использовать выявленные уязвимости в системе. Злоумышленник применяет инструменты использования уязвимостей, такие как Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit и Netsparker.

3.5.2. Атаки доступа

Существует несколько распространенных типов атак доступа.

– Взлом пароля. Злоумышленники пытаются раскрыть пароли критически важных систем с применением фишинговых атак, словарных атак, атак методом перебора, анализатора сетевого трафика или методов социальной инженерии. Атаки методом перебора паролей включают повторяющиеся попытки подбора пароля с помощью различных инструментов, таких как Ophcrack, L0phtCrack, THC Hydra, RainbowCrack

и Medusa.

– Атака передачей хеша. Злоумышленник, уже получивший доступ к компьютеру пользователя, использует вредоносное ПО для доступа к сохраненным хешам паролей. Затем эти хеши используются для аутентификации на других удаленных серверах или устройствах без необходимости перебора паролей.

– Злоупотребление доверием. Хакер с помощью доверенного хоста пытается получить доступ к сетевым ресурсам. Например, доверенным является внешний хост, получающий доступ к внутренней сети через VPN. Если этот доверенный хост атакован, хакер может использовать его для получения доступа к внутренней сети.

– Переадресация портов. Злоумышленник использует взломанную систему в качестве базы для атак на другие целевые объекты (см. рис. 3.5.2).

– Атака через посредника. Злоумышленник располагается между двумя доверяемыми объектами, чтобы читать, изменять или перенаправлять данные, которыми они обмениваются.

– Подмена адреса IP, MAC, DHCP. Атаки, в которых одно устройство пытается выдавать себя за другое путем подделки данных адреса. Существует несколько типов атак с использованием подмены. Например, подмена MAC-адреса происходит, когда один компьютер принимает пакеты данных по MAC-адресу другого компьютера, который является настоящим местом назначения данных.

3.5.3. Атаки методами социальной инженерии

Социальная инженерия – это атака доступа, в ходе которой осуществляются попытки манипуляции отдельными людьми, чтобы побудить их совершить определенные действия или разгласить конфиденциальную информацию, такую как пароли и имена пользователей. Обычно для ее проведения необходимо применять социальные навыки для манипулирования пользователями внутри сети с целью получения информации, необходимой для доступа к сети.

Социальные инженеры часто полагаются на готовность людей помочь. Они также используют человеческие слабости. Например, злоумышленник может обратиться к уполномоченному сотруднику с неотложной проблемой, при которой требуется немедленный сетевой доступ. Злоумышленник может сыграть на тщеславии или жадности сотрудника или сослаться на известный авторитет.

Примеры психологических атак:

– претекстинг. Злоумышленник звонит человеку и вводит его в заблуждение, стремясь получить доступ к конфиденциальным данным. Например, злоумышленник притворяется, что ему необходимы личные или финансовые данные для подтверждения подлинности получателя;

– спам. Злоумышленник использует спам, чтобы обманом заставить пользователя перейти по зараженной ссылке или загрузить зараженный файл;

– фишинг. Существует множество вариантов этого метода социальной инженерии. В наиболее распространенном варианте злоумышленник рассылает отдельным пользователям по электронной почте специально разработанный привлекательный спам, рассчитывая, что пользователь нажмет ссылку или загрузит вредоносный код;

– услуга за услугу (взаимовыгодный обмен). Злоумышленник запрашивает личную информацию в обмен на что-то, например, на подарок;

– несанкционированное проникновение. Злоумышленник проникает в закрытую зону следом за уполномоченным лицом с корпоративным пропуском. Таким образом, он получает доступ в защищенную зону;

– приманка. Злоумышленник оставляет зараженное вредоносным ПО физическое устройство, например, USB-накопитель, в общедоступном месте, например, в туалетной комнате для сотрудников компании. Нашедший устройство может вставить его в свой компьютер. На хосте под управлением ОС Windows функция автозапуска может автоматически установить вредоносное ПО;

– визуальное хакерство. Злоумышленник физически следит за жертвой при вводе учетных данных, таких как идентификатор пользователя рабочей станции, PIN-код в банкомате или комбинация на физическом замке. Такой подход также называется «взгляд через плечо».

Фишинг – распространенный метод социальной инженерии, используемый злоумышленниками, который заключается в отправке электронных писем, замаскированных под письма от настоящей организации (такой как банк).

Ниже описаны варианты фишинговых атак:

– направленный фишинг. Это фишинговая атака, предназначенная специально для определенного человека или организации, поэтому она с большей вероятностью достигнет цели;

– уэйлинг. Похож на направленный фишинг, но ориентирован на крупные цели, например, на топ-менеджеров организации;

– фарминг. В ходе этой атаки происходит взлом служб доменных имен путем добавления записей в локальные файлы узла. Фарминг также включает порчу DNS путем взлома серверов DHCP, указывающих серверы DNS своим клиентам;

– атака типа «водопой» (watering hole). В ходе этой атаки сначала выявляются веб-сайты, регулярно посещаемые целевой группой. Далее злоумышленник пытается взломать эти веб-сайты, заразив их вредоносным ПО, которое предназначается только для членов этой целевой группы и может идентифицировать их;

– вишинг. Это фишинговая атака с использованием голоса и телефонной системы вместо электронной почты;

– смишинг. Это фишинговая атака с использованием текстовых SMS вместо электронной почты.

3.5.4. Атаки типа «отказ в обслуживании»

Атаки типа «отказ в обслуживании» (DoS) – это получившая широкую известность разновидность сетевой атаки. DoS-атака приводит к перебоям в обслуживании пользователей, устройств или приложений.

Существует два главных источника DoS-атак:

– перегрузка большим объемом трафика. Сеть, хост или приложение не может обработать огромные объемы данных, что приводит к сбою системы или очень сильному замедлению ее работы;

– пакеты с неправильным форматированием. Пакеты данных с неправильным форматированием отправляются на хост или в приложение, и получатель не может обработать непредвиденное условие. Атака с переполнением буфера – это метод, используемый в DoS-атаках этого типа. Например, злоумышленник пересылает пакеты, содержащие ошибки, которые приложение не может выявить, или пакеты с неправильным форматированием. Это вызывает замедление работы или сбой принимающего устройства. Считается, что DoS-атаки создают высокий риск, поскольку они могут легко нарушить бизнес-процессы или работу важных сетевые сервисов и нанести большой ущерб. Проводить такие атаки относительно несложно, это под силу даже неопытным злоумышленникам.

3.5.5. Атаки DDoS

Если злоумышленникам удается взломать много хостов, они могут организовать распределенную DoS-атаку (DDoS). Назначение DDoS-атак аналогично DoS-атакам, за исключением большего масштаба, поскольку DDoS-атака имеет несколько скоординированных источников. В ходе DDoS-атаки могут использоваться сотни или даже тысячи источников, например, в DDoS-атаках на основе интернета вещей.

При описании компонентов DDoS-атаки используются следующие термины:

- зомби – группа взломанных хостов (или агентов). Эти хосты запускают вредоносный код – так называемые роботы (или боты). Вредоносное ПО, превращающее хосты в зомби, постоянно пытается распространять себя аналогично интернет-червю;
- боты – вредоносное ПО, предназначенное для инфицирования хоста и взаимодействия с системой-обработчиком. Боты также могут регистрировать нажатия клавиш, собирать пароли, захватывать и анализировать пакеты и многое другое;

- ботнет – группа зомби, инфицированных самостоятельно распространяющимся вредоносным ПО (т.е. ботами) и управляемых обработчиками;
- обработчики – главные серверы управления и контроля (CnC или C2), осуществляющие управление группами зомби. Для удаленного управления зомби организатор ботнета может использовать протокол IRC или веб-сервер на сервере C2;
- ботмастер – злоумышленник, управляющий ботнетом и обработчиками.

Атаки с переполнением буфера

Цель злоумышленника при использовании DoS-атаки с переполнением буфера – найти на сервере слабое место в защите системной памяти и использовать его. Использование буферной памяти путем ее переполнения непредвиденными значениями обычно делает систему неработоспособной, создавая DoS-атаку.

Например, злоумышленник вводит входные данные, объем которых больше, чем ожидается приложением, которое работает на сервере. Приложение принимает большой объем входных данных и сохраняет его в памяти. В результате оно использует связанный буфер памяти и может перезаписать соседние блоки памяти, что в конечном итоге приводит к повреждению системы и сбою в ее работе.

Одним из первых примеров использования пакетов с неправильным форматированием стала атака Ping of Death (ping-запрос смерти). В ходе этой старой атаки злоумышленник отправлял ping-запрос смерти, который представлял собой ping-запрос в виде IP-пакета, размер которого превышал максимальный размер пакета в 65 535 байт. Принимающий хост не мог обработать пакет такого размера, что приводило к его сбою.

Атаки с переполнением буфера постоянно видоизменяются. Например, в Microsoft Windows 10 была обнаружена уязвимость к удаленной атаке типа «отказ в обслуживании». Злоумышленник создал вредоносный код для доступа к памяти вне диапазона. Когда к этому коду обращается процесс Windows AHCACHE.SYS, он пытается вызвать сбой системы, запрещая обслуживание пользователя.

По некоторым оценкам треть вредоносных атак является результатом переполнения буфера.

3.5.6. Методы обхода средств защиты сетевых ресурсов

Известно, что вредоносное ПО и методы атак наиболее эффективны, когда они остаются необнаруженными. По этой причине во множестве атак используются методы уклонения, чтобы скрыть информационное наполнение атаки. Их целью является предотвращение обнаружения средствами защиты сетей и хостов.

Ниже приведены некоторые методы уклонения, используемые хакерами:

– шифрование и туннелирование. В данном методе уклонения используется туннелирование, чтобы скрыть содержимое, или шифрование для скремблирования содержимого, затрудняя выявление и определение вредоносного ПО многими методиками обнаружения, применяемыми для обеспечения безопасности;

– исчерпание ресурсов. При применении этого метода уклонения поддерживается высокая загруженность хоста, чтобы не позволить ему правильно использовать методики обнаружения, применяемые для обеспечения безопасности;

– фрагментации трафика. В рамках этого метода уклонения информационное наполнение вредоносного ПО разделяется на более мелкие пакеты для обхода этапа обнаружения системой безопасности сети. После того как фрагментированные пакеты обойдут средства обнаружения системы безопасности, вредоносное ПО восстанавливается и может начать отправку конфиденциальных данных за пределы сети;

– неправильная интерпретация на уровне протокола. В этом методе уклонения средства защиты сети неправильно обрабатывают функции PDU, такие как контрольная сумма или значение TTL. Это может вынудить межсетевой экран игнорировать пакеты, которые он должен проверять;

– подмена трафика. При использовании этого метода уклонения хакер пытается обмануть систему предотвращения вторжений (IPS), скрывая данные в информационном наполнении. Для этого они кодируются в другом формате. Например, злоумышленник может использовать кодировку трафика в формате Unicode вместо ASCII. IPS не распознает истинного значения данных, но целевая оконечная система может их прочитать;

– вставка трафика. Аналогична подмене трафика, но злоумышленник вставляет дополнительные байты данных во вредоносную последовательность данных. Правила IPS пропускают вредоносные данные, принимая полную последовательность данных;

– разворот хоста. В этом методе предполагается, что злоумышленник взломал внутренний хост и хочет расширить свой доступ в той сети, куда он проник. Например, злоумышленник получил доступ к паролю администратора на взломанном хосте и пытается войти в систему на другом хосте, используя те же учетные данные;

– руткиты. Это сложный инструмент, используемый опытными хакерами. Он интегрируется с самыми низкими уровнями операционной системы. Когда программа пытается получить список файлов, процессов и сетевых подключений, руткит предоставляет подчищенную версию выходных данных, удаляя все изобличающие данные. Цель руткита —

полностью скрыть действия хакера в локальной системе.

Данный перечень методов обхода средств защиты не является исчерпывающим, поскольку постоянно разрабатываются новые методы атак. По этой причине специалисты по сетевой безопасности должны быть знакомы с новейшими методами атак для их обнаружения.

3.6. Особенности реализации сетевых атак

Злоумышленники в процессе реализации киберпреступлений используют различные инструменты, в том числе следующие:

– взломщики паролей;
– инструменты взлома беспроводных сетей;
– инструменты сканирования и взлома сетей;
– инструменты создания пакетов;
– анализаторы пакетов;
– детекторы руткитов;
– инструменты технической экспертизы;
– отладчики;
– хакерские операционные системы;
– средства шифрования;
– средства использования уязвимостей;
– сканеры уязвимостей.

Эти инструменты могут использоваться для запуска различных атак, включая:

– подслушивание;
– модификация данных;
– спуфинг IP-адресов;
– взлом пароля;
– отказ в обслуживании;
– атака через посредника;
– компрометация ключа;
– анализ сетевого трафика.

Вредоносное ПО (или вредоносный код) разрабатывается с целью повредить, разрушить, украсть данные либо в целом причинить вред или совершить незаконные действия в отношении данных, хостов или сетей. Три наиболее распространенных типа вредоносного ПО: вирусы, интернет-черви и трояны.

Вирус – это тип вредоносного ПО, который распространяется путем внедрения своей копии в другую программу.

Интернет-черви похожи на вирусы, так как тоже реплицируются и могут нанести сравнимый ущерб. Для работы вируса требуются программы на хосте, а интернет-черви могут функционировать самостоятельно.

Троян – это программа, которая маскируется под подлинную, но содержит вредоносный код, использующий права пользователя, запустившего эту программу.

Вредоносное ПО продолжает развиваться. В настоящее время наиболее распространенным типом атак являются вирусы-вымогатели. Вирусы-вымогатели – это вредоносное ПО, которое запрещает доступ к зараженной компьютерной системе или хранящимся в ней данным, пока владелец не заплатит киберпреступнику.

Различные типы инструментов, используемых злоумышленниками для организации атак на сети, можно отнести к одной из следующих категорий:

– разведывательные атаки – несанкционированное обнаружение и сопоставление систем, служб или уязвимостей;

– атаки доступа используют известные уязвимости, чтобы получить доступ к учетным записям в Интернете, конфиденциальным базам данных и другой секретной информации;

– социальная инженерия – это попытка манипулирования отдельными людьми, чтобы заставить их совершить определенные действия или разгласить конфиденциальную информацию, такую как пароли и имена пользователей;

– отказ в обслуживании. Происходит переполнение сети большим объемом трафика, или отправляются пакеты с неправильным форматированием, которые получатель не может обработать, в результате чего работа устройства существенно замедляется или даже происходит его поломка;

– переполнение буфера. Используется слабое место в защите системной памяти для ее переполнения непредвиденными значениями. Цель состоит в выведении ее из строя.

Для того чтобы оставаться в тени и продолжать атаку, злоумышленники используют различные методы уклонения, в том числе следующие:

– шифрование и туннелирование;
– исчерпание ресурсов;
– фрагментация трафика;
– неправильная интерпретация на уровне протокола;
– подмена трафика;
– вставка трафика;
– разворот узла;
– руткиты.

3.6.1. Атаки, реализуемые с использованием уязвимостей протокола IP

Существуют различные типы атак, нацеленные на IP:

– атаки на основе ICMP. Злоумышленники используют пакеты эхозапросов (ping) протокола ICMP для обнаружения подсетей и хостов в защищенной сети, чтобы создавать лавинные DoS-атаки, а также изменять таблицы маршрутизации хоста;

– DoS-атаки. Хакеры пытаются лишить законных пользователей доступа к информации или службам;

– DDoS-атаки. Аналогичны DoS-атакам, но представляют собой одновременную, скоординированную атаку из нескольких компьютеров-источников;

– атаки с подменой адресов. Злоумышленники подменяют IP-адрес источника в IP-пакете для выполнения открытой подмены или подмены вслепую;

– атаки через посредника (MITM). Злоумышленники внедряются между источником и назначением для прозрачного мониторинга, захвата пакетов и контроля обмена данными. Они могут просто подслушивать, проверяя собранные пакеты, или изменять пакеты и пересылать по первоначальному целевому адресу;

– перехват сеанса. Злоумышленники получают доступ к физической сети, а затем используют атаку через посредника для перехвата сеанса.

Назначение DDoS-атаки аналогично DoS-атаке, за исключением большего масштаба, поскольку DDoS-атака имеет несколько скоординированных источников. DDoS-атаки также ввели новые понятия, такие как ботнет, системы-обработчики и компьютеры-зомби.

DDoS-атака может проходить следующим образом:

1. Хакер (ботмастер) строит или покупает ботнет, состоящий из хостов-зомби. Сервер контроля и управления (CnC) взаимодействует с зомби по незащищенному каналу с использованием IRC, P2P, DNS, HTTP или HTTPS;

2. Компьютеры-зомби продолжают искать и заражать все новые цели для создания новых зомби;

3. Когда все готово, ботмастер через системы-обработчики отдает приказ начать DDoS-атаку на выбранную цель.

У ботов есть такая же, как у интернет-червей способность распространять себя. При этом они также могут использоваться для отслеживания нажатия клавиш, сбора паролей, захвата и анализа пакетов, сбора финансовой информации, запуска DoS-атак, ретрансляции спама и создания лазеек на зараженном хосте.

Существует множество потенциальных источников DoS- и DDoS-атак. Хотя DDoS-атаки очень легко обнаружить, бороться с ними сложно. Незащищенные устройства IoT используются для многократного увеличения размеров ботнетов. Для борьбы с подобными атаками можно использовать ряд контрмер:

- внедрение межсетевых экранов и мониторинг IPS;

- ограничение скорости входящего и исходящего трафика нормальными базовыми параметрами;
- максимальное увеличение памяти и повышение надежности всех устройств.

Атаки с подменой IP-адреса происходят, когда хакер создает пакеты с ложной информацией об IP-адресе источника, чтобы скрыть личность отправителя или выдать себя за другого пользователя. Затем хакер может получить доступ к данным, которые недоступны другими способами, или обойти конфигурации системы безопасности. Подмена адресов обычно применяется в рамках других атак, например, в smurf-атаках.

3.6.2. Атаки, реализуемые с использованием уязвимостей протокола TCP

Несмотря на то, что протокол TCP ориентирован на соединения и достаточно надежен, в нем существуют некоторые уязвимости, которые могут быть использованы.

Протокол TCP уязвим к сканированию портов. Сетевые приложения используют порты TCP или UDP. Злоумышленники выполняют сканирование портов оконечных устройств, чтобы определить предлагаемые ими службы.

В лавинных атаках с применением TCP SYN используется трехстороннее квитирование TCP. При этом хакер непрерывно отправляет на целевой объект пакеты запросов сеанса TCP SYN со случайно выбранным поддельным исходным IP-адресом. Целевое устройство отправляет в ответ пакет TCP SYN-ACK на поддельный IP-адрес и ожидает пакет TCP ACK. Эти ответы никогда не приходят. В конечном итоге целевые хосты оказываются перегружены наполовину открытыми TCP-соединениями и отказывают в предоставлении служб TCP (например, электронной почты, передачи файлов или http) законным пользователям.

Перехват сеанса TCP представляет собой еще одну уязвимость TCP. Несмотря на сложность реализации, такой перехват позволяет хакеру взять под контроль уже аутентифицированный хост при обмене данными с целевым объектом. Злоумышленнику пришлось бы подменить IP-адрес одного хоста, спрогнозировать следующий порядковый номер и отправить подтверждение (ACK) на другой хост. В случае успеха злоумышленник сможет отправлять, но не получать данные от целевого устройства.

3.6.3. Туннелирование DNS

Ботнеты стали распространенным методом, применяемым злоумышленниками в своих атаках. Чаще всего ботнеты используются для распространения вредоносного ПО или запуска DDoS-атак и фишинговых атак.

Иногда на предприятиях упускают из виду DNS как протокол,

который может использоваться ботнетами. Из-за этого, когда выясняется, что DNS-трафик является частью инцидента, атака уже завершена. Аналитик по безопасности должен быть в состоянии обнаружить, что злоумышленник использует туннелирование DNS для кражи данных, а затем предотвратить и сдержать атаку. Для этого аналитику по безопасности необходимо внедрить решение, которое может блокировать исходящую связь от зараженных хостов.

Хакеры, использующие туннелирование DNS, помещают в трафик DNS трафик, не относящийся к DNS. Этот метод часто позволяет обойти решения по обеспечению безопасности. Для использования хакером туннелирования DNS изменяются различные типы записей DNS, такие как TXT, MX, SRV, NULL, A или CNAME. Например, в записи TXT может храниться большинство команд, предназначенных для отправки на зараженные хосты в DNS-ответах. Атака с использованием туннелирования DNS и записи TXT выполняется следующим образом:

– данные разбиваются на несколько закодированных фрагментов;

– каждый фрагмент помещается в метку доменного имени нижнего уровня в DNS-запросе;

– так как ответ локального или сетевого DNS-сервера на этот запрос отсутствует, запрос отправляется на рекурсивные DNS-серверы интернет-провайдера;

– рекурсивная служба DNS перенаправляет запрос на доверенный сервер доменных имен злоумышленника;

– этот процесс повторяется, пока не будут отправлены все запросы, содержащие фрагменты данных;

– когда доверенный сервер доменных имен злоумышленника получает DNS-запросы от зараженных устройств, он отправляет ответ на каждый запрос, содержащий инкапсулированные, зашифрованные команды;

– вредоносное ПО, находящееся на скомпрометированном хосте, собирает фрагменты данных и выполняет скрытые в них команды.

Для того чтобы иметь возможность остановить туннелирование DNS, необходимо использовать фильтр, который проверяет DNS-трафик. Обратите особое внимание на DNS-запросы, длина которых превышает среднее значение, а также запросы, содержащие подозрительное доменное имя.

3.7. Защита сетей от кибератак. Политика информационной безопасности

Термин «политика» (от греч. *politika* – государственные или общественные дела) используется в человеческом обществе давно. Существует много трактовок этого понятия, из которых чаще всего

применяются следующие:

– сфера деятельности, связанная с отношениями между социальными группами, сутью которой является определение форм, задач, содержания деятельности государства;

– направление деятельности государства или каких-либо социальных групп в той или иной области в определенный период;

– образ действий, направленных на достижение чего-либо, поведение, определяющее отношения с людьми;

– общее намерение и направление, официально выраженное руководством.

Политики обычно рассчитаны на долгий срок и содержат руководство по разработке более конкретных правил для ситуаций и систем. Политики могут относиться к различным вопросам, таким как управленческие решения по настройке электронной почты организации, обеспечению режима секретности или защите факсов.

Политики поддерживаются стандартами, процедурами и руководствами, в которых должно содержаться общее направление обязательной деятельности для организации. Примеры областей, для которых необходимы политики: физическая защита, безопасность персонала и оборудования, защита сетей, управление рисками и инцидентами информационной безопасности.

Стандарт представляет собой правило, указывающее конкретное направление действий или ответную реакцию на данную ситуацию. Стандарты являются обязательными директивными указаниями (директивами), которые должны выполняться в соответствии с политиками.

Базис устанавливает, как для конкретных технологий используются средства управления. Он создается для обеспечения функции защиты таким образом, чтобы для наиболее часто используемых систем они управлялись единым образом, поддерживая нужный уровень безопасности в пределах всей организации.

Процедуры определяют конкретные действия, как политики, стандарты, базисы и руководства будут реализованы в данной ситуации. Это технологии или процессы, имеющие отношение к конкретным платформам, приложениям или процессам. С целью обеспечения конкретных технических или процедурных требований внутри организации, где они применяются, процедуры как можно точнее должны поддерживать организационные политики, стандарты, базисы и руководства. Примеры процедур: сертификация и аккредитация, оценка рисков информационной безопасности, обнаружение вторжений, тесты на проникновение, реагирование на чрезвычайные ситуации, восстановление после аварий, резервирование, реагирование на инциденты ИБ.

Руководства содержат рекомендации по выполнению требований, которые желательно учитывать при осуществлении защиты. Они, не являясь обязательными, должны соблюдаться, если нет документированных причин не делать этого.

Для организации общий подход в области ОИБ отражается в разработанном, утвержденном и строго выполняемом всеми ее сотрудниками и партнерами документе – политике ОИБ организации (ПолИБ).

ПолИБ содержит позицию организации по отношению к деятельности в области ОИБ, её стремление соответствовать государственным, международным требованиям и стандартам в этой области. ПолИБ определяет стратегию и тактику построения в организации системы защиты информации. В российской терминологии документ, определяющий стратегию, часто называют концепцией, а документ, определяющий тактику, – политикой. За рубежом принято создавать единый документ, включающий одновременно стратегию и тактику защиты. ПолИБ организации является основой для разработки целого ряда документов в области ОИБ: стандартов, руководств, процедур, практик, регламентов, должностных инструкций и пр.

Согласно самому первому определению, приведенному в стандарте «Оранжевая книга» (Trusted Compute System Evaluation Criteria), ПолИБ – это набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации. Гостехкомиссия России определила такую ПолИБ как совокупность правил, регламентирующих права субъектов к объектам доступа. После этого данный термин определялся как в международных, так и российских стандартах и руководящих документах в основном как ПолИБ организации:

– совокупность требований и правил по ОИБ для объекта ИБ, выработанных в соответствии с требованиями руководящих и нормативных документов в целях противодействия множеству угроз ИБ, с учетом ценности защищаемой информационной сферы и стоимости СОИБ;

– документированные решения в области ОИБ;

– совокупность (одно или несколько) документированных пра вил, процедур, практических приемов в области безопасности, которыми руководствуется организация в своей деятельности.

Взаимоувязанная совокупность документов в области стандартизации Банка России (СТО БР ИББС – 1.0) вводит понятие ПолИБ организации.

Различают ПолИБ организации в целом (тогда она называется корпоративной ПолИБ) и ее подразделений.

ПолИБ сети определяется как документ, в рамках единой

информационной инфраструктуры и СОИБ организации формально устанавливающий правила доступа к ее компьютерной сети, на основе которых пользователи этой сети (сотрудники и партнеры организации) накапливают, применяют и распоряжаются ее активами.

В современной практике ОИБ термин «ПолИБ» может употребляться как в широком, так и в узком смысле. В широком смысле ПолИБ определяется как система документированных управленческих решений по ОИБ организации. В узком – ПолИБ отдельный нормативный документ, определяющий требования безопасности, систему мер и/или порядок действий, а также ответственность сотрудников организации и средства управления для определенной области ОИБ.

Также известно понятие «частная ПолИБ», или ПолИБ по конкретным вопросам или проблемам, или ПолИБ по конкретным системам, ориентированная на отдельную область ОИБ или технологию, используемую в организации или ее подразделениях. Например, это ОИБ в части, касающейся ИБ, ОИБ телекоммуникационных систем и сервисов, антивирусная защита, доступ в Интернет, использование средств криптографической защиты и т.д. В них формулируются требования по созданию и эксплуатации СЗИ, организации информационных и бизнес-процессов организации по конкретному направлению ОИБ.

Таким образом, частные ПолИБ являются составляющими корпоративной ПолИБ организации, поскольку конкретизируют ее. Частная ПолИБ – это документация, детализирующая положения ПолИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности организации.

Поскольку основу ПолИБ составляет, как правило, конкретный способ управления каким-либо видом доступа, определяющим порядок обращения субъектов системы к ее объектам, название этого способа и определяет название частной ПолИБ. Как показывает опыт, наиболее часто разрабатываемыми в организациях частными ПолИБ являются политики для следующих областей:

- физической защиты (включая вопросы организации пропускного режима, регистрации сотрудников и посетителей, использования средств сигнализации и видеонаблюдения и т.п.);
- организации режима секретности;
- ОИБ при процессе транспортировки носителей информации;
- обращения с информацией, составляющей государственную тайну;
- опубликования материалов в открытых источниках;
- доступа сторонних пользователей (организаций) в ПС органи зации;
- оценки рисков ИБ;
- управления паролями;

− контроля доступа и защиты от несанкционированного доступа;

− назначения, распределения ролей и обеспечения доверия к персоналу;

− использования интернета;

− разработки и лицензирования ПО;

− установки и обновления версий ПО;

− приобретения ИС и их элементов (программных и аппаратных средств);

− использования отдельных универсальных ИТ в масштабе организации:

1) электронной почты;
2) сетевых сервисов;
3) программно-технических средств защиты;
4) межсетевых экранов (МЭ);
5) технологии виртуальных частных сетей (ВЧС);
6) средств антивирусной защиты;
7) средств криптографической защиты информации;
8) электронной цифровой подписи (ЭЦП);
9) инфраструктуры открытых ключей;
10) модемов и других коммуникационных средств;
11) мобильных аппаратных средств;
12) проведения внешних и внутренних аудитов ИБ;
13) резервирования информации.

В РС БР ИББС-2.0 по документации в области ОИБ отмечается, что деятельность организации по ОИБ осуществляется на основе действующих законодательных актов и нормативных документов РФ по ОИБ, нормативных актов Банка России и внутренних документов самой организации по ОИБ.

В состав внутренних документов рекомендуется включать следующие виды документов, организованных в виде иерархической структуры (рис. 3.7.1):

− документы 1-го уровня, содержащие положения корпоративной ПолИБ организации и определяющие высокоуровневые цели, содержание и основные направления деятельности по ОИБ, предназначенные для организации в целом;

− документы 2-го уровня, содержащие положения частных ПолИБ и детализирующие положения корпоративной ПолИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности организации;

− документы 3-го уровня, содержащие положения ИБ, применяемые к процедурам (порядку выполнения действий или операций) ОИБ,

правила и параметры, устанавливающие способ выполнения конкретных действий, связанных с ИБ в рамках технологических процессов, используемых в организации, либо ограничения по выполнению отдельных действий, связанных с реализацией защитных мер в используемых технологических процессах (технические задания, регламенты работ, порядки, инструкции по эксплуатации, руководства по администрированию и т.п.);

− документы 4-го уровня, отражающие достигнутые промежуточные и окончательные результаты, относящиеся к ОИБ организации.

Рис. 3.7.1. Иерархия документов в области ОИБ для организации

Согласно ГОСТ Р ИСО/МЭК 17799-2005, на верхнем уровне ПолИБ должны быть оформлены следующие документы: «Концепция обеспечения ИБ» (или просто «Концепция ИБ»), «Правила допустимого использования ресурсов информационной системы», «План обеспечения непрерывности бизнеса». На практике можно встретить и документы с такими названиями: «Регламент управления ИБ», «Технический стандарт ИБ» и т.п. Данные документы могут выпускаться в двух редакциях: для внешнего и внутреннего использования. По аналогии с определением концепции ИБ РФ Межведомственной комиссии по ИБ Совета Безопасности РФ концепция ИБ организации – это официально принятая ее руководством система взглядов на проблему ОИБ, методы и средства защиты жизненно важных интересов организации в информационной сфере. Эта система взглядов взаимоувязывает правовые,

организационные и программно-аппаратные меры защиты и основана на анализе защищенности ИС в разрезе видов угроз и динамики их развития.

Концепция ИБ отражает стратегию и тактику ОИБ организации и отвечает на три основных вопроса: что защищать, от чего защищать и как защищать. Таким образом, концепция ИБ организации во многом схожа с корпоративной ПолИБ, хотя второй документ содержит более конкретное наполнение стратегии и тактики правилами, процедурами, практическими приемами и руководящими принципами в области ОИБ, которыми руководствуется организация в своей деятельности.

ПолИБ также можно разделить на две следующие части: организационную (административную), выполняемую людьми, и техническую, реализуемую с помощью оборудования и программ.

Руководствуясь признанными в организации принципами ОИБ, проведя идентификацию активов и производственных процессов, оценив риски ИБ, учитывая собственный опыт и лучшие мировые практики, извлекая уроки по результатам постоянного мониторинга ИБ, разрабатывают две модели ИБ: угроз ИБ и нарушителей ИБ. Все это вместе является основой ПолИБ.

Упрощенный взгляд на разработку и реализацию ПолИБ представлен на рис. 3.7.2.

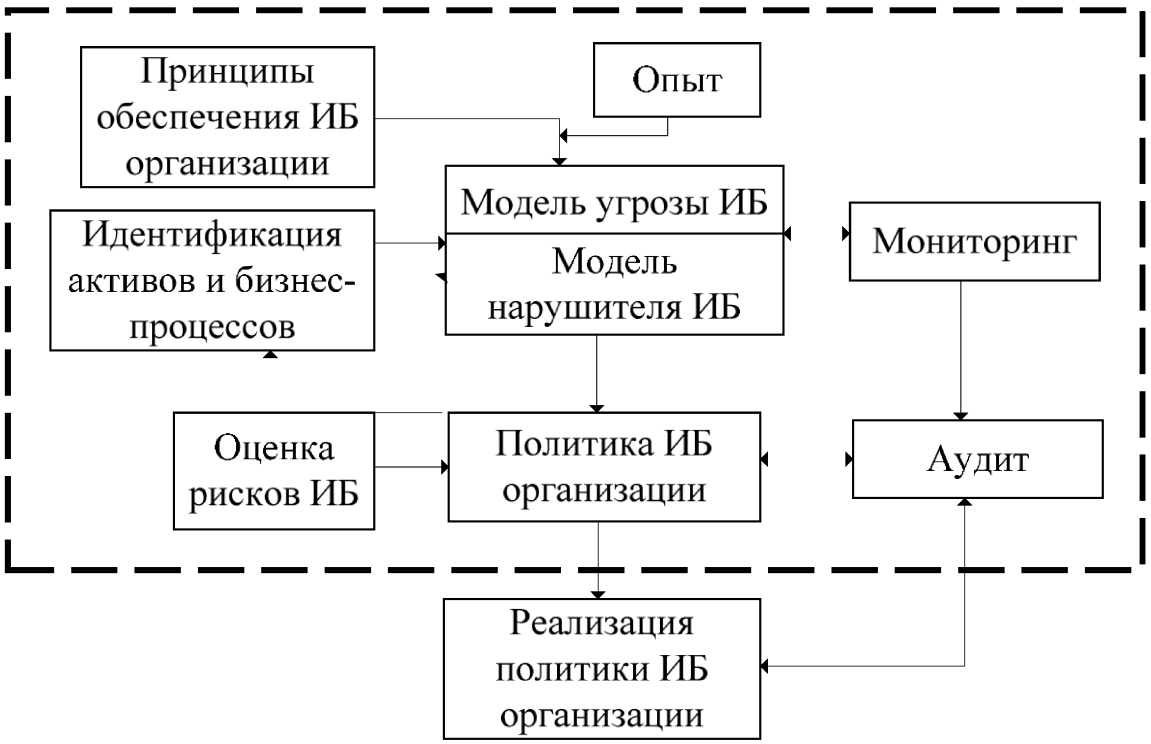


Рис. 3.7.2. Разработка и реализация ПолИБ

После соответствующих процедур согласования и утверждения

ПолИБ вступает в силу, реализуется силами всех определенных заранее должностных лиц и соблюдается всеми, к кому она применима. ПолИБ является основным документом, выполнение которого на практике оценивается при проведении аудита ИБ (как внешнего, так и внутреннего) и каждодневного мониторинга событий, влияющих на ИБ.

На стадии разработки ПолИБ пишется, в нее вносятся одобренные после обсуждения коррективы и в соответствии с установленной заранее процедурой ПолИБ утверждается. Затем на стадии внедрения ПолИБ доводится до сведения всех заинтересованных лиц (сотрудники, бизнес-партнеры, клиенты), обеспечивается ее соответствие всем необходимым стандартам, нормам и требованиям и непосредственное соблюдение (рис. 3.7.3).

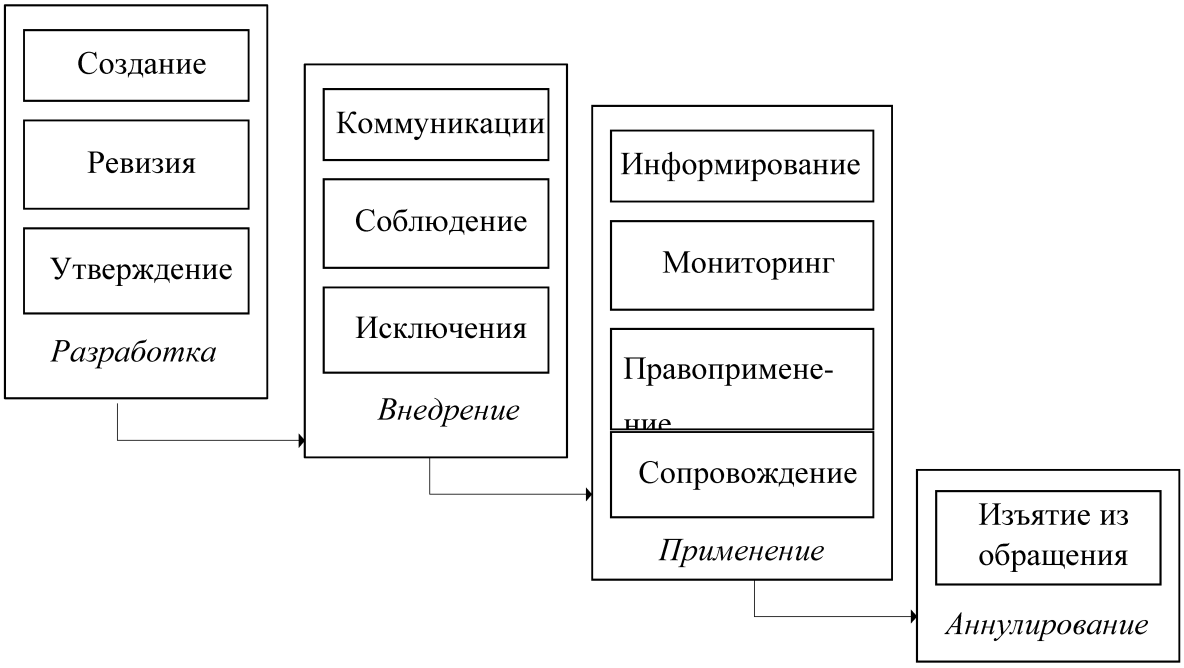


Рис. 3.7.3. Стадии жизненного цикла ПолИБ

На стадии применения ПолИБ поддерживается в актуальном состоянии (в нее вносятся соответствующие текущему уровню развития организации изменения), ее основные положения с изменениями доводятся до сведения всех заинтересованных лиц, а также постоянно проверяется ее соответствие всем установленным требованиям. Также должным образом контролируется исполнение ПолИБ всеми, на кого она распространяется.

Наконец, на стадии аннулирования, чаще всего после ее замены новой редакцией или совершенно новым по содержанию документом, ПолИБ изымается из обращения в связи с ненадобностью.

Все шаги жизненного цикла ПолИБ должны быть обязательно

выполнены, а некоторые из них, такие как сопровождение, информирование, мониторинг соблюдения и правоприменение, выполняются итерационно во время всего жизненного цикла.

3.8. Обеспечение киберзащиты мобильных устройств

3.8.1. Основы безопасной работы с мобильными устройствами

Мобильные устройства – ряд устройств, включающий в себя смартфоны, планшеты, электронные книги, телефоны, КПК и т.д. главной особенностью которых является размер, а также количество выполняемых ими функций.

Первый в мире сотовый телефон – Motorola DynaTAC 8000X – был выпущен в сентябре 1983 года, но первый звонок с устройства был совершен гораздо раньше. За несколько десятилетий телефоны превратились из громоздких аппаратов в лёгкие и умные мини-компьютеры, способные поддерживать связь со всем миром посредством интернета.

Сенсорные модели являются популярнейшей на данный момент разновидностью смартфонов. Техника управляется надавливанием пальца или специального стилуса. Это зависит от типа экрана, так как одни дисплеи (они называются ёмкостными) включаются от тепла тела, а другим (резистивным) нужно точное нажатие в определённую точку. На данный момент большинство моделей выпускается с ёмкостными экранами, хотя некоторые производители проводят интересные эксперименты со стилусом, позволяя создавать рисунки и заметки «от руки». Сенсорные аппараты представляют собой моноблок без клавиатуры, управление осуществляется через многофункциональный дисплей.

Слайдер состоит из двух частей, которые выдвигаются в горизонтальной плоскости. В собранном состоянии слайдер компактен – остаётся только экран и динамик. Для набора сообщений выдвигается клавиатура.

Устройство телефона «раскладушки» состоит из клавиатуры и экрана, а подвижный шарнир позволяет весьма эффектно сложить телефон после завершённого разговора.

Моноблок выпускается в трех разновидностях:

– с цифровой физической клавиатурой;

– с флипом; это специальная накладка, которая защищает клавиатуру от негативных факторов окружающей среды;

– с QWERTY-клавиатурой; он схож с классическими моделями, только обладает уникальной клавиатурой с цифрами и алфавитом для удобства набирания больших объёмов текста.

Спутниковые устройства также можно отнести к мобильным телефонам, так как они не привязаны к одной точке. Связь осуществляется

через спутниковую систему, она гораздо дороже сотового аналога, но является незаменимой в труднодоступных местах: открытое море, северный полюс, тайга и прочие места, где нет покрытия обычных сетей.

Планшет – это устройство с сенсорным экраном, которое имеет размеры обычной книги и выполняет функции компьютера. Планшеты имеют меньший размер и вес чем ноутбуки, что позволяет их с легкостью носить с собой. Из-за размеров и вычислительные мощности планшетов меньше, но при этом время автономной работы больше. А по сравнению со смартфонами они имеют больший размер экрана, что лучше при долгом просмотре видео или текстовой информации.

На сегодняшний день смартфоны и планшеты стали неотъемлемой частью жизни. В этой связи все чаще смартфоны и планшеты становятся объектами, инструментами или предметами преступлений.

Обеспечение безопасности мобильных устройств требует многоуровневого подхода. И хотя для обеспечения безопасности нужно решить ряд основных задач, в каждом конкретном случае подход может иметь свои особенности. Чтобы достичь максимального уровня защиты, нужно найти оптимальный подход.

К базовым способам защиты данных в мобильных устройствах относят логин и пароль. Логин позволяет опознать пользователя, выполнить главную функцию аутентификации. Пароль предотвращает от несанкционированного доступа, то есть решает главную задачу информационной безопасности. В мобильных телефонах существует понятие PIN-кода. Этот защитный механизм, решающий задачу безопасности, прямо не связанный с аутентификацией. Нельзя обойтись только логином, так как логин фигурирует в формах запросов и отчётах, его иногда приходится сообщать в службу поддержки.

С появлением вычислительных сетей выяснилось, что пароль в открытом виде передавать опасно, так как его может перехватить злоумышленник. Логичным решением было внедрить шифрование пароля. Так появились Digest Authentication и NTLM.

Single-Sign-On. Другим неприятным аспектом всеохватного запароливания оказалось то, что не очень-то удобно держать в голове больше одной-двух пар логина и пароля, вводить их всякий раз при входе в программу, особенно если этих программ больше одной. Результатом решения проблемы стали аутентификация oAuth и принцип SSO, то есть Single-Sign-On (войти один раз). Идея oAuth проста. Вместо того чтобы каждый раз требовать у пользователя его логин и пароль, это делается один раз, на основании полученных сведений нужно получить так называемый токен у доверенного сервера и далее проводить операции уже с этим токеном. Это особенно удобно в контексте обмена данными между мобильным или web приложением и удалённым сервером, где аутентифицирующие сведения (credentials) необходимо передавать с каждым запросом. SSO решает другую задачу. В рамках использования web-сервисов все приложения, использующие один и тот же доверенный

сервер для oAuth-аутентификации (например, сайты с Гугл-аккаунтом), автоматически разделяют между собой сведения пользователя (credentials). То есть, введя логин и пароль в одном приложении, в другое пользователь заходит уже опознанным. Для мобильных приложений данный подход тоже работает, но с оговорками, и требует от разработчиков дополнительных усилий. Сведения пользователя нужно сохранять на устройстве, чтобы их можно было вычитать при последующем запуске приложения, а также чтобы другие приложения, которым это нужно (и которые имеют право доступа к этим сведениям), могли ими воспользоваться для автоматической аутентификации.

В зависимости от платформы и технологии, пароли могут храниться (чаще всего) в KeyChain (iOS, Android). Данные здесь шифруются, доступ к ним ограничен – в общем, это самое безопасное место на устройстве, защищённость которого гарантируется на уровне операционной системы.

С точки зрения кибербезопасности хранение паролей в базах данных является ненадежным. Плохой идеей также будет отправлять логины с паролями в системный журнал. Замечание средней недопустимости можно получить за временное хранение пароля в публичных переменных – хорошим тоном считается вычитка сведений о пользователе из KeyChain по мере необходимости, без хранения их где-либо ещё.

TouchID/Fingerprints. Широко известно, что человек обладает уникальными отпечатками пальцев. Кроме того, уникальными являются отпечатки носов и ушей, причём если пальцы – атрибут в основном сугубо человеческий, то носы есть и у домашних животных. На практике опознавание по отпечаткам носов используется для идентификации кошек, собак и коров. Пока что технология распознавания в телефонах сосредоточилась на дактилоскопии, закрепившейся в криминалистической практике ещё сто лет назад. Кроме того, что многие телефоны оснащены сканерами отпечатков пальцев и уже упоминавшимся PIN-кодом, ряд из них дополняется графическим ключом – то есть можно задать вместо цифровой комбинации некий кодовый рисунок, соединяя точки на экране в той или иной последовательности.

Face ID. Одна из недавних технологий, предложенных Apple – аутентификация посредством распознавания лица. Если для отпечатков пальцев достаточно теоретически несложной алгоритмической обработки, то для распознавания лиц прибегают к идеям Розенблатта и строят нейросеть. Конечно же, мощности нейросети в iPhone недостаточно для игры в шахматы или ГО, но со своей задачей она справляется. Телефон теперь может опознать своего хозяина визуально.

Multifactor authentication. Идея заключается в том, что подделать один канал аутентификации проще, чем два. Побочным эффектом является то, что сегодня в типичную корпоративную сеть без телефона войти не удастся: ведь на него приходит пин-код, который нужно ввести для подтверждения своей личности; приходится сначала вводить логин и пароль, а затем подтверждать личность ещё и посредством пин-кода.

Применение данной технологии для мобильных приложений выглядит немного спорным, но вполне возможным.

Блокчейн. После того, как биткоин и прочие криптовалюты произвели ажиотажный общественный резонанс, было бы странно, если бы лежащий в основе трансакций этих валют блокчейн не привлёк внимание разработчиков систем безопасности. Применительно к человеку, сама по себе технология блокчейн уже сегодня работает в Эстонии как платформа для электронного гражданства; есть подобные попытки в Бразилии и Финляндии. Японская компания Sony совместила технологии MFA и блокчейн (U.S. patent 2017/0310653 A1*).

Перейдем к рассмотрению нескольких дополнительных способов защиты мобильных устройств.

Решения для защиты конечных устройств помогают защитить устройства: они отслеживают файлы и процессы на каждом мобильном устройстве, которое получает доступ к сети. Такие решения выполняют постоянный мониторинг проявлений вредоносной активности, поэтому могут выявить угрозы на ранних стадиях. При обнаружении подобной активности решения для защиты конечных устройств сразу предупреждают пользователя, а значит, угрозы могут быть устранены еще до того, как они нанесут ущерб. Примерами таких решений могут быть программы «Dr.Web Security Space», «Kaspersky Internet Security», а также другие аналогичные программы, предустановленные производителем мобильных устройств.

VPN. Виртуальная частная сеть (VPN) обеспечивает зашифрованное подключение устройств к сети через интернет. Зашифрованное подключение гарантирует безопасную передачу конфиденциальных данных. Такое подключение запрещает неавторизованным лицам прослушивать трафик и позволяет авторизованным пользователям безопасно работать удаленно. Для использования VPN на мобильном устройстве необходимо установить программу VPN-клиент или воспользоваться предустановленной (при ее наличии).

Защита электронной почты. Электронная почта – это не только самое важное средство связи, но и главное направление атаки с целью нарушения безопасности. Более того, по данным последнего Полугодового отчета Cisco (Одна из крупнейших в мире компаний, специализирующихся в области высоких технологий) за 2020 г. по информационной безопасности, электронная почта является основным средством распространения вирусов-вымогателей и другого вредоносного ПО. Чтобы обеспечить надлежащий уровень безопасности электронной почты, нужна система защиты от сложных угроз, которая оперативно выявляет, блокирует и устраняет угрозы, предотвращает утечку данных и защищает передачу важной информации с помощью сквозного шифрования.

Брокер безопасного доступа к облачным сервисам. Система защиты сети должна предусматривать, где и как работают сотрудники, включая и облачные сервисы. Для решения этой задачи понадобится брокер

безопасного доступа к облачным сервисам (CASB) – инструмент, который играет роль шлюза между локальной инфраструктурой и облачными приложениями (Salesforce, Dropbox и т.д.). Такой брокер выявляет вредоносные облачные приложения и блокирует проникновения с помощью средства предотвращения утечки данных.

3.8.2. Характеристика и операционные системы мобильных устройств

Впервые термин «smartphone» (что в переводе с английского языка означает «умный телефон») был введён в употребление компанией Nokia в 2001 году, когда последняя выпустила свой новый слайдер. Это было «умное» сотовое устройство, которое работало на базе платформы Symbian. Данное событие имело в некотором роде историческое значение, ведь позже термин «смартфон» стали использовать и другие производители высокотехнологичной мобильной техники, а платформы, на которых они работали стали называть мобильными операционными системами (ОС или OS). Таким образом мобильная операционная система – это операционная система для смартфонов, планшетов, КПК или других мобильных устройств. Она обеспечивает управление аппаратными средствами мобильного устройства, организует работу с файлами и выполнение прикладных программ, осуществляет ввод и вывод данных.

На сегодняшний день существует огромное количество различных мобильных ОС, многие из которых давно утратили свою популярность, другие же наоборот пользуются огромным спросом среди пользователей мобильных устройств. Рассмотрим основные из них.

Symbian. OS Symbian официально является собственностью Nokia. Это означает, что любая другая компания должна будет получить разрешение от Nokia перед использованием этой операционной системы. Nokia в 2008 году была гигантом в недорогом сегменте рынка мобильных телефонов, поэтому Java Symbian была наиболее часто используема в первых смартфонах. Symbian Anna и BELLE два последних обновления, которые использовались в смартфонах Nokia. Некоторые мобильные телефоны, работающие на Symbian OS: это Nokia C6-01, Nokia 603, Nokia 700, Nokia 808, Nokia E6 (ANNA) и Nokia 701 (Belle). Также Symbian является популярным выбором среди Nokia Dual SIM мобильных телефонов. В 2014 году корпорация Nokia прекратила поддержку Symbian OS.

Современные смартфоны Nokia (например, Nokia G21) работают под управлением ОС Android. Android. 20 сентября 2008 – это дата, когда Google выпустил первую Android OS под названием «Astro». Первым в мире смартфоном с ОС Android является смартфон HTC Dream или T-mobile G1.

По состоянию на начало 2021 года на долю пользователей Android-смартфонов приходится 71% от общего количества пользователей смартфонов. По статистике на 2021 год Android является самой

популярной ОС в мире. Рассмотрим более детально устройство данной операционной системы.

Операционная система Android – это система с открытым исходным кодом. Существует мнение что Linux и Android – это одно и то же, но это не совсем так. Linux – полностью открытая система, независимо от конкретного семейства. Компания Google приняла решение разработать операционную систему (Рис. 3.8.1) для сотового телефона с той же базовой внутренней оболочкой, что и в Linux, чтобы она была при этом совместима практически со всем существующим программным обеспечением.

Первый уровень – это Application Framework, второй – это прокси-серверы Binder IPC, третий – это системные службы Android, четвертый – HAL или полная форма, представляющая уровень аппаратной абстракции, и последний – ядро Linux. Таким образом, единственной частью Linux, из которой состоит операционная система Android, является ядро Linux.

Android Application Framework. Эта платформа приложений используется разработчиками приложений для Android. Приложения для Android запрограммированы на языке Java. После программирования приложения инструменты Android SDK помогают скомпилировать данные и файлы ресурсов, такие как XML-файлы, файлы JAR, файлы манифеста и другие изображения и прочее, в один архивный пакет с расширением .apk. Этот файл apk можно использовать для установки приложения на устройствах Android. Теперь, поскольку операционная система Android ведет себя как среда Linux, поведение приложения здесь то же самое. Каждое приложение рассматривается как отдельный пользователь от другого и работает на своей собственной виртуальной машине. Это делает программный код приложения изолированным, а также предотвращает заражение от других, если это не указано явно. Каждое другое приложение имеет свой собственный идентификатор пользователя, а каждый другой процесс имеет собственную виртуальную машину. Платформа приложений Android работает по принципу наименьших привилегий. Принцип наименьших привилегий означает, что всякий раз, когда нужно запустить новое приложение, но нет доступной памяти, система Android автоматически закроет старое приложение, которое не нужно запускать в фоновом режиме. Это одна из лучших частей безопасности операционной системы Android. Этот принцип позволяет каждому приложению иметь только тот доступ, который необходим для его работы.

Binder IPC известен как Binder Inter-Process Communication. Этот интерфейс позволяет программисту создавать приложения для связи с другими приложениями. На практике чаще всего взаимодействуют не приложения, а процессы. Binder IPC помогает запускать несколько процессов одновременно на параллельном уровне. Эта реализация связующего поставляется через ядро операционной системы Android. Возникают вопросы о том, почему механизм связывания должен оставаться в ядре и почему он не может работать из механизмов Linux IPC? Основная причина этого заключается в том, что механизм связывания

избегает ненужного распределения пространства в отличие от других механизмов IPC в системе Linux. Это фактически позволяет высокоуровневой структуре взаимодействовать со службами операционной системы Android.

Рис. 3.8.1. Структурная схема ОС Android

Системные сервисы операционной системы Android. Сервис – это скомпилированный фрагмент кода, который долгое время работает на фоне операционной системы Android без какого-либо интерфейса. Любое приложение, будь то пользователь или система, может запустить службу, но оно все равно будет работать в фоновом режиме, даже если приложение закрыто. Существует два типа услуг:

– запущенные Услуги. Запущенные сервисы обычно запускаются, когда приложение требует этого. Однако тип обслуживания Started обычно выполняет только одну операцию и ничего не возвращает;

– Связанные Услуги. Ограниченные сервисы предлагают интерфейс связи клиент-сервер. Связанная служба работает до запуска приложения переднего плана, а затем останавливается после уничтожения действия приложения.

Системные сервисы android предоставляют пользователям необходимую информацию для того, чтобы они правильно работали. И эти коммуникации между системными службами и пользовательскими приложениями осуществляются с помощью Binder IPC из ядра. Удивительно, но не все приложения в Android написаны на Java. Некоторые из них написаны на C и C ++. Те приложения, которые должны быть в тесном контакте с оборудованием, написаны на C и C ++. Основная причина этого заключается в том, что большую часть времени системные службы должны находиться в постоянном контакте с оборудованием. Это важно, чтобы скомпилированный фрагмент кода был быстрым. Когда необходимо решить задачи аппаратного ускорения и высокой производительности, C намного быстрее, чем Java или любой другой язык. Аппаратные службы, которые постоянно используются, например, датчики приближения, акселерометр или сенсорный экран, должны быть написаны на C. Другое оборудование, такое как Камера или звук, в основном использует вызовы JNI. Таким образом, работа сенсорных экранов всегда будет быстрее, чем запуск камеры или воспроизведение песни через музыкальный проигрыватель. При создании системного сервиса следует обратить внимание, что сервисы, как правило, запускаются в основном процессе, и он не создает отдельный процесс. Таким образом, если программый код будет выполнять некую интенсивную работу с процессором и графическим процессором, например, исполнение игры с высоким разрешением, то предпочтительным для него является создание новых потоков в том же сервисе. В противном случае возможно появления диалогового окна «Приложение не отвечает».

Уровень аппаратной абстракции. HAL или Hardware Abstraction Layer специально разработан для поставщиков. Этот слой помогает вставить функциональность без каких-либо изменений в системе. Каждая конкретная система реализует HAL по-разному. HAL состоит из двух типовых структур: Модуль и Устройство. Структура модуля в HAL

хранится в виде разделяемой библиотеки в формате .so, который состоит из основных метаданных, таких как номер версии, автор, который разработал модуль, и тому подобное. Структура устройства – это фактическое аппаратное обеспечение продукта. В Linux приложения взаимодействуют с базовым оборудованием через системные вызовы. В операционной системе Android приложения взаимодействуют с оборудованием через программный интерфейс приложения (API) Java.

Ядро Linux. Компиляция ядра Linux для операционной системы Android аналогична компиляции его для базовой ОС Linux. Разница лишь в том, что версия для Android немного более продвинутая, чем версия для Linux. Основная причина в том, что ядро Android состоит из дополнительных функций, таких как wakelocks, двойное нажатие для разблокировки и другие подобные функции, встроенные в мобильное операционное устройство. Такие функции, как wakelock, важны, поскольку ядро будет работать на портативном устройстве, и оно должно быть более агрессивным в управлении памятью и батареями; в отличие от базового Linux, где управление энергопотреблением не является проблемой. Эти дополнительные требования возникают в ядре, а не в системе, поскольку эти особенности не должны влиять на встроенные драйверы. Основная причина, по которой Android основан на ядре Linux, заключается в том, что он имеет открытый исходный код. Любой может пойти дальше и модифицировать ядро Linux без каких-либо аппаратных ограничений или даже каких-либо проблем с лицензионным платежом.

Разница между Linux и Android. Всякий раз, когда загружается операционная система Android, она в основном загружает ядро, как и любой другой дистрибутив Linux, но остальная часть программного обеспечения полностью отличается от Linux. Приложения Linux не будут работать на Android, а также наоборот, если они не скомпилированы в среде chroot. Библиотеки, представленные в типичном дистрибутиве Linux и Android, полностью отличаются друг от друга. В принципе, нельзя получить доступ к корневому терминалу в Android, как в случае с Linux. Это основная причина, почему некоторые разработчики и пользователи устанавливают Busybox, SuperSU и его двоичные файлы после получения на устройстве прав суперпользователя, чтобы у них был более детальный доступ к командной строке, ядру и оболочке. В Android нет оболочки по умолчанию, но ее можно получить, установив эмулятор терминала из магазина Google Play. На текущий момент последней версией является Android 12.

iOS принято считать одной из самых известных и качественных операционных систем, конкурирующих в данный момент с ОС Android. Она подходит для различных персональных устройств от фирмы Apple и устанавливается только на устройства упомянутого производителя.

Система не подходит для работы на других устройствах. Первая версия iOS (или на тот момент iPhone OS) вышла 29 июня 2007 года и поддерживала работу двух устройств: iPhone и iPod touch. Это была модифицированная версия OS X (работающей на ноутбуках Apple), и сотрудниками компании была решена задача ее адаптации под мобильный процессор и сенсорный экран. В iPhone OS было заложено много возможностей, прославивших iPhone и знакомых основной массе пользователей до сих пор. К последним следует отнести жест «Slide to unlock», жест приближения фотографий двумя пальцами (Pinch to zoom) и так далее. При этом отсутствовали многие привычные и важные элементы. Например, MMS, поиск по контактам, функция копирования и вставки. Все это появится только в следующих версиях системы. Также на начальный момент запуска не существовало облака iCloud, поэтому все данные на смартфон переносились через iTunes. Все это начало кардинально меняться с выходом новых моделей iPhone (Рис. 3.8.2).

Рис. 3.8.2. Развитие iOS

iOS использует достаточно уникальный подход к обеспечению кибербезопасности. Для того чтобы гарантировать безопасность ОС, для нее разрабатываются устройства, содержащие большое количество механизмов защиты. Программистам, которые создают программы для данных ОС, запрещается в полной мере пользоваться низкоуровневым функционалом, который доступен в системе. Поэтому они вынуждены работать с теми интерфейсами и библиотеками, которые рекомендуют сами создатели iOS. Это создает иллюзию, что при написании программного обеспечения нельзя допустить ошибок, позволяющих скомпрометировать данные пользователя или саму ОС.

На данный момент существует ограничение на установку программного обеспечения на устройства с iOS. Установка может быть осуществлена только из одного магазина – «App Store». Эта особенность породила сообщество, которое постоянно исследует новые версии ОС для того, чтобы предоставить доступ пользователям к закрытым функциям ОС. Процесс открытия такого доступа называется jailbreak.

Jailbreak – это процесс, при котором для получения привилегированного доступа используются различные уязвимости в ОС. Для разработки эксплойтов используются уязвимости как программного обеспечения iOS, так и прошивка самого аппаратного обеспечения устройств. Также разработка может включать в себя создание bootkit-ов.

Одной из отличительных особенностей операционной системы iOS является скорость выхода новых версий. Скорость не означает качество, и поэтому новые версии ОС могут существовать в beta версии несколько месяцев, а порой даже иметь несколько beta версий. За период с 2019 по 2021 год на устройствах Apple работало как минимум 5 версий ОС от 10 до 15, и это только major версии, между которыми было выпущено несколько обновлений, связанных с безопасностью системы.

Быстрый поиск по бюллетеням безопасности Apple показал, что количество уязвимостей в iOS постоянно снижается, хотя некоторое их количество остается (Рис. 3.8.3, данные взяты со страниц support.apple). Более половины уязвимостей, которые приведены в статистике, являются уязвимостями, приводящими к повреждению памяти. Эти уязвимости наиболее опасны, так как в оперативной памяти могут находиться данные, которые используются программами и самой ОС.

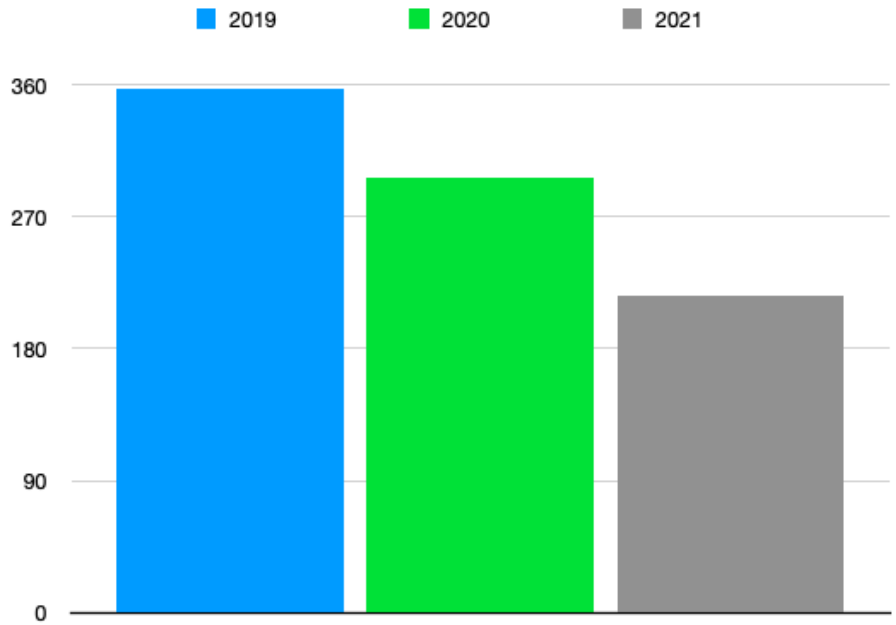


Рис. 3.8.3. Количество зарегистрированных и опубликованных уязвимостей

Большое количество проблем с работой с памятью в iOS не случайны. Эта операционная система использует язык программирования, который явился результатом эволюции языка программирования C.

Уязвимость для любой ОС означает нарушение прав разграничения доступа к хранимым данным, нарушение работоспособности всей ОС. Уязвимость для iOS означает нарушение работоспособности и открытие полного функционала операционной системы.

iOS – это ОС с закрытым исходным кодом несмотря на то, что Apple открывала часть исходных кодов, относящихся к ядру операционной системы. Процедура исправлений уязвимостей в iOS остается непрозрачным процессом. Отмечались ситуации, когда уязвимость публиковалась, под нее выпускается патч, а потом, спустя релиз, эта уязвимость снова появлялась, так как в очередном обновлении оказывались отмененными изменения, связанные с исправлениями проблдем безопасности. Так случилось с уязвимостью CVE-2018-4344. Эта уязвимость просуществовала практически 9 лет. Она была исправлена (предположительно) в версии iOS 11.4.2. Исправление не решило проблему, а превратило в iOS 12 Memory Leak и только в iOS 13 уязвимость была исправлена полностью. Уязвимость находится в системном вызове lio_listio и может приводить к условию Race Condition. Как результат, использование этой уязвимости может привести к освобождению памяти по одному и тому же адресу несколько раз.

Изначально уязвимость описывалась как Dos, который нельзя было использовать для выполнения jailbreak, но спустя время команда, которая создала один из популярных jailbreak – unc0ver, использовала модификацию уязвимости для атаки на ОС вплоть до iOS 13.

CVE-2021-1782 была исправлена после того, как было установлено, что эта уязвимость используется злоумышленниками для атаки на пользовательские устройства. О деталях атак ничего неизвестно, команда unc0ver сообщила, что использует уязвимость для jailbreak всех версий ОС вплоть до iOS 14.3.

Самое уязвимое и болезненное место любой ОС – это процедура загрузки. Именно на этом этапе инициализируются все правила безопасности, которые позволяют работать ОС так, как было заявлено. Если вмешаться в этот процесс, то можно полностью изменить любую процедуру и отключить любую защиту. Чтобы этого не происходило, загрузка iOS защищается процедурой безопасной загрузки. Вся прошивка устройства верифицируется перед запуском, и если верификация завершается провалом, то устройство уходит в режим Recovery. Если не получается восстановить работоспособность ОС, включается низкоуровневое восстановление системы, известное как режим DFU.

Именно в этом режиме и была найдена уязвимость, которая не может быть исправлена программно. Уязвимость была добавлена в набор

инструментов, который называется checkm8. Для использования этого эксплойта нужно иметь физический доступ к устройству. Этот метод стал одним из ключевых для создания другого актуального jailbreak – checkra1n.

Даже операционные системы, которые проектируются как защищенные, могут быть атакованы с использованием программных и аппаратных уязвимостей. Об этом стоит всегда помнить при использовании мобильных устройств.

BlackBerry OS. В своё время RIM (ныне BlackBerry ltd) был достаточно известным производителем мобильных устройств, который прославился QWERTY клавиатурой, безопасностью и опциями для бизнесменов. Первый релиз операционной системы вышел в 1999 году. На сегодняшний день данная операционная система не имеет такой популярности как Android или iOS. Последней версией, вышедшей 2013 году, является BlackBerry OS 10. Рассмотрим данную версию ОС более подробно с точки зрения кибербезопасности.

Никаких «альтернативных» прошивок или аналогов Jailbreak здесь не существует. Root права до сих пор никто не смог получить. На устройство в качестве системных файлов могут быть загружены только файлы, подписанные компанией BlackBerry. Если 10 раз неправильно введен пароль для разблокировки устройства – данные сбрасываются. Обойти его до сих пор не удалось. Существует возможность поставить уникальный по принципу действия графический пароль. Упоминаний о несанкционированной слежке за пользователями данной операционной системы в известных истиочниках не встречаются. В браузере присутствует блокировка всплывающих окон, защита от фишинга. У фирменного мессенджера также присутствуют особенности, связанные с безопасностью: приватный чат, временные сообщения. Просто так ваши данные никто не сможет просмотреть. Присутствует вышеуказанное приложение «менеджер паролей» (однако, справедливости ради, Chimera tool научилась его взламывать). В BB World попадают действительно проверенные с точки зрения безопасности приложения. Наличие BlackBerry Balance для корпоративных клиентов. Можно зашифровать все данные на устройстве и карте памяти. У BB ID отсутствует двухфакторная аутентификация. BB Protect в новых версиях OS можно легко обойти с помощью «миксовой» прошивки. Но даже с учетом этих минусов, доступ к данным в телефоне никто не получит, если, например, украдет телефон. Максимум – сбросят защиту и начнут пользоваться с чистого листа. Сама архитектура и построение операционной системы способствует тому, чтобы она была достаточно безопасной. И это действительно так – даже с некоторыми оговорками. Несмотря на прекращение поддержки (выпуск новых обновлений), в данном аспекте BB OS 10 даже сейчас выглядит достаточно бодро на фоне своих конкурентов.

ОС Windows Phone. Мобильная операционная система, разработанная компанией Microsoft, вышла в октябре 2010 года. Последней версией, вышедшей в марте 2015 года, является Windows Phone 8.1. Затем на ее основе была выпущена ОС Windows 10 Mobile, поддержка которой прекратилась в декабре 2019 года. На сегодняшний день данная операционная система не имеет такой популярности как Android или iOS. Компания Microsoft сосредоточилась на разработке операционных систем для стационарных устройств (персональных компьютеров, ноутбуков). Но некоторые особенности ОС Windows Phone с точки зрения кибербезопасности все же рассмотрим.

Ключевое отличие Windows Phone от Android (и одновременно то, что в некотором роде роднило систему с iOS) – закрытость. Это одновременно являлось и плюсом, и минусом системы. С одной стороны, она была гораздо более безопасной, чем Android. С другой же стороны, из закрытости Windows Phone следовали и недостатки, которые в общем свойственны и iOS, но там они компенсировались популярностью системы, а в случае с Windows Phone стали одним из ключевых моментов, из-за которых этой популярности система в итоге не получила.

Закрытость системы вместе с поздним (на фоне Android и iOS) запуском системы привели к тому, что разработчики не стремились реализовывать свои программы на Windows Phone. В большинстве случаев их делали по остаточному принципу.

Принять решение о выпуске программ для Windows Phone могли в основном крупные компании, такие как «Яндекс», или энтузиасты. В итоге приложения для этой операционной системы получали серьезную (в сравнении, например, с Android) задержку в обновлениях и, как следствие, запаздывание нового функционала. Примечательно, что эта тенденция касалась и приложений от самого Microsoft.

Еще одна особенность, вытекающая из закрытости системы, – неизменный интерфейс. Минимальные изменения, такие как установка фонов на определенных экранах, в Windows Phone были возможны. Но в глобальном плане интерфейс оставался неизменным: два экрана, на левом – квадратные или прямоугольные значки приложений или виджетов, на правом – приложения в виде списка.

Во многом благодаря грамотной оптимизации работы операционной системы она требовала меньше ресурсов. К примеру, на Windows Phone 8.1 и Windows 10 Mobile вполне успешно работали устройства с 1 гигабайтом оперативной памяти, в то время как на тот момент устройства на Android с объемом ОЗУ меньше 2 гигабайт можно было уже не рассматривать — они бы тормозили нещадно и постоянно.

Следствием такой оптимизации Windows Phone явилась дешевизна устройств. Наиболее недорогие аппараты можно было купить примерно за 3 тысячи рублей, а за 30 тысяч можно было купить топовую Nokia 1520 с

огромным по тем временам 6-дюймовым экраном и очень хорошей для своей ценовой категории камерой с оптикой ZEISS с разрешением в 20 мегапикселей. К примеру, выпущенный в том же 2013 году Samsung Galaxy Note 3 стоил 35 тысяч, имел камеру с разрешением только в 13 мегапикселей.

BADA. Samsung представила платформу Bada 10 ноября 2009 года. Анонс был сухим и непонятным: пообещали выпустить систему для телефонов и набор SDK для разработчиков. И еще было известно, что «bada» с корейского переводится как «океан».

Рис. 3.8.4. Структурная схема ОС BADA

Чуть больше деталей появилось только к концу года. Уже стало понятно, что Bada OS – операционная система для сенсорных телефонов. ОС основана на базе старой платформы SHP и интерфейса TouchWiz. В системе обеспечивается поддержка Flash, акселерометра, датчика приближения и т.п.

Главную идея проекта Bada можно сформулировать как «Создание смартфона для всех». Samsung решила перенести все функции «умных» телефонов в более доступные модели с сенсорными экранами. Для этого сделали единую платформу и магазин приложений. В момент выхода

компанией-разработчиком анонсировался запуск конкурса для разработчиков с призовым фондом почти в 3 миллиона долларов.

Комплект разработчика программ (SDK) для Bada открыли в январе 2010 года, но только для крупных разработчиков, которые получили одобрение со стороны Samsung. Полностью открытый комплект SDK появился только в мае 2010 г.

Компания Samsung потратила много маркетинговых сил, чтобы объяснить, что Bada является не просто операционной системой, а представляет собой мобильную платформу.

По задумке, на основе платформы Bada можно было создать альтернативную операционную систему с самостоятельным уникальным ядром и прочими компонентами, но сама компания Samsung этим не занималась. Платформа должна была работать на самых разных телефонах – от бюджетных с резистивным экраном до дорогих флагманов. При этом единый набор SDK позволял выпускать приложения сразу для всех устройств. На практике все заявленные возможности платформы проявить не удалось, по этой причине Bada принято считать обычной операционной системой.

Система Bada, которая стояла в телефонах Samsung, в большей степени относится к закрытым операционным системам. Например, разработчик не имел возможности создать альтернативное приложение для звонков, поскольку система не позволяла сторонним программам получать доступ к этим функциям. Компания Samsung анонсировала политику, заключающуюся в том, что в отличие от Apple и других конкурентов, процент с продаж приложений в фирменном магазине системы для ее создателя не будет начислятся.

Презентация первого смартфона на Bada прошла в феврале 2010 года в рамках выставки MWC, когда был представлен Samsung Wave. В данной модели компания реализовала имеющиеся на тот момент новые технологии: впервые на рынке появился Bluetooth 3.0, поддержка стандарта Wi-Fi 802.11n и Super AMOLED дисплей. Также в Wave дебютировал новый интерфейс TouchWIZ 3.0 с обновленными виджетами и встроенной поддержкой социальных сетей.

В итоге Bada OS имела признаки типовой мобильной операционной системой того времени. Реализованная многозадачность была неполноценной: Samsung Wave мог держать несколько стандартных программ в памяти, но при этом в фоне могло работать только одно стороннее приложение. В магазине Samsung Apps на запуске первого смартфона уже был базовый набор приложений и игр, социальные сети были встроены в саму систему.

3.8.3. Защита мобильных устройств при работе с сетевыми ресурсами и «облачными» хранилищами данных

Большинство обладателей мобильных устройств уже не один год пользуются облачными хранилищами данных: Google Drive, Microsoft OneDrive, Dropbox. Это лишь некоторые из множества популярных сервисов облачного хранения данных. Пользователи выбирают облачные хранилища исходя из совместимости с установленными на их устройствах программами и сервисами. В данном разделе облачные сервисы рассматриваются с точки зрения кибербезопасности.

Многие популярные облачные хранилища довольно удобны, однако у них есть критический недостаток с точки зрения кибербезопасности. Он заключается в том, что существует вероятность получения доступа к личным файлам, находящимся в облачном хранилище, посторонними лицами.

Шифрование данных защищает от посторонних. Однако, поскольку облачные сервисы шифруют данные, это означает, что у них имеются ключи шифрования, и они могут как зашифровать данные, так и расшифровать их. Пользователям остаётся только надеяться, что сервисы не будут заглядывать в их файлы. Также приходится доверять сервисам хранение ключей шифрования.

Шифрование. Секрет надёжности облачных хранилищ заключается в первую очередь в том, кто контролирует ключи шифрования и дешифрования данных. Сервисы облачного хранения данных используют разные методы защиты. Данные могут сохраняться в безопасных помещениях с вооружённой охраной и биометрическими замками. Они могут быть зашифрованы последними алгоритмами, с которыми не справятся даже суперкомпьютеры.

Существуют разные подходы к защите данных в облачных хранилищах. Нужно принимать во внимание три фактора: данные в процессе передачи, данные при хранении в облаке и данные на вашем мобильном устройстве. В процессе передачи данные отправляются с компьютера, смартфона или ноутбука на сервер и в обратном направлении. В остальных случаях данные хранятся на сервере или на мобильном устройстве. Чтобы система считалась надёжной, данные в процессе передачи должны быть защищены одним из протоколов, чтобы никто не мог при перехвате прочитать их. При передаче данных в интернете обычно используют шифрование TLS/SSL. Оно применяется прежде чем данные отправляются в интернет, и снимается, когда данные доставляются в облачное хранилище. Это же происходит при передаче данных в обратном направлении. Шифрование TLS/SSL обеспечивает достаточно безопасную передачу данных, но оно не работает, когда данные прибыли в пункт назначения. Если отправляемые в облачное хранилище данные не были

зашифрованы до того, как к ним применяется шифрование TLS/SSL, после прибытия данные не зашифрованы и их можно прочитать.

Данные могут передаваться в двух окружениях. Это могут быть публичные сети, например, интернет и частные локальные сети дома или на работе. Зачастую частные сети являются более защищёнными по сравнению с общедоступными. Некоторые защищённые сервисы облачного хранения данных позволяют хранить личные файлы на собственном оборудовании внутри частной сети, что может усилить их безопасность.

При нахождении файлов в облачном хранилище, они располагаются на серверах. Чтобы данные были защищены, к ним должен быть закрыт неавторизованный доступ. Защита может быть физической, процедурной, программно-аппаратной. Серверы должны находиться в безопасном месте, и у посторонних не должно быть к ним доступа. Многие сервисы облачного хранения данных обеспечивают такую защиту. Если процедуры безопасности облачного сервиса не сработают или кто-то проникнет в место хранения файлов, личные данные могут попасть в чужие руки. Более безопасным вариантом хранения данных является их шифрование перед отправкой в облачные сервисы. Прочитать такие данные сможет только тот, кто сумеет их расшифровать. Типовым вариантом шифрования в таких сценариях работы является алгоритм AES-256 или подобные.

Зашифровать и расшифровать данные может только тот, у кого есть ключи шифрования. Во многих случаях ключи шифрования находятся в сервисе облачного хранения. Сервис использует протоколы TLS/SSL для передачи данных, затем применяет ключ шифрования и сохраняет данные на своих серверах. Это удобно, но в данном случае сервису доверяют защиту данных пользователей. Более безопасным подходом является самостоятельное хранение ключей шифрования. Наиболее надёжные системы не знают ключей шифрования. Приложение на персональном мобильном устройстве использует ключи для шифрования данных перед их отправкой на сервер и для дешифрования при получении данных с сервера. На самом сервере ключей нет. Если приложение защиты имеет открытый исходный код и достаточно популярно, существуют весомые основания доверять ему. Разбирающиеся в программировании энтузиасты проверяют исходный код таких приложений и анализируют их возможности. Также нужно подумать о безопасности хранения данных на мобильном устройстве. Большинство сервисов облачного хранения данных, даже самые надёжные, защищают данные только тогда, когда они покинули мобильное устройство. Если кто-то получает доступ к мобильному устройству, он получает и доступ к личным данным, если они не зашифрованы. Но, например, в NordLocker находящиеся в облачном хранилище данные зашифрованы и на пользовательских устройствах. Для их расшифровки нужно выполнить вход в учётную запись NordLocker.

Шифрование данных на мобильном устройстве пользователя обеспечивает дополнительный уровень защиты. Такие системы, где только пользователь может шифровать и дешифровать свои данные, называются сквозным шифрованием. Если используется сервис, когда данные сохраняются в собственной защищённой частной сети, для обеспечения максимальной надёжности требуется некоторая форма сквозного шифрования.

VPN. Безопасные облачные хранилища призваны защищать пользовательские данные, но это не означает, что они не собирают никакой информации о пользователях. Многие ведут записи относительно пользовательской активности в сервисе. Могут записываться дата и время входа в учётную запись, длительность сеанса работы, IP-адрес и т.д. Сбор персональной информации и её привязка к адресу может пригодиться самим сервисам. Для пользователей же это несёт потенциальную угрозу. Чтобы минимизировать риски реализации этой угрозы, при подключении к облачному хранилищу в ряде случаев используют сервисы VPN.

Месторасположение. В зависимости от принципов работы защищённого облачного хранилища сервис может иметь доступ к следующей информации:

− платёжные сведения, имя и другие указываемые при регистрации данные;

− метаданные, такие как IP-адрес и некоторые другие сведения;

− информация о разрешениях на доступ к зашифрованным файлам;

− названия файлов и папок, в которых где хранятся зашифрованные данные.

Пользователю необходимо продумать защиту от угроз, чтобы указанные данные не попали в чужие руки. Сервис может быть зарегистрирован в одной стране, а физически данные располагаются в другой. Например, для Sync.com в обоих случаях это Канада. MEGA располагается в Новой Зеландии и там же может хранить данные. Или же хранит их в неуказанных европейских странах, где якобы есть адекватный уровень защиты в соответствии со статьёй 45 GDPR. Решение о том, где именно будут храниться данные, может приниматься на основе местонахождения пользователя смартфона.

Комплексный подход. Таким образом, наиболее защищённые сервисы облачного хранения данных могут не быть такими популярными и удобными при работе с мобильного устройства, как Google Drive. У них может отсутствовать синхронизация со сторонними сервисами вроде Office 365 и т.д., но несмотря на это, они будут обеспечивать высокий уровень защиты данных. К таким сервисам можно отнести Tresorit, Sync.com, NordLocker, Nextcloud, MEGA.nz и т.д. Также для обеспечения комплексной кибербезопасности использование мобильных устройств при работе с сетевыми ресурсами и облачными хранилищами данных должно осуществляться в соответствии с основами безопасной работы мобильных

устройств, уже рассмотренных нами в разделе 3.8.1.

3.9. Защита информации от методов социальной инженерии

3.9.1. Основные типы воздействий с использованием социальной инженерии

Социальная инженерия – метод получения необходимого доступа к информации, основанный на особенностях психологии людей. Основной целью социальной инженерии является получение доступа к конфиденциальной информации, паролям, банковским данным и другим защищенным системам. Хотя термин социальной инженерии появился не так давно, сам метод получения информации таким способом используется довольно долго. Сотрудники ЦРУ и КГБ, которые хотят заполучить некоторую государственную тайну, политики и кандидаты в депутаты, да и мы сами, при желании получить что-либо, часто даже не понимая этого, используем методы социальной инженерии.

Для того, чтобы обезопасить себя от воздействия социальной инженерии, необходимо понять, как она работает. Рассмотрим основные типы социальной инженерии и методы защиты от них (рис. 3.9.1).

Претекстинг – это набор действий, отработанных по определенному, заранее составленному сценарию, в результате которого жертва может выдать какую-либо информацию или совершить определенное действие. Чаще всего данный вид атаки предполагает использование голосовых средств, таких как Skype, телефон и т.п.

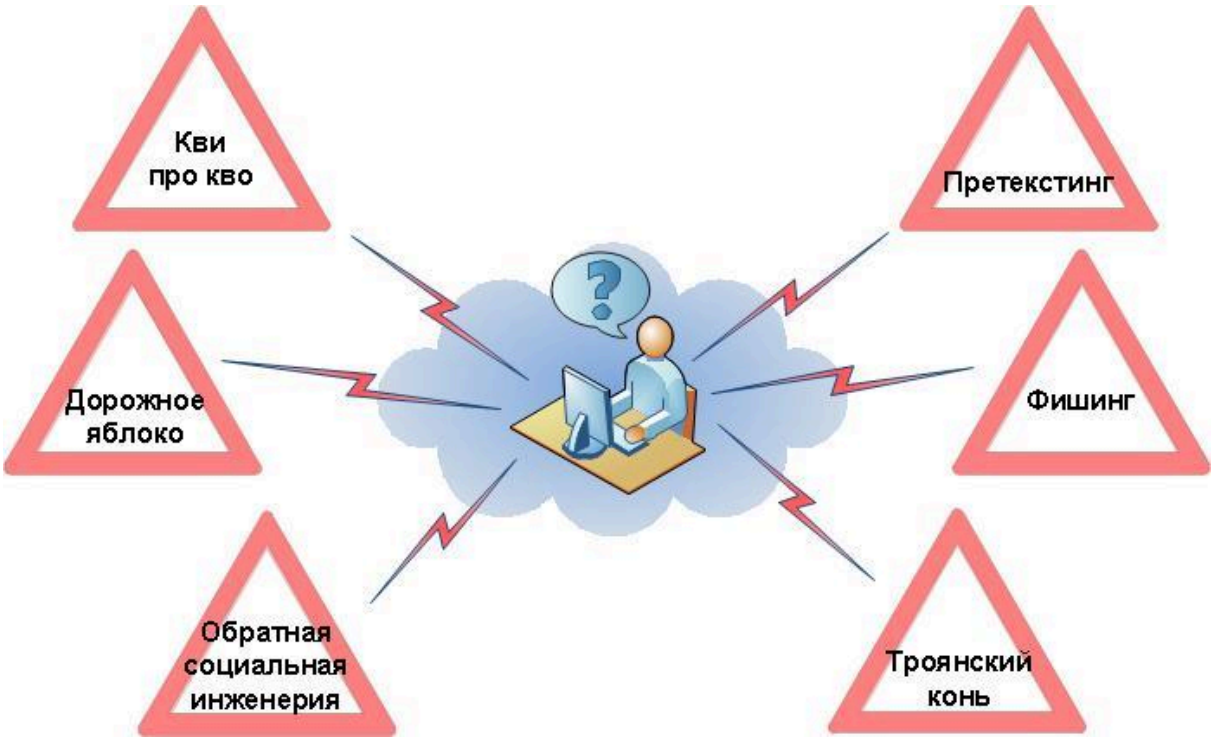


Рис. 3.9.1. – Основные типы социальной инженерии

Для использования этой техники злоумышленнику необходимо изначально иметь некоторые данные о жертве (имя сотрудника; должность; название проектов, с которыми он работает; дату рождения). Злоумышленник изначально использует реальные запросы с именем сотрудника компании и, после того как войдет в доверие, получает необходимую ему информацию.

Фишинг – техника интернет-мошенничества, направленная на получение конфиденциальной информации пользователей – авторизационных данных различных систем. Основным видом фишинговых атак является поддельное письмо, отправленное жертве по электронной почте, которое выглядит как официальное письмо от платежной системы или банка. В письме содержится форма для ввода персональных данных (пин-кодов, логина и пароля и т.п.) или ссылка на web-страницу, где располагается такая форма. Причины доверия жертвы подобным страницам могут быть разные: блокировка аккаунта, поломка в системе, утеря данных и прочее.

Троянский конь – это техника основывается на любопытстве, страхе или других эмоциях пользователей. Злоумышленник отправляет письмо жертве посредством электронной почты, во вложении которого находится «обновление» антивируса, ключ к денежному выигрышу или компромат на сотрудника. На самом же деле во вложении находится вредоносная программа, которая, после того как пользователь запустит ее на своем компьютере, будет использоваться для сбора или изменения информации злоумышленником.

Qui pro quo (услуга за услугу) – данная техника предполагает обращение злоумышленника к пользователю по электронной почте или корпоративному телефону. Злоумышленник может представиться, например, сотрудником технической поддержки и информировать о возникновении технических проблем на рабочем месте. Далее он сообщает о необходимости их устранения. В процессе «решения» такой проблемы, злоумышленник подталкивает жертву на совершение действий, позволяющих атакующему выполнить определенные команды или установить необходимое программное обеспечение на компьютере жертвы.

Дорожное яблоко – этот метод представляет собой адаптацию троянского коня и состоит в использовании физических носителей (CD, флэш-накопителей). Злоумышленник обычно подбрасывает такой носитель в общедоступных местах на территории компании (парковки, столовые, рабочие места сотрудников, туалеты). Для того чтобы у сотрудника возник интерес к данному носителю, злоумышленник может нанести на носитель логотип компании и какую-нибудь подпись. Например, «данные о продажах», «зарплата сотрудников», «отчет в

налоговую» и другое.

Обратная социальная инженерия – данный вид атаки направлен на создание такой ситуации, при которой жертва вынуждена будет сама обратиться к злоумышленнику за «помощью». Например, злоумышленник может выслать письмо с телефонами и контактами «службы поддержки» и через некоторое время создать обратимые неполадки в компьютере жертвы. Пользователь в таком случае позвонит или свяжется по электронной почте с злоумышленником сам, и в процессе «исправления» проблемы злоумышленник сможет получить необходимые ему данные.

3.9.2. Методы борьбы с социальной инженерией в интересах обеспечения кибербезопасности

Основным способом защиты от методов социальной инженерии является обучение сотрудников. Все работники компании должны быть предупреждены об опасности раскрытия персональной информации и конфиденциальной информации компании, а также о способах предотвращения утечки данных. Кроме того, у каждого сотрудника компании, в зависимости от подразделения и должности, должны быть инструкции о том, как и на какие темы можно общаться с собеседником, какую информацию можно предоставлять для службы технической поддержки, как и что должен сообщить сотрудник компании для получения той или иной информации от другого сотрудника.

Кроме того, можно выделить следующие правила:

- Пользовательские учетные данные являются собственностью компании.

Всем сотрудникам в день приема на работу должно быть разъяснено, что те логины и пароли, которые им выдали, нельзя использовать в других целях (на web-сайтах, для личной почты и т.п.), передавать третьим лицам или другим сотрудникам компании, которые не имеют на это право. Например, очень часто, уходя в отпуск, сотрудник может передать свои авторизационные данные своему коллеге для того, чтобы тот смог выполнить некоторую работу или посмотреть определенные данные в момент его отсутствия.

- Необходимо проводить вступительные и регулярные обучения сотрудников компании, направленные на повышение знаний по информационной безопасности.

Проведение таких инструктажей позволит сотрудникам компании иметь актуальные данные о существующих методах социальной инженерии, а также не забывать основные правила по информационной безопасности.

- Обязательным является наличие регламентов по безопасности, а также инструкций, к которым пользователь должен всегда иметь доступ. В инструкциях должны быть описаны действия сотрудников при возникновении той или иной ситуации.

Например, в регламенте можно прописать, что необходимо делать и куда обращаться при попытке третьего лица запросить конфиденциальную информацию или учетные данные сотрудников. Такие действия позволят вычислить злоумышленника и не допустить утечку информации.

- На компьютерах сотрудников всегда должно быть актуальное антивирусное программное обеспечение.

На компьютерах сотрудников также необходимо установить брандмауэр.

- В корпоративной сети компании необходимо использовать системы обнаружения и предотвращения атак.

Также необходимо использовать системы предотвращения утечек конфиденциальной информации. Все это позволит снизить риск возникновения фитиновых атак.

- Все сотрудники должны быть проинструктированы, как вести себя с посетителями.

Необходимы четкие правила для установления личности посетителя и его сопровождения. Посетителей всегда должен сопровождать кто-то из сотрудников компании. Если сотрудник встречает неизвестного ему посетителя, он должен в корректной форме поинтересоваться, с какой целью посетитель находится в данном помещении и где его сопровождение. При необходимости сотрудник должен сообщить о неизвестном посетителе в службу безопасности.

- Необходимо максимально ограничить права пользователя в системе.

Например, можно ограничить доступ к web-сайтам и запретить использование съемных носителей. Ведь если сотрудник не сможет попасть на фишинговый сайт или использовать на компьютере флэш-накопитель с «троянской программой», то и потерять личные данные он также не сможет.

Исходя из всего перечисленного, можно сделать вывод: основной способ защиты от социальной инженерии – это обучение сотрудников. Необходимо знать и помнить, что незнание не освобождает от ответственности. Каждый пользователь системы должен знать об опасности раскрытия конфиденциальной информации и знать способы, которые помогут предотвратить утечку.

Контрольные вопросы:

1. Почему к ранним версиям Windows применим термин дисковая операционная система?
2. Охарактеризуйте основные компоненты графического интерфейса Windows.
3. В чем заключаются отличия пользовательского режима работы Windows и режима ядра?
4. Охарактеризуйте файловые системы операционной системы Windows.

5. Опишите алгоритм загрузки Windows.

6. Назовите назначение пяти корневых кустов Windows.

7. Охарактеризуйте инструментарий регистрации событий Windows.

8. Поясните принципы работы и назначение межсетевого экрана Windows.

9. Перечислите мероприятия по усилению защиты устройств с операционной системой Windows.

10. Перечислите базовые команды консольного интерфейса Linux.

11. Что понимается под конфигурационными файлами сервисов и служб в Linux?

12. Каким образом устроена традиционная система регистрации событий в Linux?

13. Охарактеризуйте файловые системы операционной системы Linux.

14. Каким образом реализован традиционный механизм доступа к объектам файловой системы в Linux?

15. Какие задачи обеспечения безопасности кроме задач правильного управления доступом к объектам файловой подсистемы выделяют в Linux?

16. Перечислите основные требования к современным защищенным операционным системам.

17. Охарактеризуйте дополнительные средства защиты и безопасности в операционной системе Astra Linux Special Edition.

18. Защиту каких видов информации может обеспечить операционная система специального назначения Astra Linux?

19. Перечислите мероприятия по усилению защиты устройств с операционной системой Linux.

20. Назовите и охарактеризуйте уровни модели взаимодействия открытых систем OSI.

21. Назовите и охарактеризуйте уровни стека коммуникационных протоколов TCP/IP.

22. Перечислите основные типы межсетевых экранов.

23. Перечислите основные виды кибератак на сетевые ресурсы.

24. Что такое туннелирование прикладных протоколов, в частности, туннелирование протокола DNS?

25. Дайте общую характеристику политике информационной безопасности предприятия.

26. Назовите основные принципы безопасной работы с мобильными устройствами.

27. Перечислите ключевые особенности работы мобильных устройств с сетевыми ресурсами и облачными хранилищами данных.

28. Что такое Jailbreak применительно к устройствам iPhone?

29. Какая задача обычно решается пользователями мобильных устройств с помощью VPN?

30. Перечислите основные угрозы, связанные с методами социальной инженерии, и поясните направления противодействия этим угрозам.

Литература к главе 3

1. Таненбаум, Э. Современные операционные системы / Э. Таненбаум. – Санкт-Петербург : Питер, 2021. – 1040 с. – Текст : непосредственный.

2. Гордеев, А. В. Системное программное обеспечение / А. В. Гордеев, Ю. А. Молчанов. Санкт-Петербург, 2011. – 739 с. – Текст : непосредственный.

3. Партыка, Т. Л. Операционные системы, среды и оболочки : учебное пособие / Т. Л. Партыка. – Москва : Форум, 2011. – 360 с. – Текст : непосредственный.

4. Таненбаум Э., Бос Х. Современные операционные системы / Э. Таненбаум, Х. Бос. – 4-е изд. — Санкт-Петербург : Питер, 2015 – 1120 с. – Текст : непосредственный.

5. Денисов, Д. В. Аппаратное обеспечение вычислительных систем / Д. В. Денисов, В. В. Артюхин, М. Ф. Седненков. – Москва : Маркет ДС, 2013. – 184 с.

6. Макаренко, С. И. Операционные системы, среды и оболочки : учебное пособие / С. И. Макаренко – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2008. – 210 с. – Текст : непосредственный.

7. Практические основы компьютерно-технической экспертизы : учебно-методическое пособие / А. Б. Нехорошев [и др.]. – Саратов : Научная книга, 2007. – 264 с. – Текст : непосредственный.

8. Судебная экспертиза: типичные ошибки : учебное пособие / под ред. Е. Р. Россинской. – Москва : Проспект, 2014. – Текст : непосредственный. – 544 с.

9. Сборник примеров заключений эксперта по судебной компьютерно-технической экспертизе : практическое пособие для экспертов / Н. А. Хатунцев, Я. И. Васильев [и др.]. – Москва : РФЦСЭ М., 2016. – 144 с. – Текст : непосредственный.

10. Шелупанов, А. А. Формальные основы системы поддержки формирования частных методик производства компьютерно-технической экспертизы / А. А. Шелупанов, А. Р. Смолина – Текст : непосредственный // Информационно-управляющие системы – 2017. – № 3(88)/2017 – С. 99-104.

11. Костромин, В. А. Основы работы в ОС Linux. Курс ИНТУИТ.ру. – URL : https://www.intuit.ru, свободный. – Загл. с экрана. – Текст : электронный.

12. Костромин, В. А., Разделы диска и средства для работы с ними в Линукс. URL : http://www.linuxcenter.ru/lib/books/partitioning/, свободный. – Загл. с экрана. – Текст : электронный.

13. Microsoft Windows 2000 Active Directory Services. Учебный курс MCSE. – Москва : Русская Редакция, 2004. – 608 с. – Текст : непосредственный.

Глава 4. Источники и каналы утечки информации. Основы технической защиты информации.

4.1. Классификация и характеристика технических каналов утечки информации

4.1.1. Основные понятия, источники и каналы утечки информации

Информация – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления [1].

Виды представления информации:

- документированная;
- речевая;
- телекоммуникационная.

Сообщение является формой представления информации.

Носителем информации в зависимости от физической природы могут быть акустические, электрические, электромагнитные колебания.

Документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать [1].

В речевом виде информация формируется в процессе переговоров людей либо прослушивания аудиозаписей. Передача речевой информации на расстояние осуществляется при помощи акустических колебаний, распространяющихся в различных средах.

В телекоммуникационном виде информация циркулирует в системах ее обработки и передачи по линиям и каналам связи (системам телекоммуникации) при помощи электрических или электромагнитных колебаний.

Имеется ряд областей, в которых безопасность информации может быть нарушена, поскольку возможных путей ее утечки существует достаточно большое количество, и хорошая защита ее на одном этапе может быть напрасной, так как на других этапах правила обращения с такой информацией нарушаются, что может привести к ее компрометации. Поэтому в организации обеспечения безопасности информации следует придерживаться системного подхода.

Среди возможных путей утечки информации можно отметить следующие [2]:

1. Несанкционированное ознакомление с конфиденциальной информацией посторонних лиц, что возможно при неправильной

организации работы с документами и/или хранении документов в любом виде (в рукописном, машинописном или машиночитаемом. К этому же случаю можно отнести и просто хищение или уничтожение важных документов при их неправильном хранении.

2. Подробное обсуждение самой информации или непосредственно связанных с ней тем в присутствии посторонних лиц.

3. Наличие среди лиц, имеющих доступ к конфиденциальной информации, тайного агента потенциального или реального оппонента, а также прямой переход сотрудника фирмы на сторону такого оппонента или конкурирующей организации.

4. Получение (перехват) конфиденциальной информации при передаче ее от одного корреспондента другому – в устном виде, в письменном виде или по техническим средствам связи. Разновидностью нарушения безопасности информации может являться ее уничтожение или модификация, что осуществляется вторжением в компьютер или в линию связи. При этом оппонент может не иметь доступа к самой информации, однако он имеет возможность вывести ее из строя, тем самым причинив значительный ущерб владельцу информации. К этому типу нарушения безопасности информации относится и запуск в программное обеспечение ЭВМ вирусного программного обеспечения, стирающего или модифицирующего информацию, вследствие чего она безвозвратно теряется.

5. Целенаправленное подслушивание с помощью технически средств бесед, разговоров на специфичные темы, а также перехват побочных излучений (акустических, электрических, магнитных) от аппаратуры связи или от компьютера и его терминалов (дисплей, принтер и т.п.).

Естественно, что наиболее полно и последовательно системный подход осуществляется в специальных государственных службах. В таких службах, во-первых, имеется информация ограниченного распространения, разглашение которой может нанести ущерб всему обществу, поэтому эту информацию необходимо тщательно охранять. Во-вторых, такие учреждения имеют практическую (физическую, организационную и юридическую) возможность осуществлять системный подход к охране своих тайн. Что касается неправительственных и негосударственных учреждений, и тем более частных лиц, то их возможности по защите информации значительно меньше.

Специально для несанкционированного подслушивания конфиденциальных бесед и разговоров изготавливаются так называемые «жучки», которые представляют собой микрофон, совмещенный с УКВ

передатчиком или включенный в телефонную или электрическую сеть. Такие «жучки», закамуфлированные под предметы быта или оргтехники или встроенные в них, имеют очень небольшие размеры и массу, и их обнаружение зачастую бывает очень затруднительно. Иногда они встраиваются в стену помещения, и тогда их можно обнаружить только с помощью специалистов и специализированной поисковой аппаратуры.

Технические средства обработки информации, средства связи а также терминальные устройства вычислительных машин при своей работе имеют побочные акустические и электромагнитные излучения, которые могут быть связаны с элементами или символами обрабатываемой или передаваемой информации, или же нести другую информацию, которая может быть использована для несанкционированного получения конфиденциальной информации. Такие излучения при благоприятных для подслушивания (перехвата) условиях могут быть перехвачены с помощью специальных устройств, установленных в относительной близости к источнику излучения, и проанализированы аналитиками оппонента с целью получения конфиденциальной информации. При организации системного подхода к обеспечению безопасности информации следует учитывать уровень побочных акустических и электромагнитных излучений аппаратуры, которую собираются применить для обработки конфиденциальной информации [2].

Таким образом, безопасность информации может быть нарушена в нескольких областях. Несмотря на то, что имеются общие принципы и подходы к организации системного обеспечения безопасности информации, все же в каждом конкретном случае пути и методы решения этой задачи будут различны в зависимости от особенностей информации, ее ценности и возможностей владельца по ее защите. Следует также отметить, что выработка всеобъемлющего системного подхода к обеспечению безопасности информации и его реализация являются весьма сложными и трудоемкими задачами. Однако практически во всех случаях информация становится наиболее уязвимой, когда она выходит за пределы учреждения или из-под контроля владельца, а это всегда имеет место при передаче информации от одного корреспондента другому. Для успешного решения задач по защите информации необходимо иметь достаточно глубокие знания об ее источниках и каналах утечки.

4.1.2. Классификация технических каналов утечки информации

Под **техническим каналом утечки информации (ТКУИ)** понимают совокупность объекта разведки, технического средства разведки (ТСР), с помощью которого добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал [4].

По сути, под ТКУИ понимают способ получения с помощью ТСР разведывательной информации об объекте. Причем под **разведывательной информацией** обычно понимаются сведения или совокупность данных об объектах разведки независимо от формы их представления.

Сигналы являются материальными носителями информации. По своей физической природе сигналы могут быть электрическими, электромагнитными, акустическими, и т.д. То есть сигналами, как правило, являются электромагнитные, механические и другие виды колебаний (волн), причем информация содержится в их изменяющихся параметрах.

В зависимости от природы сигналы распространяются в определенных физических средах. В общем случае средой распространения могут быть газовые (воздушные), жидкостные (водные) и твердые среды. Например: воздушное пространство, конструкции зданий, соединительные линии и токопроводящие элементы, грунт (земля) и т.п.

Как было сказано выше, основными видами представления информации, представляющими интерес с точки зрения защиты, являются:

- документированная;
- акустическая (речевая);
- телекоммуникационная.

Документированная информация содержится в графическом или буквенно-цифровом виде на бумаге, а также в электронном виде на магнитных и других носителях. Особенность документальной информации заключается в том, что она в сжатом виде содержит сведения, подлежащие защите [4].

Речевая информация возникает в ходе ведения в помещениях разговоров, а также при работе систем звукоусиления и звуковоспроизведения [4].

Носителем речевой информации являются акустические колебания (механические колебания частиц упругой среды), распространяющиеся от источника колебаний в окружающее пространство в виде волн различной длины.

Речевой сигнал является сложным акустическим сигналом в диапазоне частот от 20...30 Гц до 16...20 кГц.

Телекоммуникационные данные циркулируют в технических средствах обработки и хранения информации, а также в каналах связи при ее передаче. Носителем информации при ее обработке техническими

средствами и передаче по проводным каналам связи является электрический ток, а при передаче по радио и оптическому каналам – электромагнитные волны.

Основными объектами защиты информации являются:

– информационные ресурсы, содержащие сведения, отнесенные к государственной тайне, и конфиденциальную информацию;

– средства и системы информатизации (средства вычислительной техники, информационно–вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, технические средства приема, передачи и обработки информации ограниченного доступа (звукозапись, звукоусиление, звукосопровождение, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки графической, смысловой и буквенно-цифровой информации), их информативные физические поля. То есть системы и средства, непосредственно обрабатывающие информацию, отнесенную к государственной тайне, а также конфиденциальную информацию. Эти средства и системы часто называют **основными техническими средствами и системами (ОТСС)** [2].

Под **ОТСС** понимают технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации. К таким средствам относятся: электронно-вычислительная техника, режимные абонентские телефонные станции (АТС), системы оперативно-командной и громкоговорящей связи, системы звукоусиления, звукового сопровождения и звукозаписи и т.д.

При выявлении технических каналов утечки информации ОТСС необходимо рассматривать как систему, включающую основное (стационарное) оборудование, оконечные устройства, соединительные линии (совокупность проводов и кабелей, прокладываемых между отдельными ОТСС и их элементами), распределительные и коммутационные устройства, системы электропитания, системы заземления.

Отдельные технические средства или группа технических средств, предназначенных для обработки конфиденциальной информации, вместе с помещениями, в которых они размещаются, составляют **объект ОТСС.** Под объектами ОТСС понимают также выделенные помещения, предназначенные для проведения закрытых мероприятий.

Наряду с ОТСС в помещениях устанавливаются технические средства и системы, непосредственно не участвующие в обработке конфиденциальной информации, но использующиеся совместно с ОТСС и находящиеся в зоне электромагнитного поля, создаваемого ими. Такие

технические средства и системы называются **вспомогательными техническими средствами и системами (ВТСС)** [2]. К ним относятся: технические средства открытой телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, электрификации, радиофикации, часофикации, электробытовые приборы и т.д.

В качестве канала утечки информации наибольший интерес представляют ВТСС, имеющие выход за пределы **контролируемой зоны** (КЗ), т.е. зоны, в которой исключено появление лиц и транспортных средств, не имеющих постоянных или временных пропусков [2].

Кроме соединительных линий ОТСС и ВТСС за пределы контролируемой зоны могут выходить провода и кабели, к ним не относящиеся, но проходящие через помещения, где установлены технические средства, а также металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции. Такие провода, кабели и токопроводящие элементы называются **посторонними проводниками.**

В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата, технические каналы утечки информации можно разделить на **электромагнитные, электрические и параметрический**.

4.1.3. Характеристика технических каналов утечки информации

Электромагнитные каналы утечки информации.

К электромагнитным относятся каналы утечки информации, возникающие за счет различного вида побочных электромагнитных излучений (ЭМИ) ОТСС [5]:

– излучений элементов ОТСС;

– излучений на частотах работы высокочастотных (ВЧ) генераторов ОТСС;

– излучений на частотах самовозбуждения усилителей низкой частоты (УНЧ) ОТСС.

В ОТСС носителем информации является электрический ток, параметры которого (сила тока, напряжение, частота и фаза) изменяются по закону информационного сигнала. При прохождении электрического тока по токоведущим элементам ОТСС вокруг них (в окружающем пространстве) возникает электрическое и магнитное поле. В силу этого элементы ОТСС можно рассматривать как излучатели электромагнитного поля, модулированного по закону изменения информационного сигнала.

В состав ОТСС и ВТСС могут входить различного рода высокочастотные генераторы. К таким устройствам можно отнести: задающие генераторы, генераторы тактовой частоты, генераторы стирания и подмагничивания магнитофонов, гетеродины радиоприемных и телевизионных устройств, генераторы измерительных приборов и т.д.

Классификация технических каналов утечки информации, обрабатываемой ОТСС, приведена на рисунке 4.1 [2].

Рис. 4.1.1. Классификация технических каналов утечки информации, обрабатываемой ТСПИ

В результате внешних воздействий информационного сигнала (например, электромагнитных колебаний) на элементах ВЧ-генераторов наводятся электрические сигналы. Приемником магнитного поля могут быть катушки индуктивности колебательных контуров, дроссели в цепях электропитания и т.д. Приемником электрического поля являются провода высокочастотных цепей и другие элементы. Наведенные электрические сигналы могут вызвать непреднамеренную модуляцию собственных ВЧ-колебаний генераторов. Эти промодулированные ВЧ-колебания излучаются в окружающее пространство.

Электромагнитные излучения на частотах самовозбуждения усилителей низкой частоты технических средств передачи информации (УНЧ ТСПИ). Самовозбуждение УНЧ ТСПИ (например, усилителей систем звукоусиления и звукового сопровождения, магнитофонов, систем громкоговорящей связи и т.п.) возможно за счет случайных преобразований отрицательных обратных связей (индуктивных или емкостных) в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов. Частота самовозбуждения лежит в пределах рабочих частот нелинейных элементов УНЧ (например, полупроводниковых приборов, электровакуумных ламп и т.п.). Сигнал на частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом. Самовозбуждение наблюдается, в основном, при переводе УНЧ в нелинейный режим работы, т.е. в режим перегрузки.

Перехват побочных электромагнитных излучений ТСПИ осуществляется средствами радио-, радиотехнической разведки, размещенными вне контролируемой зоны.

Зона, в которой возможны перехват (с помощью разведывательного приемника) побочных электромагнитных излучений и последующая расшифровка содержащейся в них информации (т.е. зона, в пределах которой отношение «информационный сигнал/помеха» превышает допустимое нормированное значение), называется (опасной) **зоной 2** [4].

Причинами возникновения электрических каналов утечки информации могут быть:

– наводки электромагнитных излучений ОТСС на соединительные линии ВТСС и посторонние проводники, выходящие за пределы контролируемой зоны;

– просачивание информационных сигналов в цепи электропитания ТСПИ:

– просачивание информационных сигналов в цепи заземления ОТСС.

Наводки электромагнитных излучений ОТСС возникают при излучении элементами ОТСС (в том числе и их соединительными линиями) информационных сигналов, а также при наличии гальванической связи соединительных линий ОТСС и посторонних проводников или линий ВТСС. Уровень наводимых сигналов в значительной степени зависит от мощности излучаемых сигналов, расстояния до проводников, а также длины совместного пробега соединительных линий ОТСС и посторонних проводников.

Пространство вокруг ОТСС, в пределах которого на случайных антеннах наводится информационный сигнал выше допустимого (нормированного) уровня, называется (опасной) **зоной** 1 [4].

Случайной антенной является цепь ВТСС или посторонние

проводники, способные принимать побочные электромагнитные излучения.

Случайные антенны могут быть сосредоточенными и распределенными. **Сосредоточенная случайная антенна** представляет собой компактное техническое средство, например телефонный аппарат, громкоговоритель радиотрансляционной сети и т.д. К **распределенным случайным антеннам** относятся случайные антенны с распределенными параметрами: кабели, провода, металлические трубы и другие токопроводящие коммуникации.

Просачивание информационных сигналов в цепи электропитания возможно при наличии магнитной связи между выходным трансформатором усилителя (например, УНЧ) и трансформатором выпрямительного устройства. Кроме того, токи усиливаемых информационных сигналов замыкаются через источник электропитания, создавая на его внутреннем сопротивлении падение напряжения, которое при недостаточном затухании в фильтре выпрямительного устройства может быть обнаружено в линии электропитания. Информационный сигнал может проникнуть в цепи электропитания также в результате того, что среднее значение потребляемого тока в оконечных каскадах усилителей в большей или меньшей степени зависит от амплитуды информационного сигнала, что создает неравномерную нагрузку на выпрямитель и приводит к изменению потребляемого тока по закону изменения информационного сигнала.

Просачивание информационных сигналов в цепи заземления.

Кроме заземляющих проводников, служащих для непосредственного соединения ОТСС с контуром заземления, гальваническую связь с землей могут иметь различные проводники, выходящие за пределы контролируемой зоны. К ним относятся нулевой провод сети электропитания, экраны (металлические оболочки) соединительных кабелей, металлические трубы систем отопления и водоснабжения, металлическая арматура железобетонных конструкций и т.д. Все эти проводники совместно с заземляющим устройством образуют разветвленную систему заземления, на которую могут наводиться информационные сигналы. Кроме того, в грунте вокруг заземляющего устройства возникает электромагнитное поле, которое также является источником информации.

Перехват информационных сигналов по электрическим каналам утечки возможен путем непосредственного подключения к соединительным линиям ВТСС и посторонним проводникам, проходящим через помещения, где установлены ТСПИ, а также к их системам электропитания и заземления. Для этих целей используются специальные средства радио- и радиотехнической разведки, а также специальная измерительная аппаратура [2].

Съем информации с использованием аппаратных закладочных устройств. В последние годы участились случаи съема информации, обрабатываемой в ОТСС. путем установки в них электронных устройств перехвата информации **– закладочных устройств.**

Электронные устройства перехвата информации, устанавливаемые в ОТСС, иногда называют **аппаратными закладками.** Они представляют собой мини-передатчики, излучение которых модулируется информационным сигналом. Наиболее часто закладки устанавливаются в ОТСС иностранного производства, однако возможна их установка и в отечественных средствах.

Перехваченная с помощью закладочных устройств информация или непосредственно передается по радиоканалу, или сначала записывается на специальное запоминающее устройство, а уже затем по команде передается на запросивший ее объект.

Параметрический канал перехвата информации. Перехват обрабатываемой в технических средствах информации возможен также путем их **«высокочастотного облучения».** При взаимодействии облучающего электромагнитного поля с элементами ОТСС происходит переизлучение электромагнитного поля. В ряде случаев это вторичное излучение модулируется информационным сигналом. При съеме информации для исключения взаимного влияния облучающего и переизлученного сигналов может использоваться их временная или частотная развязка. Например, для облучения ОТСС могут использовать импульсные сигналы.

При переизлучении параметры сигналов изменяются. Поэтому данный канал утечки информации часто называют **параметрическим.**

Для перехвата информации по данному каналу необходимы специальные высокочастотные генераторы с антеннами, имеющими узкие диаграммы направленности и специальные радиоприемные устройства.

4.1.4. Классификация каналов утечки акустической (речевой) информации

Под **акустической** понимается информация, носителем которой являются акустические сигналы. В том случае, если источником информации является человеческая речь, акустическая информация называется **речевой.**

Акустический сигнал представляет собой возмущения упругой среды, проявляющиеся в возникновении акустических колебаний различной формы и длительности. Акустическими называются механические колебания частиц упругой среды, распространяющиеся от источника колебаний в окружающее пространство в виде волн различной длины.

Рис. 4.1.2. Классификация технических каналов утечки

акустической (речевой) информации

Первичными источниками акустических колебаний являются механические колебательные системы, например органы речи человека, а вторичными – преобразователи различного типа, в том числе электроакустические. Последние представляют собой устройства, предназначенные для преобразования акустических колебаний в электрические и обратно. К ним относятся пьезоэлементы, микрофоны, телефоны, громкоговорители и другие устройства.

В зависимости от формы акустических колебаний различают **простые (тональные) и сложные** сигналы. Тональный – это сигнал, вызываемый колебанием, совершающимся по синусоидальному закону. Сложный сигнал включает целый спектр гармонических составляющих.

Речевой сигнал является сложным акустическим сигналом в диапазоне частот от 200...300 Гц до 4...6 кГц.

В зависимости от физической природы возникновения информационных сигналов, среды распространения акустических колебаний и способов их перехвата технические каналы утечки акустической (речевой) информации можно разделить на **воздушные, вибрационные, электроакустические, оптико-электронный и параметрические** [2].

4.1.5. Характеристика каналов утечки акустической (речевой) информации

В воздушных технических каналах утечки информации средой распространения акустических сигналов является воздух, и для их перехвата используются миниатюрные высокочувствительные микрофоны и специальные направленные микрофоны.

Миниатюрные микрофоны объединяются (или соединяются) с портативными звукозаписывающими устройствами (диктофонами) или специальными миниатюрными передатчиками.

Автономные устройства, конструкционно объединяющие миниатюрные микрофоны и передатчики, называют закладочным устройствами перехвата речевой информации, или просто **акустическими закладками.**

Перехваченная закладочными устройствами речевая информация может передаваться по радиоканалу, оптическому каналу (в инфракрасном диапазоне длин волн), по сети переменного тока, соединительным линиям ВТСС, посторонним проводникам (трубам водоснабжения и канализации, металлоконструкциям и т.п.). Причем для передачи информации по трубам и металлоконструкциям могут использоваться не только электромагнитные, но и механические ультразвуковые колебания.

Прием информации, передаваемой закладочными устройствами, осуществляется, как правило, на специальные приемные устройства,

работающие в соответствующем диапазоне длин волн. Однако встречаются закладочные устройства, прием информации с которых можно осуществлять с обычного телефонного аппарата. Такие устройства устанавливаются или непосредственно в корпусе телефонного аппарата, находящегося в контролируемом помещении и называемом «телефоном-наблюдателем», или подключаются к телефонной линии, чаще всего в телефонной розетке. Подобное устройство конструктивно объединяет миниатюрный микрофон и специальный блок коммутации и часто называется **«телефонным ухом».** Блок коммутации подключает микрофон к телефонной линии при дозвоне по определенной схеме до «телефона-наблюдателя» или подаче в линию специального кодированного сигнала.

Использование портативных диктофонов и акустических закладок требует проникновения на контролируемый объект (в помещение). В том случае, когда это не удается, для перехвата речевой информации используются направленные микрофоны.

В вибрационных (структурных) технических каналах утечки информации средой распространения акустических сигналов являются конструкции зданий, сооружений (стены, потолки, полы), трубы водоснабжения, отопления, канализации и другие твердые тела. Для перехвата акустических колебаний в этом случае используются контактные микрофоны (стетоскопы).

Контактные микрофоны, соединенные с электронным усилителем называют **электронными стетоскопами.**

По вибрационному каналу также возможен перехват информации с использованием закладочных устройств. В основном для передачи информации используется радиоканал, поэтому такие устройства часто называют **радиостетоскопами.** Возможно использование закладочных устройств с передачей информации по оптическому каналу в ближнем инфракрасном диапазоне длин волн, а также по ультразвуковому каналу (по металлоконструкциям здания).

Электроакустические технические каналы утечки информации возникают за счет электроакустических преобразований акустических сигналов в электрические и включают перехват акустических колебаний через ВТСС, обладающих «микрофонным эффектом», а также путем «высокочастотного навязывания».

Некоторые элементы ВТСС, в том числе трансформаторы, катушки индуктивности, электромагниты вторичных электрочасов, звонков телефонных аппаратов, дроссели ламп дневного света, электро-реле и т.п., обладают свойством изменять свои параметры (емкость, индуктивность, сопротивление) под действием акустического поля, создаваемого источником акустических колебаний. Изменение параметров приводит либо к появлению на данных элементах электродвижущей силы (ЭДС), изменяющейся по закону воздействующего информационного

акустического поля, либо к модуляции токов, протекающих по этим элементам, информационным сигналом. Например, акустическое поле, воздействуя на якорь электромагнита вызывного телефонного звонка, вызывает его колебание. В результате чего изменяется магнитный поток сердечника электромагнита. Изменение этого потока вызывает появление ЭДС самоиндукции в катушке звонка, изменяющейся по закону изменения акустического поля.

ВТСС, кроме указанных элементов, могут содержать непосредственно электроакустические преобразователи. К таким ВТСС относятся некоторые датчики пожарной сигнализации, громкоговорители ретрансляционной сети и т.д. Эффект электроакустического преобразования акустических колебаний в электрические часто называют **«микрофонным эффектом».** Причем из ВТСС, обладающих «микрофонным эффектом», наибольшую чувствительность к акустическому полю имеют абонентские громкоговорители и некоторые датчики пожарной сигнализации.

Перехват акустических колебаний в данном канале утечки информации осуществляется путем непосредственного подключения к соединительным линиям ВТСС, обладающих «микрофонным эффектом», специальных высокочувствительных низкочастотных усилителей. Например, подключая такие средства к соединительным линиям телефонных аппаратов с электромеханическими вызывными звонками, можно прослушивать все разговоры в помещениях, где установлены эти аппараты.

Технический канал утечки информации путем **«высокочастотного навязывания»** может быть осуществлен путем несанкционированного контактного введения токов высокой частоты от соответствующего генератора в линии (цепи), имеющие функциональные связи с нелинейными или параметрическими элементами ВТСС, на которых происходит модуляция высокочастотного сигнала информационным. Информационный сигнал в данных элементах ВТСС появляется вследствие электроакустического преобразования акустических сигналов в электрические. В силу того, что нелинейные или параметрические элементы ВТСС для высокочастотного сигнала, как правило, представляют собой несогласованную нагрузку, промодулированный высокочастотный сигнал будет отражаться от нее и распространяться в обратном направлении по линии или излучаться. Для приема излученных или отраженных высокочастотных сигналов используются специальные приемники с достаточно высокой чувствительностью. Для исключения влияния зондирующего и переотраженного сигналов могут использоваться импульсные сигналы [2].

Наиболее часто такой канал утечки информации используется для перехвата разговоров, ведущихся в помещении, через телефонный аппарат,

имеющий выход за пределы контролируемой зоны. Для исключения воздействия высокочастотного сигнала на аппаратуру АТС в линию, идущую в ее сторону, устанавливается специальный высокочастотный фильтр.

Оптико-электронный (лазерный) канал утечки акустической информации образуется при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекол окон, картин, зеркал и т.д.). Отраженное лазерное излучение (диффузное или зеркальное) модулируется по амплитуде и фазе (по закону вибрации поверхности) и принимается приемником оптического (лазерного) излучения, при демодуляции которого выделяется речевая информация. Причем лазер и приемник оптического излучения могут быть установлены в одном или разных местах (помещениях).

Для перехвата речевой информации по данному каналу используются сложные лазерные акустические локационные системы, иногда называемые **«лазерными микрофонами».** Работают они, как правило, в ближнем инфракрасном диапазоне волн.

Параметрический канал утечки информации может быть реализован и путем **«высокочастотного облучения»** помещения, где установлены полуактивные закладочные устройства, имеющие элементы, некоторые параметры которых (например, добротность и резонансная частота объемного резонатора) изменяются по закону изменения акустического (речевого) сигнала.

При облучении мощным высокочастотным сигналом помещения, в котором установлено такое закладочное устройство, в последнем при взаимодействии облучающего электромагнитного поля со специальными элементами закладки (например, четвертьволновым вибратором) происходит образование вторичных радиоволн, т.е. переизлучение электромагнитного поля, а специальное устройство закладки (например, объемный резонатор) обеспечивает амплитудную, фазовую или частотную модуляцию переотраженного сигнала по закону изменения речевого сигнала. Подобного вида закладки иногда называют **полуактивными.**

Для перехвата информации по данному каналу кроме закладочного устройства необходимы специальный передатчик с направленным излучением и приемник.

4.2. Способы перехвата защищаемой информации

4.2.1. Основные причины утечки информации

Основным направлением противодействия утечке информации является обеспечение физической (технические средства, линии связи, персонал) и логической (операционная система, прикладные программы и данные) защиты информационных ресурсов. При этом безопасность достигается комплексным применением аппаратных, программных и криптографических методов и средств защиты, а также организационных мероприятий.

Основными причинами утечки информации являются [2]:

– несоблюдение персоналом норм, требований, правил эксплуатации аппаратной среды (АС);

– ошибки в проектировании АС и систем защиты АС;

– ведение противостоящей стороной технической и агентурной разведок.

Несоблюдение персоналом норм, требований, правил эксплуатации АС может быть как умышленным, так и непреднамеренным. От ведения противостоящей стороной агентурной разведки этот случай отличает то, что в данном случае лицом, совершающим несанкционированные действия, двигают личные побудительные мотивы. Причины утечки информации достаточно тесно связаны с видами утечки информации.

В соответствии с ГОСТ Р 50922-2006 рассматриваются три вида утечки информации:

– разглашение;

– несанкционированный доступ к информации;

– получение защищаемой информации разведками (как отечественными, так и иностранными).

Под **разглашением** информации понимается несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к защищаемой информации.

Под **несанкционированным доступом** [4] понимается получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации. При этом заинтересованным субъектом, осуществляющим несанкционированный доступ к информации, может быть: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

Получение защищаемой информации разведками может осуществляться с помощью технических средств (техническая разведка) или агентурными методами (агентурная разведка).

Канал утечки информации – совокупность источника информации,

материального носителя или среды распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя. Одним из основных свойств канала является месторасположение средства выделения информации из сигнала или носителя, которое может располагаться в пределах контролируемой зоны, охватывающей аппаратную среду, или вне ее [4].

Применительно к АС выделяют следующие каналы утечки:

1. **Электромагнитный канал.** Причиной его возникновения является электромагнитное поле, связанное с протеканием электрического тока в аппаратных компонентах АС. Электромагнитное поле может индуцировать токи в близко расположенных проводных линиях (наводки). Электромагнитный канал в свою очередь делится на следующие каналы:

• радиоканал (высокочастотное излучение);
• низкочастотный канал;
• сетевой канал (наводки на сеть электропитания);
• канал заземления (наводки на провода заземления);
• линейный канал (наводки на линии связи между компьютерными системами).

2. **Акустический (виброакустический) канал.** Связан с распространением звуковых волн в воздухе или упругих колебаний в других средах, возникающих при работе устройств отображения информации АС.

3. **Визуальный канал.** Связан с возможностью визуального наблюдения злоумышленником за работой устройств отображения информации АС без проникновения в помещения, где расположены компоненты системы. В качестве средства выделения информации в данном случае могут рассматриваться фото-, видеокамеры и т.п.

4. **Информационный канал.** Связан с доступом (непосредственным и телекоммуникационным) к элементам АС, к носителям информации, к самой вводимой и выводимой информации (и результатам), к программному обеспечению (в том числе к операционным системам), а также с подключением к линиям связи. Информационный канал может быть разделен на следующие каналы:

• канал коммутируемых линий связи,
• канал выделенных линий связи,
• канал локальной сети,
• канал машинных носителей информации,
• канал терминальных и периферийных устройств.

4.2.2. Возможные каналы утечки информации

Утечка акустической информации из-за применения подслушивающих устройств. Для перехвата и регистрации акустической информации существует огромный арсенал разнообразных средств

разведки: микрофоны, электронные стетоскопы, радиомикрофоны или так называемые радиозакладки, направленные и лазерные микрофоны, аппаратура магнитной записи. Набор средств акустической разведки, используемых для решения конкретной задачи, сильно зависит от возможности доступа агента в контролируемое помещение или к интересующим лицам.

Применение тех или иных средств акустического контроля зависит от условий применения, поставленной задачи, технических и, прежде всего, финансовых возможностей организаторов подслушивания.

Перехват носителей в виде электромагнитного, магнитного и электрического полей, а также электрических сигналов с информацией осуществляют органы добывания радио и радиотехнической разведки. При перехвате решаются следующие основные задачи:

– поиск по демаскирующим признакам сигналов с информацией в диапазоне частот, в которых они могут находиться;

– обнаружение и выделение сигналов, интересующих органы добывания;

– усиление сигналов и съем с них информации;

– анализ технических характеристик принимаемых сигналов;

– определение местонахождения (координат) источников представляющих интерес сигналов:

– обработка полученных данных с целью формирования первичных признаков источников излучения или текста перехваченного сообщения.

Типовой комплекс включает:

– приемные антенны;

– радиоприемник;

– анализатор технических характеристик сигналов;

– радиопеленгатор;

– регистрирующее устройство.

Антенна предназначена для преобразования электромагнитной волны в электрические сигналы, амплитуда, частота и фаза которых соответствует аналогичным характеристикам электромагнитной волны.

4.2.3. Структура комплекса средств перехвата

В радиоприемнике производится поиск и селекция радиосигналов по частоте, усиление и демодуляция (детектирование) выделенных сигналов, усиление и обработка демодулированных (первичных) сигналов: речевых, цифровых данных, видеосигналов и т.д. [6].

Для анализа радиосигналов после селекции и усиления они подаются на входы измерительной аппаратуры анализатора, определяющей параметры сигналов: частотные, временные, энергетические, виды модуляции, структуру кодов и др.

Радиопеленгатор предназначен для определения направления на источник излучения (пеленг) и его координат.

Анализатор и пеленгатор могут иметь собственные радиоприемники (или их элементы) и антенны.

Регистрирующее устройство обеспечивает запись сигналов для документирования и последующей обработки.

Антенны представляют собой конструкцию из токопроводящих элементов, размеры и конфигурация которых определяют эффективность преобразования радиосигналов в электрические. Для обеспечения эффективного излучения и приема в широком диапазоне используемых радиочастот создано большое количество видов и типов антенн, классификация которых представлена на рис. 4.2.1.

Назначение передающих и приемных антенны ясно из их наименований. По своим основным электрическим параметрам они не отличаются. Многие из них в зависимости от схемы подключения (к передатчику или приемнику) могут использоваться как передающие или приемные. Однако если к передающей антенне подводится большая мощность, то в ней принимаются специальные меры по предотвращению пробоя между элементами антенны, находящимися под более высоким напряжением [6].

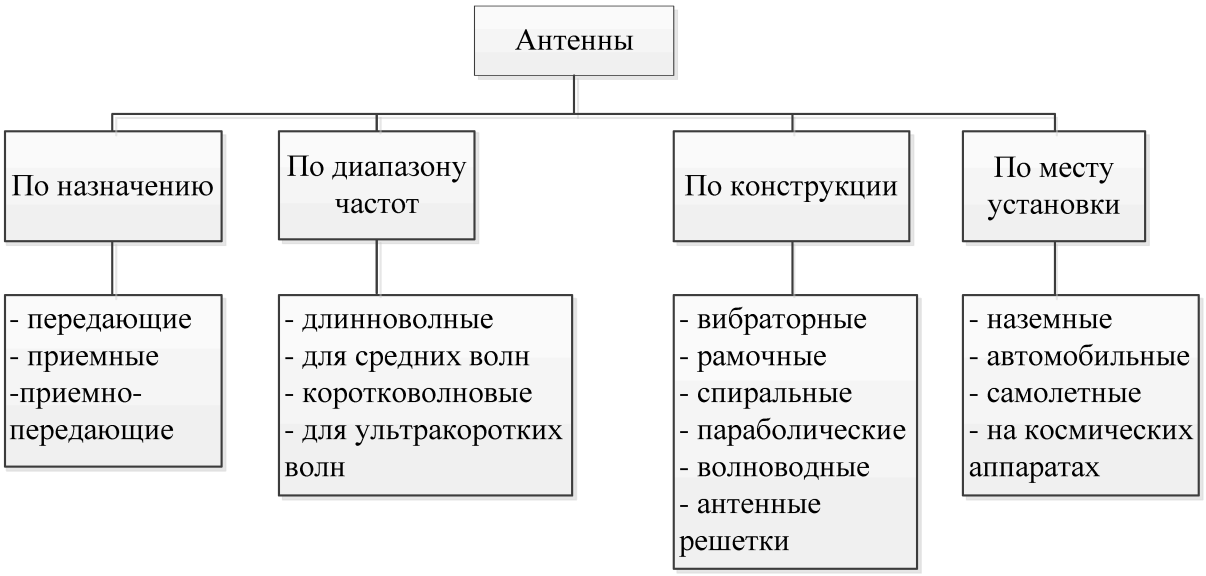


Рис. 4.2.1. Классификация антенн

4.2.4. Классификация антенн

Эффективность антенн зависит от согласования размеров элементов антенны с длинами излучаемых или принимаемых волн. Размеры и конструкция антенн отличаются как для различных диапазонов частот, так и внутри диапазонов.

Если для стационарных антенн требование к геометрическим размерам антенны может быть достаточно просто выполнено для коротких

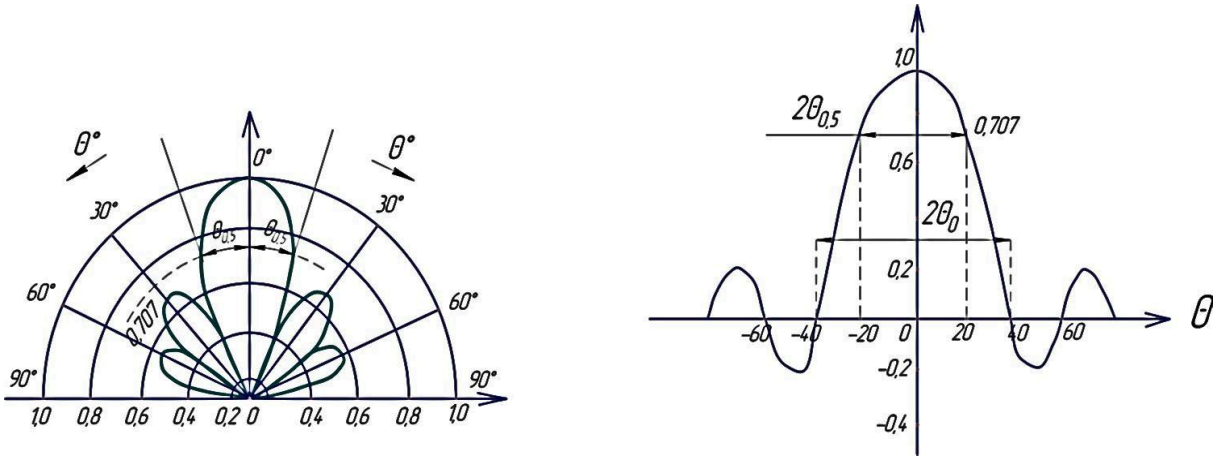
и ультракоротких волн, то для антенн, устанавливаемых на мобильных средствах, оно неприемлемо. Например, рациональная длина антенны для обеспечения связи на частоте 30 МГц составляет 2,5 м, что неудобно для пользователя. Поэтому применяют укороченные антенны, но при этом уменьшается их эффективность. По данным, укорочение антенны в 2 раза уменьшает эффективность до 60%, в 5 раз (до 50 см) – до 10%, а эффективность антенны, укороченной в 10 раз, составляет всего около 3% от рационального варианта.

По конструкции антенны разделяются на проволочные (вибраторные), рупорные, параболические, рамочные, спиральные, антенные решетки и различные их комбинации.

Возможности антенн как приемных, так и передающих определяются следующими характеристиками [6]:

- диаграммой направленности;
- коэффициентом полезного действия;
- коэффициентом направленного действия;
- коэффициентом усиления;
- полосой частот.

Диаграмма направленности представляет собой графическое изображение уровня излучаемого и принимаемого сигнала от угла поворота антенны в горизонтальной и вертикальной плоскостях. Диаграммы в прямоугольных и полярных координатах изображены на рис. 4.2.2.



а) полярные координаты б) прямоугольные координаты

Рис. 4.2.2. Диаграммы направленности в прямоугольных и полярных координатах

4.2.5. Утечка информации за счет скрытного и дистанционного видеонаблюдения

Из средств данного типа наиболее широко применяются скрыто

устанавливаемые фото-, кино -, и видеокамеры с выходным отверстием объектива несколько миллиметров.

Используются также миниатюрные видеосистемы, состоящие из микровидеокамеры с высокой чувствительностью и микрофона, которые устанавливаются на двери или в стене. Для конспиративного наблюдения используются также микровидеокамеры в настенных часах, в датчиках пожарной сигнализации, небольших радиомагнитолах, а также в галстуке или брючном ремне. Видеоизображение может записываться на малогабаритный видеомагнитофон или передаваться с помощью малогабаритного передатчика по радиоканалу в другое помещение или автомашину на специальный или стандартный телеприемник. Расстояние передачи, в зависимости от мощности передачи достигает от 200 метров до 1 км. При использовании ретрансляторов расстояние передачи может быть значительно увеличено.

Привлекает внимание автомобильная система скрытого видеонаблюдения. Видеокамера, обеспечивающая круговой обзор, закамуфлирована под наружную антенну сотового телефона. Плоский экран устанавливается либо на солнцезащитном козырьке, либо в «бардачке», пульт управления – или в пепельнице, или в кармане на двери. Видеосигнал, в зависимости от комплектации, может записываться прямо на видеомагнитофон либо передаваться по радиолинии на расстояние до 400 м. Видеокамера комплектуется сменными объективами с различными углами зрения.

Лазерный съем речевой информации. Для дистанционного перехвата информации (речи) из помещений иногда используют лазерные устройства. Из пункта наблюдения в направлении источника звука посылается зондирующий луч. Зондирующий луч обычно направляется на стекла окон, зеркала, другие отражатели.

Все эти предметы под действием речевых сигналов, циркулирующих в помещении, колеблются и своими колебаниями модулируют лазерный луч, приняв который в пункте наблюдения, можно путем несложных преобразований восстановить все речевые сигналы, циркулирующие в контролируемом помещении. На сегодняшний день создано целое семейство лазерных средств акустической разведки. Такие устройства состоят из источника излучения (гелий-неоновый лазер), приемника этого излучения с блоком фильтрации шумов, двух пар головных телефонов, аккумулятора питания и штатива. Наводка лазерного излучения на оконное стекло нужного помещения осуществляется с помощью телескопического визира. Съем речевой информации с оконных рам с двойными стеклами с хорошим качеством обеспечивается с расстояния до 250 метров. Однако на качество принимаемой информации кроме параметров системы оказывают влияние следующие факторы:

– параметры атмосферы (рассеяние, поглощение, турбулентность, уровень фона);

– качество обработки зондируемой поверхности (шероховатости и неровности, обусловленные как технологическими причинами, так и воздействием среды – грязь, царапины и пр.);

– уровень фоновых акустических шумов;

– уровень перехваченного речевого сигнала.

Кроме того, применение подобных средств требует больших затрат не только на саму систему, но и на оборудование по обработке полученной информации. Применение такой сложной системы требует высокой квалификации и серьезной подготовки операторов.

Из всего этого можно сделать вывод, что применение лазерного съема речевой информации дорогое удовольствие и довольно сложное, поэтому надо оценить необходимость защиты информации от этого вида разведки.

Пути утечки информации в вычислительных системах. Вопросы безопасности обработки информации в компьютерных системах пока еще волнуют в нашей стране не слишком широкий круг специалистов.

До сих пор эта проблема более-менее серьезно вставала у нас, пожалуй, только перед рядом государственных и военных органов, а также перед научными кругами. Теперь же появилось большое число фирм и банков, эффективная деятельность которых практически немыслима без использования компьютеров. Как только должностные лица этих и других организаций это поймут, перед ними сразу же встанут именно вопросы защиты имеющейся у них критичной информации.

Так что, пока еще есть время, стоит очень серьезно задуматься над имеющимся зарубежным опытом, чтобы не изобретать собственного велосипеда. В частности, для начала небесполезно будет ознакомиться с классификацией и принципами оценивания безопасности компьютерных систем, используемыми в США. Различают два типа некорректного использования ЭВМ:

– доступ к ЭВМ лиц, не имеющих на это права;

– неправильные действия тех лиц, которые имеют право на доступ к ЭВМ (так называемый санкционированный доступ).

Обычно разработчиков систем волнует только решение второй проблемы. Анализ вероятных путей утечки информации или ее искажений показывает, что при отсутствии специальных мер защиты, обеспечивающих выполнение функций, возложенных на вычислительную систему, возможно [4]:

– снятие дистанционными техническими средствами секретных сообщений с мониторов ЭВМ, с принтеров (перехват электромагнитных излучений);

– получение информации, обрабатываемой в ЭВМ, по цепям питания;

– акустическая или электроакустическая утечка вводимой информации;

– перехват сообщений в канале связи;

– навязывание ложного сообщения;

– считывание (изменение) информации ЭВМ при несанкционированном доступе.

– хищение носителей информации и производственных отходов;

– чтение остаточной информации в ЗУ системы после выполнения санкционированных запросов;

– копирование носителей информации;

– несанкционированное использование терминалов зарегистрированных пользователей;

– маскировка под зарегистрированного пользователя с помощью хищения паролей и других реквизитов разграничения доступа;

– маскировка несанкционированных запросов под запросы операционной системы (мистификация);

– использование программных ловушек;

– получение защищаемых данных с помощью серии разрешенных запросов;

– использование недостатков языков программирования и операционных систем;

– преднамеренное включение в библиотеки программ специальных блоков типа «троянских коней»;

– злоумышленный вывод из строя механизмов защиты.

В особую группу следует выделить специальные закладки для съема информации с компьютеров.

Миниатюрный радиомаяк, встроенный в упаковку, позволяет проследить весь путь следования закупленной ЭВМ, транслируя сигналы на специальный передатчик. Узнав таким путем, где установлена машина, можно принимать любую обработанную компьютером информацию через специально вмонтированные электронные блоки, не относящиеся к ЭВМ, но участвующие в ее работе. Самая эффективная защита от этой закладки – экранированное помещение для вычислительного центра.

По мнению специалистов, универсальных «компьютерных закладок» сегодня не бывает. Те закладки, которые удавалось обнаружить, можно условно разделить на три типа: те, которые выбирают информацию по ключевым словам или знакам, те, которые передают всю информацию, находящуюся на винчестере ЭВМ, и просто уничтожающие ее.

Утечка информации за счет ПЭМИН. Одной из наиболее вероятных угроз перехвата информации в системах обработки данных считается утечка за счет перехвата побочных электромагнитных излучений

и наводок (ПЭМИН), создаваемых техническими средствами. ПЭМИН существуют в диапазоне частот от единиц Гц до полутора ГГц и способны переносить (распространять) сообщения, обрабатываемые в автоматизированных системах. Дальность распространения ПЭМИН исчисляется десятками, сотнями, а иногда и тысячами метров. Наиболее опасными источниками ПЭМИН являются дисплеи, проводные линии связи, накопители на магнитных дисках и буквопечатающие аппараты последовательного типа.

Например, с дисплеев можно снять информацию с помощью специальной аппаратуры на расстоянии до 500-1500 метров, с принтеров до 100-150 метров. Перехват ПЭМИН может осуществляться и с помощью портативной аппаратуры. Такая аппаратура может представлять собой широкополосный автоматизированный супергетеродинный приемник. В качестве устройств регистрации принятых сигналов (сообщений) может использоваться магнитный носитель или дисплей.

Электромагнитная наводка – передача (индуцирование) электрических сигналов из одного устройства (цепи) в другое, непредусмотренная схемными или конструктивными решениями и возникающая за счет паразитных электромагнитных связей. Электромагнитные наводки могут приводить к утечке информации по токопроводящим коммуникациям, имеющим выход за пределы контролируемой зоны [2].

Причинами возникновения электрических каналов утечки информации являются наводки информативных сигналов, под которыми понимаются токи и напряжения в токопроводящих элементах, вызванные побочными электромагнитными излучениями, ёмкостными и индуктивными связями.

В зависимости от физических причин возникновения наводки информативных сигналов можно разделить на:

– наводки информативных сигналов в электрических цепях ТСОИ, вызванные информативными ПЭМИН ТСОИ (ПЭМИН – ток в проводнике);

– наводки информативных сигналов в соединительных линиях ВТСС и посторонних проводниках, вызванные информативными ПЭМИН ТСОИ;

– наводки информативных сигналов в электрических цепях ТСОИ, вызванные внутренними ёмкостными и индуктивными связями («просачивание» информативных сигналов в цепи электропитания через блоки питания ТСОИ, ток – ток);

– наводки информативных сигналов в цепях заземления ТСОИ, вызванные информативными ПЭМИН ТСОИ, а также гальванической связью схемной (рабочей) земли и блоков ТСОИ (ПЭМИН – ток в

проводнике , ток – ток). Схема канала утечки информации через ПЭМИН представлена на рисунке 4.2.3.

Уровень наводок зависит от расстояния между источником излучения и случайной антенной, типа случайной антенны (сосредоточенная или распределённая), длины параллельного пробега и величины переходного затухания линий, напряжения информативного сигнала в линии и уровня шумов (помех) и других факторов.

Помимо естественных технических каналов утечки информации существуют и специально создаваемые ТКУИ, например, технические каналы утечки информации, создаваемые путем «высокочастотного облучения» СВТ или создаваемые путем внедрения в СВТ электронных устройств перехвата информации (закладных устройств).

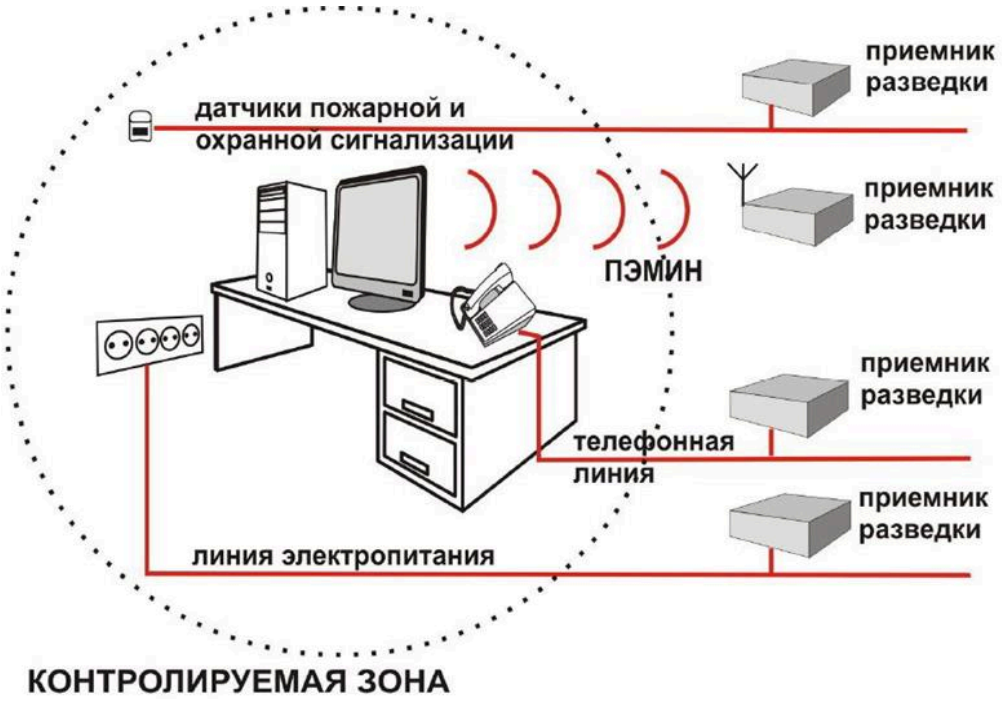


Рис. 4.2.3. Схема канала утечки информации через ПЭМИН

Утечка информации при использовании средств связи и различных проводных коммуникаций. В данном случае, когда речь заходит о возможности перехвата информации при использовании линий связи и проводных коммуникаций, следует иметь в виду, что перехват может осуществляться не только с телефонных линий и не только речевой информации. В этот раздел можно отнести:

– прослушивание и запись переговоров по телефонным линиям;

– использование телефонных линий для дистанционного съема аудио- информации из контролируемых помещений;

– перехват факсимильной информации;

– перехват разговоров по радиотелефонам и сотовой связи;

– использование сети 220 В и линий охранной сигнализации для передачи акустической информации из помещений;

– перехват пейджинговых сообщений.

Прослушивание и запись переговоров по телефонным линиям. Телефонные абонентские линии обычно состоят из трех участков: магистрального (от АТС до распределительного шкафа (РШ)), распределительного (от РШ до распределительной коробки (КРТ)), абонентской проводки (от КРТ до телефонного аппарата). Последние два участка – распределительный и абонентский являются наиболее уязвимыми с точки зрения перехвата информации. Подслушивающее устройство может быть установлено в любом месте, где есть доступ к телефонным проводам, телефонному аппарату, розетке или в любом месте линии вплоть до КРТ.

Наиболее простой способ подслушивания это подключение параллельного телефонного аппарата или «монтерской» трубки. Используются также специальные адаптеры для подключения магнитофонов к телефонной линии. Адаптеры сделаны таким образом, что диктофон, установленный на запись в режиме акустопуска, включается только при поднятой трубке телефонного аппарата. Это дает возможность экономно расходовать пленку на кассете, не сматывая ее вхолостую.

Прослушивание телефонных линий может вестись не только гальванически (прямым подсоединением), а и с помощью индукционных или емкостных датчиков. Такое подсоединение практически не обнаруживается с помощью тех аппаратных средств, которые широко используются для поисковых целей.

Самыми распространенными из подобных средств прослушивания являются телефонные контроллеры радиоретрансляторы которые чаще называются телефонными передатчиками или телефонными «закладками». Телефонные закладки подключаются параллельно или последовательно в любом месте телефонной линии и имеют значительный срок службы, так как питаются от телефонной сети. Эти изделия чрезвычайно популярны в промышленном шпионаже благодаря простоте и дешевизне.

Большинство телефонных «закладок» автоматически включаются при поднятии телефонной трубки и передают разговор по радиоканалу на приемник пункта перехвата, где он может быть прослушан и записан. Такие «закладки» используют микрофон телефонного аппарата и не имеют своего источника питания, поэтому их размеры могут быть очень небольшими. Часто в качестве антенны используется телефонная линия. Для маскировки телефонные «закладки» выпускаются в виде конденсаторов, реле, фильтров и других стандартных элементов и узлов, входящих в состав телефонного аппарата.

Чаще всего телефонные «закладки» стараются устанавливать за пределами офиса или квартиры, что существенно снижает риск. Для

упрощения процедуры подключения подслушивающих устройств и уменьшения влияния на телефонную линию используются изделия с индуктивным датчиком съема информации. Особенностью подобных устройств является то, что требуется автономный источник питания и устройство должно иметь схему автоматического включения при снятии телефонной трубки. Качество перехватываемой информации практически всегда хуже.

Использование телефонных линий для дистанционного съема аудиоинформации из контролируемых помещений. Отдельное место занимают системы, которые предназначены не для подслушивания телефонных переговоров, а для использования телефонных линий при прослушивании контролируемых помещений, где установлены телефонные аппараты или проложены провода телефонных линий. Примером такого устройства может служить «телефонное ухо». «Телефонное ухо» представляет собой небольшое устройство, которое подключается параллельно к телефонной линии или розетке в любом удобном месте контролируемого помещения. Для прослушивания помещения необходимо набрать номер абонента, в помещении которого стоит «телефонное ухо». Услышав первый гудок АТС необходимо положить трубку и через 10-15 секунд повторить набор номера. Устройство дает ложные гудки занято в течение 40-60 секунд, после чего гудки прекращаются, и включается микрофон в устройстве «телефонное ухо» – начинается прослушивание помещения. В случае обычного звонка «телефонное ухо» пропускает все звонки после первого, выполняя роль обычной телефонной розетки и не мешая разговору.

Кроме того, возможно использование телефонной линии для передачи информации с микрофона, скрытно установленного в помещении. При этом используется несущая частота в диапазоне от десятков до сотен килогерц с целью не препятствовать нормальной работе телефонной связи. Практика показывает, что в реальных условиях дальность действия подобных систем с приемлемой разборчивостью речи существенно зависит от качества линии, прокладки телефонных проводов, наличия в данной местности радиотрансляционной сети, наличия вычислительной и оргтехники и т.д.

Из числа так называемых «беззаходовых» систем съема речевой информации с контролируемых помещений, когда используются телефонные линии, следует отметить возможность съема за счет электроакустического преобразования, возникающего в телефонных аппаратах, и за счет высокочастотного (ВЧ) навязывания. Но эти каналы утечки используются все реже. Первый из-за того, что современные телефонные аппараты не имеют механических звонков и крупных металлических деталей, а второй из-за своей сложности и громоздкости аппаратуры. Но, тем не менее, меры защиты от утечки информации по

этим каналам применяются, они общеизвестны и недорогие.

Использование сети 220 В для передачи акустической информации из помещений. Для этих целей применяют так называемые сетевые закладочные устройства. К этому типу «закладок» чаще всего относят устройства, которые встраиваются в приборы, питающиеся от сети 220 В, или сетевую арматуру (розетки, удлинители и т.д.). Передающее устройство состоит из микрофона, усилителя и собственно передатчика несущей низкой частоты. Частота несущей частоты обычно используется в диапазоне от 10 до 350 кГц. Передача и прием осуществляется по одной фазе, или если фазы разные, то их связывают по высокой частоте через разделительный конденсатор. Приемное устройство может быть изготовлено специально, но иногда применяют доработанные блоки бытовых переговорных устройств, которые сейчас продаются во многих специализированных магазинах электронной техники. Сетевые передатчики подобного класса легко камуфлируются под различного рода электроприборы, не требуют дополнительного питания от батарей и трудно обнаруживаются при использовании поисковой аппаратуры, широко применяемой в настоящее время.

Параметрические технические каналы утечки информации. В результате воздействия акустического поля меняется давление на все элементы высокочастотных генераторов ОТСС и ВТСС. При этом изменяется (незначительно) взаимное расположение элементов схем, проводов в катушках индуктивности, дросселей и т.п., что может привести к изменениям параметров высокочастотного сигнала, например, к модуляции его информационным сигналом. Поэтому этот канал утечки информации называется параметрическим. Это обусловлено тем, что незначительное изменение взаимного расположения, например, проводов в катушках индуктивности (межвиткового расстояния) приводит к изменению их индуктивности, а, следовательно, к изменению частоты излучения генератора, т.е. к частотной модуляции сигнала.

Или воздействие акустического поля на конденсаторы приводит к изменению расстояния между пластинами и, следовательно, к изменению его емкости, что, в свою очередь, также приводит к частотной модуляции высокочастотного сигнала генератора. Наиболее часто наблюдается паразитная модуляция информационным сигналом излучений гетеродинов радиоприемных и телевизионных устройств, находящихся в выделенных помещениях и имеющих конденсаторы переменной емкости с воздушным диэлектриком в колебательных контурах гетеродинов.

Промодулированные информационным сигналом высокочастотные колебания излучаются в окружающее пространство и могут быть перехвачены и детектированы средствами радиоразведки. Параметрический канал утечки информации может быть реализован и путем «высокочастотного облучения» помещения, где установлены

полуактивные закладные устройства, имеющие элементы, некоторые параметры которых (например, добротность и резонансная частота объемного резонатора) изменяются по закону изменения акустического (речевого) сигнала.

При облучении мощным высокочастотным сигналом помещения, в котором установлено такое закладное устройство, в последнем при взаимодействии облучающего электромагнитного поля со специальными элементами закладки (например, четвертьволновым вибратором) происходит образование вторичных радиоволн, т.е. переизлучение электромагнитного поля. А специальное устройство закладки (например, объемный резонатор) обеспечивает амплитудную, фазовую или частотную модуляцию переотраженного сигнала по закону изменения речевого сигнала. Подобного вида закладки иногда называют полуактивными. Для перехвата информации по данному каналу кроме закладного устройства необходимы специальный передатчик с направленной антенной и приемник.

4.3. Классификация технических средств разведки

Перехват информации, циркулирующей между объектами ТКС по каналам связи, возможен как при передаче ее по линиям, использующим излучающие средства радиосвязи, так и при передаче по проводным линиям.

Возможность ведения технической разведки из-за пределов охраняемой территории объектов ТКС определяется наличием технических каналов утечки информации. Все возможные каналы утечки информации на объектах ТКС могут быть сведены в три основных класса: акустические каналы, оптические каналы и каналы утечки технических средств. По виду среды распространения опасных сигналов акустические каналы могут подразделяться на атмосферные и виброакустические, оптические каналы – на каналы видимого и инфракрасного диапазонов волн, а каналы утечки технических средств – на полевые, к которым относятся электрические и магнитные поля указанных средств, и линейные, к которым относятся различного рода цепи и токопроводящие конструкции, выходящие за пределы охраняемой территории объектов ТКС.

Основные каналы утечки информации на объектах ТКС рассматриваются с учетом физических полей [5]:

– утечка по акустическому каналу;

– утечка по виброакустическому каналу;

– утечка по каналам проводной и радиосвязи, не имеющим шифрующей и дешифрирующей аппаратуры;

– утечка по электромагнитным каналам;

– утечка через вторичные источники электропитания основных технических средств за счет неравномерности тока потребления;

– утечка, возникающая при воздействии электрических, магнитных и акустических полей опасного сигнала на вспомогательных технических средствах;

– утечка за счет тока опасного сигнала в цепях заземления;

– утечка за счет взаимного влияния между цепями, по которым передается конфиденциальная информация, и цепями вспомогательных технических средств, имеющими выход за пределы зоны безопасности объекта (другими словами, использование эффекта индуктивности любых неэкранированных проводников);

– утечка информации за счет побочных электромагнитных излучений наводок, образованных основными техническими средствами.

Необходимо отметить, что выявление всех возможных каналов утечки конфиденциальной информации из ТКС является необходимым условием для определения путей и способов решения проблемы ее защиты, а также конкретных мер по их реализации.

Канал побочных электромагнитных излучений и наводок (ПЭМИН), является одним из основных каналов, через который вероятные нарушители стараются получить сведения закрытого характера. Это пристальное внимание он завоевал в силу своей стабильности, достоверности, неявной формы получения информации и возможности последующего анализа полученной информации. Охота ведется как за государственной, военной, так и за коммерческой информацией. Ее анализ производится по многим параметрам, что позволяет получать достаточно достоверную информацию. Работа компьютера и других радиотехнических средств ТКС сопровождается побочными электромагнитными излучениями, модулированными информативными сигналами. Так ПЭМИН от персональных компьютеров типа IBM наблюдаются в диапазоне частот от десятков кГц до сотен МГц с уровнями в ближайшей зоне от 40 до 80 дБ. Существующие методы радиоперехвата информации позволяют фиксировать информативные массивы работающих компьютеров на расстоянии до сотен метров. Аналогичный перехват информации может осуществляться через незащищенные цепи питания и заземления.

Известно, что при работе ключом при передаче сообщений прослеживается индивидуальный почерк радиста. Можно классифицировать перехваченные сигналы также по индивидуальным признакам пользователя при нажатии клавиши ввода информации.

Необходимо помнить о том, что многие подсистемы демаскируют себя применением только им присущих устройств и режимов работы. В некоторых случаях данное обстоятельство приобретает важное значение. Даже при приеме на бытовой приемник обычно легко различаются

дежурный и рабочий режимы работы, особенности структуры сигнала в каналах связи, адресные сигналы и тому подобные характеристики информации, которые при совокупном анализе ситуации вносят свой определенный вклад в «копилку» нарушителя.

Однако известны случаи, когда перехват ПЭМИН оказывается возможным без применения сложной приемной аппаратуры и необходимости длительного накопления и анализа информации. Во-первых, это перехват высвечиваемой информации компьютера с помощью объектного телевизионного приемника. При этом можно существенно улучшить возможности приема путем проведения незначительных изменений в телевизионном приемнике. Во-вторых, это перехват излучений от низкочастотных электромеханических устройств с последовательным кодом передачи информации.

Многими специалистами, осознающими реальную опасность утечки коммерческих секретов, предпринимаются действия, направленные на ослабление (закрытие) естественных каналов различными методами. В связи с этим попытки нарушителей создавать и использовать искусственные каналы утечки будут усиливаться.

Известны следующие источники утечки информации. Для каждого конкретного помещения существует свой набор технических средств, которые могут создавать опасные сигналы и способствовать их распространению, то есть служить источниками утечки. Эту технику можно разделить на две основные группы:

1. Основные технические средства:
- телефонные аппараты городской АТС;
- телефонные аппараты внутренней связи;
- факс;
- компьютеры (возможно укомплектованные модемами);
- средства размножения документов типа ксерокс.

2. Вспомогательные средства:
- телевизор;
- магнитофон, видеоаппаратура;
- радиоприемник;
- радиотрансляционный громкоговоритель, селекторная связь;
- датчики охранной и пожарной сигнализации;
- кондиционер;
- телетайп;
- объектовая сеть электрификации;
- табельное электрооборудование помещения.

Радиоразведка (РР) – одна из составляющих радиоэлектронной разведки, противной стороной которой в конфликте радиоэлектронных

систем являются системы и средства радиосвязи [5].

Обеспечивает добывание, обработку и анализ информации, передаваемой по каналам радиосвязи различного назначения посредством изменения параметров сигналов работающих средств радиосвязи (радиотелеметрия).

В ходе развития конфликта в системах радиосвязи разрабатывались и применялись различные способы и техника закрытия от разведки, циркулирующей в системах радиосвязи информации абонентов. В свою очередь, радиоразведка разрабатывала и применяла методы, способы и технику вскрытия защищаемой информации. Итогом конфликта являются сложившиеся структура радиоразведки и процесс добывания информации абонентов.

Структура сил и средств радиоразведки практически во всех странах базируется на одинаковых принципах. Нижний уровень структуры составляет аппаратура радиоразведки (АРР), образующая категорию технических средств разведки (ТСР). Функционально и технически сопряженные ТСР образуют комплексы технической разведки (КТСР), а совокупности КТСР образуют системы технической радиоразведки (СТРР).

В системах технической разведки организационно создаются органы разведки, а именно: посты радиоперехвата (ПРП), посты радиопеленгования (ПРПЛ), радиопеленгаторная сеть (ПРПЛС), командные пункты (КП) и центры обработки разведывательной информации.

Получаемая от различных технических средств разведки и комплексов средств разведки информация обрабатывается в органах радиоразведки аналитиками, использующими сопряженную с электронно-вычислительными машинами специальную аппаратуру и программное обеспечение дешифрации и декодирования.

Процесс добывания информации абонентов основывается на реализации трех основных функций (методов) радиоразведки:

– поиск (по диапазону, в заданном секторе частот) и наблюдение (непрерывное, периодическое, контрольное), в результате которых производится обнаружение сигналов «вышедших в эфир» средств радиосвязи (СРС);

– радиопеленгование (определение местоположения работающего радиосредства либо направления на источник радиоизлучения); прием и измерение параметров (первичный анализ) сигналов, циркулирующих в системе радиосвязи;

– фиксирование (запись) перехваченных сигналов и оперативное извлечение из них информации абонентов (радиоперехват); обработка информации в органах управления разведкой.

Первая функция – обнаружение сигналов «вышедших в эфир» СРС –

решается постами радиоперехвата, оборудованными разведывательными радиоприемниками, приспособленными для быстрого сканирования заданного диапазона частот и отображения наблюдаемых сигналов, работающих СРС в удобном для анализа виде.

Вторая функция – определение местоположения, реализуется постами радиопеленгования. Наиболее крупные системы радиоразведки сопрягаются с системами определения местоположения объектов различной ведомственной принадлежности и с глобальными навигационными системами.

Разведданные, получаемые при выполнении этих двух функций (частота, позывной, пеленг), обеспечивают определение принадлежности разведуемого СРС («тактическую привязку») к конкретным объекту, сети, системе связи, органу управления.

Третья функция – измерение параметров (первичный анализ) сигналов, циркулирующих в системах радиосвязи, используется для «настройки» системы радиоразведки на соответствующий источник излучений путем определения рабочей частоты и параметров сигналов. Реализация данной функции осуществляется постами инструментального анализа сигналов, которые в отличие от постов радиоперехвата дополнительно оборудуются частотомерами, анализаторами спектра сигналов, определителями временных параметров импульсных сигналов и другой специальной аппаратурой анализа излучений. Инструментальный анализ (называемый еще «тонкий анализ»), как правило, используется для накопления данных по конкретному излучению СРС для последующей идентификации сигналов в процессе разведки.

Эти три функции обеспечивают выполнение главной задачи радиоразведки – получение разведывательной информации от объектов разведки и определение принадлежности СРС.

Радиотехническая разведка (РТР) – составляющая радиоэлектронной разведки, противной стороной которой в конфликте радиоэлектронных систем являются радиоэлектронные средства (РЭС), входящие в состав радиолокационных систем обнаружения, предупреждения, оповещения, определения координат объектов, целей, наведения оружия, радионавигационных систем, систем радиотелеуправления [5].

Обеспечивает добывание информации о параметрах излучаемых сигналов РЭС, определение типа РЭС и его принадлежности к конкретному образцу вооружения, техники, системе, а также направление (азимут) на работающее РЭС и их количество в секторе разведки.

Структуру органов радиотехнической разведки составляют органы, аналогичные радиоразведке, но в отличие от нее нижний уровень составляет аппаратура радиотехнической разведки, конструктивно исполненная для работы в диапазоне электромагнитных волн (ЭМВ).

В ходе ведения радиотехнической разведки реализуются функции:

– обнаружение сигналов работающих РЭС в секторе разведки, заданном диапазоне частот ЭМВ;

– определение направления (азимута) и местоположения работающего РЭС, направления перемещения движущегося объекта, на борту которого установлено данное РЭС;

– измерение параметров принятых сигналов, исследование структуры излучения и его «привязка» к определенному типу РЭС, конкретному образцу вооружения, техники, системе;

– «запоминание» средствами РТР характеристик принятых сигналов для последующего анализа (идентификации) вновь обнаруженных РЭС; обработка информации в органах радиотехнической разведки.

Радиолокационная разведка

Под радиолокационной разведкой понимается область радиолокации, предназначенная для добывания информации о характере, количественном составе оперативной обстановки (конкретном объекте, цели) в интересах своевременного предупреждения и наведения огневых средств поражения (боевых группировок), сил и средств охраны и контроля объектов, а также получения радиолокационных карт местности.

Под радиолокацией подразумевается обнаружение и определение координат объектов при направленном облучении их высокочастотной электромагнитной энергией и приеме ее после отражения от этих объектов.

Система радиолокационной разведки предназначена для обеспечения информацией о наземном (воздушном, морском) противнике, в т. ч. о группах организованной преступности, с целью их своевременного обнаружения и отражения ударов.

В ходе ведения радиолокационной разведки решаются задачи:

– непрерывное наблюдение в секторе разведки с целью своевременного обнаружения противника;

– определение местоположения и характеристик движущихся целей (скорость, курсовой параметр, высота и др.);

– определение количества и типа целей, их состава, интервалов и дистанций между ними, построения боевого порядка, характера маневра целей и т.п.;

– передачу данных о противнике на соответствующие командные пункты для своевременного отражения нападения.

По решаемым техническим функциям радиолокационная разведка подразделяется на параметрическую и видовую разведку.

Радиолокационная параметрическая разведка обеспечивает добывание информации, содержащейся в пространственных, скоростных и отражательных характеристиках космических, воздушных, морских и

наземных объектов, получаемых в результате облучения разведывательным сигналом и возвращения (отражения) от объекта разведки данного сигнала.

Радиолокационная видовая разведка обеспечивает добывание информации, содержащейся в изображениях космических, воздушных, наземных и морских объектов, получаемых по отраженным от них сигналов, а также отображение (съемку) радиолокационной карты местности [5].

Разведка за счет образования технических каналов утечки информации

Развитие радиоэлектронной разведки позволило установить, что помимо возможности прямого перехвата информации, циркулирующей в каналах радиосвязи, радионавигации, радиолокации, радиотелеуправления, существует возможность получения информации по так называемым каналам утечки информации, образуемым при работе технических средств за счет побочных электромагнитных излучений и наводок.

Кроме того, образование технических каналов утечки информации возможно за счет подачи на разведуемое средство специального облучающего сигнала, который в этом устройстве модулируется информационным сигналом, после чего принимается разведприемником. Зачастую подаваемый специальный разведывательный сигнал провоцирует самовозбуждение генераторов, гетеродинов, усилителей, входящих в состав ТСПИ, которые начинают излучать сигнал, содержащий информацию на неконтролируемых частотах.

Разведка по техническим каналам утечки информации обеспечивает добывание информации, содержащейся в телефонных, телеграфных, телеметрических и т.п. сообщениях и в документах (текстах, таблицах, рисунках, картах, снимках и т.п.) с использованием радиоэлектронной специальной аппаратуры, регистрирующей побочные электромагнитные излучения (ПЭМИ) и электрические сигналы, наводимые ПЭМИ в токопроводящих цепях и средах различных основных технических средств и систем (ОТСС), токопроводящих элементах конструкций зданий и сооружений (системы заземления, сети электропитания ОТСС, цепи связи в том же кабеле, линии связи с параллельными пробегами, линии связи в соседних помещениях и т.п.).

Методы добывания информации по техническим каналам, как правило, используются агентурной разведкой, спецслужбами, ведущими оперативно-розыскную деятельность, коммерческой разведкой, а также группами организованной преступности, злоумышленниками.

Классификационная схема основных (наиболее распространенных) технических каналов утечки информации приведена на рисунке 4.3.1.

Данные технические каналы утечки информации сгруппированы по

двум методам ведения разведки (за счет пассивного перехвата и за счет активного перехвата) и отличаются друг от друга технической реализацией задач разведки.

Первая группа каналов утечки информации основана на использовании эффектов рассеяния работающих ОТСС и ВТСС, микрофонного эффекта (за счет электроакустических преобразований), а также прямой регистрации информационных сигналов путем использования технической аппаратуры приема.

Вторая группа каналов предусматривает применение технических приемо-передающих устройств (эффект «ВЧ, НЧ-навязывания», подача лазерного луча, использование радиозакладных устройств и т.п.).

Рис. 4.3.1. Классификация технических каналов утечки информации

Компьютерная разведка

С зарождением компьютерных технологий управления, связи и информации, с появлением ведомственных, региональных, международных глобальных телекоммуникационных систем (как закрытых, так и общего пользования) возник принципиально новый вид разведки, комплексно соединивший в себе классические методы пассивной радиотехнической разведки, разведки по техническим каналам утечки информации и активные методы радиоэлектронной борьбы – это компьютерная разведка (КР).

Компьютерная разведка – один из видов разведки, противной стороной которой являются операционное обеспечение, информационные массивы, базы данных, системы комплексной защиты информации телекоммуникационных систем и отдельных ПЭВМ. Обеспечивает добывание разведывательной информации из электронных баз данных ПЭВМ телекоммуникационных (компьютерных) систем.

На ведение компьютерной разведки влияют условия эксплуатации разведуемой системы, адекватность политики безопасности системы, содержание и характер информации (открытая, конфиденциальная, секретная), обрабатываемый в системе и т.д. Например, если операционная система используется главным образом для организации документооборота, наиболее вероятен несанкционированный доступ (НСД) к файлам.

Компьютерную разведку можно систематизировать по следующим аспектам [5]:

а) цель разведки: несанкционированные чтение и копирование информации;

б) способы воздействия на операционную систему:

– использование легальных каналов чтения файлов пользователем, доступ которого, согласно политике безопасности, определен некорректно, либо запрещен;

– создание нелегальных каналов получения информации с помощью программных закладок;

в) вид (характер) воздействия:

– активное воздействие;

– пассивное воздействие – наблюдение за процессами, происходящими в системе путем перехвата излучений ОТСС и ВТСС;

г) использование особенностей защиты системы:

– неадекватная (не обеспечивающая необходимый уровень защиты) политика безопасности системы, в том числе возможные ошибки администратора;

– ошибки и недокументированные возможности программного обеспечения операционной системы, в том числе, т. н. «люки», позволяющие обходить систему защиты (обычно «люки» создаются разработчиками

программного обеспечения для тестирования и отладки систем); ранее внедренная программная закладка (на стадии разработки, поставки либо эксплуатации ОТСС и сетевого оборудования);

д) способы воздействия на объект атаки (объект разведки):

– непосредственное воздействие санкционированным пользователем;

– несанкционированное повышение полномочий пользователем;

– работа от имени другого пользователя;

– использование результатов работы другого пользователя (например, несанкционированный перехват информационных потоков, инициированных другим пользователем);

е) способы действий органов разведки (злоумышленников):

– интерактивный режим (вручную);

– в пакетном режиме (с помощью специально написанной программы, выполняющей целевые разведывательные воздействия на операционную систему без непосредственного участия органа разведки (злоумышленника, нарушителя);

ж) объекты атаки:

– операционная система в целом;

– объекты (модули) операционной системы (файловая система, файлы, устройства и т.д.);

– субъекты операционной системы (пользователи, системные процессы и т.д.);

– каналы передачи данных (радио-, радиорелейные, проводные, кабельные, в т. ч. волоконно-оптические);

– структура сигнала, используемая для передачи информации в каналах передачи данных (каналах связи);

з) средства атаки:

– штатные средства операционной системы без использования дополнительного программного обеспечения;

– программное обеспечение третьих фирм (к этому классу относятся как компьютерные вирусы и другие вредоносные программы, которые легко можно найти в Internet, так и программное обеспечение, изначально разработанное для других целей: отладчики, сетевые мониторы, сканеры и т.д.);

– специально разработанное программное обеспечение. В интересах компьютерной разведки реализуются следующие основные типы атак на операционную систему.

Сканирование файловой системы. Суть атаки заключается в просмотре файловой системы и попытках ее считывания (либо копирования, либо удаления) всех файлов подряд. При получении доступа к какому-либо файлу или каталогу сканирование продолжается. Как правило, при больших объемах файловой системы обнаруживается хотя бы

одна ошибка администратора, что позволяет получить доступ к разведуемой информации. Атака может осуществляться специальной программой, выполняющей вышеуказанные действия в автоматическом режиме. Данная атака особенно эффективна, если политика безопасности допускает анонимный или гостевой вход в систему либо атака осуществляется от имени другого пользователя.

Кража ключевой информации. В простейшем случае атака заключается в подсмотре пароля, набираемого пользователем. В условиях, когда современные системы не высвечивают на экране дисплея вводимый пароль, тот может быть восстановлен по характеру движения рук по клавиатуре, для чего достаточно несколько тренировочных сеансов профессиональным специалистом. Некоторые программы входа в операционную систему удаленного сервера допускают ввод пароля из командной строки. При вводе пароля в командной строке последний отображается на экране и может быть прочтен визуально. В свою очередь, при использовании длинных, трудных для запоминания паролей (от 7 до 14 символов смешанного буквенно-цифрового типа с использованием строчных и заглавных букв) пользователи нередко используют для хранения ключевой информации внешние носители (ключевая дискета, Touch Memory, в т. ч. бумажные носители), которые могут быть утеряны, похищены.

Подбор пароля. При подборе пароля исследуются общие принципы и порядок назначения паролей, характерные для адекватной политики безопасности разведуемой системы, для чего используются следующие методы:

Тотальный перебор. Последовательно опробуются все возможные комбинации – варианты паролей с длительностью символов не больше 4-6. В ином случае метод неэффективен.

Тотальный перебор, оптимизированный по статистике встречаемости символов. Согласно различным исследованиям, статистика встречаемости символов в алфавите паролей близка к статистике встречаемости символов в естественном языке. При практическом применении данного метода вначале опробуются пароли, состоящие из наиболее встречающихся символов, что значительно снижает время подбора. Иногда при подборе паролей используется также статистика встречаемости биграмм и триграмм – комбинаций двух и трех последовательных символов соответственно.

Для подбора паролей написано множество программ. Многие из них основаны на принципе поочередной подачи на вход системы аутентификации операционной системы различных вариантов паролей, другие используют принципы подбора вариантов пароля путем генерации хеш–функции и ее последующего сравнения с известным образом пароля. И в первом и во втором случаях среднее время подбора пароля зависит от

производительности, вычислительной мощности компьютера и эффективности реализации алгоритма генерации хеш-функции в программе, подбирающей пароли (пароль из 6–8 символов, не включающий цифр, знаков препинания, варьируется от нескольких секунд до нескольких часов).

Тотальный перебор, оптимизированный с помощью словарей. При использовании для построения паролей смысловых слов (в сочетании с цифровыми индексами) используются парольные словари, адаптированные для разных стран мира (огромное количество подобных словарей содержит internet). Действительно, английский язык содержит около 100000 слов, что в 6,5 меньше всех комбинаций из четырех английских букв. В случае отсутствия подбираемого пароля в словаре, опробуются все возможные словарные комбинации из словаря, слова из словаря с добавлением различных буквенно-цифровых индексов и т.д. Обычно данный метод используется в комбинации с предыдущим.

Подбор пароля с использованием знаний о пользователе. Для более легкого запоминания многие пользователи выбирают пароли в виде своего имени, имен друзей, близких, фамилии, даты рождения, номера телефонов, автомобилей и т.д., что позволяет (зная пользователя) вскрыть пароль за 10–20 попыток.

Подбор образа пароля. Если подсистема аутентификации операционной системы устроена так, что образ пароля существенно короче самого пароля, подбирается не пароль, а его образ. При подборе образа пароля необходимо получить сам пароль, но это возможно только в том случае, если хеш–функция, применяемая в системе, не обладает достаточной стойкостью.

Сбор мусора. Во многих операционных системах информация, уничтоженная пользователем, не уничтожается физически, а помечается как уничтоженная. С помощью специальных программ такая информация восстанавливается (так называемый «мусор»). Сбор «мусора» может осуществляться не только на дисках компьютера, но и в оперативной памяти.

Повышение полномочий. Как правило, данная атака осуществляется санкционированным пользователем сети, который, используя ошибки в программном обеспечении операционной системы и/или политике безопасности, получает доступ к информации, превышающий полномочия, предоставленные ему политикой безопасности. Обычно это достигается путем запуска программы от имени другого пользователя или подмены динамически подгружаемой библиотеки. Данный метод особенно эффективен в операционных системах, в которых допускается временное повышение полномочий пользователя (например, UNIX), а также вследствие того, что санкционированный пользователь может оказаться сотрудником, завербованным разведкой либо работающим в интересах

групп организованной преступности.

Программные закладки могут «загружаться» в операционное обеспечение на стадии разработки, изготовления и на стадии целевой установки на разведуемый объект. Наряду с компьютерными вирусами, которые захватывают значительную часть ресурсов компьютеров, затрудняют работу других программ, нейтрализуют систему защиты, приводят к зависанию компьютеров, а зачастую и к краху операционной системы.

Радиотепловизионная разведка

Радиотепловизионная разведка по своей физической сущности подразделяется на пассивную и активную радиотепловую разведку.

Пассивная радиотепловая разведка (РТплР) обеспечивает добывание информации, содержащейся в изображениях наземных объектов, получаемых от различного собственного теплового излучения в инфракрасном диапазоне.

Тепловое излучение представляет собой превращение тепловой энергии тела в лучистую энергию вследствие сложных внутриатомных процессов, возникающих под действием температуры тела.

Величина теплового излучения зависит от структуры тела, его температуры и коэффициента черноты. Мощность Ф теплового излучения твердого тела, имеющего наблюдаемую поверхность *S,* которая нагрета до абсолютной температуры *T,* определяется известным законом Стефана-Больцмана:

Коэффициент излучения может меняться в пределах от 0 до 1. Наименьшее значение он имеет у тел с белыми поверхностями (например, у полированного алюминия k_E = 0,05), наибольшее – у черных тел. Тело, у которого k_e= 1, называется абсолютно черным и служит эталоном при измерениях. Наибольшее влияние на величину теплового радиоизлучения оказывает температура поверхности тела. На рисунке 4.3.2. приведены зависимости от длины волны интенсивности излучения 1см^2 поверхности абсолютно черного тела с температурами 300, 500, 600 К.

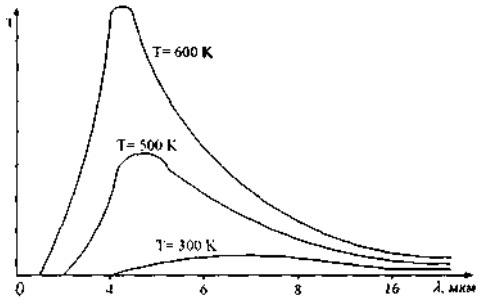


Рис. 4.3.2. Графики спектральной плотности излучения черного тела при различной температуре поверхности

Большим тепловым излучением обладают различные промышленные предприятия, наземные и надводные цели. Мощные энергетические установки промышленных предприятий во время работы выделяют много тепла.

Характеристики теплового излучения промышленных предприятий определяются количеством, типами, мощностями и расположением энергетических установок.

Большинство наземных малоразмерных целей представляют собой объекты автомобильной и бронетанковой техники. Наиболее нагретыми частями этих объектов являются капот, обшивка брони над двигателем и выхлопные патрубки. Максимум индикатрисы излучения, как правило, направлен назад и вверх.

Распознавание объекта основано на принципе теплового контраста – разности теплового излучения наблюдаемого объекта и фона (фон еще называют «подстилающей поверхностью»), на котором наблюдаемый объект проецируется. Все теплообнаружители («тепловизоры», теплопеленгаторы, тепловые головки самонаведения ракет и др.) работают по принципу использования теплового контраста (ТК) между объектом и фоном. ТК между отдельными точками предмета позволяет получить снимки этого предмета эвапорографом.

Тепловизорами оснащаются органы наземной разведки, артиллерийской разведки, они устанавливаются на бронетехнике, кораблях, самолетах, вертолетах, используются в зенитно-ракетных комплексах (в частности, в головках самонаведения ракет).

Для определения местоположения разведуемого объекта из теплопеленгаторных станций может создаваться теплопеленгаторная сеть.

Активная радиотепловая (инфракрасная) разведка обеспечивает добывание информации посредством облучения (подсвета) цели инфракрасным излучением и получения обратного, возвращенного информативного сигнала.

Оптико-электронная разведка

Оптико-электронная разведка (ОЭР) обеспечивает добывание информации на основе обнаружения, регистрации (приема), аналитического анализа излучаемых и отражаемых от объектов разведки сигналов в оптическом диапазоне ЭМВ. Как правило, ОЭР является дополнительным, обеспечивающим видом разведки, т. к. средствами ОЭР вооружены органы космической, воздушной, наземной, морской разведки различных силовых, правоохранительных структур, групп организованной преступности. ОЭР в себя включает:

– телевизионную разведку (ТВР). ТВР обеспечивает добывание информации, содержащейся в изображениях объектов, получаемых в видимом диапазоне ЭМВ с использованием телевизионной аппаратуры;

визуальную оптико-электронную разведку (ВОЭР). ВОЭР обеспечивает добывание информации, содержащейся в изображениях объектов, полученных с использованием приборов ночного видения в оптическом диапазоне ЭМВ;

– разведку лазерных излучений, т.е. сигналов лазерной техники в оптическом диапазоне волн ЭМВ;

– фоторазведку (ФР). ФР обеспечивает получение изображения объектов в видимом оптическом диапазоне ЭМВ с использованием различных типов фотоаппаратуры.

Акустическая разведка

Подразделения и средства акустической разведки состоят на вооружении артиллерийской разведки, в системах противовоздушной обороны, морской разведки, а также состоят в арсенале средств агентурной разведки, структур ведущих оперативно-розыскную деятельность, групп организованной преступности.

Обеспечивает добывание информации, содержащейся непосредственно в произносимой либо воспроизводимой специальной техникой речи (акустическая речевая разведка), а также в параметрах акустических сигналов, сопутствующих работе ТСПИ (акустическая сигнальная разведка).

Основным физическим параметром, обеспечивающим добывание акустической информации является акустическая мощность (АМ) – энергия, излучаемая источником звуковых колебаний в единицу времени. АМ при гармонических колебаниях определяется величиной движущей силы, скоростью смещения и сдвигом фазы между силой и скоростью смещения.

Исследование (разведка) акустических колебательных процессов (работы) акустических и электроакустических приборов и устройств (чувствительность, звуковое давление, характеристика направленности), акустические свойства материалов и конструкций (коэффициент поглощения, отражения и др.) осуществляется обычно электроакустическими методами: звуковые колебания преобразуются в переменные электрические напряжения и токи, измерение которых дает необходимую информацию.

Гидроакустическая разведка (ГАР), как правило, входит в состав морской разведки и разведки в акваториях рек и водоемов. ГАР обеспечивает добывание информации за счет разведки гидроакустических шумовых полей, гидролокационных параметров объектов, изображений, сигналов звукопроводной связи.

Химическая разведка

Это комплекс мероприятий, направленных на выявление заражения

ядовитыми веществами местности в районах расположения войск, и на направлениях их действия, проводимых с целью предупреждения поражения личного состава химическим оружием.

Одним из наиболее важных стратегических направлений в обеспечении безопасности от воздействия различных химических веществ в случае военной угрозы их применения или техногенной аварии на производствах является химическая разведка. Потенциальную опасность также имеют помещения по хранению токсичных веществ и мероприятия по их транспортировке.

В основе химической разведки лежит процесс постоянного и непрерывного наблюдения. Именно он позволяет вовремя обнаружить первые признаки отравляющих токсичных веществ. На основе этих данных осуществляется химический контроль опасной территории, а также определяется точный объем ликвидационных мероприятий.

Радиационная разведка

Это комплекс мероприятий по защите личного состава войск от радиационного поражения, который проводится с целью, своевременного обнаружения применения ядерного оружия и радиоактивного заражения местности, оповещения личного состава о радиационной опасности, обозначения радиоактивно зараженной местности знаками «Радиационная опасность».

Важность радиационной разведки обусловлена необходимостью оказания немедленной медицинской помощи в случае заражения людей, животных, а также определения объема санитарной обработки местности и оборудования. Выбор правильной тактики в ситуации радиационного облучения зависит от того, насколько четкими и достоверными будут данные, получаемые от разведывательных служб.

С этой целью используются различные технические приборы, которые всегда должны быть готовы к работе. На исходные данные оказывает влияние также квалификация, опыт разведчика или наблюдателя.

Сейсмическая разведка

Сейсмическая разведка – разведка сейсмических волн, создаваемых объектами разведки.

Основой методики сейсморазведочных работ являются возбуждение сейсмических волн и измерение времени пробега этих волн от источника до расстановки сейсмоприемников, обычно располагаемых вдоль прямой линии, направленной на источник.

Вызванные взрывом или другим способом упругие волны, распространяясь во всех направлениях от источника колебаний, проникают в толщу земной коры на большие глубины. В процессе

распространения в земной коре упругие волны претерпевают процессы отражения и преломления. Это приводит к тому, что часть сейсмической энергии возвращается к поверхности Земли, где вызывает дополнительные сравнительно слабые колебания. Эти колебания регистрируются специальной, достаточно сложной аппаратурой. Зная времена пробега до отдельных сейсмоприемников и скорость распространения волн, можно воссоздать траектории сейсмических волн. Структурную информацию получают в результате изучения траекторий волн, попадающих в две основные категории: головные, или преломленные, у которых главная часть пути проходит вдоль границы раздела двух слоев и, следовательно, приблизительно горизонтальна, и отраженные волны, у которых энергия первоначально распространяется вниз, а в некоторой точке отражается обратно к поверхности, так что общий путь практически вертикален. Для траекторий волн обоих типов времена пробега зависят от физических свойств горных пород и элементов залегания пластов. Задача сейсморазведки состоит в том, чтобы получить информацию о породах, в частности об элементах залегания пластов, из наблюдаемых времен вступления волн и (в меньшей степени) из вариаций амплитуды, частоты и формы сигнала [5].

4.4. Основы технической защиты информации

4.4.1. Основные направления защиты информации от утечки по техническим каналам

Государственная политика в сфере формирования информационных ресурсов и информатизации направлена на создание условий для эффективного и качественного информационного обеспечения решения стратегических и оперативных задач социального и экономического развития Российской Федерации [3].

Основными направлениями государственной политики в сфере информатизации являются:

– обеспечение условий для развития и защиты всех форм собственности на информационные ресурсы;

– формирование и защита государственных информационных ресурсов; создание и развитие федеральных и региональных информационных систем и сетей, обеспечение их совместимости и взаимодействия в едином информационном пространстве Российской Федерации;

– создание условий для качественного и эффективного информационного обеспечения граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений на основе государственных информационных ресурсов;

– обеспечение национальной безопасности в сфере информатизации, а также обеспечение реализации прав граждан, организаций в условиях информатизации;

– содействие формированию рынка информационных ресурсов, услуг, информационных систем, технологий, средств их обеспечения;

– формирование и осуществление единой научно-технической и промышленной политики в сфере информатизации с учетом современного мирового уровня развития информационных технологий;

– поддержка проектов и программ информатизации;

– создание и совершенствование системы привлечения инвестиций и механизма стимулирования разработки и реализации проектов информатизации;

– развитие законодательства в сфере информационных процессов, информатизации и защиты информации.

Система передачи информации ОВД организуется в соответствии с иерархической структурой.

При этом в высших звеньях управления (УВД–МВД) конфиденциальная информация циркулирует в своем большинстве в документальном и телекоммуникационном виде, реже – в речевом виде. Для ее закрытия на объектах (помещения УВД, МВД) применяется комплекс организационных и технических мероприятий силами и средствами отдела связи и спецтехники.

Для закрытия информации в линиях связи применяются специальные технические средства. В низших звеньях управления (ОВД–УВД, связь взаимодействия подразделений ОВД) основные объемы информации передаются в речевом виде. На объектах подразделений ОВД информационная безопасность обеспечивается лишь организационно-режимными мерами, для защиты информации в линиях связи практически никаких технических средств не применяется.

4.4.2. Классификация методов и средств защиты речевой информации

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

Пассивные методы защиты акустической (речевой) информации направлены на [2]:

– ослабление акустических (речевых) сигналов на границе контролируемой зоны до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;

– ослабление информационных электрических сигналов в соединительных линиях ВТСС, имеющих в своем составе электроакустические преобразователи (обладающие микрофонным эффектом), до величин, обеспечивающих невозможность их выделения средством разведки на фоне естественных шумов;

– исключение (ослабление) прохождения сигналов высокочастотного навязывания во вспомогательные технические средства, имеющие в своем составе электроакустические преобразователи (обладающие микрофонным эффектом);

– обнаружение излучений акустических закладок и побочных электромагнитных излучений диктофонов в режиме записи;

– обнаружение несанкционированных подключений к телефонным линиям связи.

Активные методы защиты акустической (речевой) информации направлены на [2]:

– создание маскирующих акустических и вибрационных помех с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения информационного акустического сигнала средством разведки;

– создание маскирующих электромагнитных помех в соединительных линиях ВТСС, имеющих в своем составе электроакустические преобразователи (обладающие микрофонным эффектом), с целью уменьшения отношения сигнал/шум до величин, обеспечивающих невозможность выделения информационного сигнала средством разведки;

– электромагнитное подавление диктофонов в режиме записи;

– ультразвуковое подавление диктофонов в режиме записи;

– создание маскирующих электромагнитных помех в линиях электропитания ВТСС, обладающих микрофонным эффектом, с целью уменьшения отношения сигнал/шум до величин, обеспечивающих невозможность выделения информационного сигнала средством разведки;

– создание прицельных радиопомех акустическим и телефонным радиозакладкам с целью уменьшения отношения сигнал/шум до величин, обеспечивающих невозможность выделения информационного сигнала средством разведки;

– подавление средств несанкционированного подключения к телефонным линиям;

– уничтожение (вывод из строя) средств несанкционированного подключения к телефонным линиям.

Ослабление акустических (речевых) сигналов осуществляется путем звукоизоляции помещений.

Ослабление информационных электрических сигналов в соединительных линиях ВТСС и исключение (ослабление) прохождения сигналов высокочастотного навязывания во вспомогательные технические средства осуществляется методами фильтрации сигналов.

4.4.3. Защита телефонных линий от утечки информации

При защите телефонных аппаратов и телефонных линий необходимо учитывать несколько аспектов:

– телефонные аппараты (даже при положенной трубке) могут быть использованы для перехвата акустической речевой информации из помещений,

в которых они установлены, то есть для подслушивания разговоров в этих помещениях;

– телефонные линии, проходящие через помещения, могут использоваться в качестве источников питания акустических закладок, установленных в этих помещениях, а также для передачи перехваченной информации;

– и, конечно, возможен перехват (подслушивание) телефонных разговоров путем гальванического или через индукционный датчик подключения к телефонной линии закладок (телефонных ретрансляторов), диктофонов и других средств несанкционированного съема информации.

Телефонный аппарат имеет несколько элементов, имеющих способность преобразовывать акустические колебания в электрические, то есть обладающих «микрофонным эффектом». К ним относятся: звонковая цепь, телефонный и микрофонный капсюли. За счет электроакустических преобразований в этих элементах возникают информационные (опасные) сигналы.

При положенной трубке телефонный и микрофонный капсюли гальванически отключены от телефонной линии, и при подключении к ней специальных высокочувствительных низкочастотных усилителей возможен перехват опасных сигналов, возникающих в элементах только звонковой цепи. Амплитуда этих опасных сигналов, как правило, не превышает долей мВ.

При использовании для съема информации метода «высокочастотного навязывания», несмотря на гальваническое отключение микрофона от телефонной линии, сигнал навязывания благодаря высокой частоте проходит в микрофонную цепь и модулируется по амплитуде информационным сигналом.

Следовательно, в телефонном аппарате необходимо защищать как звонковую цепь, так и цепь микрофона.

Для защиты телефонного аппарата от утечки акустической (речевой) информации по электроакустическому каналу используются как пассивные, так и активные методы и средства.

К наиболее широко применяемым пассивным методам защиты относятся:

– ограничение опасных сигналов;
– фильтрация опасных сигналов;
– отключение преобразователей (источников) опасных сигналов.

4.4.4. Демаскирующие признаки электронных устройств перехвата информации

Обнаружение электронных устройств перехвата информации (закладных устройств), так же как и любых других объектов, производится по их демаскирующим признакам.

Каждый вид электронных устройств перехвата информации имеет свои демаскирующие признаки, позволяющие обнаружить закладку.

Наиболее информативными признаками **проводной микрофонной** системы являются:

– тонкий провод неизвестного назначения, подключенный к малогабаритному микрофону (часто закамуфлированному и скрытно установленному) и выходящий в другое помещение;

– наличие в линии (проводе) неизвестного назначения постоянного (в несколько вольт) напряжения и низкочастотного информационного сигнала.

– Демаскирующие признаки автономных **некамуфлированных** акустических закладок включают:

– признаки внешнего вида – малогабаритный предмет (часто в форме параллелепипеда) неизвестного назначения;

– одно или несколько отверстий малого диаметра в корпусе;

– наличие автономных источников питания (например, аккумуляторных батарей);

– наличие полупроводниковых элементов, выявляемых при облучении обследуемого устройства нелинейным радиолокатором;

– наличие в устройстве проводников или других деталей, определяемых при просвечивании его рентгеновскими лучами. **Камуфлированные акустические закладки** по внешнему виду, на первый взгляд, не отличаются от объекта имитации, особенно если закладка устанавливается в корпус бытового предмета без изменения его внешнего вида. Такие закладки можно выявить путем разборки предмета.

Закладки, устанавливаемые в малогабаритные предметы, ограничивают возможности последних. Эти ограничения могут служить косвенными признаками закладных устройств. Чтобы исключить возможность выявления закладки путем ее разборки, места соединения разбираемых частей склеивают.

Некоторые камуфлированные закладные устройства не отличаются от оригиналов даже при тщательном внешнем осмотре. Их можно обнаружить только при просвечивании предметов рентгеновскими лучами.

В ряде случаев закамуфлированное закладное устройство обнаруживается по наличию в обследуемом предмете не свойственных ему полупроводниковых элементов (выявляемых при облучении его нелинейным радиолокатором). Например, обнаружение полупроводниковых элементов в пепельнице или в папке для бумаг может указать на наличие в них закладных устройств.

Наличие портативных звукозаписывающих и видеозаписывающих устройств в момент записи можно обнаружить по наличию их побочных электромагнитных излучений (излучений генераторов подмагничивания и электродвигателей).

Дополнительные демаскирующие признаки **акустических радиозакладочных устройств:**

– радиоизлучения (как правило, источник излучения находится в ближней зоне) с модуляцией радиосигнала информационным сигналом;

– наличие (как правило) небольшого отрезка провода (антенны), выходящего из корпуса закладки.

Вследствие того, что при поиске радиозакладок последние находятся в ближней зоне излучения и уровень сигналов от них, как правило, превышает уровень сигналов от других РЭС, у большинства радиозакладок обнаруживаются побочные излучения и, в частности, излучения на второй и третьей гармониках, субгармониках и т.д.

Дополнительные демаскирующие признаки **сетевых акустических закладочных устройств:**

наличие в линии электропитания высокочастотного сигнала (как правило, несущая частота от 40 до 600 кГц, но возможно наличие сигнала на частотах до 7 МГц), модулированного информационным низкочастотным сигналом;

– наличие тока утечки (от единиц до нескольких десятков мА) в линии электропитания при всех отключенных потребителях;

– отличие емкости линии электропитания от типовых значений при отключении линии от источника питания (на распределительном щитке электропитания) и отключении всех потребителей.

Дополнительные демаскирующие признаки **акустических и телефонных закладочных устройств** с передачей информации по телефонной линии **на высокой частоте**:

наличие в линии высокочастотного сигнала (как правило, несущая частота до 7 МГц) с модуляцией его информационным сигналом.

Дополнительные демаскирующие признаки **телефонных радиозакладочных устройств**:

– радиоизлучения с модуляцией радиосигнала информационным сигналом, передаваемым по телефонной линии:

– отличие сопротивления телефонной линии от «00» при отключении телефонного аппарата и отключении линии (отсоединении телефонных проводов) на распределительной коробке (щитке);

– отличие сопротивления телефонной линии от типового значения (для данной линии) при отключении телефонного аппарата, отключении и закорачивании линии на распределительной коробке (щитке);

– падение напряжения (от нескольких десятых до 1,5...2 В) в телефонной линии (по отношению к другим телефонным линиям, подключенным к данной распределительной коробке) при положенной и поднятой телефонной трубке;

– наличие тока утечки (от единиц до нескольких десятков мА) I телефонной линии при отключенном телефоне.

Дополнительные демаскирующие признаки **акустических**

закладочных устройств типа «телефонного уха»:

– отличие сопротивления телефонной линии от «00» при отключении телефонного аппарата и отключении линии (отсоединении телефонных проводов) на распределительной коробке (щитке);

– падение напряжения (от нескольких десятых до 1,5...2 В) в телефонной линии (по отношению к другим телефонным линиям, подключенным к данной распределительной коробке) при положенной телефонной трубке;

– наличие тока утечки (от единиц до нескольких десятков мА) 1 телефонной линии при отключенном телефоне;

– подавление (не прохождение) одного-двух вызывных звонков при наборе номера телефонного аппарата.

Дополнительные демаскирующие признаки **полуактивных акустических радиозакладочных устройств**:

– облучение помещения направленным (зондирующим) мощным излучением (как правило, гармоническим);

– наличие в помещении переизлученного зондирующего излучения с амплитудной или частотной модуляцией информационным акустическим сигналом [2].

4.4.5. Методы и средства поиска электронных устройств перехвата информации

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, программно-аппаратных комплексов контроля, нелинейных локаторов, рентгеновских комплексов, обычных тестеров, а также специальной аппаратуры для проверки проводных линий и т.д.

Метод поиска закладных устройств во многом определяется использованием той или иной аппаратуры контроля. К основным методам поиска закладных устройств можно отнести:

– специальное обследование выделенных помещений;

– поиск радиозакладочных устройств с использованием индикаторов поля, радиочастотомеров и интерсепторов;

– поиск радиозакладочных устройств с использованием сканерных приемников и анализаторов спектра;

– поиск радиозакладочных устройств с использованием программно-аппаратных комплексов контроля;

– поиск портативных звукозаписывающих устройств с использованием детекторов диктофонов (по наличию их побочных электромагнитных излучений генераторов подмагничивания и электродвигателей);

– поиск портативных видеозаписывающих устройств с использованием детекторов видеокамер (по наличию побочных электромагнитных излучений генераторов подмагничивания и электродвигателей видеокамер);

– поиск закладочных устройств с использованием нелинейных локаторов;

– поиск закладочных устройств с использованием рентгеновских комплексов;

– проверка с использованием ВЧ-пробника (зонда) линий электропитания, радиотрансляции и телефонной связи;

– измерение параметров линий электропитания, телефонных линий связи и т.д.;

– проведение тестового «прозвона» всех телефонных аппаратов, установленных в проверяемом помещении, с контролем (на слух) прохождения всех вызывных сигналов АТС.

Простейшими и наиболее дешевыми обнаружителями радиоизлучений: закладных устройств являются **индикаторы электромагнитного поля,** которые световым или звуковым сигналом сигнализируют о наличии в точке расположения антенны электромагнитного поля с напряженностью выше пороговой (фоновой). Более сложные из них – **частотомеры** обеспечивают, кроме того, измерение несущей частоты наиболее «сильного» в точке приема сигнала.

Для обнаружения излучений закладных устройств в ближней зоне могут использоваться и специальные приборы, называемые **интерсепторами.** Интерсептор автоматически настраивается на частоту наиболее мощного сигнала и осуществляет его детектирование. Некоторые интерсепторы позволяют не только производить автоматический или ручной захват радиосигнала, осуществлять его детектирование и прослушивание через динамик, но и определять частоту обнаруженного сигнала и вид модуляции.

Чувствительность обнаружителей поля мала, поэтому они позволяют обнаруживать излучения радиозакладочных устройств в непосредственной близости от них.

Существенно лучшую чувствительность имеют специальные (профессиональные) радиоприемники с автоматизированным сканированием радиодиапазона **(сканерные приемники** или **сканеры).** Они обеспечивают поиск в диапазоне частот, перекрывающем частоты почти всех применяемых радиозакладочных устройств – от десятков кГц до единиц ГГц. Лучшими возможностями по поиску радиозакладочных устройств обладают **анализаторы спектра.** Кроме перехвата излучений закладных устройств они позволяют анализировать и их характеристики, что немаловажно при обнаружении радиозакладочных устройств, использующих для передачи информации сложные виды сигналов.

Возможность сопряжения сканирующих приемников с переносными компьютерами послужило основой для создания автоматизированных комплексов для поиска радиозакладочных устройств (так называемых **программно-аппаратных комплексов контроля).** Кроме программно-аппаратных комплексов, построенных на базе сканирующих приемников и переносных компьютеров, для поиска закладочных устройств используются и специально разработанные многофункциональные комплексы, такие, например, как «0SCOR-5000».

Специальные комплексы и аппаратура для контроля проводных линий позволяют проводить измерение параметров (напряжений, токов, сопротивлений и т.п.) телефонных, слаботочных линий и линий электропитания, а также выявлять в них сигналы закладных устройств.

Обнаружители пустот позволяют обнаруживать возможные места установки закладных устройств в пустотах стен или других деревянных или кирпичных конструкциях.

Большую группу образуют средства обнаружения или локализации закладных устройств по физическим свойствам элементов электрической схемы или конструкции. Такими элементами являются: полупроводниковые приборы, которые применяются в любых закладных устройствах, электропроводящие металлические детали конструкции и т.д. Из этих средств наиболее достоверные результаты обеспечивают средства для обнаружения полупроводниковых элементов по их нелинейным свойствам **– нелинейные радиолокаторы.**

Принципы работы нелинейных радиолокаторов близки к принципам работы радиолокационных станций, широко применяемых для радиолокационной разведки объектов. Существенное отличие заключается в том, что если приемник радиолокационной станции принимает отраженный от объекта зондирующий сигнал (эхо-сигнал) на частоте излучаемого сигнала, то приемник нелинейного локатора принимает 2-ю и 3-ю гармоники отраженного сигнала. Появление в отраженном сигнале этих гармоник обусловлено нелинейностью характеристик полупроводников.

Металлоискатели (металлодетекторы) реагируют на наличие в районе поиска электропроводных материалов, прежде всего металлов, и позволяют обнаруживать корпуса или другие металлические элементы закладки.

Переносные **рентгеновские установки** применяются для просвечивания предметов, назначения которых не удается выявить без их разборки прежде всего тогда, когда она невозможна без разрушения найденного предмета.

4.4.6. Защита информации телекоммуникационных систем (ТКС) от утечки по техническим каналам

Фильтрация информационных сигналов.

Одним из методов локализации опасных сигналов, циркулирующих в технических средствах и системах обработки информации, является

фильтрация. В источниках электромагнитных полей и наводок фильтрация осуществляется с целью предотвращения распространения нежелательных электромагнитных колебаний за пределы устройства – источника опасного сигнала. Фильтрация в устройствах – рецепторах электромагнитных полей и наводок должна исключить их воздействие на рецептор.

Для фильтрации сигналов в цепях питания ОТСС используются разделительные трансформаторы и помехоподавляющие фильтры.

Разделительные трансформаторы. Такие трансформаторы должны обеспечивать развязку первичной и вторичной цепей по сигналам наводки. Это означает, что во вторичную цепь трансформатора не должны проникать наводки, появляющиеся в цепи первичной обмотки. Проникновение наводок во вторичную обмотку объясняется наличием нежелательных резистивных и емкостных цепей связи между обмотками.

Для уменьшения связи обмоток по сигналам наводок часто применяется внутренний экран, выполняемый в виде заземленной прокладки или фольги, укладываемой между первичной и вторичной обмотками. С помощью этого экрана наводка, действующая в первичной обмотке, замыкается на землю. Однако электростатическое поле вокруг экрана также может служить причиной проникновения наводок во вторичную цепь.

Разделительные трансформаторы используются с целью решения ряда задач, в том числе для:

– разделения по цепям питания источников и рецепторов наводки, если они подключаются к одним и тем же шинам переменного тока;

– устранения асимметричных наводок;

– ослабления симметричных наводок в цепи вторичной обмотки, обусловленных наличием асимметричных наводок в цепи первичной обмотки.

Средства развязки и экранирования, применяемые в разделительных трансформаторах, обеспечивают максимальное значение сопротивления между обмотками и создают для наводок путь с малым сопротивлением из первичной обмотки на землю. Это достигается обеспечением высокого сопротивления изоляции соответствующих элементов конструкции (до 10 МОм) и незначительной емкости между обмотками. Указанные особенности трансформаторов для цепей питания обеспечивают более высокую степень подавления наводок, чем обычные трансформаторы.

Разделительный трансформатор со специальными средствами экранирования и развязки обеспечивает ослабление информационного сигнала наводки в нагрузке на 126 дБ при емкости между обмотками 0,005 пФ и на 140 дБ при емкости между обмотками 0,001 пФ.

Средства экранирования, применяемые в разделительных трансформаторах, должны не только устранять влияние асимметричных наводок на защищаемое устройство, но и не допустить на выходе

трансформатора симметричных наводок, обусловленных асимметричными наводками на его входе. Применяя в разделительных трансформаторах специальные средства экранирования, можно существенно (более чем на 40 дБ) уменьшить уровень таких наводок.

Помехоподавляющие фильтры. В настоящее время существует большое количество различных типов фильтров, обеспечивающих ослабление нежелательных сигналов в разных участках частотного диапазона. Это фильтры нижних и верхних частот, полосовые и заграждающие фильтры и т.д. Основное назначение фильтров – пропускать без значительного ослабления сигналы с частотами, лежащими в рабочей полосе частот, и подавлять (ослаблять) сигналы с частотами, лежащими за пределами этой полосы.

Для исключения просачивания информационных сигналов в цепи электропитания используются **фильтры нижних частот.**

Фильтр нижних частот (ФНЧ) пропускает сигналы с частотами ниже граничной частоты ($f_c < f_{гр}$) и подавляет – с частотами выше граничной частоты.

Последовательная ветвь ФНЧ должна иметь малое сопротивление для постоянного тока и нижних частот. Вместе с тем для того, чтобы высшие частоты задерживались фильтром, последовательное сопротивление должно расти с частотой. Этим требованиям удовлетворяет индуктивность L.

Параллельная ветвь ФНЧ, наоборот, должна иметь малую проводимость для низких частот с тем, чтобы токи этих частот не шунтировались параллельным плечом. Для высоких частот параллельная ветвь должна иметь большую проводимость, тогда колебания этих частот будут ею шунтироваться и их ток на выходе фильтра будет ослабляться. Таким требованиям отвечает емкость С.

Более сложные многозвенные ФНЧ (Чебышева, Баттерворта, Бесселя и т.д.) конструируют на основе сочетаний различных единичных звеньев.

Количественно величина ослабления (фильтрации) нежелательных (в том числе и опасных) сигналов защитным фильтром оценивается в соответствии с выражением:

$A = 20\lg(U_1/U_2) = 10\lg(P_1/P_2)$,дБ,

где U_1 (P_1) – напряжение (мощность) опасного сигнала на входе фильтра;

U_2 (P_2) – напряжение (мощность) опасного сигнала на выходе фильтра при включенной нагрузке Z_n.

Основные требования, предъявляемые к защитным фильтрам, заключаются в следующем:

величины рабочего напряжения и тока фильтра должны соответствовать напряжению и току фильтруемой цепи;

– величина ослабления нежелательных сигналов в диапазоне рабочих частот должна быть не менее требуемой;

– ослабление полезного сигнала в полосе прозрачности фильтра должно быть незначительным;

– габариты и масса фильтров должны быть минимальными;

– фильтры должны обеспечивать функционирование при определенных условиях эксплуатации (температура, влажность, давление) и механических нагрузках (удары, вибрация и т.д.);

– конструкции фильтров должны соответствовать требованиям техники безопасности.

К фильтрам цепей питания наряду с общими предъявляются следующие дополнительные требования:

– затухание, вносимое такими фильтрами в цепи постоянного тока или переменного тока основной частоты, должно быть минимальным (например, 0,2 дБ и менее) и иметь большое значение (более 60 дБ) в полосе подавления, которая в зависимости от конкретных условий может быть достаточно широкой (до 10 ГГц);

– сетевые фильтры должны эффективно работать при сильных проходящих токах, высоких напряжениях и высоких уровнях мощности проходящих и задерживаемых электромагнитных колебаний;

– ограничения, накладываемые на допустимые уровни нелинейных искажений формы напряжения питания при максимальной нагрузке, должны быть достаточно жесткими (например, уровни гармонических составляющих напряжения питания с частотами выше 10 кГц должны быть на 80 дБ ниже уровня основной гармоники).

Рассмотрим влияние этих параметров более подробно.

Напряжение, приложенное к фильтру, должно быть таким, чтобы оно не вызывало пробоя конденсаторов фильтра при различных скачках питающего напряжения, включая скачки, обусловленные переходными процессами в цепях питания. Чтобы при заданных массе и объеме фильтр обеспечивал наилучшее подавление наводок в требуемом диапазоне частот, его конденсаторы должны обладать максимальной емкостью на единицу объема или массы. Кроме того, номинальное значение рабочего напряжения конденсаторов выбирают исходя из максимальных значений допускаемых скачков напряжения цепи питания, но не более их.

Ток через фильтр должен быть таким, чтобы не возникало насыщения сердечников катушек фильтра. Кроме того, следует учитывать, что с увеличением тока через катушку увеличивается реактивное падение напряжения на ней. Это может привести к тому, что:

– ухудшается эквивалентный коэффициент стабилизации напряжения в цепи питания, содержащей фильтр;

– возникает взаимозависимость переходных процессов в различных нагрузках цепи питания.

Наибольшие скачки напряжения при этом возникают во время

отключения нагрузок, так как большинство из них имеет индуктивный характер.

Характеристики фильтров зависят от числа использованных реактивных элементов. Так, например, фильтр из одного параллельного конденсатора или одной последовательной индуктивной катушки может обеспечить затухание лишь 20 дБ/декада вне полосы пропускания, а LC–фильтр из десяти или более элементов – более 200 дБ/декада.

Из-за паразитной связи между входом и выходом фильтра на практике трудно получить затухание более 100 дБ. Если фильтр неэкранированный и сигнал подается на него и снимается с помощью неэкранированных соединений (проводов), то развязка между входом и выходом обычно не превышает 40...60 дБ. Для обеспечения развязки более 60 дБ необходимо использовать экранированные фильтры с разъемами и использовать для соединения экранированные провода.

Фильтры с гарантируемым затуханием 100 дБ выполняют в виде узла с электромагнитным экранированием, который помещается в корпус, изготовленный из материала с высокой магнитной проницаемостью магнитного экрана. Этим существенно уменьшается возможность возникновения внутри корпуса паразитной связи между входом и выходом фильтра из-за магнитных электрических или электромагнитных полей.

Из-за влияния паразитных емкостей и индуктивностей фильтр зачастую не обеспечивает требуемого затухания на частотах, превышающих граничную частоту (1с) на две декады, и полностью может потерять работоспособность на частотах, превышающих граничную частоту на несколько декад [2].

4.4.7. Пространственное и линейное зашумление информативных сигналов

Реализация пассивных методов защиты, основанных на применении экранирования и фильтрации, приводит к ослаблению уровней побочных электромагнитных излучений и наводок (опасных сигналов) ОТСС и тем самым к уменьшению отношения опасный сигнал/шум (с/ш). Однако в ряде случаев, несмотря на применение пассивных методов защиты, на границе контролируемой зоны отношение с/ш превышает допустимое значение. В этом случае применяются активные меры защиты, основанные на создании помех средствам разведки, что также приводит к уменьшению отношения с/ш.

Для исключения перехвата побочных электромагнитных излучений по электромагнитному каналу используется пространственное зашумление, а для исключения съема наводок информационных сигналов с посторонних проводников и соединительных линий ВТСС – линейное зашумление.

К системе пространственного зашумления, применяемой для создания маскирующих электромагнитных помех, предъявляются

следующие требования:

– система должна создавать электромагнитные помехи в диапазоне частот возможных побочных электромагнитных излучений ОТСС;

– создаваемые помехи не должны иметь регулярной структуры;

– уровень создаваемых помех (как по электрической, так и по магнитной составляющей поля) должен обеспечить отношение с/ш на границе контролируемой зоны меньше допустимого значения во всем диапазоне частот возможных побочных электромагнитных излучений ОТСС;

– система должна создавать помехи как с горизонтальной, так и с вертикальной поляризацией (поэтому выбору антенн для генераторов помех уделяется особое внимание);

– на границе контролируемой зоны уровень помех, создаваемых системой пространственного зашумления, не должен превышать требуемых норм по ЭМС.

Цель пространственного зашумления считается достигнутой, если отношение опасный сигнал/шум на границе контролируемой зоны не превышает некоторого допустимого значения, рассчитываемого по специальным методикам для каждой частоты информационного (опасного) побочного электромагнитного излучения ОТСС.

В системах пространственного зашумления в основном используются помехи типа «белого шума» или «синфазные помехи».

Системы, реализующие метод «синфазной помехи», в основном применяются для защиты ПЭВМ. В них в качестве помехового сигнала используются импульсы случайной амплитуды, совпадающие (синхронизированные) по форме и времени существования с импульсами полезного сигнала. Вследствие этого по своему спектральному составу помеховый сигнал аналогичен спектру побочных электромагнитных излучений ПЭВМ. То есть, система зашумления генерирует «имитационную помеху», по спектральному составу соответствующую скрываемому сигналу.

В настоящее время в основном применяются системы пространственного зашумления, использующие помехи типа «белый шум», то есть излучающие широкополосный шумовой сигнал (как правило, с равномерно распределенным энергетическим спектром во всем рабочем диапазоне частот), существенно превышающий уровни побочных электромагнитных излучений. Такие системы применяются для защиты широкого класса технических средств: электронно-вычислительной техники, систем звукоусиления и звукового сопровождения, систем внутреннего телевидения и т.д.

4.4.8. Обнаружение и подавление диктофонов, видеокамер и акустических закладных устройств

Диктофоны и акустические закладки в своем составе содержат большое количество полупроводниковых приборов, поэтому наиболее эффективным

средством их обнаружения является нелинейный локатор, устанавливаемый на входе в выделенное помещение и работающий в составе системы контроля доступа.

К типовым представителям устройств этого класса относится, например, **нелинейный локатор** «Циклон-Рамка». Локатор имеет два датчика, выносной пульт управления и может скрытно устанавливаться в дверной проем выделенного помещения, что позволяет контролировать наличие у посетителей (как в ручной клади, так и под одеждой) любых радиоэлектронных устройств, в том числе диктофонов и подслушивающих устройств, как во включенном, так и в выключенном состояниях. Зона контроля локатора составляет: по высоте – 2,2 м, по длине – 1,5м, по ширине – 1,5 м.

Для обнаружения работающих в режиме записи диктофонов применяются так называемые **детекторы диктофонов.** Принцип действия приборов основан на обнаружении слабого магнитного поля, создаваемого генератором подмагничивания или работающим двигателем диктофона в режиме записи. Электродвижущая сила (ЭДС), наводимая этим полем в датчике сигналов (магнитной антенне), усиливается и выделяется из шума специальным блоком обработки сигналов. При превышении уровня принятого сигнала некоторого установленного порогового значения срабатывает световая или звуковая сигнализация. Во избежание ложных срабатываний порог обнаружения необходимо корректировать практически перед каждым сеансом работы, что является недостатком подобных приборов.

Детекторы диктофонов выпускаются в переносном и стационарном вариантах. К переносным относятся детекторы «Сова», RM-100, TKD-800, а к стационарным – PTRD-14, PTRD-16, PTRD-18 и т.д.

В переносном (носимом) варианте блок анализа детектора размещается в кармане оператора, поисковая антенна в рукаве (обычно крепится на предплечье), а датчик сигнализации вибраторного типа – на поясе или в кармане. В ходе переговоров оператор приближает антенну (руку) к возможным местам установки диктофона (портфель, одежда собеседника и т.д.). При обнаружении излучений (превышении магнитного поля установленного оператором порогового значения) включенного на запись диктофона скрытый сигнализатор-вибратор начинает вибрировать, сигнализируя оператору о возможной записи разговора.

Для защиты выделенных помещений в основном используются детекторы диктофонов, выполненные в стационарных вариантах. В отличие от переносных детекторов, имеющих один датчик сигналов, стационарные детекторы диктофонов оборудованы несколькими датчиками (например, детектор PTRD-18 имеет возможность подключения до 16 датчиков одновременно), что позволяет существенно повысить вероятность обнаружения диктофонов.

Стационарный вариант предполагает установку (заделку) антенн в стол для переговоров и в кресла (подлокотники). Блок анализа и индикатор наличия диктофонов размещается в столе руководителя или у дежурного (в этом случае создается дополнительный канал управления). При наличии у беседующего диктофона в одежде или в вещах (папка, портфель и т.д.) у руководителя скрытным образом будет срабатывать индикация этого факта.

Ввиду слабого уровня магнитного поля, создаваемого работающими диктофонами (особенно в экранированных корпусах), дальность их обнаружения детекторами незначительна. Например, дальность обнаружения диктофона L- 400 в режиме записи в условиях офиса даже при использовании стационарного детектора PTRD-018 не превышает 45...65 см. Дальность обнаружения диктофонов в неэкранированных корпусах может составлять 1...1,5 м.

Принцип действия устройств электромагнитного подавления основан на генерации в дециметровом диапазоне частот (обычно в районе 900 МГц) мощных шумовых сигналов. В основном для подавления используются импульсные сигналы. Излучаемые направленными антеннами помеховые сигналы, воздействуя на элементы электронной схемы диктофона (в частности, усилитель низкой частоты и усилитель записи), вызывают в них наводки шумовых сигналов. Вследствие этого одновременно с информационным сигналом (речью) осуществляется запись и детектированного шумового сигнала, что приводит к значительному искажению первого.

Зона подавления диктофонов зависит от мощности излучения, его вида, а также от типа используемой антенны. Обычно зона подавления представляет собой сектор с углом от 30 до 80 градусов и радиусом до 1,5 м (для диктофонов в экранированном корпусе).

Системы ультразвукового подавления излучают мощные неслышимые человеческим ухом ультразвуковые колебания (обычно частота излучения около 20 кГц), воздействующие непосредственно на микрофоны диктофонов или акустических закладок, что является их преимуществом. Данное ультразвуковое воздействие приводит к перегрузке усилителя низкой частоты диктофона или акустической закладки (усилитель начинает работать в нелинейном режиме) и тем самым – к значительным искажениям записываемых (передаваемых) сигналов.

В отличие от систем электромагнитного подавления подобные системы обеспечивают подавление в гораздо большем секторе. Например, комплекс «Завеса» при использовании двух ультразвуковых излучателей способен обеспечить подавление диктофонов и акустических закладок в помещении объемом 27 м^3. Однако системы ультразвукового подавления имеют и один важный недостаток: эффективность их резко снижается, если

микрофон диктофона или закладки прикрыть фильтром из специального материала или в усилителе низкой частоты установить фильтр низких частот с граничной частотой 3,4...4 кГц.

Для обнаружения радиозакладочных устройств в выделенных помещениях могут использоваться индикаторы поля, интерсепторы, радиочастотомеры, сканерные приемники, программно-аппаратные комплексы контроля и другие технические средства.

Наиболее эффективным методом выявления радиозакладочных устройств в выделенных помещениях является постоянный (круглосуточный) радиоконтроль с использованием программно-аппаратных комплексов контроля. Для его организации в специально оборудованном помещении на объекте разворачивается стационарный пункт радиоконтроля, в состав которого, как правило, включаются один или несколько программно-аппаратных комплексов, позволяющих контролировать все выделенные помещения. На пункте радиоконтроля устанавливается опорная антенна, а в выделенных (контролируемых) помещениях – малогабаритные широкополосные антенны и звуковые колонки или выносные микрофоны, которые при установке камуфлируются. Антенны и звуковые колонки (или микрофоны) специально проложенными кабелями соединяются соответственно с блоками высокочастотного (антенного) или низкочастотного коммутаторов, установленных в помещении стационарного пункта контроля.

Если при проведении радиоконтроля обнаружена передача информации радиозакладочным устройством, то до ее выявления может быть организована постановка прицельных помех на частоте передачи закладочного устройства.

Для подавления радиозакладочных устройств также могут использоваться системы пространственного электромагнитного зашумления, применяемые для маскировки побочных электромагнитных излучений ТСПИ. Однако при этом необходимо помнить, что ввиду сравнительно низкой спектральной мощности излучаемой помехи, эти системы эффективны только для подавления маломощных (как правило, с мощностью излучения менее 10 мВт) радиозакладочных устройств. Поэтому для подавления радиозакладочных устройств необходимо использовать генераторы шума с повышенной мощностью.

Для защиты речевой информации от сетевых акустических закладок используются помехоподавляющие фильтры низких частот и системы линейного зашумления.

Помехоподавляющие фильтры устанавливаются в линии питания розеточной и осветительной сетей в местах их выхода из выделенных помещений. Учитывая, что сетевые закладки используют для передачи информации частоты свыше 40...50 кГц, для защиты информации

необходимо использовать фильтры низких частот с граничной частотой не более 40 кГц. К таким фильтрам относятся, например, фильтры типа ФСПК, граничная частота которых составляет 20 кГц.

В системах зашумления линий электропитания используются генераторы шума типа «Гром-ЗИ-4» и др.

При выборе генераторов шума особое внимание необходимо уделять полосе частот и спектральной мощности помехового сигнала. Например, генераторы шума «Гром-ЗИ-4», «Гром-ЗИ-6Ц» создают помеховый сигнал в диапазоне частот от 0,1 до 1 МГц и от 0,1 до 5 МГц соответственно. Поэтому они не эффективны для подавления сетевых закладок, использующих для передачи информации частоты ниже 100 кГц.

4.4.9. Государственное лицензирование в области защиты информации

Основные принципы, организационную структуру системы государственного лицензирования деятельности юридических лиц–предприятий, организаций и учреждений независимо от их организационно-правовой формы по защите информации, циркулирующей в технических средствах и помещениях, получивших лицензию, устанавливает постановление правительства Российской Федерации «О государственном лицензировании деятельности в области зашиты информации» от 23 августа 1994г. № 214.

В постановлении используется следующие основные понятия:

лицензирование в области защиты информации – деятельность, заключается в передаче или получении прав на проведение работ в области защиты информации;

лицензия в области защиты информации – оформленное соответсвующим образом разрешение на право проведения тех или иных работ в области защиты информации;

защита информации – комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п.;

эффективность защиты информации – степень соответствия достигнутых результатов действий по защите информации поставленной цели защиты;

безопасность информации – состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п.;

шифровальные средства:

– реализующие криптографические алгоритмы преобразования

информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для защиты информации (в т. ч. и входящие в системы и комплексы защиты информации от НСД), циркулирующей в технических средствах, при ее обработке, хранении и передаче по каналам связи, включая шифровальную технику;

– реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и «электронной подписи»;

– аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для изготовления и распределения ключевых документов, используемых в шифровальных средствах, независимо от вида носителя ключевой информации;

охраняемые сведения – сведения, составляющие государственную и иную охраняемую законом тайны;

аттестование объекта в защищенном исполнении – официальное подтверждение наличия на объекте защиты необходимых и достаточных условий, обеспечивающих выполнение установленных требований руководящих документов и норм эффективности защиты информации;

техническое средство обработки информации (ТСОИ) – техническое средство, предназначенное для приема, накопления, хранения, поиска, преобразования, отображения и передачи информации по каналам связи.

Система государственного лицензирования деятельности предприятий в области защиты информации является составной частью государственной системы защиты информации.

Деятельность системы лицензирования организуют государственные органы по лицензированию, которыми являются Федеральная служба по техническому и экспортному контролю Российской Федерации **(ФСТЭК)** и Федеральное агентство правительственной связи и информации при Президенте Российской Федерации **(ФАПСИ)** (согласно Указу президента РФ от 11 марта 2003 года № 308, «О мерах по совершенствованию государственного управления в области безопасности Российской Федерации» все обязанности ФАПСИ были распределены между Федеральной службой охраны (ФСО) России, Федеральной службой безопасности (ФСБ) России, Службой внешней разведки (СВР) России и Службой специальной связи и информации при Федеральной службе охраны Российской Федерации).

Лицензия на право деятельности по защите информации (далее-лицензия) выдается предприятию государственным органом по лицензированию по представлению органа государственной власти Российской Федерации на конкретные виды деятельности на три года, по истечении которых осуществляется ее перерегистрация в порядке, установленном для

выдачи лицензии.

Лицензия выдается подавшему заявку на ее получение предприятию-заявителю, располагающему производственной и испытательной базой, нормативной и методической документацией, научным и инженерно-техническим персоналом, при условии их соответствия требованиям государственного органа по лицензированию на основании результатов экспертизы деятельности предприятия по заявленному направлению работ. С этими требованиями заявитель имеет право ознакомиться в государственном органе по лицензированию.

Для получения лицензии представляются: заявление; представление органа государственной власти Российской Федерации; материалы экспертизы, подтверждающие наличие необходимых условий для проведения работ по заявленным видам деятельности, а также профессиональную пригодность руководителя предприятия-заявителя или лиц, уполномоченных им для руководства лицензируемой деятельностью; копии документов о государственной регистрации предпринимательской деятельности и устава предприятия.

Отказ в выдаче лицензии производится в случаях, если [7]:

– отсутствуют необходимые условия для проведения работ по заявленному виду деятельности;

– профессиональная подготовка руководителя предприятия-заявителя или лиц, уполномоченных им для руководства лицензируемой деятельностью, не соответствует установленным требованиям;

– в представленных для получения лицензии документах указаны недостоверные сведения;

– заявитель в установленном законом порядке признан виновным в недобросовестной конкуренции в лицензируемой деятельности.

4.4.10. Сертификация средств защиты информации

Сертификации в системе сертификации ФСТЭК России подлежат [8]:

– средства противодействия иностранным техническим разведкам, а также средства контроля эффективности противодействия иностранным техническим разведкам;

– средства технической защиты информации, включая средства, в которых они реализованы, а также средства контроля эффективности технической защиты информации;

– средства обеспечения безопасности информационных технологий, включая защищенные средства обработки информации.

Сертификация средств защиты информации иностранного производства, в отношении которых нормативными правовыми актами Российской Федерации установлены ограничения или запреты на их использование в Российской Федерации, в системе сертификации ФСТЭК

России не осуществляется.

Сертификация средств защиты информации осуществляется на соответствие требованиям по безопасности информации, установленным нормативными правовыми актами ФСТЭК России, а также техническими условиями, техническим заданием, заданием по безопасности, согласованными заявителями на сертификацию с ФСТЭК России.

Участниками системы сертификации ФСТЭК России являются:

– федеральный орган по сертификации;

– организации, аккредитованные ФСТЭК России в качестве органа по сертификации;

– организации, аккредитованные ФСТЭК России в качестве испытательной лаборатории;

– изготовители средств защиты информации.

ФСТЭК России в соответствии с подпунктами 13 и 13.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, организует проведение сертификации средств защиты информации, разрабатывает и устанавливает в пределах своей компетенции требования по безопасности информации к средствам защиты информации, а также в соответствии с Положением о сертификации средств защиты информации, утвержденным постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608, выполняет функции федерального органа по сертификации.

Органы по сертификации осуществляют сертификацию средств защиты информации, оформляют сертификаты соответствия средств защиты информации требованиям по безопасности.

Испытательные лаборатории проводят сертификационные испытания средств защиты информации и по их результатам оформляют технические заключения и протоколы. Испытательные лаборатории должны обеспечивать полноту сертификационных испытаний средств защиты информации и достоверность их результатов.

Изготовители разрабатывают и (или) производят средства защиты информации в соответствии с требованиями по безопасности информации.

Изготовители средств защиты информации, составляющей государственную тайну, должны иметь лицензию ФСТЭК России на проведение работ, связанных с созданием средств защиты информации, составляющей государственную тайну.

Сертификация средств защиты информации осуществляется по следующим схемам:

– для единичного образца средства защиты информации – проведение испытаний образца средства защиты информации и проверки организации его технической поддержки;

– для партии средства защиты информации – проведение испытаний выборки образцов средства защиты информации и проверки организации его технической поддержки;

– для серийного производства средства защиты информации – проведение испытаний выборки образцов средства защиты информации и проверки организации его производства и технической поддержки.

Сертификация единичного образца или партии средства защиты информации организуется заявителем, планирующим применять средство защиты информации, в случае, если отсутствуют идентичные серийно производимые сертифицированные средства защиты информации.

Сертификация серийного производства средства защиты информации организуется заявителем, осуществляющим разработку и (или) производство средства защиты информации.

Срок действия сертификата соответствия не может превышать 5 лет.

Контрольные вопросы:

1. Дайте определение понятия «информация».
2. Дайте определение источников и каналов утечки информации.
3. Приведите классификацию технических каналов утечки информации.
4. Назовите основные объекты защиты информации.
5. Что называют основными техническими средствами и системами?
6. Что называют вспомогательными техническими средствами и системами?
7. Перечислите основные причины утечки информации.
8. Дайте определение Зоны 1 и Зоны 2.
9. Охарактеризуйте виды технической разведки.
10. Приведите классификацию методов и средств защиты информации.
11. Приведите классификацию демаскирующих признаков электронных устройств перехвата информации.
12. Лицензирование в области защиты информации – это…
13. Аттестование объекта в защищенном исполнении – это…
14. Сертификации в системе сертификации ФСТЭК России подлежат…
15. Срок действия сертификата соответствия не может превышать…

Литература к главе 4

1. Об информации, информационных технологиях и о защите информации : федеральный закон от 27.07.2006 № 149-ФЗ. – URL:

http://www.consultant.ru/document/cons_doc_LAW_61798 (дата обращения: 13.05.2022). – Текст : электронный.

2. Хорев, А. А. Техническая защита информации : учебное пособие для студентов высших учебных заведений, обучающихся по специальностям в области информационной безопасности : в 3 т. / А. А. Хорев ; М-во образования и науки Российской Федерации, Федеральное агентство по образованию, Московский гос. ин-т электронной техники (технический ун-т). – Москва : НПЦ «Аналитика», 2008. – Текст : непосредственный.

3. Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента Российской Федерации от 05.12.2016 № 646. – URL: https://mvd.consultant.ru/documents/1056046 (дата обращения: 13.05.2022). – Текст : электронный.

4. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). – Москва : Гостехкомиссия России, 2002. – 80 с. – Текст : непосредственный.

5. Меньшаков, Ю. К. Теоретические основы технических разведок : учеб. издание / Ю. К. Меньшаков. – Москва : ИПЦ «Маска», 2017. – 572 с. – Текст : непосредственный.

6. Лукин, А. Н**.** Распространение радиоволн : учебно-методическое пособие / А. Н. Лукин, Е. А. Москалева, С. Л. Анисимов. – Воронеж : Воронежский институт МВД России, 2016. – 100 с. – Текст : непосредственный.

7. О лицензировании деятельности по технической защите конфиденциальной информации : постановление Правительства Российской Федерации от 3 февраля 2012г. № 79. – URL: https://fstec.ru/litsenzionnaya-deyatelnost/tekhnicheskaya-zashchita-informatsii/75-postanovleniya/225-postanovlenie-pravitelstva-rossijskoj-federatsii-ot-3-fevralya-2012-g-n-79 (дата обращения: 13.05.2022). – Текст : электронный.

8. Положение о системе сертификации средств защиты информации: приказ ФСТЭК России от 3 апреля 2018 г. № 55. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/119-polozheniya/1594-polozhenie-utverzhdeno-prikazom-fstek-rossii-ot-3-aprelya-2018-g-n-55 (дата обращения: 13.05.2022). – Текст : электронный.

Глава 5. Основы криптографической защиты информации

5.1. Криптография и криптоанализ

5.1.1. Требования к защите информации

В переводе с греческого языка слово *криптография* означает тайнопись. Смысл этого термина выражает основное предназначение криптографии – защитить или сохранить в тайне необходимую информацию.

Криптография дает средства для защиты информации, и поэтому она является частью деятельности по обеспечению безопасности информации.

Существуют различные методы *защиты информации*:

1. Физическое ограничение доступа к информации (путем хранения ее в надежном сейфе или строго охраняемом помещении. При хранении информации такой метод удобен, однако при ее передаче приходится использовать другие средства.)

2. Применение различных методов сокрытия информации:

– скрытие канала передачи информации (используя нестандартный способ передачи сообщений);

– маскировка канала передачи закрытой информации в открытом канале связи (применение тех или других стеганографических способов либо обмен открытыми сообщениями, смысл которых согласован заранее);

– существенное затруднение возможности перехвата противником передаваемых сообщений, использованием специальных методов передачи по широкополосным каналам, сигналов под уровнем шумов, либо с использованием «прыгающих» несущих частот и т.п.

В отличие от перечисленных методов криптография не «прячет» передаваемые сообщения, а преобразует их в форму, недоступную для понимания противником.

Помимо сокрытия существуют и другие проблемы защиты передаваемой информации. Например, при полностью открытом информационном обмене возникает проблема достоверности полученной информации. Для ее решения необходимо обеспечить:

– проверку и подтверждение подлинности содержания и источника сообщения;

– предотвращение и обнаружение обмана и других умышленных нарушений со стороны самих участников информационного обмена.

Для решения этой проблемы обычные средства, применяемые при построении систем передачи информации, подходят далеко не всегда. Именно криптография дает средства для обнаружения обмана в виде подлога или отказа от ранее совершенных действий, а также других неправомерных действий.

Поэтому можно сказать, что современная *криптография* является

областью знаний, связанной с обеспечением таких **требований к безопасности информации, как** [1]**:**

– конфиденциальность,

– целостность,

– аутентификация,

– невозможность отказа сторон от авторства.

5.1.2. Оценка возможностей противоборствующей стороны

При этом обычно исходят из предположения о полном контроле противником канала связи. Это означает, что противник может не только пассивно перехватывать передаваемые сообщения для последующего их анализа, но и активно изменять их, а также отправлять поддельные сообщения от имени одного из абонентов.

Обеспечение **конфиденциальности** – решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней. В зависимости от контекста вместо термина «конфиденциальная» информация могут выступать термины «секретная», «частная», «ограниченного доступа» информация.

Обеспечение **целостности** – гарантирование невозможности несанкционированного изменения информации. Для гарантии целостности необходим простой и надежный критерий обнаружения любых манипуляций с данными. Манипуляции с данными включают вставку, удаление и замену.

Обеспечение **аутентификации –** разработка методов подтверждения подлинности сторон (идентификация) и самой информации в процессе информационного взаимодействия. Информация, передаваемая по каналу связи, должна быть аутентифицирована по источнику, времени создания, содержанию данных, времени пересылки и т.д.

Обеспечение **невозможности отказа от авторства** – предотвращение возможности отказа субъектов от некоторых из совершенных ими действий [1].

Методология разработки и анализа средств защиты

Не существует единого шифра, подходящего для всех случаев жизни. Выбор способа шифрования (то есть криптографического алгоритма и режима его использования) зависит от особенностей передаваемой *информации* (ее ценности, объема, способа представления, необходимой скорости передачи и т.д.), а также возможностей владельцев по защите своей информации (стоимость применяемых технических устройств, удобство использования, надежность функционирования и т.п.). Имеется большое разнообразие *видов* защищаемой информации: текстовая, телефонная, телевизионная, компьютерная и т.д., причем у каждого вида информации имеются свои существенные особенности, которые надо

учитывать при выборе способа шифрования. Большое значение имеют объемы и требуемая скорость передачи шифрованной информации, а также помехозащищенность используемого канала связи. Все это существенным образом влияет на выбор криптографического алгоритма и организацию защищенной связи.

Наличие надежного криптографического алгоритма и правильный выбор режима еще не гарантируют владельцу защищенность передаваемой информации. Немаловажную роль играет правильность их использования. Поскольку даже самые стойкие шифры при неправильном использовании существенно теряют свои качества, то конфиденциальность передаваемой информации во многом зависит от того, какие *ошибки* допускает ее владелец при использовании криптографической защиты. А то, что все пользователи допускают ошибки, – неизбежно и является непреложным и важным (для криптоаналитика) фактом, поскольку любые криптографические средства, какими бы они ни были удобными и прозрачными, всегда мешают пользователям в работе, а различные тонкости известны только криптоаналитикам и, как правило, непонятны пользователям этих средств. Более того, в качестве субъектов взаимодействия могут выступать не только люди, но и различные процессы, осуществляющие обработку информации в автоматизированной системе без участия человека. Поэтому защищенность информации в системе существенно зависит от того, насколько правильно там реализована криптографическая подсистема, отвечающая за выполнение криптографических функций. Одно наличие такой подсистемы еще ничего не гарантирует.

При разработке и анализе средств защиты информации необходимо учитывать следующие факторы [1]:

1. Формы представления информации (документальная, речевая и телекоммуникационная);
2. Степень конфиденциальности (ценность) передаваемой информации;
3. Время, в течение которого информация должна сохранять конфиденциальность;
4. Наличие средств защиты информации необходимой стойкости шифрования (засекречивания);
5. Оценка возможностей противоборствующей стороны по перехвату, дешифрованию, имитации (навязыванию) ложной информации.

В зависимости от своей физической природы информация может быть представлена в документальной, речевой и телекоммуникационной форме.

В документальной форме информация передается в случае необходимости документирования тех или иных действий (приказы, распоряжения, директивы и т.п.).

Обмен информацией в речевой форме осуществляется, как правило, в реальном масштабе времени при необходимости обеспечения высокой оперативности передачи информации.

В телекоммуникационной форме информация передается с использованием технических средств связи и телекоммуникационных систем. В этом случае возможно обеспечение документирования и высокой оперативности передачи информации.

Степень конфиденциальности (ценность) передаваемой информации оценивается пользователем (или исполнителем) в случае частной информации или ведомственными приказами, инструкциями, наставлениями в случае государственных структур.

В ряде случаев информация имеет конфиденциальный характер лишь в течение небольшого промежутка времени:

– передача команд боевого управления небольшим подразделениям в скоротечных боевых действиях;

– передача команд группам задержания подразделений вневедомственной охраны;

– управление средствами огневого поражения противника (пуски ракет, целеуказания авиации, артиллерии) и др.

Часто информация сохраняет конфиденциальность в течение длительного периода времени, иногда – в течение нескольких десятков лет:

– передача документов, приказов, директив и т.п., определяющих стратегические планы управления войсками;

– дипломатическая переписка;

– деятельность органов внутренней и внешней разведки страны и др.

Необходима оценка временного фактора и с точки зрения оперативности передачи информации.

При необходимости передачи информации в реальном масштабе времени целесообразно использовать технические средства с обеспечением автоматического закрытия информации.

В случае, если в высокой оперативности нет необходимости, целесообразно использовать методы предварительного шифрования информации без применения технических средств автоматического ее закрытия.

В зависимости от перечисленных временных факторов, формы представления информации и степени конфиденциальности определяются средства ее защиты.

Поскольку применение криптографических методов защиты информации связано с рядом организационных и технических сложностей, обусловленных в первую очередь необходимостью использования ключей шифрования и расшифрования, то в первую очередь целесообразно оценить возможность применения некриптографических методов и средств

защиты, перечисленных выше и обеспечивающих сокрытие факта передачи информации.

Существуют многочисленные способы скрытия самого факта переписки или самого факта передачи сообщения. Это относится как к переписке по почте, так и к общению с помощью технических средств связи (использование заранее установленных кодовых фраз при обмене речевой информацией, применение систем широкополосных сигналов (ШПС), псевдослучайной перестройки рабочей частоты (ППРЧ), узконаправленных систем передачи информации и др.). Методами скрытия самого факта передачи сообщения занимается стеганография (от греческих слов «stege» – «крыша» и «grapho» – «пишу»).

Однако такие методы не всегда в достаточной степени могут обеспечить выполнение заданных требований к защите информации.

Для повышения безопасности все стеганографические способы скрытия информации, как правило, сочетаются с криптографическими способами закрытия информации.

При передаче информации высокой степени конфиденциальности, не требующей высокой оперативности управления, но требующей высокой стойкости к вскрытию этой информации противоборствующей стороной, целесообразно использовать системы предварительного шифрования и передачу информации в зашифрованном виде по специальным каналам: фельдъегерско-почтовой связи, дипломатической почты и т.п., не требующим применения дорогостоящей аппаратуры автоматического закрытия.

При передаче информации в реальном масштабе времени (в речевом или телекоммуникационном виде) без применения аппаратуры автоматического закрытия не обойтись.

Однако в ряде случаев возможно использование стенографических методов сокрытия самого факта передачи информации, в некоторых случаях (например, когда информация имеет конфиденциальный характер лишь в течение небольшого промежутка времени и степень конфиденциальности этой информации невысока) возможно использование простейших устройств защиты (например, маскираторов речи или аппаратуры автоматического закрытия информации, обеспечивающей временную стойкость к вскрытию).

В других случаях, требующих обеспечения высокой степени конфиденциальности, стойкости к вскрытию и выполнения перечисленных выше требований к защите информации, необходимо применение сложных технических средств криптографической защиты с выполнением организационных и технических мероприятий по формированию, размножению, учету, хранению и распределению ключей.

При оценке возможностей противоборствующей стороны, как было отмечено ранее, обычно исходят из предположения о полном контроле

противником канала связи. Это означает, что противник может не только пассивно перехватывать передаваемые сообщения для последующего их анализа, но и активно изменять их, а также отправлять поддельные сообщения от имени одного из абонентов.

5.1.3. Классические модели защиты информации

Традиционной задачей криптографии является проблема обеспечения конфиденциальности информации при передаче сообщений по контролируемому противником каналу связи. В простейшем случае эта задача описывается взаимодействием трех субъектов (сторон). Владелец информации, называемый обычно *отправителем*, осуществляет преобразование исходной (*открытой*) информации (сам процесс преобразования называется *шифрованием*) в форму передаваемых *получателю* по открытому каналу связи шифрованных сообщений с целью ее защиты от противника (рис. 5.1.1).

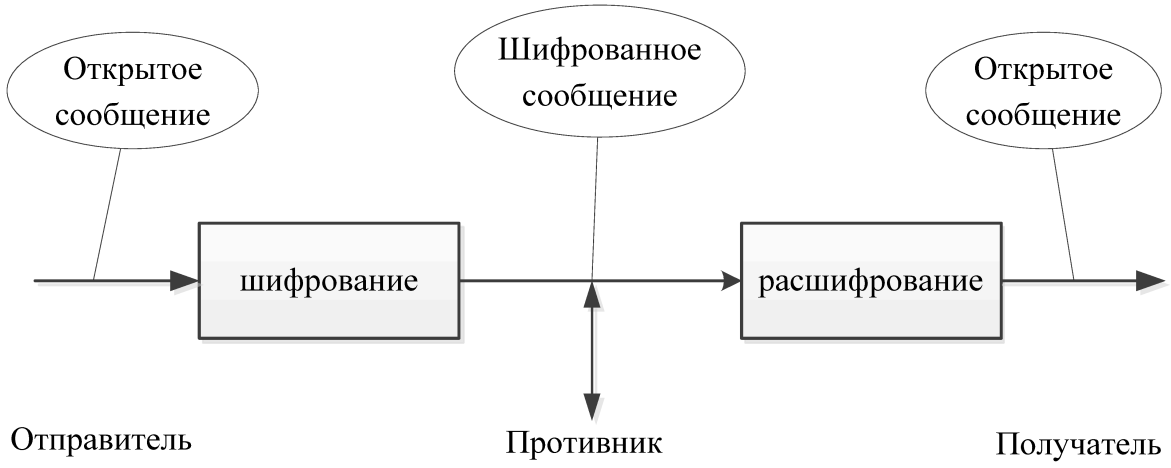


Рис. 5.1.1. Передача шифрованной информации

Под противником понимается любой субъект, не имеющий права ознакомления с содержанием передаваемой информации [2]. В качестве противника может выступать *криптоаналитик*, владеющий методами раскрытия шифров. Законный получатель информации осуществляет *расшифрование* полученных сообщений. Противник пытается овладеть защищаемой информацией (его действия обычно называют *атаками*). При этом он может совершать как пассивные, так и активные действия. *Пассивные* атаки связаны с прослушиванием, анализом трафика, перехватом, записью передаваемых шифрованных сообщений, *дешифрованием*, то есть попытками «взломать» защиту с целью овладения информацией.

При проведении *активных* атак противник может прерывать процесс

передачи сообщений, создавать поддельные (сфабрикованные) или модифицировать передаваемые шифрованные сообщения. Эти активные действия называют попытками *имитации* и *подмены* соответственно.

Различают *симметричные* и *асимметричные* криптосистемы. В симметричных системах знание ключа зашифрования k_1 позволяет легко найти ключ расшифрования k_2 (в большинстве случаев эти ключи просто совпадают). В асимметричных криптосистемах знание ключа k_1, не позволяет определить ключ k_2. Поэтому для симметричных криптосистем оба ключа должны сохраняться в секрете, а для асимметричных – только один – ключ расшифрования k_2, а ключ k_1 можно сделать открытым (общедоступным). В связи с этим их называют еще *шифрами с открытым ключом* [2].

Симметричные криптосистемы принято подразделять на *поточные* и *блочные* системы. Поточные системы осуществляют зашифрование отдельных символов открытого сообщения. Блочные же системы производят зашифрование блоков фиксированной длины, составленных из подряд идущих символов сообщения.

Асимметричные криптосистемы, как правило, являются блочными. При их использовании можно легко организовать передачу конфиденциальной информации в сети с большим числом пользователей. В самом деле, для того чтобы послать сообщение, отправитель открыто связывается с получателем, который либо передает свой ключ отправителю, либо помещает его на общедоступный сервер. Отправитель зашифровывает сообщение на открытом ключе получателя и отправляет его получателю. При этом никто, кроме получателя, обладающего ключом расшифрования, не сможет ознакомиться с содержанием передаваемой информации. В результате такая система шифрования с общедоступным ключом позволяет существенно сократить объем хранимой каждым абонентом секретной ключевой информации.

5.1.4. Методы криптоанализа потоковых шифров

Рассмотрим некоторые методы анализа потоковых шифрсистем на примере наиболее стойких из них – шифров гаммирования.

Условно структуру шифрсистемы гаммирования можно представить состоящей из двух частей (узлов): узел управления (формирования ШГ) и узел, обеспечивающий собственно зашифрование. В двоичном случае управляющая (шифрующая) гамма представляет собой случайную последовательность «0» и «1», а узел зашифрования (как и узел расшифрования) – сумматор по модулю 2 (М2).

Требования к управляющему блоку:

– период управляющей гаммы должен превышать максимально возможную длину открытых сообщений, подлежащих шифрованию;

– статистические свойства управляющей гаммы должны

приближаться к свойствам случайной равновероятной последовательности;

– в управляющей гамме должны отсутствовать простые аналитические зависимости между близко расположенными знаками;

– криптографический алгоритм получения знаков управляющей гаммы должен обеспечивать высокую сложность определения секретного ключа.

Требование к шифрующему блоку:

– применение алгоритма шифрования должно носить универсальный характер и не зависеть от вида шифруемой информации.

Иногда выдвигается дополнительное требование:

– способ построения шифрующего блока должен обеспечивать криптографическую стойкость шифра при перекрытиях управляющей гаммы, в частности при повторном использовании ключей.

Заметим, что выполнение перечисленных требований является необходимым, но не достаточным условием криптографической стойкости потокового шифра.

Таким образом, необходимым условием обеспечения высокой криптографической стойкости таких шифров является обеспечение высоких криптографических свойств шифрующей гаммы, в частности равновероятность (случайность) и взаимная независимость ее элементов. Обеспечить выполнение таких требований достаточно сложно. Ведь только чисто физические датчики способны формировать чисто случайные числовые последовательности. Применение таких датчиков на практике весьма проблематично либо из-за их больших массогабаритных характеристик, низкой скорости работы, либо с точки зрения их безопасности для обслуживающего персонала и по другим причинам. Поэтому для формирования шифрующих гамм используют так называемые датчики псевдослучайных чисел, например, на основе линейных рекуррентных регистров (ЛРР). Такие регистры формируют линейные рекуррентные последовательности (ЛРП), обладающие рядом как положительных, так и отрицательных качеств.

В частности, положительным качеством ЛРП является равновероятность ее элементов. Например, в двоичной последовательности нулей и единиц максимальной длины, сформированной соответствующим ЛРР, единиц на одну больше, чем нулей. При большой длине ее периода это будет соответствовать примерно одинаковым вероятностям их появления $P(0) = P(1) = 0{,}5$.

С другой стороны, известно, что ЛРП имеет период, для двоичного случая его величина определяется выражением

$$n = 2^m - 1,$$

где n – длина периода ЛРП, m – число элементов памяти регистра сдвига с обратными связями – ЛРР.

Известно также, что, зная 2m элементов последовательности, сформированной таким ЛРР, можно легко определить не только все элементы этой последовательности, но и структуру ЛРР, при помощи которого она сформирована. Поэтому в чистом виде такие последовательности использовать в качестве шифрующих гамм нельзя. Для их усложнения используют специальные устройства (узлы усложнения ШГ), обеспечивающие выполнение приведенных выше требований.

При криптоанализе потоковых шифров гаммирования используют два подхода: **статистический и аналитический.**

В первую очередь, необходимо исследовать вероятностные **(статистические)** характеристики гаммы. Как мы уже знаем, имеются подходы к получению оценок вероятностей элементов неравновероятной гаммы по шифртексту, которые можно использовать при бесключевом чтении.

Второй подход **(аналитический)** связан с попытками *линеаризации* уравнений гаммообразования, то есть сведения задачи нахождения ключей криптографических алгоритмов к решению некоторой системы линейных уравнений.

При таком подходе определяющую роль играет линейная сложность исследуемых последовательностей. Значение линейной сложности определяет размеры системы линейных уравнений, которую надо решить для определения ключа по известной шифрующей гамме. Поэтому линейная сложность определяет эффективность криптоатаки на основе известного открытого текста для шифров гаммирования в классе методов линеаризации. Это обусловливает актуальность разработки методов построения псевдослучайных последовательностей с высокой линейной сложностью.

К вопросу о статистических зависимостях в шифрующей гамме примыкают методы анализа, основанные на наличии у функции усложнения хороших приближений в классе линейных функций. Примером отображений, не имеющих линейных статистических аналогов хорошего качества, является класс бент-функций.

В случае наличия у функции усложнения линейного приближения криптоаналитик может заменить исследуемую схему схемой с линейной функцией усложнения. Если усложнению подвергалась линейная рекуррентная последовательность, то при такой замене результирующая гамма является суммой линейной рекурренты и некоторой случайной последовательности с «завышенной» вероятностью появления нуля. Тем самым задача сводится фактически к возможности определения ключа по «искаженному» выходу линейного регистра сдвига. Если число искажений невелико, то их появление не оказывает существенного влияния на сложность определения ключа.

Отметим, что функция усложнения может обеспечивать высокий уровень линейной сложности и хорошие статистические качества результирующей гаммы (например, равновероятность появления ее элементов), но при этом она может иметь приближение в классе линейных функций с большой вероятностью совпадения значений, что сводит на нет перечисленные положительные качества.

При оценке криптографических качеств потоковых шифров, помимо **алгебраических и статистических** свойств шифрующей гаммы, необходимо учитывать также наличие между знаками гаммы зависимостей **комбинаторного** характера. Например, при использовании в качестве гаммы линейной рекуррентной последовательности с малым числом ненулевых коэффициентов в законе рекурсии может иметь место ситуация, когда значительное число знаков гаммы зависит лишь от небольшого числа знаков ключа. Если такая ситуация имеет место, то криптоаналитик получает возможность проверки гипотез о значениях части ключа, основываясь на статистических свойствах открытых сообщений, что является несомненной слабостью соответствующего алгоритма шифрования.

Таким образом, при создании криптографически стойких потоковых шифрсистем необходимо учитывать возможности применения криптоаналитиком всей совокупности **статистических, аналитических и комбинаторных свойств** используемых преобразований. При этом дополнительные трудности создают постоянно возрастающие возможности вычислительной техники, позволяющие провести экспериментальные исследования тех характеристик потоковых шифров, которые не удается изучить теоретически.

В целом же вывод о криптографической стойкости конкретного шифра может быть сделан только на основе его комплексных исследований, проведенных с привлечением квалифицированных специалистов-криптографов [2].

Особенности криптоанализа блоковых шифров.

Базовым при использовании блоковых шифров является режим простой замены. В связи с этим рассмотрим ряд вопросов, связанных с эксплуатацией блоковых шифров в этом режиме и влияющих на их криптографическую стойкость.

Как отмечалось выше, **серьезным недостатком режима простой замены** является то, что зашифрование одинаковых блоков исходного текста дает идентичные блоки шифртекста. В результате криптоаналитик лишь на основе шифрованных данных может делать выводы о свойствах исходного текста. Примером таких выводов может служить определение факта рассылки писем с одинаковым содержанием в несколько адресов. Если некоторые блоки открытого текста повторились, то во всех зашифрованных сообщениях, независимо от используемых ключей, на

одинаковых местах будут встречаться повторяющиеся блоки шифрованных текстов.

Другой пример – передача ключей в зашифрованном виде по линиям связи. Повторение блоков в одном шифрованном тексте показывает, что часть битов в передаваемом ключе повторились и что в дальнейшем трудоемкость перебора ключей при их тотальном опробовании может быть сокращена за счет учета повторений.

Показательно, что при случайном выборе блоков открытого текста их повторение является не столь уж редким событием. Напомним известный *парадокс «дней рождений»*, который заключается в том, что если имеется выборка объема, сравнимого с $\sqrt{N}$, из множества из N элементов, то вероятность того, что в ней окажутся два одинаковых элемента, сравнима с 1/2. Этот парадокс показывает, что при случайном выборе блоков открытого текста для получения повтора достаточно взять в среднем порядка $\sqrt{N}$ блоков, где N – общее число блоков, которые теоретически могут встретиться в открытом тексте. Применительно к алгоритмам DES и ГОСТ, которые оперируют с двоичными векторами длины 64, это означает, что в среднем, уже среди 2^{32} блоков открытого текста, будут встречаться повторяющиеся. Следует отметить, что при шифровании осмысленных текстов на естественных языках повторения будут появляться еще чаще, поскольку в осмысленных текстах в силу используемой лексики и грамматических правил встречаются далеко не все сочетания букв и знаков алфавита.

К блоковым шифрам, используемым в режиме простой замены, могут быть применены и некоторые методы анализа шифров простой замены в обычных алфавитах. В частности, при достаточно большой длине шифртекста можно применять **методы анализа, использующие статистические характеристики открытых текстов**. Например, вычисляя частоты появления блоков в шифрованном тексте и проводя опробование часто повторяющихся блоков, начиная с наиболее вероятных сочетаний знаков в открытом тексте, можно составить словарь соответствия между блоками открытого и шифрованного текстов. Далее, развивая текст по смыслу с учетом избыточности открытых текстов, найденные блоки открытого текста можно дополнять соседними блоками. При этом одновременно восстанавливается открытый текст и дополняется словарь соответствия. Этот метод эффективен, когда наблюдается стандартность переписки. Например, всегда стандартны заголовки деловых бумаг, юридических и прочих документов.

Еще одна слабость блоковых шифров в режиме простой замены при шифровании осмысленных текстов связана с тем фактом, что в открытом тексте могут появляться не все сочетания знаков, что проявляется в фактическом сокращении числа используемых соответствий между

блоками открытого и шифрованного текстов. Однако эта слабость легко устранима, если перед шифрованием применить к открытому тексту процедуру сжатия информации, например, использовать стандартные алгоритмы архивации данных.

Следующим моментом, на который следует обратить внимание, является проблема последнего неполного блока данных при шифровании текстов, длины которых не кратны размеру блока. При использовании блокового шифра этот неполный блок должен быть каким-либо образом дополнен до стандартной длины. Если при этом алгоритм дополнения выбран неудачно, например, блок дополняется одними нулями, то при определении соответствующего блока открытого текста у криптоаналитика появляются дополнительные возможности. Эта проблема может показаться надуманной, поскольку относится только к последнему блоку сообщения. Однако именно в конце сообщения обычно ставится подпись, и, следовательно, появляются подходы к определению по шифртексту авторства сообщения.

Отдельно остановимся на методах анализа криптографических алгоритмов, основанных на принципе многократного использования блоковых шифров. Р. Меркль и М. Хеллман на примере DES показали, как, используя *метод встречи посередине*, можно вскрыть схему двукратного шифрования.

Рассмотрим метод вскрытия блокового шифра при использовании двойного шифрования в общем случае.

Предположим, что известны блок M открытого текста и соответствующий ему блок C шифрованного текста. Алгоритм вскрытия неизвестных ключей k_1 и k_2 состоит из двух этапов.

На первом этапе перебираются все возможные варианты ключа k_1. Для каждого варианта k ключа k_1 вычисляются значения $ADR(k) = E_k(M)$, после чего значения k помещаются в память по адресу $ADR(k)$.

На втором этапе опробуются возможные варианты ключа k_2. Для опробуемого варианта k' ключа k_2 вычисляются значения $ADR(k') = D_{k'}(C)$ и производится обращение в память по адресу $ADR(k')$. Если по этому адресу памяти записи отсутствуют, то происходит переход к опробованию следующего варианта k' ключа k_2. Если же по адресу $ADR(k')$ в памяти хранится ключ k, то образуется допустимая пара ключей (k, k'), удовлетворяющая равенству $C = E_{k'}(E_k(M))$.

Заметим, что в ячейку памяти с номером $ADR(k')$ могут попасть несколько вариантов ключа k (для этого память необходимо соответствующим образом организовать). Для каждого из них пара (k, k') является допустимым ключом.

Несложно заметить, что для реализации данного алгоритма требуется $2|K|$ опробований и столько же операций обращения к памяти,

где $|K|$ — общее число ключей шифра. Таким образом, вместо $|K|^2$ операций, требуемых при полном переборе ключей, затраты метода встречи посередине составляют порядка $4|K|$ операций (операции опробования и обращения к памяти для простоты считают приблизительно равносильными по сложности). Заметим, что такой резкий эффект снижения трудоемкости достигается за счет использования большой (и специальным образом организованной) памяти.

Кроме перебора ключей и метода встречи посередине, при исследованиях блоковых шифров успешно применяются методы *линейного и дифференциального анализа*.

Идея метода линейного анализа состоит в *линеаризации* уравнений шифрования, то есть замене сложных преобразований, описывающих алгоритм шифрования, их приближениями в классе линейных функций. Под приближением в классе линейных функций (или *линейным аналогом*) понимается линейная функция, значения которой для достаточно большого числа наборов аргументов совпадают со значениями данной функции шифрования. Чем выше вероятность совпадения значений линейного аналога со значениями функции шифрования при случайном и равновероятном выборе аргументов, тем лучше качество аналога.

Таким образом, линейный анализ сводит задачу определения ключей к решению системы линейных уравнений, в которой правые части уравнений известны с некоторой вероятностью. Из общих принципов математической статистики вытекает, что если распределение значений правых частей уравнений системы отлично от равномерного распределения, и имеется достаточно большое число уравнений, то решение такой системы линейных уравнений может быть найдено статистическими методами.

Блоковые шифры строятся, как правило, по итеративному принципу. Поэтому даже использование на каждой итерации функций, не имеющих хороших аналогов, не гарантирует отсутствия аналогов в результирующем преобразовании. Проблема построения блоковых шифров, для которых удается доказать отсутствие линейных аналогов, является весьма сложной задачей современной прикладной криптографии.

Методы дифференциального (или иначе, разностного) анализа строятся в предположении, что криптоаналитик имеет для анализа несколько текстов, зашифрованных на одном ключе, и дополнительно предполагается известной информация о том, как различаются между собой открытые тексты (при этом сами открытые тексты могут быть неизвестны). В этом случае криптоаналитик получает информацию о том, как заданные отличия в открытых текстах проявляются в шифртекстах, или, другими словами, как разность аргументов шифрующего преобразования отражается на изменении его значений. Поскольку шифрующее преобразование

однозначно определяется ключом, то информация о зависимостях между разностями значений аргументов и разностями соответствующих значений функции шифрования может быть использована при построении алгебраических и статистических методов вскрытия ключей алгоритма шифрования.

Заметим, что аналогичная ситуация возникает в случае, когда криптоаналитику удается получить результат зашифрования некоторого сообщения на разных ключах с дополнительной информацией о различиях использованных ключей. В ряде работ некоторые разновидности такого подхода, получившие название *метода дифференциальных искажений*, применялись для вскрытия ключей криптографических алгоритмов, использовавшихся для защиты информации в платежных системах на основе интеллектуальных карт [3].

5.2. Алгоритмы симметричного и асимметричного шифрования

5.2.1. Модели шифров. Ключевая система шифра

Под *шифром* обычно понимается семейство обратимых преобразований, каждое из которых определяется некоторым параметром, называемым ключом, а также порядком применения данного преобразования, называемым *режимом шифрования* [1].

Ключ — это важнейший компонент шифра, отвечающий за выбор преобразования, применяемого для зашифрования конкретного сообщения. Обычно ключ представляет собой некоторую буквенную или числовую последовательность. Эта последовательность как бы «настраивает» алгоритм шифрования.

Каждое преобразование однозначно определяется ключом и описывается некоторым *криптографическим алгоритмом*. Один и тот же криптографический алгоритм может применяться для шифрования в различных режимах. Тем самым реализуются различные способы шифрования (простая замена, гаммирование и т.п.). Каждый режим шифрования имеет как свои преимущества, так и недостатки. Поэтому выбор режима зависит от конкретной ситуации. При расшифровании используется криптографический алгоритм, который в общем случае может отличаться от алгоритма, применяемого для зашифрования сообщения. Соответственно могут различаться ключи зашифрования и расшифрования. Пару алгоритмов зашифрования и расшифрования обычно называют *криптосистемой* (*шифрсистемой*), а реализующие их устройства – *шифртехникой*.

Если обозначить через M открытое, а через C шифрованное сообщения, то процессы зашифрования и расшифрования можно записать в виде равенств

$E_{k_1}(M) = C$,

$D_{k_2}(C) = M$,

в которых алгоритмы зашифрования E и расшифрования D должны удовлетворять равенству

$D_{k_2}\left(E_{k_1}(M)\right) = M$.

Пусть X, K, Y – конечные множества возможных открытых текстов, ключей и шифрованных текстов соответственно; $E_k : X \to Y$ – правило зашифрования на ключе $k \in K$. Множество $\{E_k : k \in K\}$ обозначим через E, а множество $\{E_k(x) : x \in X\}$ – через $E_k(X)$. Пусть $D_k : E_k(X) \to X$ – правило расшифрования на ключе $k \in K$, и D – это множество $\{D_k : k \in K\}$

Здесь и далее мы будем предполагать, что если $k \in K$ представляется в виде $k = (k_з, k_p)$, где $k_з$ – ключ зашифрования, а k_p – ключ расшифрования (причем $k_з \neq k_p$), то E_k понимается как функция $E_{k_з}$, а D_k – как функция D_{k_p}.

Определение. *Шифром (шифрсистемой) назовем совокупность*

$$\sum_A = (X, K, Y, E, D)$$

введенных множеств, для которых выполняются следующие свойства:

1) *для любых* $x \in X$ и $k \in K$ *выполняется равенство* $D_k\left(E_k(x)\right) = x$;

2) $Y = \bigcup_{k \in K} E_k(X)$.

Неформально, шифр – это совокупность множеств возможных открытых текстов (то, что шифруется), возможных ключей (то, с помощью чего шифруется), возможных шифртекстов (то, во что шифруется), правил зашифрования и правил расшифрования.

Отметим, что условие 1) отвечает требованию однозначности расшифрования. Условие 2) означает, что любой элемент $y \in Y$ может быть представлен в виде $E_k(x)$ для подходящих элементов $x \in X$ и $k \in K$. Отметим также, что в общем случае утверждение «для любых $k \in K$ и $y \in E_k(X)$ выполняется равенство $E_k\left(D_k(y)\right) = y$» является неверным.

Введем теперь вероятностную модель шифра. Следуя К. Шеннону, определим априорные распределения вероятностей $P(X)$, $P(K)$ на множествах X и K соответственно. Тем самым для любого $x \in X$ определена вероятность $p_X(x) \in P(X)$ и для любого $k \in K$ – вероятность $p_K(k) \in P(K)$, причем выполняются равенства

$\sum_{x \in X} p_X(x) = 1$ и $\sum_{k \in K} p_K(k) = 1$.

В тех случаях, когда нам требуется знание распределений $P(X)$ и

$P(K)$, мы будем пользоваться *вероятностной моделью* Σ_B, состоящей из пяти множеств, связанных условиями 1) и 2) определения 1, и двух вероятностных распределений:

$$\Sigma_B = (X, K, Y, E, D, P(X), P(K)) \quad (5.2.1)$$

Вероятностные характеристики шифров используются лишь в *криптоанализе* – разделе криптографии, посвященном решению задач *вскрытия* (или *взлома*) шифров.

В большинстве случаев множества X и Y представляют собой объединения декартовых степеней некоторых множеств A и B соответственно, так что для некоторых натуральных L и L_1.

$$X = \bigcup_{i=1}^{L} A^i, Y = X = \bigcup_{i=1}^{L_1} B^i$$

Множества A и B называют соответственно *алфавитом открытого текста* и *алфавитом шифрованного текста*. Другими словами, открытые и шифрованные тексты записываются привычным образом в виде последовательностей букв [2].

В зависимости от соотношений между ключами k_1 и k_2 различают симметричные и асимметричные криптосистемы.

В **симметричных** криптосистемах знание ключа зашифрования k_1 позволяет легко определить ключ расшифрования k_2 (в большинстве случаев эти ключи совпадают). Поэтому в симметричных криптосистемах оба ключа должны сохраняться в секрете. Данное обстоятельство является одним из основных факторов, ограничивающих практическое применение такого рода криптосистем, поскольку при большом количестве корреспондентов, использующих однотипные криптосистемы, возникает проблема управления секретными ключами, состоящая в реализации процедур генерирования, проверки, учета, хранения и распределения секретных ключей.

Управление секретными ключами осуществляется при помощи систем установки и управления ключами.

Система установки ключей определяет алгоритмы и процедуры генерации, распределения, передачи и проверки ключей.

Система управления ключами определяет порядок использования, смены, хранения, резервирования, восстановления, замены или изъятия из обращения скомпрометированных, а также уничтожения ключей, срок действия которых истек.

Для практического использования такого типа криптосистем необходимо предварительное распределение ключей.

Чтобы использовать эти ключи, необходимо осуществить их первоначальный выбор и установку.

Для генерации ключей могут использоваться различные алгоритмы. Выбранные ключи передаются взаимодействующим сторонам по защищенным каналам связи.

При малом числе корреспондентов эта проблема решается достаточно просто – это либо их личная встреча, либо использование специальных курьеров. При большом числе корреспондентов используется предварительная рассылка большого объема ключевой информации и последующие ее учет, хранение и использование. Поэтому на практике применяют специальные системы предварительного распределения ключей, предусматривающие распределение и хранение не самих ключей, а некоторой меньшей по объему исходной информации, на основе которой в дальнейшем каждая сторона может вычислить ключ для взаимодействия с другой стороной [3].

Система предварительного распределения ключей включает два алгоритма. С помощью первого алгоритма осуществляется генерация исходной информации. Эта информация включает открытую часть, которая передается всем сторонам или размещается на общедоступном сервере, а также секретные части каждой стороны. Второй алгоритм предназначен для вычисления действующего значения ключа по имеющейся у абонентов секретной и общей открытой части исходной ключевой информации.

Система распределения ключей рассматриваемого типа должна учитывать возможность компрометации некоторых ключей и обеспечивать их восстановление путем исключения скомпрометированных и подключения новых абонентов.

Предварительно распределенные ключи могут использоваться для шифрования ключей сеансового взаимодействия.

Для передачи зашифрованных ключей по открытому каналу связи между не доверяющими друг другу абонентами требуется решение комплекса задач по установлению подлинности различных аспектов взаимодействия, начиная от подлинности субъектов взаимодействия, подлинности передаваемых сообщений, подлинности сеанса связи и заканчивая подтверждением аутентичности полученных абонентами ключей.

Для централизованного управления пересылкой ключей создаются специальные доверенные центры, выполняющие функции центров распределения ключей.

В **асимметричных** криптосистемах знание одного ключа k_1 или k_2 не позволяет определить другой ключ k_2 или k_1, соответственно.

Поэтому в секрете можно хранить только один ключ. Другой ключ при этом может быть открытым (общедоступным). В связи с этим асимметричные криптосистемы называют криптосистемами с открытым ключом.

Для того чтобы передать сообщение, отправитель связывается с

получателем по открытому каналу. Получатель создает (генерирует) пару ключей. Один из них делает секретным и оставляет у себя, а другой открытый ключ либо передает отправителю, либо помещает на общедоступный сервер. Отправитель зашифровывает сообщение на открытом ключе получателя и отправляет его по открытому каналу связи. При этом только получатель, обладающий секретным ключом расшифрования, сможет ознакомиться с содержанием передаваемого сообщения. В результате такая система шифрования с общедоступным ключом позволяет существенно сократить объем хранимой каждым абонентом секретной ключевой информации. Возникающая при практической реализации таких криптосистем проблема обеспечения аутентичности открытых ключей решается путем создания доверенной инфраструктуры центров сертификации открытых ключей. Создание такой инфраструктуры значительно проще рассмотренной выше системы предварительного централизованного распределения ключей симметричных криптосистем.

Симметричные криптосистемы в зависимости от способа их практической реализации принято подразделять на потоковые и блоковые. Потоковые системы осуществляют зашифрование отдельных символов (элементов) открытого сообщения последовательно один за другим. В блоковых системах производится зашифрование блоков фиксированной длины, составленных из последовательно передаваемых символов сообщения.

Асимметричные криптосистемы, как правило, являются блоковыми.

Следует отметить некоторые различия приведенных выше понятий в отечественной и зарубежной литературе.

Так, в отечественной литературе, например, в [1], принято считать, что законные пользователи осуществляют процедуры зашифрования/расшифрования с использованием имеющихся у этих пользователей соответствующих ключей. Противник, не имея ключа расшифрования, производит дешифрование перехваченных шифрованных сообщений.

В зарубежной литературе законные пользователи осуществляют процедуры шифрования/дешифрования (incripto/decripto), а противник без ключа производит криптоанализ перехваченных криптограмм.

В дальнейшем по тексту будут использоваться названия процедур, принятые в отечественной литературе.

5.2.2. Основные требования к шифрам

Впервые основные требования к шифрам сформулированы известным криптографом XIX века голландцем Керкгоффсом. Разносторонний ученый, преподававший 6 иностранных языков, историю и математику, он в возрасте 47 лет написал книгу «Военная криптография».

В ней сформулированы 6 конкретных требований к шифрам, два из которых относятся к стойкости шифрования, а остальные – к эксплуатационным качествам. Одно из них («компрометация системы не должна причинять неудобств корреспондентам») стало называться *«правилом Керкгоффса».* Суть этого правила состоит в том, что *стойкость* (или надежность) шифра определяется лишь секретностью ключа. Другими словами, оценка качества шифра (на основе некоторого шифрованного текста) должна проводиться при условии, что о данном шифре известно все, кроме использованного ключа [1].

Во введенных ранее моделях шифров, помимо основных алгебраических (или функциональных) свойств шифров, постулируемых в модели, множества сообщений и ключей наделяются соответствующими априорными вероятностными свойствами, что позволяет формализовать многие постановки задач синтеза и анализа шифров. Так, и сегодня при разработке новых классов шифров широко используется принцип Шеннона *рассеивания и перемешивания,* состоящий в использовании при шифровании многих итераций «рассеивающих» и «перемешивающих» преобразований.

Разработанные К. Шенноном концепции *теоретической* и *практической секретности* (или стойкости) позволяют количественно оценивать криптографические качества шифров и пытаться строить в некотором смысле *идеальные* или *совершенные шифры.* Моделируется также и язык открытых сообщений. А именно, предлагается рассматривать язык как *вероятностный процесс,* который создает дискретную последовательность символов в соответствии с некоторой вероятностной схемой.

Опираясь на концепцию *избыточной информации,* содержащейся в текстовых сообщениях К. Шеннон показал, что успех криптоанализа определяется тем, насколько избыточность, имеющаяся в сообщении, «переносится» в шифрованный текст. Если шифрование «стирает» избыточность, то восстановить текст сообщения по криптограмме становится принципиально невозможно.

Задачу дешифрования К. Шеннон рассматривает как задачу вычисления апостериорных знаний противника о шифре после перехвата криптограммы. Дело в том, что вероятности сообщений и ключей составляют априорные знания противника, которыми он располагает в соответствии с правилом Керкгоффса. После перехвата криптограммы он может (по крайней мере, в принципе, поскольку множества сообщений и ключей *конечны)* вычислить апостериорные вероятности возможных ключей и сообщений, которые могли быть использованы при составлении данной криптограммы. Вот эти вероятности и составляют апостериорные знания противника. С этой точки зрения показателен следующий пример.

Понятие *совершенной секретности* К. Шеннон определяет

требованием, чтобы апостериорные знания противника в точности совпадали бы с априорными знаниями. Он приводит пример *совершенного шифра,* которым является шифр Вернама (со случайной равновероятной гаммой). Следует подчеркнуть, что все рассуждения о стойкости шифров К. Шеннон проводит лишь для одной постановки задачи криптоанализа: когда противник располагает лишь *одной криптограммой* и требуется найти текст сообщения. Для других постановок задач требуются отдельные исследования.

Теоретической мерой секретности (или стойкости) по К. Шеннону является энтропийная характеристика — *неопределенность шифра по открытому сообщению,* которая измеряет (в статистическом смысле), насколько «близка» *средняя* криптограмма из N букв к единственному «решению». Он выводит формулу для приближенного вычисления минимального N, при котором находится единственное «решение». Такая величина получила название *расстояния единственности.* Формула для расстояния единственности связывает между собой неопределенность шифра по открытому тексту и избыточность текста. Чем большим оказывается расстояние единственности, тем более шифр приближается к совершенному шифру, для которого формально расстояние единственности равно ∞.

Наконец, К. Шеннон вводит понятие *рабочей характеристики* шифра, подходя к практической оценке стойкости. Он формулирует также основные критерии оценки качества секретных систем с позиций практики их использования.

5.2.3. Простейшие шифры и их свойства

Классификация шифров. С целью исследования свойств шифров рассмотрим их классификацию, предложенную в [2] и представленную на рисунке 5.2.1.

В качестве первичного классификационного признака, в соответствии с которым осуществляется классификация шифров, используется тип преобразования, осуществляемого с открытым текстом при шифровании. Если фрагменты открытого текста (отдельные буквы или группы букв) заменяются некоторыми их эквивалентами в шифртексте, то соответствующий шифр относится к классу шифров замены.

Если буквы открытого текста при шифровании меняются местами друг с другом, то такой шифр называется шифром перестановки.

С целью повышения надежности шифрования шифрованный текст, полученный применением некоторого шифра, может быть зашифрован с помощью другого шифра. Различные такие композиции образуют класс композиционных шифров.

Для исследования свойств шифров замены воспользуемся моделью (рис. 5.2.1).

Алгебраическая модель шифра замены

В соответствии с моделью (5.2.1) определим модель $\sum_A(X,K,Y,E,D)$ произвольного шифра замены.

Будем считать, что открытые и шифрованные тексты являются словами в алфавитах A и B соответственно: $X \subset A^*$, $Y \subset B^*$, $|A|=n$, $|B|=m$. Здесь и далее C^* обозначает множество слов конечной длины в алфавите C, n и m – мощности алфавитов A и B, соответственно [2].

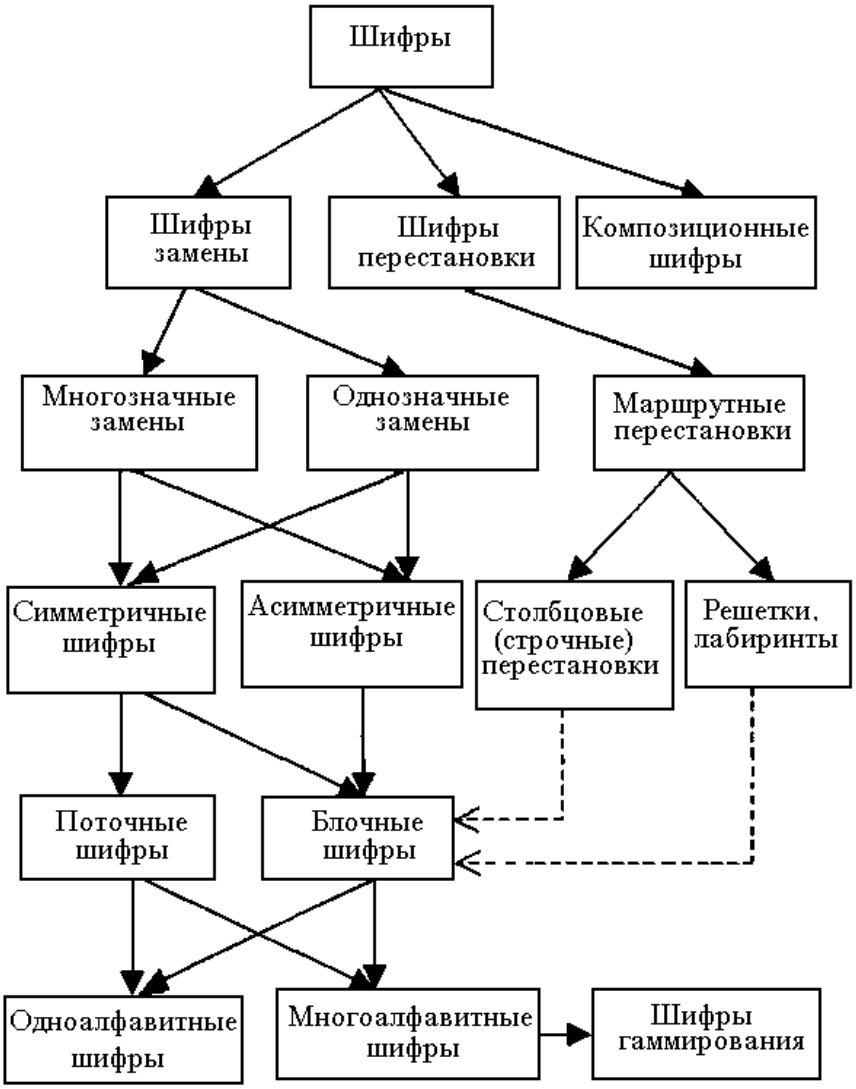


Рис. 5.2.1. Классификация шифров.

Перед зашифрованием открытый текст предварительно представляется в виде последовательности подслов, называемых шифрвеличинами.

При зашифровании шифрвеличины заменяются некоторыми их эквивалентами в шифртексте – шифробозначениями. Как шифрвеличины, так и шифробозначения представляют собой слова из A^* и B^*

соответственно.

Обозначим:

$U = \{u_1, u_2, ..., u_N\}$ – множество возможных шифрвеличин;

$N = C_n^p =$ – мощность алфавита шифрвеличин;

n – число букв исходного алфавита открытого текста;

p – количество букв из A, составляющих шифрвеличины;

$V = \{v_1, v_2, ..., v_M\}$ – множество возможных шифробозначений;

$M = C_m^r$ – мощность алфавита шифробозначений;

m – число букв исходного алфавита шифрованного текста

r – количество букв из B, составляющих шифробозначения.

Эти множества должны быть такими, чтобы любые тексты $x \in X$, $y \in Y$ можно было представить словами из U^*, V^* соответственно. Из требования однозначности расшифрования следуют неравенства: $N \geq n$, $M \geq m$, $M \geq N$.

В случае, когда алфавиты открытого и шифрованного сообщений совпадают и в качестве шифрвеличин и шифробозначений рассматриваются буквы алфавита A, модель шифра замены значительно упрощается.

Для введения модели такого шифра определим множества из (5.2.1).

$X = Y = \bigcup_{i=1}^{L} A^i$ – множества возможных открытых и шифрованных сообщений, соответственно;

$K \subseteq S(A)$ – множество возможных ключей;

$S(A)$ – симметрическая группа подстановок множества A;

$x = (x_1, .., x_i)$ – некоторое открытое сообщение, состоящее из i букв алфавита A;

$y = (y_1, .., y_i)$ – некоторое шифрованное сообщение, состоящее из i букв алфавита A;

$E_k(x) = (k(x_1), ..., k(x_i))$ – правило зашифрования шифра замены в алфавите A;

$D_k(y) = (k^{-1}(y_1), ..., k^{-1}(y_i))$ – правило расшифрования шифра замены в алфавите A;

$k = (k(x_1), ..., k(x_i))$ – подстановки из $S(A)$, соответствующая правилу $E_k(x)$;

k^{-1} – подстановка, обратная к k.

Аналогично для введения модели шифра замены в случае, когда алфавиты открытого и шифрованного сообщений не совпадают, определим множества из определения (5.2.1) [2].

$X = \bigcup_{i=1}^{L} A^i$, $Y = \bigcup_{i=1}^{L} B^i$ – множества открытых и шифрованных сообщений в алфавитах A и B, соответственно ($|A| = |B|$);

K – множество всех биекций множества A на множество B.

$E_k(x) = (k(x_1),...,k(x_l))$ и $D_k(y) = (k^{-1}(y_1),...k^{-1}(y_l))$ – правила зашифрования и расшифрования;

k – подстановка, соответствующая биекции из K;

k^{-1} – подстановка, обратная k.

В целях исследования свойств шифров замены воспользуемся введенными в их моделях обозначениями.

Разделение шифров на однозначные и многозначные связано с видом функции $E_k(x)$.

В общем случае функция $E_k(x)$ в определении (5.2.1) является многозначной и выбор ее значений представляет собой некоторые трудности. Более удобными для использования являются однозначные функции.

Неформально это означает, что в случае использования многозначных функций допускается неоднозначность зашифрования, а при использовании однозначных функций зашифрование является однозначным. Однако в соответствии с условием 1) модели (5.2.1) в обоих случаях должно обеспечиваться выполнение требования однозначности расшифрования.

При использовании однозначной функции $E_k(x)$ каждой шифрвеличине открытого текста при зашифровании ставится в соответствие только одна шифрвеличина в соответствии с подстановкой $k(x_i)$ используемой симметрической группы подстановок $S(A)$.

При использовании многозначной функции $E_k(x)$ требуется использование алфавита B большей, чем A мощности. $|B| > |A|$, так как при зашифровании каждой шифрвеличине может быть поставлено в соответствие шифробозначение из некоторой группы шифробозначений в соответствии с биекцией $k(x_i)$ используемого множества биекций множества A на множество B. При этом для обеспечения выполнения требования однозначности расшифрования группы шифробозначений, соответствующих различным шифрвеличинам, не должны пересекаться.

Примером шифра многозначной замены являются шифры – омофоны, известные из истории криптографии. Эти шифры были разработаны с целью «разрушения» «наследственных связей» между статистическими характеристиками открытых и соответствующих им шифрованных текстов.

В омофонах каждая группа шифробозначений содержит одинаковое

количество n элементов. При этом требуется использование алфавита шифробозначений объемом в n раз большим, чем объем алфавита шифрвеличин: $|B| = n \cdot |A|$. Выполнение этого условия представляет определенные трудности, поэтому в порядке модификации омофонов были разработаны так называемые шифры пропорциональной замены, в которых количество элементов в различных группах шифробозначений зависит от частот появления соответствующих шифрвеличин в открытом тексте.

Указанные обстоятельства обусловили более широкое использование на практике шифров однозначной замены.

В качестве одного из наиболее распространенных в настоящее время шифров однозначной замены может рассматриваться шифр гаммирования.

Свойства симметричных и асимметричных шифров классификации, представленной на рисунке 5.2.1, рассмотрены ранее.

Разделение шифров на симметричные и асимметричные состоит в соотношении ключей зашифрования/расшифрования. Если ключ зашифрования совпадает с ключом расшифрования (или знание одного ключа позволяет легко определить другой ключ): $k_з = k_р$, то такие шифры называют симметричными, если же $k_з \neq k_р$ – асимметричными.

Разделение шифров замены на потоковые и блоковые связаны, в первую очередь, со способом их практической реализации.

Ранее было отмечено, что перед зашифрованием открытый текст представляется в виде последовательности шифрвеличин. При зашифровании шифрвеличины заменяются некоторыми их эквивалентами в шифртексте – шифробозначениями. При этом мощность N множества U возможных шифрвеличин зависит от n – числа букв исходного алфавита открытого текста A и p – количества букв из A, составляющих шифрвеличины.

Множество шифрвеличин U может быть представлено в виде расширения степени p исходного алфавита открытого текста: $U \in A^p$, для некоторого $p \in N$. Тогда при $p = 1$ соответствующий шифр замены считается потоковым, при $p > 1$ – блоковым.

Разделение шифров на одноалфавитные и многоалфавитные определяется режимом использования $S(A)$ симметрических групп подстановок из K – множества возможных ключей.

Если каждая шифрвеличина открытого текста преобразуется в соответствующее шифробозначение шифрованного текста с использованием одной и той же симметрической группы подстановок, то такой шифр замены называется одноалфавитным шифром или шифром простой замены. Если же каждая шифрвеличина открытого текста преобразуется в соответствующее шифробозначение шифрованного текста с использованием другой симметрической группы подстановок из K, то

такой шифр замены называется многоалфавитным [3].

Алгебраическая модель шифра перестановки

Для исследования свойств шифров перестановки воспользуемся моделью (5.2.1).

Введем обозначения для описания алгебраической модели такого шифра.

$X = Y = A^L$ – множества возможных открытых и шифрованных сообщений, соответственно;

L – длина блока открытого сообщения, в котором осуществляются перестановки букв (символов);

$K \subseteq S_L$ – множество возможных ключей;

S_L – симметрическая группа подстановок множества $\{1, 2, ..., L\}$.

Для любого ключа k, открытого текста $x = (x_1, ..., x_L)$ и шифрованного текста $y = (y_1, ..., y_L)$ правила зашифрования и расшифрования шифра перестановки определяются формулами

$$E_k(x) = \left(x_{k(1)}, ..., x_{k(L)}\right),\ D_k(y) = \left(y_{k^{-1}(1)}, ..., y_{k^{-1}(L)}\right),$$

где k^{-1} – подстановка, обратная к k.

Ключом шифра перестановки является перестановка номеров букв открытого текста в рамках некоторого блока открытого текста длиной L. Зависимость ключа от длины текста создает неудобства в использовании шифра. В силу этого был предложен ряд частных шифров перестановок, которые можно применять для зашифрования текстов любой длины [2].

Маршрутные перестановки

Широкое применение получили так называемые *маршрутные перестановки*, основанные на некоторой геометрической фигуре. Отрезок открытого текста записывается в такую фигуру по некоторой траектории. Шифрованным текстом является последовательность, полученная при выписывании текста по другой траектории. Например, можно записывать сообщение в прямоугольную таблицу, выбрав такой маршрут: будем двигаться по горизонтали, начиная с левого верхнего угла, поочередно слева направо и справа налево. Списывать же сообщение будем по другому маршруту: по вертикалям, начиная с верхнего правого угла и двигаясь поочередно сверху вниз и снизу-вверх.

Пример (*маршрутной перестановки*).

Зашифруем указанным выше способом фразу: *пример маршрутной перестановки*, используя прямоугольную таблицу размером 4x7:

п	р	и	м	е	р	м
н	т	у	р	ш	р	а
о	й	п	е	р	е	с

и	к	в	о	н	а	т

Зашифрованная фраза выглядит следующим образом:

мастаеррешрноермвпуиртикионп

Обращение описанных шагов при расшифровании не представляет труда.

Широкое распространение получила разновидность маршрутной перестановки, называемая *вертикальной перестановкой*. В этой системе также используется прямоугольная таблица, в которую сообщение записывается обычным образом (по строкам слева направо). Выписывается же сообщение по вертикалям (сверху вниз), при этом столбцы выбираются в порядке, определяемом *числовым ключом*.

Пример (*вертикальной перестановки*).

Зашифруем фразу: *вот пример шифра вертикальной перестановки*, используя прямоугольник размеров 6 х 7 и числовой ключ (5,1,4,7,2,6,3).

5	1	4	7	2	6	3
в	о	т	п	р	и	м
е	р	ш	и	ф	р	а
в	е	р	т	и	к	а
л	ь	н	о	й	п	е
р	е	с	т	а	н	о
в	к	и				

Отметим, что нецелесообразно заполнять последнюю строку прямоугольника "нерабочими" буквами, так как это дало бы противнику, получившему в свое распоряжение данную криптограмму, сведения о длине числового ключа. В самом деле, в этом случае длину ключа следовало бы искать среди делителей длины сообщения. Теперь, выписывая буквы по столбцам в порядке, указанном числовым ключом, получим такую криптограмму:

ореьекрфийамааеотирнсивевлрвиркпн

Более сложные маршрутные перестановки могут использовать другие геометрические фигуры и более "хитрые" маршруты, как, например, при обходе шахматной доски «ходом коня», пути в некотором лабиринте и т.п. Возможные варианты зависят от фантазии составителя системы и, конечно, естественного требования простоты ее использования.

Ограничиваясь наиболее важными классами шифров замены и исторически известными классами шифров перестановки, сведем

результаты классификации в схему, изображенную на рис. 5.2. [2]

При расшифровании, в первую очередь, надо определить число длинных столбцов, то есть число букв в последней строке прямоугольника. Для этого нужно разделить число букв в сообщении на длину числового ключа. Ясно, что остаток от деления и будет искомым числом. Когда это число определено, буквы криптограммы можно водворить на их собственные места, и сообщение будет прочитано естественным образом.

В нашем примере $38 = 7 \cdot 5 + 3$, поэтому в заполненной таблице имеется 3 длинных и 4 коротких столбца. Согласно числовому ключу, начальные буквы криптограммы берутся из второго (по счету слева) столбца, он – длинный (так как первые три столбца – длинные), поэтому первые шесть букв образуют второй столбец. Следующие пять букв образуют пятый столбец (он – короткий). И так далее.

Прокомментируем приведенную схему. Подчеркнем, что стрелки, выходящие из любого прямоугольника схемы, указывают лишь на наиболее значимые частные подклассы шифров. Пунктирные стрелки, ведущие из подклассов шифров перестановки, означают, что эти шифры можно рассматривать и как блочные шифры замены в соответствии с тем, что открытый текст делится при шифровании на блоки фиксированной длины, в каждом из которых производится некоторая перестановка букв. Одноалфавитные и многоалфавитные шифры могут быть как поточными, так и блочными. В то же время шифры гаммирования, образующие подкласс многоалфавитных шифров, относятся к поточным, а не к блочным шифрам. Кроме того, они являются симметричными, а не асимметричными шифрами.

5.3. Алгоритмы хэширования

5.3.1. Определение и задачи хэш-функций

Функция хэширования заключается в сопоставлении произвольного набора данных в виде последовательности двоичных символов и его образа фиксированной небольшой длины, что позволяет использовать эту функцию в процедурах электронной цифровой подписи для сокращения времени подписывания и проверки подписи. Эффект сокращения времени достигается за счет вычисления подписи только под образом подписываемого набора данных.

Хэш-функции имеют разнообразные применения при проведении статистических экспериментов, при тестировании логических устройств, при построении алгоритмов быстрого поиска и проверки целостности записей в базах данных. Основным требованием к хэш-функциям является равномерность распределения их значений при случайном выборе значений аргумента.

Криптографической хэш-функцией называется всякая хэш-функция, являющаяся криптостойкой, то есть удовлетворяющая ряду требований

специфичных для криптографических приложений. В криптографии хэш-функции применяются для решения следующих задач:

– построения систем контроля целостности данных при их передаче или хранении,

– аутентификация источника данных.

Хэш-функцией называется всякая функция $h:X \to Y$, легко вычислимая и такая, что для любого сообщения M значение $h(M) = H$ *(свертка)* имеет фиксированную битовую длину. X – множество всех сообщений, Y – множество двоичных векторов фиксированной длины.

Как правило хэш-функции строят на основе так называемых одношаговых сжимающих функций $y = f(x_1, x_2)$ двух переменных, где x_1, x_2 и y – двоичные векторы длины m, n и n соответственно, причем n – длина свертки, а m – длина блока сообщения.

Для получения значения $h(M)$ сообщение сначала разбивается на блоки длины m (при этом, если длина сообщения не кратна m то последний блок неким специальным образом дополняется до полного), а затем к полученным блокам $M_1, M_2,.., M_N$ применяют следующую последовательную процедуру вычисления свертки:

$$H_o = v,$$
$$H_i = f(M_i, H_{i-1}),\ i = 1,.., N,$$
$$h(M) = H_N$$

Здесь v – некоторая константа, часто ее называют инициализирующим вектором. Она выбирается из различных соображений и может представлять собой секретную константу или набор случайных данных (выборку даты и времени, например).

При таком подходе свойства хэш-функции полностью определяются свойствами одношаговой сжимающей функции.

Выделяют два важных вида криптографических хэш-функций – ключевые и бесключевые. Ключевые хэш-функции называют кодами аутентификации сообщений. Они дают возможность без дополнительных средств гарантировать как правильность источника данных, так и целостность данных в системах с доверяющими друг другу пользователями.

Бесключевые хэш-функции называются кодами обнаружения ошибок. Они дают возможность с помощью дополнительных средств (шифрования, например) гарантировать целостность данных. Эти хэш-функции могут применяться в системах как с доверяющими, так и не доверяющими друг другу пользователями [1].

5.3.2. Статистические свойства и требования

Основным требованием к хэш-функциям является равномерность распределения их значений при случайном выборе значений аргумента. Для криптографических хэш-функций также важно, чтобы при малейшем

изменении аргумента значение функции сильно изменялось. Это называется лавинным эффектом. К ключевым функциям хэширования предъявляются следующие требования:

– невозможность фабрикации,

– невозможность модификации.

Первое требование означает высокую сложность подбора сообщения с правильным значением свертки. Второе – высокую сложность подбора для заданного сообщения с известным значением свертки другого сообщения с правильным значением свертки.

К бесключевым функциям предъявляют требования:

– однонаправленность,

– устойчивость к коллизиям,

– устойчивость к нахождению второго прообраза.

Под однонаправленностью понимают высокую сложность нахождения сообщения по заданному значению свертки. Следует заметить, что на данный момент нет используемых хэш-функций с доказанной однонаправленностью.

Под устойчивостью к коллизиям понимают сложность нахождения пары сообщений с одинаковыми значениями свертки. Обычно именно нахождение способа построения коллизий криптоаналитиками служит первым сигналом устаревания алгоритма и необходимости его скорой замены.

Под устойчивостью к нахождению второго прообраза понимают сложность нахождения второго сообщения с тем же значением свертки для заданного сообщения с известным значением свертки.

5.3.3. Общие положения межгосударственного стандарта ГОСТ 34.311-95 «Информационная технология. Криптографическая защита информации. Функция хэширования»

В настоящем стандарте используются следующие обозначения [6]:

B^* – множество всех конечных слов в алфавите $B = \{0,1\}$. Чтение слов и нумерация знаков алфавита (символов) осуществляются справа налево (номер правого символа в слове равен единице, второго справа – двум и т.д.).

$|A|$ – длина слова $A \in B^*$.

$V_k(2)$ – множество всех бинарных слов длины k.

$A||B$ – конкатенация слов A, $B \in B^*$ – слово длины $|A| + |B|$, в котором левые $|A|$символов образуют слово A, а правые $|B|$ символов образуют слово B. Можно также использовать обозначение $A||B = AB$.

A^k – конкатенация k экземпляров слова $A(A \in B^*)$.

$\langle N \rangle_k$ – слово длины k, содержащее двоичную запись вычета $N(mod 2^k)$ неотрицательного целого числа N.

$\hat{A}$ – неотрицательное целое число, имеющее двоичную запись $A(A \in B^*)$.

$\oplus$ – побитовое сложение слов одинаковой длины по модулю 2.

$\oplus'$ – сложение по правилу $A\overline{\oplus'}B = \langle \hat{A} + \hat{B} \rangle_k$, $(k = |A| = |B|)$.

M – последовательность двоичных символов, подлежащая хэшированию (сообщение в системах ЭЦП), $M \in B^*$.

h – хэш-функция, отображающая последовательность $M \in B^*$ в слово $h(M) \in V_{256}(2)$.

$E_k(A)$ – результат зашифрования слова A на ключе K с использованием алгоритма шифрования по ГОСТ 28147-89 в режиме простой замены ($K \in V_{256}(2)$, $A \in V_{64}(2)$).

H – стартовый вектор хэширования.

$e := g$ – присвоение параметру e значения g.

Под хэш-функцией h понимается зависящее от параметра стартового вектора хэширования H, являющегося словом из $V_{256}(2)$] отображение

$$h: B^* \longrightarrow V_{256}(2)$$

Для определения хэш-функции необходимы:

– алгоритм вычисления шаговой функции хэширования χ, т.е. отображения

$$\chi: V_{256}(2) \times V_{256}(2) \longrightarrow V_{256}(2);$$

– описание итеративной процедуры вычисления значения хэш-функции h.

5.3.4. Шаговая функция хэширования

Алгоритм вычисления шаговой функции хэширования включает в себя три части, реализующие последовательно:

– генерацию ключей – слов длины 256 битов;

– шифрующее преобразование - зашифрование 64-битных подслов слова H на ключах K_i (i = 1, 2, 3, 4) с использованием алгоритма по ГОСТ 28147-89 в режиме простой замены;

– перемешивающее преобразование результата шифрования.

Генерация ключей:

Рассмотрим $X = (b_{256}, b_{256}, \ldots, b_i) \in V_{256}(2)$.

Пусть $X = x_4 \| x_3 \| x_2 \| x_1 =$

$= \eta_{16} \| \eta_{15} \| \ldots \| \eta_1 =$

$= \xi_{32} \| \xi_{31} \| \ldots \| \xi_1$,

где $x_i = \left(b_{i \times 64}, \ldots, b_{(i-1) \times 64+1}\right) \in V_{64}(2), i = \overline{1,4}$;

$\eta_j = \left(b_{j \times 16}, \ldots, b_{(i-1) \times 16+1}\right) \in V_{16}(2), i = \overline{1,16}$;

$\xi_k = \left(b_{k \times 8}, \ldots, b_{(k-1) \times 8+1}\right) \in V_8(2), k = \overline{1,32}$.

Обозначают $A(X) = (x_1 \oplus x_2) \| x_4 \| x_3 \| x_2$.

Используют преобразование $P : V_{256}(2) \longrightarrow V_{256}(2)$ слова $\xi_{32} \| \ldots \| \xi_1$ в слово, $\xi_{\varphi(32)} \| \ldots \| \xi_{\varphi(1)}$,

где $\varphi\big(i+1+4(k-1)\big)=8i+k, i=0\div 3, k=1\div 8.$

Для генерации ключей необходимо использовать следующие исходные данные:

– слова *H, M* ∈ $V_{256}(2)$;

– параметры: слова C_i (i = 2, 3, 4), имеющие значения

$C_2 = C_4 = 0^{256}$ и $C_3 = 1^8 0^8 1^{16} 0^{24} 1^{16} 0^8 (0^8 1^8)^2 1^8 0^8 (0^8 1^8)^4 (1^8 0^8)^4$.

При вычислении ключей реализуется следующий алгоритм:

1. Присвоить значения

i: = 1, U: = H, V: =M.

2. Выполнить вычисление

$W = U \overline{\oplus} V$, $K_1 = P(W)$

3. Присвоить *i: = i+1*.

4. Проверить условие *i = 5.*

При положительном исходе перейти к шагу 7. При отрицательном – перейти к шагу 5.

5. Выполнить вычисление

$U: = A(U) \overline{\oplus} C_i$, *V: = A(A(V)), W: =* $U \overline{\oplus} V$, $K_i = P(W)$.

6. Перейти к шагу 3.

7. Конец работы алгоритма.

Шифрующее преобразование.

На данном этапе осуществляется зашифрование 64-битных подслов слова *H* на ключах

K_i *(i = 1, 2, 3, 4).*

Для шифрующего преобразования необходимо использовать следующие исходные данные:

$H = h_4 \| h_3 \| h_2 \| h_1$, $h_i \epsilon V_{64}(2), i = \overline{1,4}$

и набор ключей K_1, K_2, K_3, K_4.

Реализуют алгоритм зашифрования и получают слова

$s_i = E_{K_i}(h_i)$, где *i=1, 2, 3, 4.*

В результате данного этапа образуется последовательность

$S = s_4 \| s_3 \| s_2 \| s_1$.

Перемешиваюшее преобразование.

На данном этапе осуществляется перемешивание полученной последовательности с применением регистра сдвига.

Исходными данными являются слова:

H, M∈$V_{256}(2)$ и слово *S*∈$V_{256}(2)$.

Пусть отображение

$$\Psi: V_{256}(2) \text{ – – –} \rightarrow V_{256}(2)$$

Преобразует слово

$$\eta_{16} \| \dots \| \eta_1, \eta_1 \in V_{16}(2), i = \overline{1,16}$$

в слово

$$\eta_1 \bar{\oplus} \eta_2 \bar{\oplus} \eta_3 \bar{\oplus} \eta_4 \bar{\oplus} \eta_{13} \bar{\oplus} \eta_{16} \| \eta_{16} \| \ldots \| \eta_2.$$

Тогда в качестве значения шаговой функции хэширования принимается слово

$$\chi(M, H) = \Psi^{61}(H \bar{\oplus} \Psi(M \bar{\oplus} \Psi^{12}(S))),$$

где $\psi^i - i$ - я степень преобразования φ.

5.3.5. Процедура вычисления хэш-функции

Исходными данными для процедуры вычисления значения функции *h* является подлежащая хэшированию последовательность $M \in B^*$. Параметром является стартовый вектор хэширования H – произвольное фиксированное слово из $V_{256}(2)$.

Процедура вычисления функции *h* на каждой итерации использует следующие величины:

$M \in B^*$ – часть последовательности *M*, не прошедшая процедуры хэширования на предыдущих итерациях;

$H \in V_{256}(2)$ – текущее значение хэш-функции;

$\sum \in V_{256}(2)$ – текущее значение контрольной суммы;

$L \in V_{256}(2)$ – текущее значение длины обработанной на предыдущих итерациях части последовательности *M*.

Алгоритм вычисления функции *h* включает в себя этапы:

Этап 1.

Присвоить начальные значения текущих величины:

1.1 $M := M$

1.2 $H := H$

1.3 $\sum := 0^{256}$

1.4 $L := 0^{256}$

1.5 Переход к этапу 2

Этап 2.

2.1 Проверить условие $|M| > 256$.

При положительном исходе перейти к этапу 3.

В противном случае выполнить последовательность вычислений:

2.2 $L := \langle \hat{L} + |M| \rangle_{256}$

2.3 $M' := 0^{256-|M|} \| M$

2.4 $\sum := \sum \bar{\oplus}' M'$

2.5 $H: \chi(M', H)$

2.6 $H: \chi(L, H)$

2.7 $H: \chi(\sum, H)$

2.8 Конец работы алгоритма

Этап 3.

3.1 Вычислить подслово $M_s \in V_{256}(2)$ слова M $(M = M_p \| M_s)$. Далее выполнить последовательность вычислений:

3.2 $H := \chi(M_s, H)$

3.3 $L := \langle L + 256 \rangle_{256}$

3.4 $\sum := \sum \bar{\oplus}' M_s$

3.5 $M := M_p$

3.6 Перейти к этапу 2.

Значение величины *H,* полученное на шаге 2.7, является значением функции хэширования *h(M).*

5.4. Использование цифровых подписей

5.4.1. Понятие электронной подписи

Электронная подпись для сообщения является числом, зависящим от самого сообщения и от некоторого секретного, известного только подписывающему субъекту, ключа. При этом предполагается, что она должна быть легко проверяемой и что осуществить проверку подписи должен иметь возможность каждый без получения доступа к секретному ключу. При возникновении спорной ситуации, связанной с отказом подписывающего от факта подписи им некоторого сообщения либо с попыткой подделки подписи, третья сторона должна иметь возможность разрешить спор.

Цифровая подпись позволяет решить следующие три задачи [4]:

– осуществить аутентификацию источника сообщения,

– установить целостность сообщения,

– обеспечить невозможность отказа от факта подписи конкретного сообщения.

Использование термина «подпись» в данном контексте оправдано тем, что цифровая подпись имеет много общего с обычной собственноручной подписью на бумажном документе. Собственноручная подпись также решает три перечисленные задачи, однако между обычной и цифровой подписями имеются существенные различия. Сведем основные различия между обычной и цифровой подписями в таблицу.

Собственноручная подпись	*Цифровая подпись*
не зависит от подписываемого текста, всегда одинакова	зависит от подписываемого текста, практически всегда разная
неразрывно связана с подписывающим лицом, однозначно определяется его психофизическими свойствами, не может быть утеряна	определяется секретным ключом, принадлежащим подписывающему лицу, может быть утеряна владельцем
неотделима от носителя (бумаги), поэтому отдельно подписывается	легко отделима от документа, поэтому верна для всех его копий

каждый экземпляр документа	
не требует для реализации дополнительных механизмов	требует дополнительных механизмов, реализующих алгоритмы ее вычисления и проверки
не требует создания поддерживающей инфраструктуры	требует создания доверенной инфрастуктуры сертификатов открытых ключей

Для реализации схемы цифровой подписи необходимы два алгоритма:

– алгоритм вычисления цифровой подписи;

– алгоритм ее проверки.

Главные требования к этим алгоритмам заключаются в исключении возможности получения подписи без использования секретного ключа и гарантировании возможности проверки подписи без знания какой-либо секретной информации.

Надежность схемы цифровой подписи определяется сложностью следующих трех задач:

– *подделки подписи,* то есть нахождения значений подписи под заданным документом лицом, не являющимся владельцем секретного ключа;

– *создания подписанного сообщения,* то есть нахождения хотя бы одного сообщения с правильным значением подписи;

– *подмены сообщения,* то есть подбора двух различных сообщений с одинаковыми значениями подписи.

Имеется множество различных схем цифровой подписи, обеспечивающих тот или иной уровень стойкости.

Принципиальной сложностью, возникающей при использовании цифровой подписи на практике, является проблема создания *инфраструктуры открытых ключей.* Дело в том, что для алгоритма проверки подписи необходима дополнительная открытая информация, связанная с обеспечением возможности открытой проверки подписи и зависящая от секретного ключа автора подписи. Эту информацию можно назвать открытым ключом цифровой подписи. Для исключения возможности подделки этой информации (открытого ключа) лицами, которые хотят выступить от лица законного владельца подписи (секретного ключа), создается инфраструктура, состоящая из центров сертификации открытых ключей и обеспечивающая возможность своевременного подтверждения достоверности принадлежности данной открытой информации заявленному владельцу и обнаружения подлога.

Создание сертификационных центров с технической точки зрения не представляет большой сложности. Они строятся во многом аналогично центрам сертификации, которые используются в криптографических системах с открытыми ключами. Однако с юридической точки зрения

здесь имеется множество проблем. Дело в том, что в случае возникновения споров, связанных с отказом от авторства или подделки подписи, такие центры должны нести юридическую ответственность за достоверность выдаваемых сертификатов. В частности, они должны возмещать понесенные убытки в случае конфликтных ситуаций, когда алгоритм проверки подписи подтверждает ее правильность. В связи с этим сложилась практика заключения договоров между участниками информационного взаимодействия с применением цифровых подписей. В таком договоре должно быть четко указано:

– кто должен нести ответственность в случае, если подписанные сделки не состоятся;

– кто должен нести ответственность в случае, если система окажется ненадежной и будет взломана, то есть будет выявлен факт подделки секретного ключа;

– какова ответственность уполномоченного по сертификатам в случае, если открытый ключ будет сфальсифицирован;

– какова ответственность владельца секретного ключа в случае его утраты;

– кто несет ответственность за плохую реализацию системы в случае повреждения или разглашения секретного ключа;

– каков порядок разрешения споров и т.п.

Поскольку данные проблемы носят юридический, а не технический характер, то для их разрешения нужен юридически правильно заключенный договор, оформленный стандартным образом на бумаге.

В настоящее время предложено несколько принципиально различных подходов к созданию схем цифровой подписи. Их можно разделить на три группы:

1) схемы на основе систем шифрования с открытыми ключами;

2) схемы со специально разработанными алгоритмами вычисления и проверки подписи;

3) схемы на основе симметричных систем шифрования.

Рассмотрим их более подробно.

5.4.2. Цифровые подписи на основе шифрсистем с открытым ключом

Идея использования систем шифрования с открытыми ключами для построения систем цифровой подписи как бы заложена в постановке задачи. Действительно, пусть имеется пара преобразований (E, D), первое из которых зависит от открытого ключа, а второе – от секретного. Для того чтобы вычислить цифровую подпись S для сообщения, владелец секретного ключа может применить к сообщению M второе преобразование D: $S = D(M)$. В таком случае вычислить подпись может только владелец секретного ключа, в то время как проверить равенство $E(S)$

$= M$ может каждый. Основными требованиями к преобразованиям E и D являются [4]:

– выполнение равенства $M = E(D(M))$ для всех сообщений M;

– невозможность вычисления значения $D(M)$ для заданного сообщения M без знания секретного ключа.

Отличительной особенностью предложенного способа построения цифровой подписи является возможность отказаться от передачи самого подписываемого сообщения M, так как его можно восстановить по значению подписи. В связи с этим подобные системы называют *схемами цифровой подписи с восстановлением текста.*

Заметим, что если при передаче сообщение дополнительно шифруется с помощью асимметричного шифра, то пара преобразований (E, D), используемая в схеме цифровой подписи, должна отличаться от той, которая используется для шифрования сообщений. В противном случае появляется возможность передачи в качестве шифрованных ранее подписанных сообщений. При этом более целесообразно шифровать подписанные данные, чем делать наоборот, то есть подписывать шифрованные данные, поскольку в первом случае противник получит только шифртекст, а во втором – и открытый, и шифрованный тексты.

Очевидно, что рассмотренная схема цифровой подписи на основе пары преобразований (E, D) удовлетворяет требованию невозможности подделки, в то время как требование невозможности создания подписанного сообщения не выполнено: для любого значения S каждый может вычислить значение $M = E(S)$ и тем самым получить подписанное сообщение. Требование невозможности подмены сообщения заведомо выполняется, так как преобразование E взаимно однозначно.

Для защиты от создания злоумышленником подписанного сообщения можно применить некоторое взаимно-однозначное отображение $R: M \mapsto \widetilde{M}$, вносящее избыточность в представление исходного сообщения, например, путем увеличения его длины, а затем уже вычислять подпись $S = D\left(\widetilde{M}\right)$. В этом случае злоумышленник, подбирая S и вычисляя значения $\widetilde{M} = E(S)$, будет сталкиваться с проблемой отыскания таких значений $\widetilde{M}$, для которых существует прообраз M. Если отображение R выбрано таким, что число возможных образов $\widetilde{M}$ значительно меньше числа всех возможных последовательностей той же длины, то задача создания подписанного сообщения будет сложной.

Рассмотрим принцип реализации ЭП в соответствии со схемой, представленной на рисунке 5.4.1.

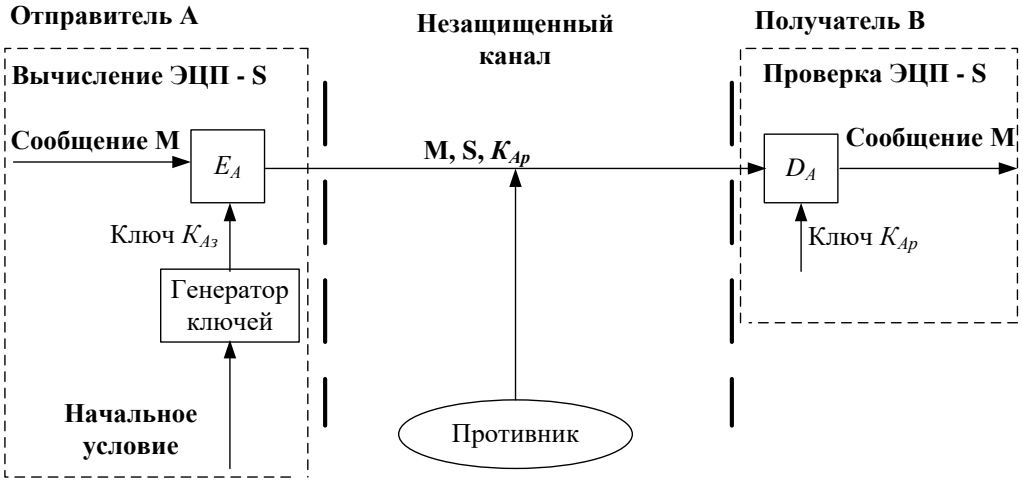


Рис. 5.4.1. Обобщенная структурная схема асимметричной криптосистемы для случая обеспечения целостности информации

Отправитель *А* некоторого сообщения *М*, в обеспечении целостности которого он заинтересован, на основе некоторых начальных условий в соответствии с используемым алгоритмом генерирует пару ключей $K_{Аз}$ и K_{Ap}. Ключ $K_{Аз}$ используется для вычисления значения ЭП $S = E_{K_{Аз}}(M)$ и хранится в секрете. Ключ K_{Ap} используется для проверки целостности принимаемого из канала связи сообщения применением обратного преобразования $D_{K_{Ap}}(S) = M$ поэтому этот ключ является открытым и передается получателю по открытому каналу связи вместе с сообщением и ЭП.

Получатель В полученный из канала связи ключ K_{Ap} использует для проверки ЭП *S* при помощи алгоритма (правила) $D_{K_{Ap}}(S) = M$. Если результат проверки положительный, то считается, что сообщение не модифицировано в канале связи.

В связи с тем, что открытый ключ передается по незащищенному каналу связи, противник, который контролирует этот канал, имеет возможность блокировать передачу сообщения отправителем *А*, сгенерировать свою пару ключей и таким образом передать ложное сообщение, либо в случае отсутствия передачи информации в какой-либо момент времени выступить от имени отправителя *А*, реализуя таким образом подмену сообщения или его имитацию, соответственно.

Для противодействия такого рода угрозам создается поддерживающая инфраструктура центров сертификации открытых ключей ЭП, которая называется системой удостоверяющих центров (СУЦ).

Одной из основных функций удостоверяющего центра является создание для открытого ключа ЭП сертификата, удостоверяющего его подлинность. При этом осуществить проверку подлинности сертификата должен иметь возможность каждый из участников информационного

взаимодействия, зарегистрированных в системе [4].

Процесс такого информационного взаимодействия представлен на рисунке 5.4.2.

Закрытый и открытый ключи ЭП генерируются в Регистрационном центре подразделения СУЦ, к которому относится отправитель *A*.

Закрытый ключ ЭП записывается на электронный носитель отправителя *A*, открытый ключ отправляется в удостоверяющий центр, в котором на этот ключ создается сертификат. Этот ключ вместе с сертификатом к нему возвращается в регистрационный центр, а затем записывается на тот же электронный носитель отправителя *A*.

Отправитель *A*, используя закрытый ключ $K_{Aз}$ и алгоритм вычисления электронной цифровой подписи $S = E_{K_{Aз}}(M)$ вычисляет для сообщения *M* значение ЭП *S*. Получателю В передается сообщение *M*, ЭП *S*, ключ для ее проверки K_{Ap} с сертификатом к нему *C*.

Получатель *B*, имея доступ по сети к реестру сертификатов, хранящемуся в удостоверяющем центре, проверяет значение ЭП с использованием ключа K_{Ap} и алгоритма $D_{K_{Ap}}(S) = M$.

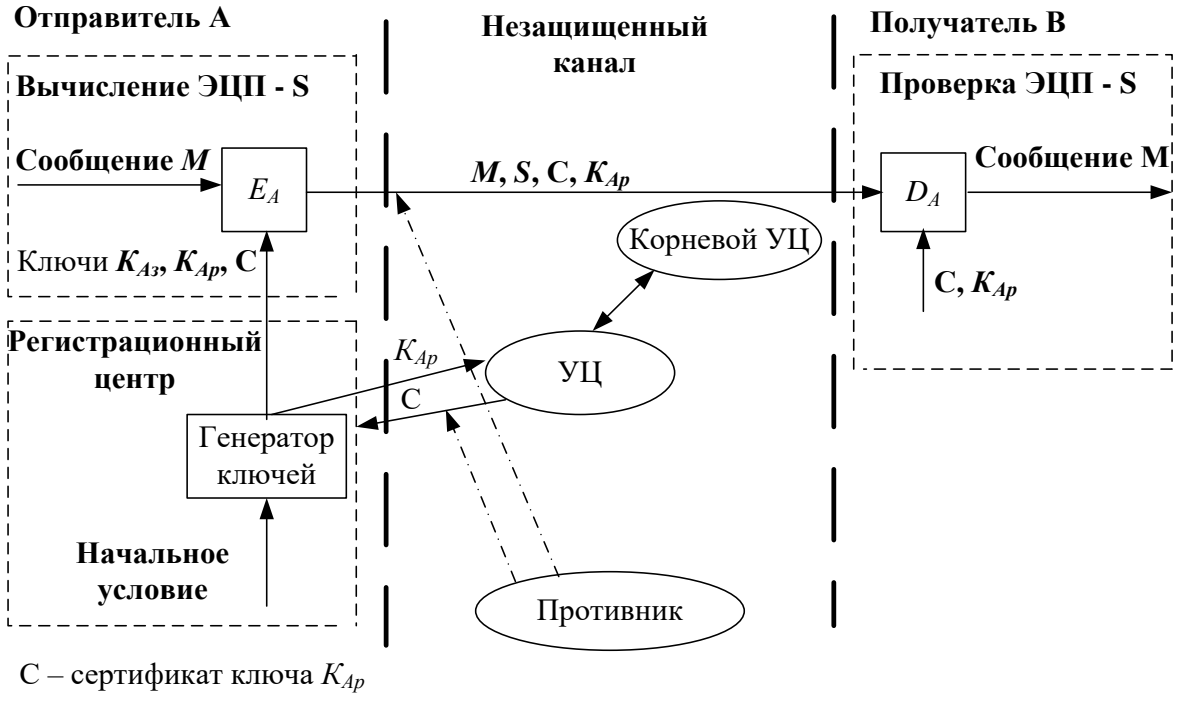


Рис. 5.4.2. Структура схемы электронной подписи с системой удостоверяющих центров

Для защиты от подделки сертификат также подписывается ЭП уполномоченного лица удостоверяющего центра, подлинность которой может быть проверена при помощи открытого ключа этого уполномоченного лица, также имеющего сертификат, который в свою

очередь подписывается с использованием закрытого ключа уполномоченного лица корневого удостоверяющего центра. Уполномоченное лицо корневого удостоверяющего центра имеет право самоподписи сертификата своего открытого ключа. Таким образом, создается конечная цепочка доверия системы удостоверяющих центров схемы электронной подписи. При включении в систему ЭП государственного уровня ЭП уполномоченного лица корневого удостоверяющего центра проверяется с использованием открытого ключа удостоверяющего центра государственного уровня, имеющего право самоподписи соответствующего сертификата ключа проверки ЭП.

Сертификаты становится действующими после их открытой публикации в реестре сертификатов.

5.4.3. Принципы организации системы удостоверяющих центров электронной подписи

СУЦ реализуется как совокупность комплекса программно-аппаратных средств определенной архитектуры и организационно-технических мероприятий, необходимых для использования криптографических функций в целях защиты от НСД к информации, аутентификации субъектов и разграничения прав доступа, подтверждения авторства и обеспечения целостности и подлинности электронных документов [7].

СУЦ, являясь инфраструктурным компонентом информационно-телекоммуникационной системы, представляет собой совокупность распределенных объектов информатизации в виде УЦ и их компонентов, территориально распределенных таким образом, чтобы предоставлять свои сервисы пользователям многоуровневой структуры управления системы ЭП.

Объекты информатизации СУЦ представляют собой программно-аппаратные комплексы, основное назначение которых заключается в выполнении функций:

– удостоверяющего центра, реализующего начальный (первый) уровень доверия СУЦ;

– удостоверяющего центра, выдающего сертификаты ключей пользователей и реализующего:

1) сервис по управлению этими сертификатами;

2) сервис по предоставлению доступа к реестру актуальных сертификатов всей системы УЦ;

3) предполагаемый к использованию для всей системы УЦ сервис по проверке статуса сертификата и сервис меток времени.

Регистрация пользователей

Для получения сертификата ключа подписи пользователь системы

ЭП, в соответствии с Регламентом УЦ, оформляет заявку на издание сертификата. Эта заявка согласовывается с уполномоченными руководящими сотрудниками подразделений системы ЭП. На основании заявки уполномоченный сотрудник из состава персонала СУЦ производит действия по идентификации личности физического лица, указанного в заявке, проверку сведений, необходимых для внесения в сертификат ключа подписи и указанных в заявке, и затем осуществляет регистрацию пользователя в УЦ.

Процесс регистрации состоит из следующих основных процедур [7]:

– передача в СУЦ заявки на издание сертификата ключа подписи, согласованной с уполномоченными руководящими сотрудниками подразделений системы ЭП;

– проверка Оператором АРМ Центра регистрации (ЦР) в соответствии с Регламентом удостоверяющего центра (УЦ) данных, содержащихся в заявке;

– регистрация пользователя в УЦ Оператором АРМ ЦР с использованием компонента АРМ Администратора и оператора ЦР;

– издание (выпуск и публикация) сертификата ключа подписи.

Процедура регистрации пользователя в УЦ состоит в выполнении следующих действий:

– оператор АРМ ЦР с использованием компонента АРМ администратора и оператора ЦР выполняет процедуру генерации открытого и закрытого ключа. Закрытый ключ помещается на отчуждаемый ключевой носитель. Оперативная память АРМ ЦР, выделяемая для генерации ключей, очищается. Защищенный ключевой носитель является единственным местом хранения закрытого ключа;

– далее оператор АРМ ЦР с использованием компонента АРМ администратора и оператора ЦР устанавливает защищенное соединение по протоколу TLS с Центром регистрации УЦ и формирует запрос на издание сертификата открытого ключа зарегистрированному пользователю УЦ.

Процедура выпуска сертификата ключа подписи состоит в выполнении следующих действий:

– запрос на выпуск сертификата ключа подписи передается в Центр сертификации того удостоверяющего центра, в ЦР которого поступил запрос на выпуск сертификата. В данном Центре сертификации производится выпуск сертификата. Выпущенный сертификат публикуется на Сервере реестра сертификатов;

– выпущенный сертификат по защищенному каналу из ЦР передается на АРМ администратора и оператора ЦР, с которого ранее был получен запрос на выпуск сертификата;

– оператор АРМ ЦР помещает сертификат на тот же защищенный ключевой носитель, что и закрытый ключ;

– далее оператор АРМ ЦР передает пользователю ключевой носитель, содержащий закрытый ключ и сертификат, и сертификат ключа подписи на бумажном носителе под роспись.

Детально регламентные действия излагаются в соответствующей инструкции для оператора АРМ ЦР.

В Удостоверяющем центре ведется эталонная база всех выпущенных сертификатов. При этом обеспечивает уникальность следующей информации в сертификатах пользователей:

– открытый ключ сертификата;

– серийный номер сертификата.

База данных ЦР удостоверяющего центра (Реестр) содержит полную информацию и историю обо всех изготовленных сертификатах для зарегистрированных в данном ЦР пользователей. При этом контролируется уникальность доменного имени субъекта сертификата (пользователя).

Уникальность сертификата пользователя в СУЦ определяется комбинацией уникального (в рамках удостоверяющего центра, выпустившего данный сертификат) серийного номера сертификата и уникального (в рамках СУЦ) отличительного имени издателя сертификата.

Срок действия закрытых ключей и связанных с ним сертификатов составляет 1 год. Периодичность издания списка отозванных сертификатов составляет 1 неделю. Периодичность издания списка отозванных сертификатов Подчиненного УЦ может быть изменена (с отражением в Регламенте Подчиненного УЦ) [7].

5.4.4. Хэш-функция и ее использование в системах цифровой подписи

Другой подход к построению схем цифровых подписей на основе систем шифрования с открытым ключом состоит в использовании бесключевых хэш-функций. Для заданного сообщения M сначала вычисляется значение хэш-функции $h(M)$, а затем уже значение подписи $S = D(h(M))$. Ясно, что в таком случае по значению подписи уже нельзя восстановить сообщение. Поэтому подписи необходимо передавать вместе с сообщениями. Такие подписи получили название *цифровых подписей с дополнением.* Заметим, что системы подписи, построенные с использованием бесключевых хэш-функций, заведомо удовлетворяют всем требованиям, предъявляемым к цифровым подписям. Например, невозможно создание сообщения с известным значением подписи, поскольку бесключевая хэш-функция должна быть однонаправленной.

В качестве системы шифрования с открытыми ключами можно использовать, например, систему RSA [2].

Функции хэширования и целостность данных

Хэш-функции – это функции, предназначенные для «сжатия» произвольного сообщения или набора данных, записанного, как правило, в двоичном алфавите, в некоторую битовую комбинацию фиксированной длины, называемую *сверткой.* Хэш-функции имеют разнообразные применения при проведении статистических экспериментов, при тестировании логических устройств, при построении алгоритмов быстрого поиска и проверки целостности записей в базах данных. Например, для осуществления быстрого поиска нужного сообщения в большом списке сообщений различной длины удобнее сравнивать друг с другом не сами сообщения, а короткие значения их сверток, играющих одновременно роль контрольных сумм. Основным требованием к таким хэш-функциям является равномерность распределения их значений при случайном выборе значений аргументов.

В криптографии хэш-функции применяются для решения следующих задач:

– построения систем контроля целостности данных при их передаче или хранении,

– аутентификации источника данных.

При решении первой задачи для каждого набора данных вычисляется значение хэш-функции (называемое *кодом аутентификации сообщения* или *имитовставкой),* которое передается или хранится вместе с самими данными. При получении данных пользователь вычисляет значение свертки и сравнивает его с имеющимся контрольным значением. Несовпадение говорит о том, что данные были изменены.

Хэш-функция, служащая для выработки имитовставки, должна позволять (в отличие от обычной контрольной суммы) осуществлять обнаружение не только случайных ошибок в наборах данных, возникающих при их хранении и передаче, но и сигнализировать об активных атаках злоумышленника, пытающегося осуществить навязывание ложной информации. Для того чтобы злоумышленник не смог самостоятельно вычислить контрольное значение свертки и тем самым осуществить успешную имитацию или подмену данных, хэш-функция должна зависеть от секретного, не известного злоумышленнику параметра – ключа пользователя. Этот ключ должен быть известен передающей и проверяющей сторонам. Такие хэш-функции будем называть *ключевыми.*

Имитовставки, формируемые с помощью ключевых хэш-функций, не должны позволять противнику создавать поддельные (сфабрикованные) сообщения *(fabrication)* при атаках типа *имитация (impersonation)* и модифицировать передаваемые сообщения *(modification)* при атаках типа «*подмена» (substitution).*

При решении второй задачи – аутентификации источника данных – мы имеем дело с не доверяющими друг другу сторонами. В связи с этим

подход, при котором обе стороны обладают одним и тем же секретным ключом, уже неприменим. В такой ситуации применяют схемы цифровой подписи, позволяющие осуществлять аутентификацию источника данных. Как правило, при этом сообщение, прежде чем быть подписано личной подписью, основанной на секретном ключе пользователя, «сжимается» с помощью хэш-функции, выполняющей функцию кода обнаружения ошибок (см. далее). В данном случае хэш-функция не зависит от секретного ключа и может быть фиксирована и известна всем. Основными требованиями к ней являются гарантии невозможности подмены подписанного документа, а также подбора двух различных сообщений с одинаковым значением хэш-функции (в этом случае говорят, что такая пара сообщений образует *коллизию).*

Формализуя сказанное, введем следующее определение. Обозначим через X множество, элементы которого будем называть сообщениями. Обычно сообщения представляют собой последовательности символов некоторого алфавита, как правило, двоичного. Пусть Y – множество двоичных векторов фиксированной длины.

Хэш-функцией называется всякая функция $h: X \to Y$, легко вычислимая и такая, что для любого сообщения M значение $h(M) = H$ *(свертка)* имеет фиксированную битовую длину.

Как правило, хэш-функции строят на основе так называемых *одношаговых сжимающих функций* $y = f(x_1, x_2)$ двух переменных, где x, и y – двоичные векторы длины m и n соответственно, причем n – длина свертки. Для получения значения $h(M)$ сообщение M сначала разбивается на блоки длины m (при этом если длина сообщения не кратна m, то последний блок неким специальным образом дополняется до полного), а затем к полученным блокам M_1, M_2,.., M_N применяют следующую последовательную процедуру вычисления свертки:

$$H_0 = \nu,$$
$$H_i = f\left(M_i, H_{i-1}\right), \quad i = 1,\ldots,N, \qquad (5.4.1)$$
$$h\left(M\right) = H_N.$$

Здесь H_i — некоторый фиксированный начальный вектор. Если функция f зависит от ключа, то этот вектор можно положить равным нулевому вектору. Если же функция f не зависит от ключа, то для исключения возможности перебора коротких сообщений (при попытках обращения хэш-функции) этот вектор можно составить из фрагментов, указывающих дату, время, номер сообщения и т.п.

При таком подходе свойства хэш-функции h полностью определяются свойствами одношаговой сжимающей функции f. Особо выделяют два важных типа криптографических хэш-функций – *ключевые* и *бесключевые.* Первые применяются в системах с симметричными ключами. Ключевые хэш-функции называют *кодами аутентификации сообщений*

(*КАС*) (*message authentication code* (*MAC)).* Они дают возможность без дополнительных средств гарантировать как правильность источника данных, так и целостность данных в системах с доверяющими друг другу пользователями. Бесключевые хэш-функции называются *кодами обнаружения ошибок* (*modification detection code* (*MDC*) *или manipulation detection code, message integrity code* (*MIC*)). Они дают возможность с помощью дополнительных средств (например, шифрования, использования защищенного канала или цифровой подписи) гарантировать целостность данных. Эти хэш-функции могут применяться в системах как с доверяющими, так и не доверяющими друг другу пользователями.

5.5. Инфраструктура открытых ключей

5.5.1. Концепция криптосистемы с открытым ключом

Системы шифрования с открытым ключом называют также асимметричными шифрсистемами [3].

Определение асимметричных шифров и основные понятия относительно их особенностей, связанных с использованием ключей, даны ранее в п.5.2. Шифрсистемы, основанные на использовании асимметричных шифров, используются для организации конфиденциальной связи в сети пользователей в соответствии со схемой, изображенной на рисунке 5.5.1.

Каждый из корреспондентов системы обладает ключом $k = (k_з, k_p)$, состоящим из открытого ключа $k_З$ и секретного ключа k_p. Открытый ключ определяет правило зашифрования E_k, а секретный ключ – правило расшифрования.

Эти правила связаны между собой соотношением $D_k (E_k (M)) = C$ для любого открытого текста M и любого шифрованного текста C.

Знание открытого ключа ***не позволяет*** за приемлемое время (или с приемлемой сложностью) определить секретный ключ.

Обозначим правила зашифрования и расшифрования (на выбранном ключе k) корреспондента A символами E_A и D_A соответственно.

При обмене информацией в реальном времени корреспондент B, желая послать конфиденциальное сообщение M корреспонденту A, связывается с ним по открытому каналу и запрашивает открытый ключ для зашифрования открытого сообщения. Получив также по открытому каналу связи от A такой ключ, B использует правило зашифрования E_A, вычисляет шифрованный текст $C = E_A (M)$, который направляет по каналу связи корреспонденту A.

Получив сообщение C, корреспондент A применяет к нему

преобразование D_A, получая открытый текст M.

Открытый ключ не требуется сохранять в тайне. Необходимо лишь обеспечить его аутентичность, что, как правило, сделать легче, чем обеспечить рассылку и сохранность секретных ключей.

Системы шифрования с открытым ключом осуществляют блоковое шифрование, поэтому открытый текст перед зашифрованием разбивается на блоки выбранного размера, которые последовательно преобразуются таким же образом, как это происходит при использовании блочного шифра в режиме простой замены.

При их использовании асимметричных криптосистем можно легко организовать передачу конфиденциальной информации в сети с большим числом пользователей, так как для рассылки открытых ключей не требуется обеспечивать их секретность [3]. Отправитель открыто связывается с получателем, который либо передает свой ключ отправителю, либо помещает его на общедоступный сервер. Отправитель зашифровывает сообщение на открытом ключе получателя и отправляет его получателю. При этом никто, кроме получателя, обладающего ключом расшифрования, не сможет ознакомиться с содержанием передаваемой информации. В результате такая система шифрования с общедоступным ключом позволяет существенно сократить объем хранимой каждым абонентом секретной ключевой информации. Возможна и другая симметричная ситуация, когда открытый и секретный ключи меняются местами. Такая ситуация возникает тогда, когда требуется обеспечение целостности информации и аутентичности различных аспектов информационного взаимодействия и не требуется обеспечения конфиденциальности информации. При этом необходимо обеспечить такое шифрование информации, при котором зашифровать сообщение мог бы только один отправитель, а расшифровать мог бы каждый.

Асимметричные системы шифрования обеспечивают значительно меньшие скорости шифрования, чем симметричные, в силу чего они обычно используются не столько для шифрования сообщений, сколько для шифрования пересылаемых между корреспондентами ключей, которые затем используются в симметричных системах.

Рассмотрим принцип функционирования асимметричной криптосистемы обеспечения конфиденциальности передаваемых сообщений в соответствии со схемой, изображенной на рисунке 5.5.1. [3, 5].

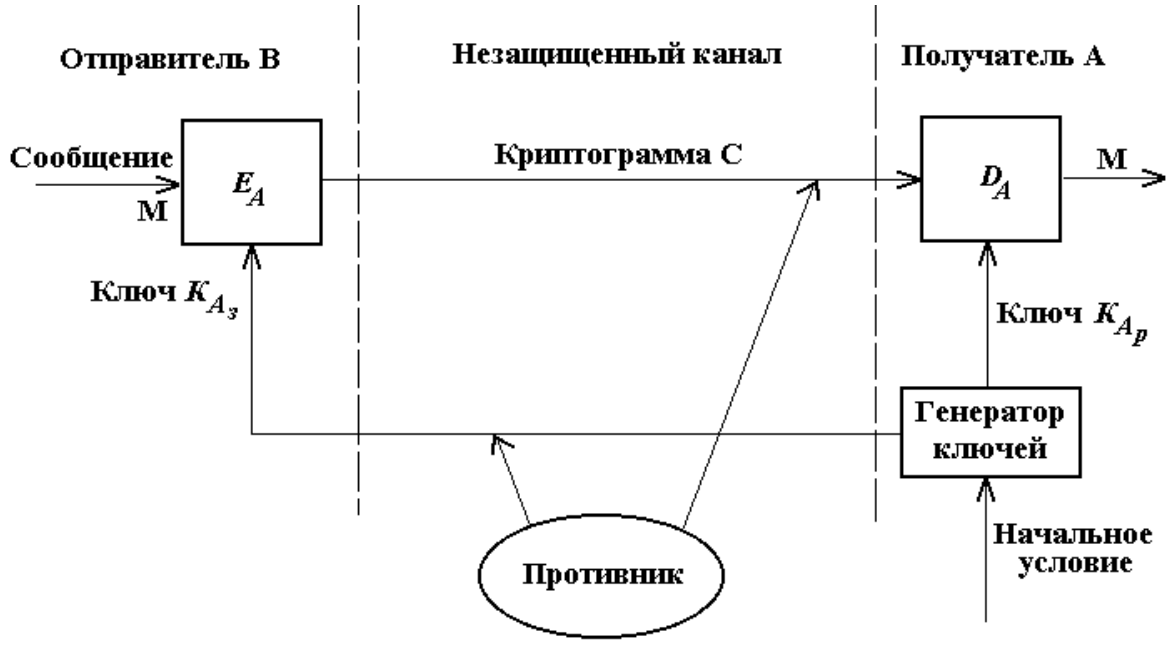


Рис. 5.5.1. Обобщенная схема криптосистемы с открытым ключом

В этой криптосистеме применяют два различных ключа, которые вырабатывает получатель A на приемной стороне: $K_{Аз}$ – открытый ключ отправителя B; $K_{Ар}$ – секретный ключ получателя. Генератор ключей целесообразно располагать на стороне получателя A (при этом не требуется пересылать секретный ключ $K_{Ар}$ по открытому каналу связи).

Значения ключей $K_{Аз}$ и $K_{Ар}$ зависят от начального состояния генератора ключей.

Раскрытие секретного ключа $K_{Ар}$ по известному открытому ключу $K_{Аз}$ должно быть вычислительно неразрешимой задачей.

Характерные особенности асимметричных криптосистем:

1. Открытый ключ $K_{Аз}$ и криптограмма C могут быть отправлены по открытому каналу связи. При этом предполагается, что противнику известны $K_{Аз}$ и C.

2. Алгоритмы зашифрования и расшифрования

$E_A : M \to C$, $D_A : C \to M$ являются открытыми.

Защита информации в асимметричной криптосистеме основана на секретности ключа $K_{Ар}$.

Требования, выполнение которых обеспечивает безопасность асимметричной криптосистемы следующие:

1. Вычисление пары ключей ($K_{Аз}, K_{Ар}$) получателем A на основе начального условия должно быть простым.

2. Отправитель *B*, зная открытый ключ $K_{Аз}$, и сообщение *M*, может легко вычислить криптограмму

$$C = E_{K_{Аз}}(M) = E_A(M).$$

3. Получатель *A*, используя секретный ключ $K_{Ар}$ и криптограмму *C*, может легко восстановить исходное сообщение

$$M = D_{K_{Ар}}(C) = D_A(C) = D_A\left[E_A(M)\right].$$

4. Противник, зная открытый ключ $K_{Аз}$, при попытке вычислить секретный ключ $K_{Ар}$, наталкивается на непреодолимую вычислительную проблему.

5. Противник, зная пару ($K_{Аз}$, *C*), при попытке вычислить открытое сообщение *M*, наталкивается на непреодолимую вычислительную проблему.

Следует отметить, что в виде, представленном на рисунке 5.5.1., криптосистема рассматриваемого типа уязвима для активных атак противника.

Поскольку открытый ключ передается по незащищенному (открытому) каналу, то противник при полном контроле этого канала может не только перехватить ключ зашифрования, но и использовать его для зашифрования ложного сообщения, то есть для дезинформации. При этом, законный получатель сообщения расшифрует ложную криптограмму на своем секретном ключе и получит осмысленный открытый текст, представляющий собой ложное сообщение.

Для противодействия такого рода атакам необходимо развертывание доверенной инфраструктуры центров сертификации открытых ключей, задачей которых является изготовление на открытые ключи сертификатов, обеспечивающих аутентичность этих ключей (рис. 5.5.2.).

С технической точки зрения создание таких центров не представляет трудностей.

Каждый корреспондент ключевой сети, предварительно зарегистрированный в центре сертификации открытых ключей (ЦСКО), прежде чем использовать ключи для обеспечения конфиденциальной связи генерирует пару ключей ($K_{Аз}$, $K_{Ар}$). Секретный ключ расшифрования $K_{Ар}$ оставляет у себя, а открытый ключ зашифрования $K_{Аз}$ отправляет в ЦСКО для изготовления сертификата на этот ключ. Этот сертификат хранится в данном центре.

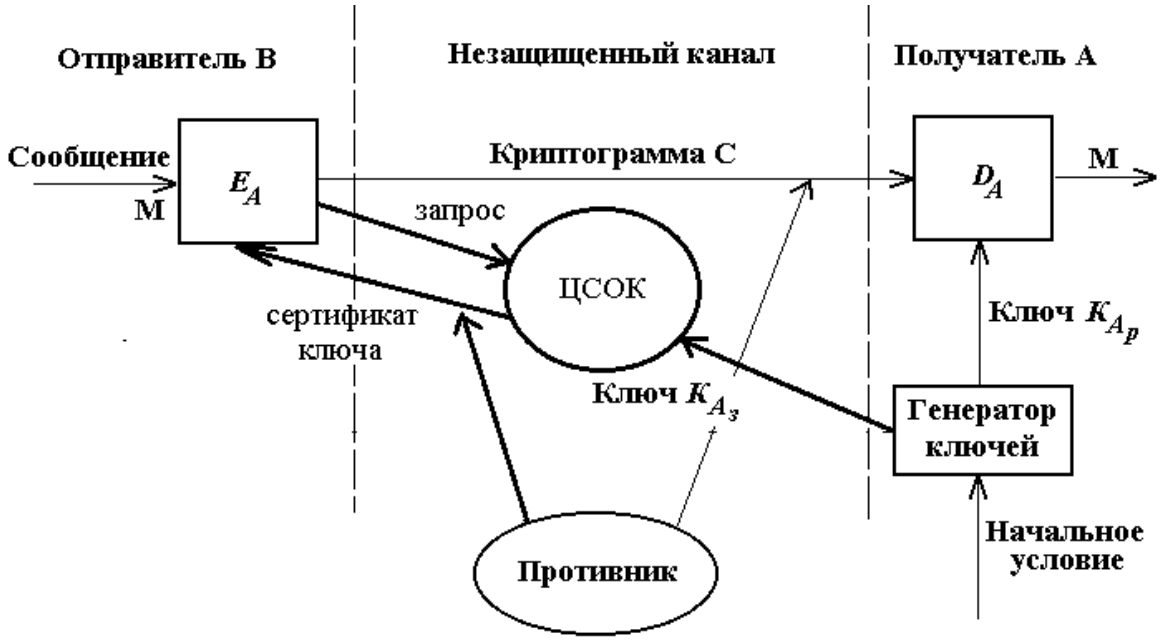


Рис. 5.5.2. Схема криптосистемы с открытым ключом и ЦСОК

Каждый корреспондент, зарегистрированный в ЦСКО (на рис. 5.5.2. это корреспондент *B*) и желающий передать другому корреспонденту, также зарегистрированному в данном центре (корреспонденту *A*), конфиденциальное сообщение, запрашивает открытый ключ для зашифрования этого сообщения не у корреспондента *A*, а в ЦСКО в составе сертификата, обеспечивающего аутентичность (гарантию принадлежности данного открытого ключа корреспонденту *A*) этого ключа. Безопасность функционирования ЦСКО обеспечивается при этом проведении комплекса организационно-технических мероприятий.

Противник при попытке перехвата сертификата, содержащего открытый ключ, сталкивается с проблемой преодоления системы безопасности ЦСКО.

5.5.2. Однонаправленные (односторонние) функции

Концепция асимметричных криптографических систем с открытым ключом основана на применении однонаправленных (односторонних) функций. Неформально такую функцию можно определить следующим образом. Пусть *X* и *Y* – некоторые произвольные множества.

Функция:

$f : X \to Y$

является однонаправленной, если для всех $x \in X$ можно легко вычислить функцию

$y = f(x)$, где $y \in Y$.

Однако, для большинства $y \in Y$ достаточно сложно получить значение $x \in X$, такое, что $f(x) = y$, при этом считают, что существует по

крайней мере одно такое значение x.

Основным критерием отнесения функции f к классу однонаправленных функций является отсутствие эффективных алгоритмов обратного преобразования:

$$Y \to X$$

В качестве первого примера однонаправленной функции рассмотрим целочисленное умножение.

Прямая задача – вычисление произведения двух очень больших целых чисел P и Q, то есть нахождение значения

$$N = P \times Q$$

является относительно несложной задачей для ЭВМ.

Обратная задача – разложение на множители большого целого числа, то есть нахождение делителей P и Q большого целого числа $N = P \times Q$, является практически неразрешимой задачей при достаточно больших значениях N. По современным оценкам теории чисел при целом $N = 2^{654}$ и $P \approx Q$ для разложения числа N потребуется около 10^{23} операций, то есть задача, практически неразрешимая на современных ЭВМ.

Следующий характерный пример однонаправленной функции – это модульная экспонента с фиксированным основанием и модулем.

Пусть A и N – целые числа, такие, что $1 \le A < N$. Определим множество Z_N:

$$Z_N = \{0,1,2,...,N-1\}.$$

Тогда модульная экспонента с основанием A по модулю N представляет собой функцию

$$f_{A,N} : Z_N \to Z_N,$$

$$f_{A,N}(x) = A^x (\mathrm{mod}\, N),$$

где x – целое число, $1 \le x\ 1 \le N - 1$.

Существуют эффективные алгоритмы, позволяющие достаточно быстро вычислить значения функции $f_{A,N}(x)$.

Если $y = A^x$, то естественно записать $x = \log_A(y)$.

Поэтому задачу обращения функции $f_{A,N}(x)$ называют задачей нахождения дискретного логарифма или задачей дискретного логарифмирования.

Задача дискретного логарифмирования формулируется следующим образом. Для известных целых A, N, y найти целое число x, такое, что

$$A^x \bmod N = y.$$

Алгоритм вычисления дискретного логарифма за приемлемое время пока не найден. Поэтому модульная экспонента считается однонаправленной функцией.

По современным оценкам теории чисел при целых числах $A \approx 2^{664}$ и $N \approx 2^{664}$ решение задачи дискретного логарифмирования (нахождение показателя степени *x* для известного *y*) потребует около 10^{26} операций, то есть эта задача имеет в 10^3 раз большую вычислительную сложность, чем задача разложения на множители. При увеличении длины чисел разница в оценках сложности значительно возрастает.

Следует отметить, что пока не удалось доказать факт отсутствия эффективного алгоритма вычисления дискретного логарифма за приемлемое время. Также не доказан факт существования такого алгоритма. В связи с этим, модульная экспонента отнесена к однонаправленным функциям условно, но в настоящее время с успехом применяется на практике.

Вторым важным классом функций, используемых при построении криптосистем с открытым ключом, являются так называемые однонаправленные функции с «потайным ходом» (с «лазейкой»).

Функция $f : X \to Y$ относится к классу однонаправленных функций с «потайным ходом» в том случае, когда она является однонаправленной и возможно эффективное вычисление обратной функции, если известно секретное число, строка или другая информация, ассоциирующаяся с данной функцией, – так называемый «потайной ход».

В качестве примера такой функции можно указать используемую в криптосистеме RSA модульную экспоненту с фиксированным модулем и показателем степени. Переменное основание модульной экспоненты используется для указания числового значения сообщения *M* либо криптограммы *C*.

Рассмотрим конкретные примеры систем шифрования с открытыми ключами.

Шифрсистема RSA

Система RSA была предложена в 1978 г. и в настоящее время является наиболее распространенной системой шифрования с открытым ключом [1].

Пусть $n = p \cdot q$ – целое число, представимое в виде произведения двух больших простых чисел *p*, *q*. Выберем числа *e* и *d* из условия

$$e \cdot d \equiv 1 \left(\mathrm{mod} \varphi(n) \right), \qquad (5.5.1)$$

где $\varphi(n) = (p-1) \cdot (q-1)$ – значение функции Эйлера от числа *n*. Пусть $k = (n, p, q, e, d)$ – выбранный ключ, состоящий из открытого ключа $k_3 - (n, e)$ и секретного ключа $k_р = (n, p, q, d)$. Пусть *M* – блок открытого текста и C – соответствующий блок шифрованного текста. Тогда правила зашифрования и расшифрования определяются формулами:

$$C = E_k(M) = M^e (\mathrm{mod}\ n), \quad D_k(C) = C^d (\mathrm{mod}\ n). \qquad (5.5.2)$$

Заметим, что в соответствии с (2) D_k (C) = *M*.

Аббревиатура *RSA* определяется начальными буквами фамилий создателей этого шифра — Rivest, Shamir, Adleman. Корректность формул (5.5.2) следует из малой теоремы Ферма.

Проанализируем вопрос о стойкости системы RSA. Нетрудно показать, что сложность нахождения секретного ключа системы RSA определяется сложностью разложения числа n на простые множители. В связи с этим нужно выбирать числа p и q таким образом, чтобы задача разложения числа n была достаточно сложна в вычислительном плане. Для этого рекомендуются следующие требования:

1) числа p и q должны быть достаточно большими, не слишком сильно отличаться друг от друга и в то же время быть не слишком близкими друг другу;

2) числа p и q должны быть такими, чтобы наибольший общий делитель чисел $p - 1$ и $q - 1$ был небольшим; желательно, чтобы НОД (p–1, $q - 1$) = 2;

3) p и q должны быть сильно простыми числами; *(сильно простым* называется такое простое число r, что $r + 1$ имеет большой простой делитель, $r - 1$ имеет большой простой делитель s такой, что число $s - 1$ также обладает достаточно большим простым делителем).

В случае, когда не выполнено хотя бы одно из указанных условий, имеются эффективные алгоритмы разложения n на простые множители.

В настоящее время самые большие простые числа, вида $n = p \cdot q$, которые удается разложить на множители известными методами, содержат в своей записи 140 десятичных знаков. Поэтому, согласно указанным рекомендациям, числа p и q в системе RSA должны содержать не менее 100 десятичных знаков.

Шифрсистема Эль-Гамаля

Шифрсистема Эль-Гамаля была предложена в 1985 г. и является фактически одним из вариантов метода выработки открытых ключей Диффи – Хеллмана (который будет рассмотрен далее). Криптографическая стойкость данной системы основана на сложности проблемы логарифмирования в мультипликативной группе конечного простого поля.

Как уже отмечалось, стойкость системы Эль-Гамаля определяется сложностью решения задачи дискретного логарифмирования в Z_p^*. В настоящее время эта задача практически нереализуема для значений p, содержащих не менее 150 десятичных знаков. Рекомендуется также, чтобы число p –1 содержало бы большой простой делитель [1, 2].

Схема Эль-Гамаля

Генерация ключей

Генерируется случайное простое число длины битов.

Выбирается случайное целое число *y* такое, что $1 < g < p$.

Выбирается случайное целое число *x* такое, что $1 < x < p$.

Вычисляется $y = g^x mod\ p$.

Открытым ключом является тройка (*p*,*g*,*y*), закрытым ключом – число.

Работа в режиме подписи

Цифровая подпись служит для того, чтобы можно было установить изменения данных и чтобы установить подлинность подписавшейся стороны. Получатель подписанного сообщения может использовать цифровую подпись для доказательства третьей стороне того, что подпись действительно сделана отправляющей стороной. При работе в режиме подписи предполагается наличие фиксированной хэш-функции $h(\cdot)$, значения которой лежат в интервале $(1, p-1)$.

Подпись сообщений

Для подписи сообщения M выполняются следующие операции:

Вычисляется дайджест сообщения : $m = h(M)$.

Выбирается случайное число $1 < k < p-1$ взаимно простое с $p-1$ и вычисляется $r = g^k mod\ p$.

С помощью расширенного алгоритма Евклида вычисляется число s, удовлетворяющее сравнению:

$m \equiv xr + ks\ (mod\ p-1)$

Подписью сообщения является пара (*r*, *s*).

Проверка подписи

Зная открытый ключ, подпись сообщения проверяется следующим образом:

Проверяется выполнимость условий: $0 < r < p$ и $0 < s < p-1$. Если хотя бы одно из них не выполняется, то подпись считается неверной.

Вычисляется дайджест

Подпись считается верной, если выполняется сравнение:

$y^r r^s \equiv g^m\ (mod\ p)$

Шифрование Эль-Гамаля. Генерация ключей

Генерируется случайное простое число длины битов.

Выбирается случайное целое число такое, что $1 < g < p$.

Выбирается случайное целое число такое, что $1 < x < p$.

Вычисляется $y = g^x mod\ p$.

Открытым ключом является тройка (*p*,*g*,*y*), закрытым ключом – число.

Работа в режиме шифрования

Шифрсистема Эль-Гамаля является фактически одним из способов выработки открытых ключей Диффи – Хеллмана. Шифрование по схеме Эль-Гамаля не следует путать с алгоритмом цифровой подписи по схеме Эль-Гамаля.

Шифрование

Сообщение шифруется следующим образом:

Выбирается сессионный ключ – случайное целое число k такое, что

Вычисляются числа $a = g^k mod\ p$ и $b = y^k M\ mod\ p$.

Пара чисел (a, b) является шифротекстом.

Очевидно, что длина шифротекста в схеме Эль-Гамаля длиннее исходного сообщения вдвое.

Расшифрование

Зная закрытый ключ, исходное сообщение можно вычислить из шифротекста по формуле:

$M = b(a^x)^{-1} mod\ p.$

При этом нетрудно проверить, что

$(a^x)^{-1} \equiv g^{-kx}\ (mod\ p)$

и поэтому

$b(a^x)^{-1} \equiv (y^k M)g^{-xk} \equiv (g^{xk} M)g^{-xk} \equiv M(mod\ p).$

Для практических вычислений больше подходит следующая формула:

$M = b(a^x)^{-1} mod\ p = b \cdot a^{(p-1-x)} mod\ p.$

Шифрсистема Мак-Элиса

Идея, лежащая в основе данной системы, состоит в выборе корректирующего кода, исправляющего определенное число ошибок, для которого существует эффективный алгоритм декодирования. С помощью секретного ключа этот код «маскируется» под общий линейный код, для которого, как известно, задача декодирования не имеет эффективного решения.

В системе Мак-Элиса параметрами системы, общими для всех абонентов, являются числа k, n, t. Для получения, открытого и соответствующего секретного ключа каждому из абонентов системы следует осуществить следующие действия:

1) Выбрать порождающую матрицу $G = G_{k'n}$ двоичного (n,k)-линейного кода, исправляющего t ошибок, для которого известен эффективный алгоритм декодирования.

2) Случайно выбрать двоичную невырожденную матрицу $S = S_{k'k}$.

3) Случайно выбрать подстановочную матрицу $P = P_{n'n}$.

4) Вычислить произведение матриц $G_1 = S \cdot G \cdot P$.

Открытым ключом является пара (G_1, t), секретным – тройка (S, G, P).

Для того чтобы зашифровать сообщение M, предназначенное для абонента A, абоненту B следует выполнить следующие действия:

1) Представить M в виде двоичного вектора длины k.

2) Выбрать случайный бинарный вектор ошибок Z длиной n, содержащий не более t единиц.

3) Вычислить бинарный вектор $C = M \cdot G_A + Z$ и направить его абоненту A.

Получив сообщение C, абонент A вычисляет вектор $C_1 = C \cdot P^{-1}$, с помощью которого, используя алгоритм декодирования кода с порождающей матрицей G, получает далее векторы M_1 и $M = M_1 \cdot S^{-1}$.

В качестве кода, исправляющего ошибки в системе Мак-Элиса, можно использовать код Гоппы. Известно, что для любого неприводимого полинома $g(x)$ степени t над полем $GF(2^m)$ существует бинарный код Гоппы длины $n = 2^m$ и размерности $k \geq n - mt$, исправляющий до t ошибок включительно, для которого имеется эффективный алгоритм декодирования. В настоящее время не известны эффективные алгоритмы дешифрования системы Мак-Элиса, использующей код Гоппы, при правильном выборе параметров системы.

Рекомендуемые параметры этой системы – $n = 1024$, $t = 38$, $k > 644$ – приводят к тому, что открытый ключ имеет размер около 2^{19} бит, а длина сообщения увеличивается при шифровании примерно в 1,6 раза, в связи с чем данная система не получила широкого распространения.

Контрольные вопросы:

1. Обеспечение конфиденциальности – это…
2. Обеспечение целостности – это…
3. Обеспечение аутентификации – это…
4. Назовите методы криптоанализа потоковых шифров.
5. Назовите особенности криптоанализа блоковых шифров.
6. Что такое «шифр»?
7. Что такое «ключ»?
8. Охарактеризуйте симметричные и ассиметричные криптосистемы.
9. Дайте определение и назовите задачи Хэш-функций.
10. Охарактеризуйте понятие электронной подписи.
11. Охарактеризуйте функции удостоверяющих центров.
12. Охарактеризуйте криптосистемы с открытым ключом.
13. Охарактеризуйте однонаправленные функции.
14. Охарактеризуйте шифрсистему RSA.
15. Охарактеризуйте шифрсистему Эль-Гамаля.

Литература к главе 5

9. Рябко, Б. А. Криптографические методы защиты информации : учебное пособие : рек. УМО по образ. / Б. А. Рябко, А. Н. Фионов. – Москва : Горячая линия – Телеком, 2014. – 229 с. – Текст : непосредственный.

10. Авсентьев, О. С. Криптографические методы защиты информации / О. С. Авсентьев, С. В. Зарубин. – Воронеж : ВИ МВД России, 2018. – 200 с. – Текст : непосредственный.

11. Авсентьев, О. С. Практикум по криптографии / О. С. Авсентьев, С. В. Зарубин, Г. В. Перминов. – Воронеж : ВИ МВД России, 2012. – 165 с. – Текст : непосредственный.

12. Молдовян, Н. А. Теоретический минимум и алгоритмы цифровой подписи : учеб. пособие / Н. А. Молдовян. – Санкт-Петербург : БХВ-Петербург, 2010. – 304 с. – Текст : непосредственный.

13. Петров, А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. – Москва: ДМК, 2000. – 448 с. – Текст : непосредственный.

14. ГОСТ 34.311-95. Информационная технология. Криптографическая защита информации. Функция хэширования. – URL: http://gostrf.com/normadata/1/4294824/4294824580.pdf (дата обращения: 13.05.2022). – Текст : электронный.

15. Об электронной подписи: федеральный закон от 06.04.2011 № 63-ФЗ. – URL: http://www.kremlin.ru/acts/bank/32938 (дата обращения: 13.05.2022). – Текст : электронный.

Глава 6. Реагирование на инциденты кибербезопасности и их обработка

6.1. Алгоритм совершения киберпреступления

В процессе атаки злоумышленники осуществляют структурированную последовательность шагов, называемую kill chain [1] (рис. 6.1.1). Первоначально kill chain использовался как военный термин для описания структуры военного вторжения. Зная последовательность действий противника, обороняющаяся сторона может выработать стратегию защиты и противостоять нападению. Впоследствии термин kill chain стал использоваться для описания компьютерных угроз. Аналогично, на основе информации об этапах компрометации ИС, сотрудники, ответственные за ИБ, могут выстраивать систему защиты ИС.

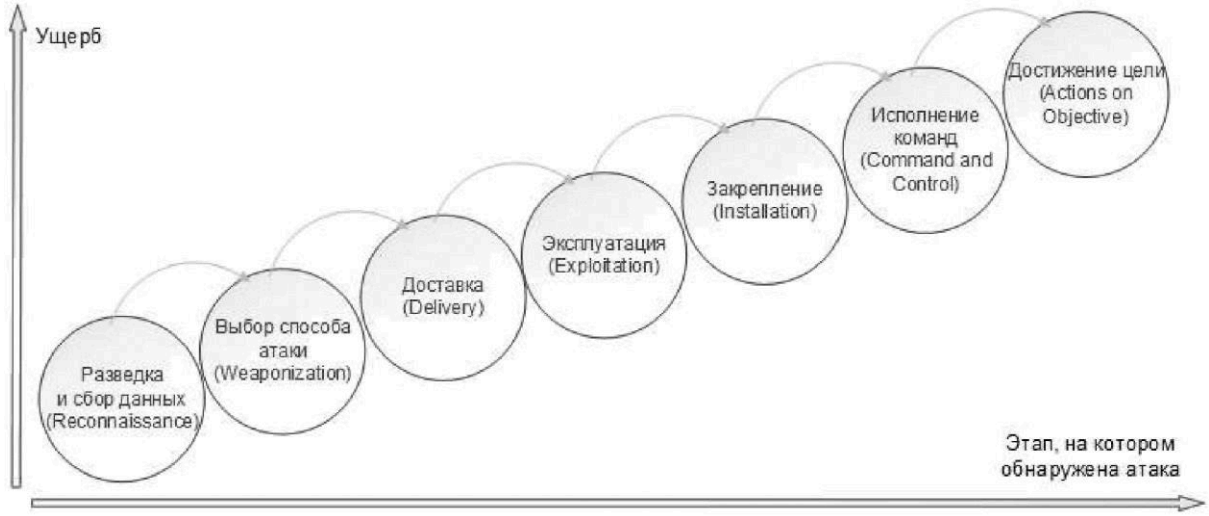


Рис. 6.1.1. Жизненный цикл кибератаки

От того, на каком этапе kill chain была обнаружена угроза, зависит эффективность расследования и размер материального и репутационного ущерба, нанесённого атакуемой организации. Обнаружение на этапе достижения цели (позднее обнаружение) означает, что система ИБ ИС оказалась неспособна противостоять атаке и злоумышленник достиг поставленных целей. Наименьший ущерб будет нанесён в случае обнаружения на этапах Доставки или Закрепления (раннее обнаружение).

На этапе разведки происходит сбор информации об организации, которая будет атакована, а также о её информационных активах. В частности, злоумышленник пытается установить организационную структуру компании, стек технологий, используемый в атакуемой организации, средства обеспечения ИБ, возможности использования социальной инженерии по отношению к сотрудникам (например, выявить их аккаунты в социальных сетях). Разведка может быть пассивной (Passive

reconnaissance) и активной (Active reconnaissance). Пассивная разведка заключается в получении информации без непосредственного воздействия на атакуемую ИС (например, просмотр DNS и WhoIs информации, связанной с ИС организации). Активная разведка включает в себя взаимодействие с атакуемой ИС: сканирование портов, поиск уязвимостей ИС и другие действия. Вся собранная злоумышленником информация служит источником знаний для следующего этапа.

На этапе выбора способа атаки (weaponization), используя информацию, полученную на этапе разведки и сбора данных, злоумышленник определяет способ атаки. При этом злоумышленник может создать новое вредоносное программное обеспечение (ПО), позволяющее эксплуатировать обнаруженные уязвимости. Злоумышленник внедряет ПО, которое будет использоваться при атаке, в файлы MS Office (.docx, .xlsx), PDF-документы, электронные письма или на съёмные носители. На этом же этапе происходит выбор способа доставки созданного вредоносного ПО в атакуемую информационную систему: с помощью заражения публичного ресурса компании, через одного из сотрудников или через компрометацию компаний-субподрядчиков, работающих с атакуемой организацией.

На этапе доставки (delivery) атакующий должен обеспечить попадание разработанного на прошлом шаге вредоносного ПО в ИС атакуемой организации. Обычно для этого используются вложения электронной почты, вредоносные и фишинговые ссылки, watering hole-атаки (заражения сайтов, которые посещают сотрудники атакуемой организации) или зараженные USB-устройства.

На этапе эксплуатации (exploitation) после попадания в ИС атакуемой организации вредоносное ПО, используя уязвимости ИБ, распространяется по сети и закрепляется на зараженных машинах в ожидании команд, поступающих от злоумышленника. Команды от злоумышленника могут поступать как через интернет (от командных центров C&C – Communication and control), так и с помощью доставки другого вредоносного ПО (например, если на машине отсутствует прямое подключение к интернету).

На этапе закрепления (installation) вредоносное ПО осуществляет заражение компьютера для того, чтобы не быть обнаруженным или удаленным после перезагрузки или установки обновления, блокирующего возможность использовать одну из уязвимостей ИС. Обычно для заражения используются утилиты несанкционированного управления (backdoor).

На этапе исполнения команд (command and control) с помощью соединения, устанавливаемого изнутри ИС атакованной организации, вредоносное ПО реализует взаимодействие с сервером управления, подконтрольным злоумышленнику (Communication And Control Server –

C&C Server). Таким образом, атакующий получает управление компьютером внутри ИС атакуемой организации.

На этапе достижение цели (actions on objective), получив управление, злоумышленник может работать с данными на скомпрометированном компьютере, не только осуществляя несанкционированный доступ, но и изменяя или удаляя их. Кроме того, атакующий может попытаться заразить другие машины в ИС, для того чтобы увеличить объем доступной информации.

6.2. Основные этапы процесса реагирования на инциденты информационной безопасности

Основными целями реагирования на инциденты ИБ являются минимизация ущерба, скорейшее восстановление исходного состояния ИС и разработка плана по недопущению подобных инцидентов в будущем. Эти цели достигаются на двух основных этапах: расследование инцидента и восстановление системы.

При расследовании требуется определить:

– начальный вектор атаки;

– вредоносные программы и инструменты, которые были использованы в процессе атаки;

– какие системы были затронуты в ходе атаки; размер ущерба, нанесенного атакой;

– завершена атака или нет, то есть достиг ли атакующий своей цели; временные рамки атаки.

После завершения расследования необходимо разработать и внедрить план восстановления системы, используя информацию, полученную при расследовании (рис. 6.2.1).

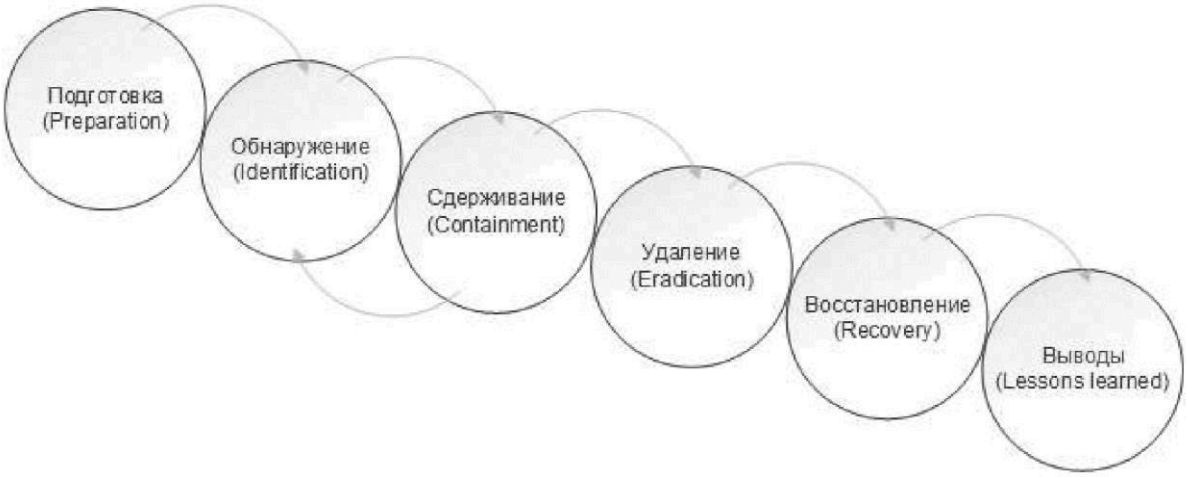


Рис. 6.2.1. Основные этапы реагирования на киберинциденты

На основе информации о жизненном цикле атаки (kill chain) возможно формирование системы защиты. Исходя из анализа стратегии, используемой при атаке на ИС, специалистами ИБ выработана стратегия реагирования на инциденты.

Подготовка (Preparation). В момент, когда происходит инцидент ИБ, от сотрудников, ответственных за ИБ, требуются моментальные и точные действия. Поэтому для эффективного реагирования необходима предварительная подготовка. Сотрудники, ответственные за ИБ, должны обеспечить защиту ИС и проинформировать пользователей, а также ИТ-персонал, о важности мер по обеспечению ИБ.

Обнаружение (Identification). Сотрудники, занимающиеся реагированием на инциденты, должны определить, является ли обнаруженное ими с помощью различных систем обеспечения ИБ событие инцидентом или нет. Для этого могут использоваться публичные отчеты, потоки данных об угрозах, средства статического и динамического анализа образцов ПО и другие источники информации. Статический анализ выполняется без непосредственного запуска исследуемого образца и позволяет выявить различные индикаторы, например, строки, содержащие URL-адреса или адреса электронной почты. Динамический анализ подразумевает выполнение исследуемой программы в защищенной среде (песочнице) или на изолированной машине с целью выявления поведения образца и сбора артефактов его работы. На рис. 6.2.2 показан цикл обнаружения индикаторов компрометации информационной системы.

Рис. 6.2.2. Цикл обнаружения индикаторов компрометации информационной системы

Сбор индикаторов компрометации является итерационным процессом. На основе первоначальной информации, полученной от SIEM-системы, происходит формирование сценариев обнаружения, применение которых, как правило, приводит к выявлению новых индикаторов компрометации. Полученные таким образом индикаторы помогают уточнить границы атаки и служат отправной точкой для нового цикла обнаружения. Дальнейшие шаги предпринимаются, только если событие решено считать инцидентом ИБ.

Сдерживание (Containment). Сотрудники, ответственные за ИБ, должны идентифицировать скомпрометированные компьютеры и настроить правила безопасности таким образом, чтобы заражение не распространилось дальше по сети. Кроме того, на этом этапе необходимо перенастроить сеть таким образом, чтобы ИС компании могла продолжать работать без зараженных машин.

Удаление (Eradication). Цель этого этапа – привести скомпрометированную ИС в состояние, в котором она была до заражения. Сотрудники, ответственные за ИБ, удаляют вредоносное ПО, а также все артефакты, которые оно могло оставить на зараженных компьютерах в ИС.

Восстановление (Recovery). Ранее скомпрометированные компьютеры вводятся обратно в сеть. При этом сотрудники, ответственные за ИБ, некоторое время продолжают наблюдать за состоянием этих машин и ИС в целом, чтобы убедиться в полном устранении угрозы.

Выводы (Lessons learned). Сотрудники, ответственные за ИБ, анализируют произошедший инцидент, вносят необходимые изменения в конфигурацию ПО и оборудования, обеспечивающего ИБ, и формируют рекомендации для того, чтобы в будущем предотвратить подобные инциденты. При невозможности полного предотвращения будущей атаки составленные рекомендации позволят ускорить реагирование на подобные инциденты.

6.3. Выявление и фиксация следов киберпреступлений

Основное отличие киберпреступлений от инцидентов в сфере информационной безопасности является то, что к инцидентам готовятся. Устанавливают средства защиты, содержащие расширенные возможности аудита событий.

Современное общество уже невозможно представить без различных средств вычислительной техники, которые не только помогают развитию общества, но и являются как орудиями преступления, так и «свидетелями» его совершения. В главе 28 Уголовного кодекса Российской Федерации [2] приведены статьи, устанавливающие преступность и наказуемость деяний в сфере компьютерной информации. Есть в кодексе и иные статьи, в которых также фигурируют средства вычислительной техники и

информация, обрабатываемая с их использованием. Однако на современном этапе любое преступление в той или иной мере имеет отношение к средствам хранения, обработки и передачи информации. И при совершении большинства преступлений помимо выявления свидетелей, проводятся ставшие уже привычными основные мероприятия в отношении технических средств:

– определение телефонов, зарегистрированных у операторов, предоставляющих услуги мобильной связи на данной территории;

– получение записей видеокамер;

– получение информации из других технических средств, сохранивших данные о событии.

Для помощи в получении и интерпретации таких данных в законодательстве Российской Федерации [3] предусмотрен специалист или эксперт: лицо «обладающее специальными знаниями».

При этом согласно ст. 168 УПК РФ следователь удостоверяется в его компетентности. В большинстве случаев это формальное действие, так как следователь не обладает достаточными знаниями, чтобы убедиться в уровне компетентности специалиста в области компьютерной информации. И данное действие сводится к выяснению образования специалиста, прохождения им дополнительного обучения, опыта работы в данной области. То есть, следователю в качестве специалиста проще всего привлечь штатного эксперта по данному направлению. Но их не так много, они заняты производством экспертиз, да и в некоторых республиках СНГ больше не входят в структуру МВД. Выход очевиден: следователи или оперативные сотрудники должны обладать определенным набором умений и навыков в данной области. Их необходимо этому обучить.

Рассмотрим общие методы и принципы выявление и фиксация следов киберпреступлений. Следует указать, что данная глава содержит основные этапы выявления и фиксации следов киберпреступлений штатными средствами операционных систем и с использованием бесплатного программного обеспечения. Данные об использовании специализированного платного программного обеспечения не приводятся ввиду специфичности их применения. Однако данные содержащиеся в данной главе позволят также определить действия пользователя по подключению и использованию внешних машинных носителей, которые могли подключаться к исследуемому устройству. Так как следует иметь в виду, что информация может сохраняться не только на самом машинном носителе, непосредственно установленном в осматриваемом компьютере, но также она сохраняется на подключенных к нему различных носителях, флэшки, внешние диски, оптические диски. Соответственно, проследив этапы подключения этих устройств, можно установить те файлы, которые не сохранены на основном носителе. В этом случае эксперт или специалист укажет следственным органам либо оперативным сотрудникам

данные для поиска соответствующих носителей. Также немаловажно определить сведения о работе с сетевыми источниками хранения данных, так как информация может сохраняться в облачных сервисах. Выявление этих хранилищ также является одной из приоритетных задач по анализу информации.

Помимо общего подхода к анализу информации, следует обратить внимание на различие подходов непосредственно к получению информации, необходимой для анализа и восстановления данных в различных операционных системах.

В операционных системах под управлением Linux подход к анализу данных определяется особенностью формирования следовой картины хранения данных. Так, в операционных системах семейства Linux, в отличие от операционных систем семейства Windows NT, информация будет храниться в определённых файлах, в которых представления времени в ряде случаев записывается как количество секунд, прошедших с 1 января 1970 года до события согласно системному времени, естественно, это затруднит анализ такой информации. В операционных системах семейства Windows NT такой подход используется для указания времени установки операционной системы в реестре. Кроме того, следует учесть, что в операционных системах семейства Linux ряд информации о работе системы и действиях пользователей возможно получить только на активной системе, то есть на включённом компьютере.

Следует иметь в виду, что не всегда возможно получить данные о киберпреступлениях непосредственно, «в лоб». Существует множество косвенных мест хранения данных. Например, разработчики компании Belkasoft получение таких данных назвали карвингом. Для пояснения этого можно привести следующий пример. При работе с офисными документами, в частности, Microsoft Word помимо самого файла создаётся как его авто- копия так, и временные файлы. Из этих файлов возможно получить либо сам файл целиком, либо его содержимое. Помимо прочего, данные, которые вводились в формате Microsoft Word, будут сохранены в оперативной памяти, файлах подкачки и гибернации. В следующих пунктах рассмотрим основные методы анализа данных на машинных носителях информации, а также способы восстановления этих данных и, соответственно, выявления и фиксации следов киберпреступлений.

6.4. Распространенные виды инцидентов кибербезопасности

При работе с компьютерными носителями информации важно обеспечение неизменности информации на осматриваемом электронном носителе информации, например, НЖМД – накопителях на жестких магнитных дисках, различных flash – носителях и т.п.

Самым приемлемым по критерию максимальной простоты и

минимальных затрат времени и материальных средств следует признать блокировку записи по USB – порту при подключении через данный интерфейс исследуемых носителей. При этом необходимо наличие переходных устройств HDD – USB адаптеров, например SATA - USB или IDE - USB. Далее необходимо отключить запись по USB порту в реестре изменением значения «WriteProtect». Надо иметь в виду, что данный способ позволяет блокировать запись и в операционной системе Windows 10. Однако данные ключи по умолчанию в реестре не существуют, их необходимо создавать вручную или создать соответствующие файлы для активации или дезактивации этих функций. Для вступления в силу изменений достаточно переподключить носитель информации.

Данные реестра для блокировки записи:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies]

"WriteProtect"=dword:00000001

Данные реестра для снятия блокировки записи:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies]

"WriteProtect"=dword:00000000

Также блокировку можно выполнять через «Локальную политику безопасности», в разделе «Административные шаблоны».

Для надежной блокировки, с наименьшими затратами возможно использование HDD – USB адаптеров с функцией блокировки записи, такие устройства выпускает компания AGESTAR, или блокиратора «Дубль 3», выпускаемого компанией «Ланпроект».

Дальнейшая работа возможна как непосредственно с исследуемым носителем информации, так и с созданными посекторной копией или образом. Предпочтительнее в дальнейшем исследовании использовать именно образ или посекторную копию предоставленного носителя информации, что позволит избежать возможных дефектов, связанных с эксплуатацией носителя информации. Кроме того, полученную посекторную копию возможно использовать как непосредственно для запуска с исследуемого системного блока или ноутбука, так и для запуска в виртуальных средах (виртуальных машинах).

Для запуска в виртуальных машинах подходят также и полученные образы носителей информации. Современные средства создания образов, например, продукты AccessData FTK Imager, Acronis, Paragon Software Group позволяют создавать сразу образы носителей информации в форматах распространённых виртуальных машин. Пожалуй, продукты AccessData FTK Imager и Acronis несколько предпочтительней, так как имеется возможность их загрузки и запуска с внешних носителей на ядре

Linux.

При создании образов носителей информации необходимо использовать режим посекторного резервного копирования с функцией копирования нераспределённого пространства. При использовании этого способа возможно использовать подключённый образ для восстановления удаленной информации.

Также возможно использование и других программных решений, сред для Windows и Linux (загрузочных носителей на базе специализированных продуктов Linux).

Удобным решением следует признать использование программно-аппаратного комплекса PC-3000. Данный комплекс позволяет создавать копии данных в том числе с неисправных носителей информации.

Осмотр средств вычислительной техники. **Правовые основы участия специалиста при проведении следственных действий определяются статьей 58 УПК РФ**. Согласно статье 58 УПК РФ: «1. Специалист – лицо, обладающее специальными знаниями, привлекаемое к участию в процессуальных действиях в порядке, установленном настоящим Кодексом, для содействия в обнаружении, закреплении и изъятии предметов и документов, применении технических средств в исследовании материалов уголовного дела, для постановки вопросов эксперту, а также для разъяснения сторонам и суду вопросов, входящих в его профессиональную компетенцию».

Началом следственных действий, связанных с осмотром средств вычислительной техники, является определение соответствия системного времени текущему, с указанием часового пояса. Если время не соответствует текущему, то целесообразно указать системное время на данный момент, например: «на 22 часа, 12 минут, 31 декабря 2022 года, московского времени системное время составляет 00 часов, 01 минуту, 1 января 2000 года, часовой пояс (UTC+03:00) Москва, Санкт-Петербург, Волгоград».

Данные о часовом поясе, используемом операционной системой, хранятся в следующем ключе реестра:

HKLM/SYSTEM\ControlSet00*\Control\TimeZoneInformation.

Также данные о часовом поясе можно определить и традиционным способом, в меню «Дата и время».

При осмотре и изъятии средств вычислительной техники основной задачей также является обеспечение сохранности информации, имеющейся на машинных носителях. Для этого необходимо предотвратить несанкционированные действия, связанные с изменением данных. Кроме того, особое внимание необходимо обратить на наличие активных

процессов в системе. К таким процессам следует отнести:

– наличие криптоконтейнеров;

– наличие логических дисков, подключенных (смонтированных) из файлов образов;

– наличие виртуальных машин (в том числе активных);

– наличие подключенных локальных сетевых ресурсов (файлов, сетевых дисков, баз данных и т.д.);

– наличие подключенных «облачных» ресурсов;

– наличие подключенных глобальных сетевых ресурсов (сайтов, файлов, P2P ресурсов и т.д.).

Следует иметь в виду, что если при наличии этих процессов не произвести сохранение данной информации, то при выключении компьютера она будет утеряна.

При копировании информации с осматриваемых средств вычислительной техники в протокол необходимо занести следующие данные:

– сведения о времени подключения носителей, на которые осуществляется копирование;

– данные носителя, на который осуществляется копирование (модель, объем, серийный номер);

– данные о копируемой информации, (расположение на первичном источнике, наименование копируемой информации, хэш-значение, объем);

– способ копирования (например, запись оптических дисков);

– применяемое для копирования программное обеспечение (например, создание образа раздела с помощью программного обеспечения).

Рассмотрим на примере операционных систем семейства Windows NT основные методы, применяемые для анализа данных с целью выявления и фиксации следов киберпреступлений. Первым шагом является получение данных об операционной системе, далее необходимо получить данные о подключении внешних устройств и сетевом оборудовании.

Получение сведений об операционной системе. Для осмотра активной системы можно использовать как штатные средства операционной системы, так и набор специализированных утилит. В ряде случаев применение специализированных средств может быть недоступно, например, при отсутствии возможности подключения внешних носителей или ограничениях, связанных с запуском программного обеспечения. Поэтому сначала рассмотрим штатные средства операционной системы.

При осмотре средств вычислительной техники при активной системе, штатными средствами операционной системы семейства Windows NT следует выполнить следующие действия.

Для определения данных об операционной системе целесообразно воспользоваться данными командной строки – «SYSTEMINFO». При этом можно как выполнить копирование информации из выводимого окна, так и сразу вывести информацию в файл. В этом случае префикс команды будет следующим:

SYSTEMINFO> [путь куда где будет создан файл]:\[имя файла].txt – например «SYSTEMINFO> D:\systeminfo.txt» будет осуществлять вывод информации о системе на локальном компьютере в текстовый файл «systeminfo.txt», расположенный в корневой директории диска «D». Аналогичные действия, по копированию информации в файл, можно применять и к остальным командам, приведенным ниже.

Применение данной команды позволит получить следующие сведения о системе:

```
Имя узла:                  IDEA-PC
Название ОС:               Майкрософт Windows 8.1 для одного языка
Версия ОС:                 6.3.9600 Н/Д построение 9600
Изготовитель ОС:           Microsoft Corporation
Параметры ОС:              Изолированная рабочая станция
Построение ОС:             Multiprocessor Free
Зарегистрированный владелец:    windows@yandex.ru
Зарегистрированная организация:
Код продукта:              00179-40433-46356-AAOEM
Дата установки:            01.08.2016, 0:24:34
Время загрузки системы:        16.12.2017, 21:06:46
Изготовитель системы:      LENOVO
Модель системы:            20251
Тип системы:               x64-based PC
Процессор(ы):              Число процессоров - 1.
                           [01]: Intel64 Family 6 Model 58 Stepping 9 GenuineIntel ~2200 МГц
Версия BIOS:               LENOVO 7ACN24WW, 25.06.2013
Папка Windows:             C:\WINDOWS
Системная папка:           C:\WINDOWS\system32
Устройство загрузки:       \Device\HarddiskVolume2
Язык системы:              ru;Русский
Язык ввода:                ru;Русский
Часовой пояс:              (UTC+03:00) Москва, Санкт-Петербург, Волгоград
Полный объем физической памяти:   6 023 МБ
Доступная физическая память:      4 029 МБ
Виртуальная память: Макс. размер: 6 983 МБ
Виртуальная память: Доступна:     4 713 МБ
Виртуальная память: Используется: 2 270 МБ
Расположение файла подкачки:      C:\pagefile.sys
Домен:                     WORKGROUP
Сервер входа в сеть:       \\MicrosoftAccount
Исправление(я):            Число установленных исправлений - 260.
```

Сетевые адаптеры: Число сетевых адаптеров - 3.
[01]: Qualcomm Atheros AR8172/8176/8178 PCI-E Fast Ethernet Controller (NDIS 6.30)
Имя подключения: Ethernet
Состояние: Носитель отключен
[02]: Broadcom 802.11n Network Adapter
Имя подключения: Беспроводная сеть
Состояние: Носитель отключен
[03]: Устройства Bluetooth (личной сети)
Имя подключения: Сетевое подключение Bluetooth
Состояние: Носитель отключен
Требования Hyper-V: Расширения режима мониторинга виртуальной машины: Да
Виртуализация включена во встроенном ПО: Да
Преобразование адресов второго уровня: Да
Доступно предотвращение выполнения данных: Да

Помимо учетных данных операционной системы получены данные о объеме оперативной памяти, расположении файла подкачки «pagefile.sys», сетевых адаптерах и др. Данная информация необходима для оценки возможностей получения доступа к сокрытой информации. К примеру, из дампа оперативной памяти и файла подкачки возможно получить множество необходимой информации, пароли, тексты, графические файлы, адреса интернета.

Так же информацию о системе можно получить из приложения «сведения о системе», для запуска которого можно использовать команду «msinfo32».

Кроме того, сведения о системе содержатся в реестре. Данные реестра, содержащие сведения об операционной системе, хранятся в ветви:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion.

Дата инсталляции «InstallDate». Дата установки операционной системы хранится в шестнадцатеричном и десятичном виде. Параметр «InstallDate» показывает количество секунд, прошедших с 1 января 1970 г. до момента установки операционной системы.

Идентификационные номера продукта и пути установки. Для получения сведений об использовании операционной системы, необходимо просмотреть данные из журнала событий Windows (рис. 6.4.1.).

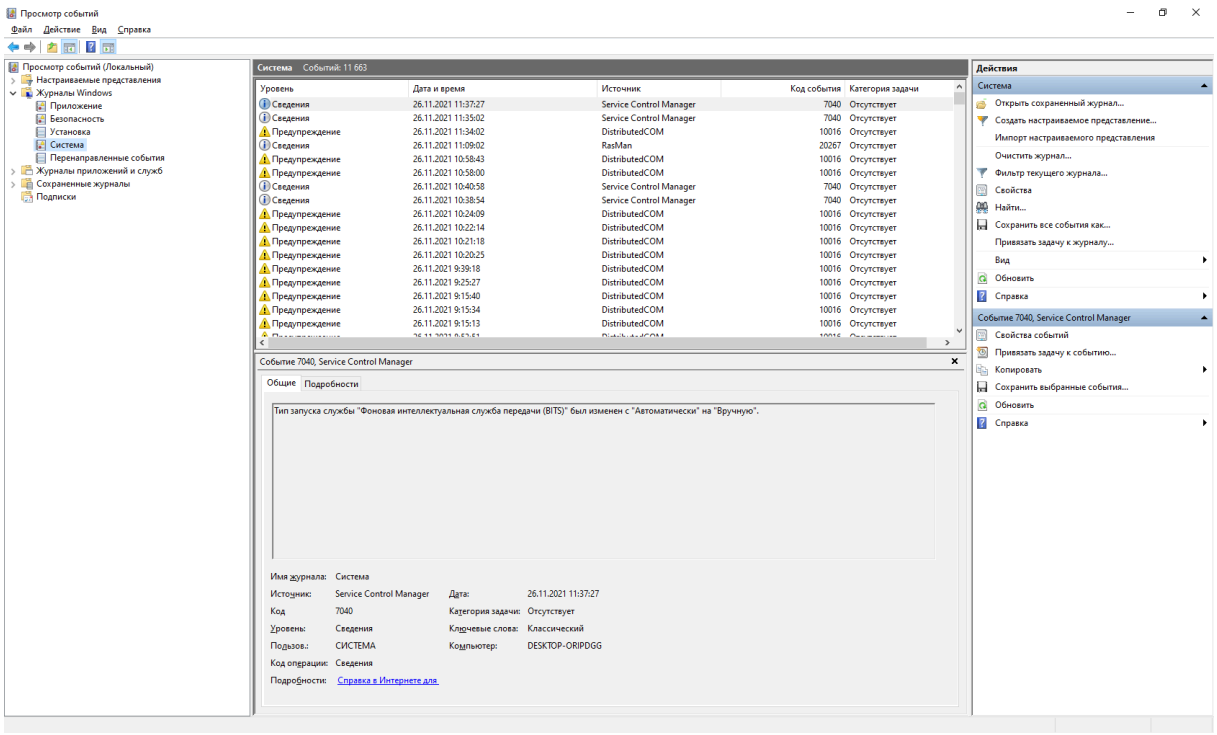


Рис. 6.4.1. Окно журнала событий Windows

Ниже приведены некоторые основные коды, отображающие работу системы для операционных систем WINDOWS 7 и выше.

Код 1. Отображает системное время изменения времени операционной системы (отображает информацию и при смене часового пояса);

Код 12. Отображает системное время запуска операционной системы;

Код 13. Отображает системное время завершения работы операционной системы;

Код 26 (источник Application Popup). Отображает информацию об использовании компьютера другими пользователями. Позволяет выявить работу иных пользователей с системой. Завершение работы Windows может привести к потере данных, открытых этим пользователем;

Код 36 (источник Time-Service). Отображает информацию об использовании компьютера другими пользователями. Завершение работы «Windows» может привести к потере данных, открытых этим пользователем;

Код 41 (источник Kernel-Power). Сообщает о перезагрузке системы в результате критического сбоя или неожиданного отключения питания;

Код 6008. Отображает сообщение об аварийном завершении работы системы.

На рисунке 6.4.2 приведены данные из журнала «Система» о времени запуска операционной системы.

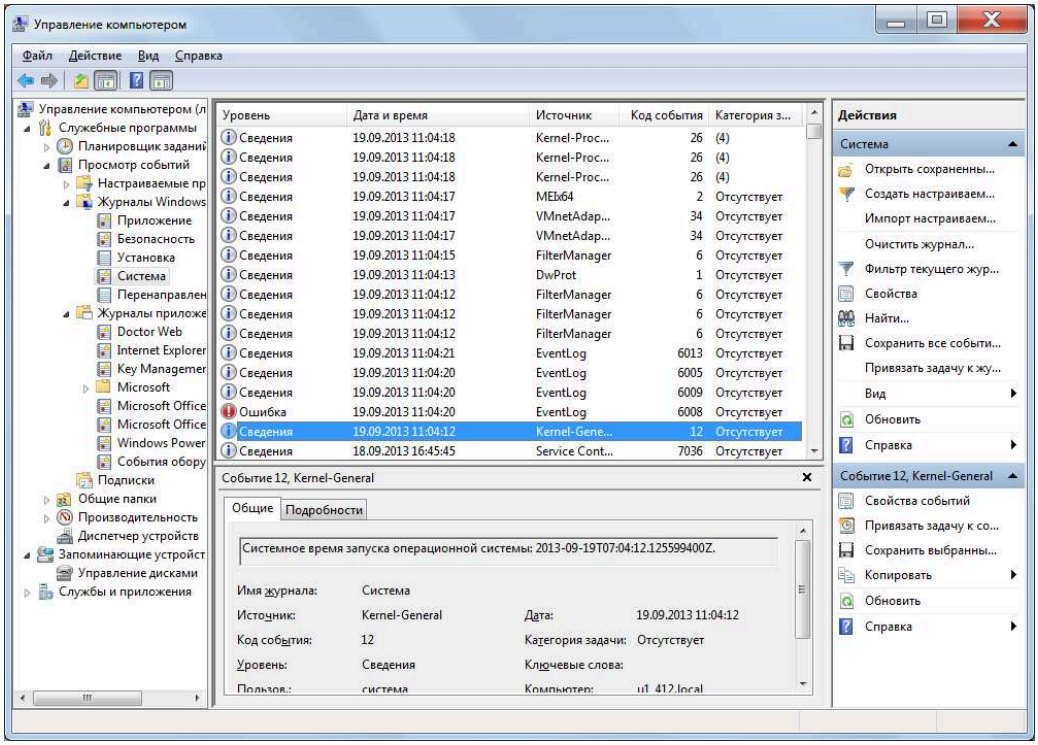


Рис. 6.4.2. Данные из журнала «Система» о времени запуска операционной системы

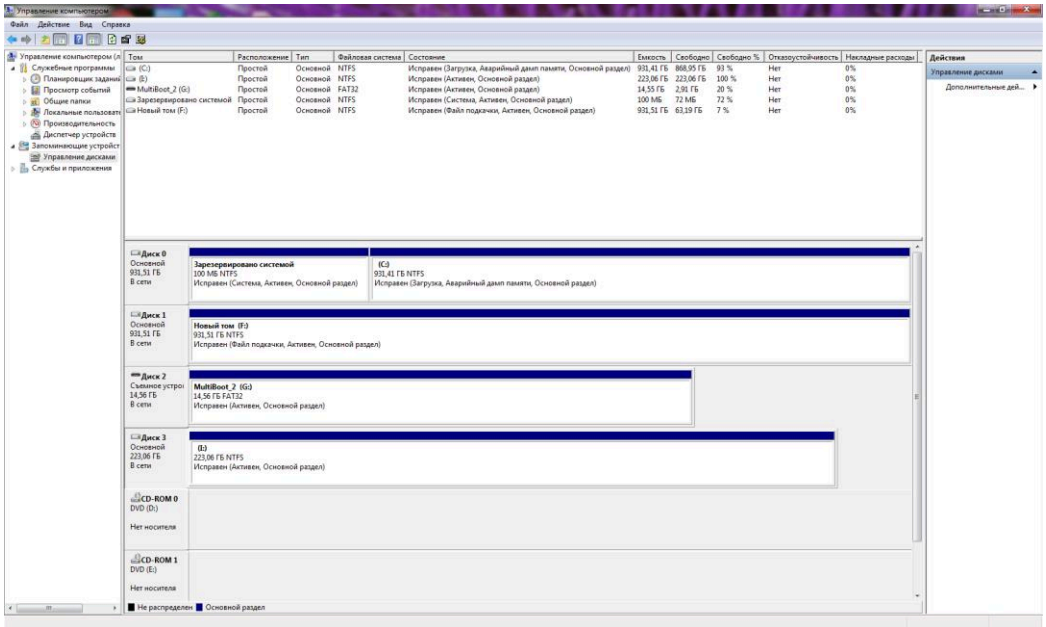


Рис. 6.4.3. Данные о подключении логических томов и дисков

Для определения подключенных в системе логических томов и дисков необходимо просмотреть подменю меню «Управление дисками», входящее в состав меню «Управление» на вкладке «Компьютер».

Далее необходимо просмотреть меню «Свойства» каждого из дисков, либо наличие логических томов и дисков, определяемых как устройство.

На рисунке 6.4.3 приведены данные о подключении логических томов и дисков в меню «Управление дисками».

При этом обозначенный на рисунке 6.4.3 «Диск 3» является виртуальным диском подключенным (смонтированным) из файла образа «Acronis». Что видно при просмотре меню «Свойства» данного диска. Содержание меню приведено на рисунке 6.4.4.

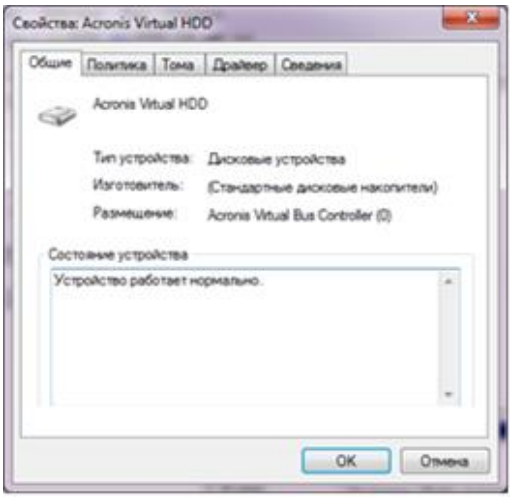


Рис. 6.4.4 Содержание меню «Свойства» виртуального раздела «Acronis»

Также информация о подключении виртуального раздела «Acronis» будет содержаться в разделе «Дисковые устройства» диспетчера устройств операционной системы семейства Windows NT. Содержание диспетчера устройств при подключенном виртуальном разделе «Acronis» приведено на рисунке 6.4.5.

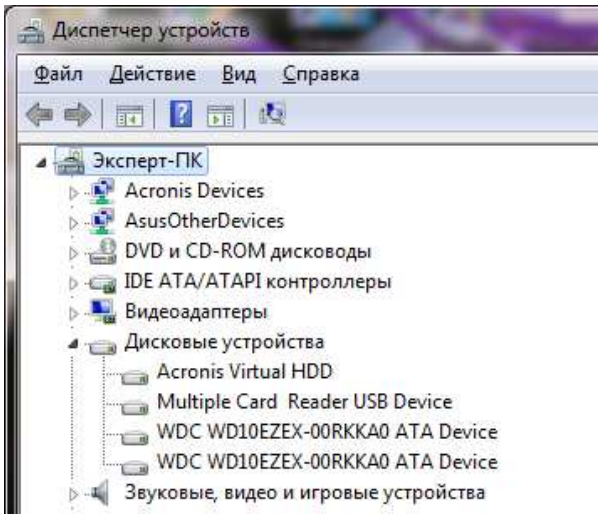


Рис. 6.4.5. Содержание панели диспетчер устройств при подключенном виртуальном разделе «Acronis»

Однако не всегда данные о подключении виртуальных разделов

отражаются в разделе «Управление дисками». Это не происходит в случаях подключения криптоконтейнеров или в ряде случаев, файлов образов как логических разделов. Так на рис. 6.4.6, 6.4.7 приведены примеры подключения файла образа логического раздела, произведенного с помощью программного обеспечения AccessData FTK Imager.

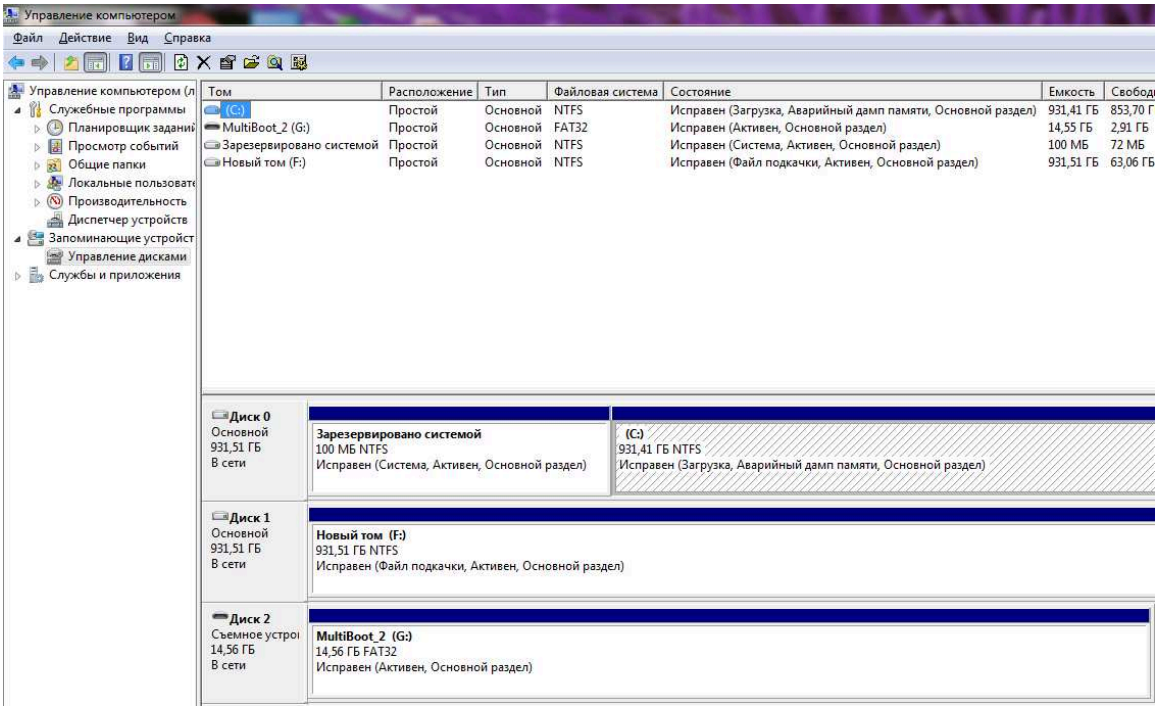


Рис. 6.4.6. Вид подключенного образа в оснастке управления дисками

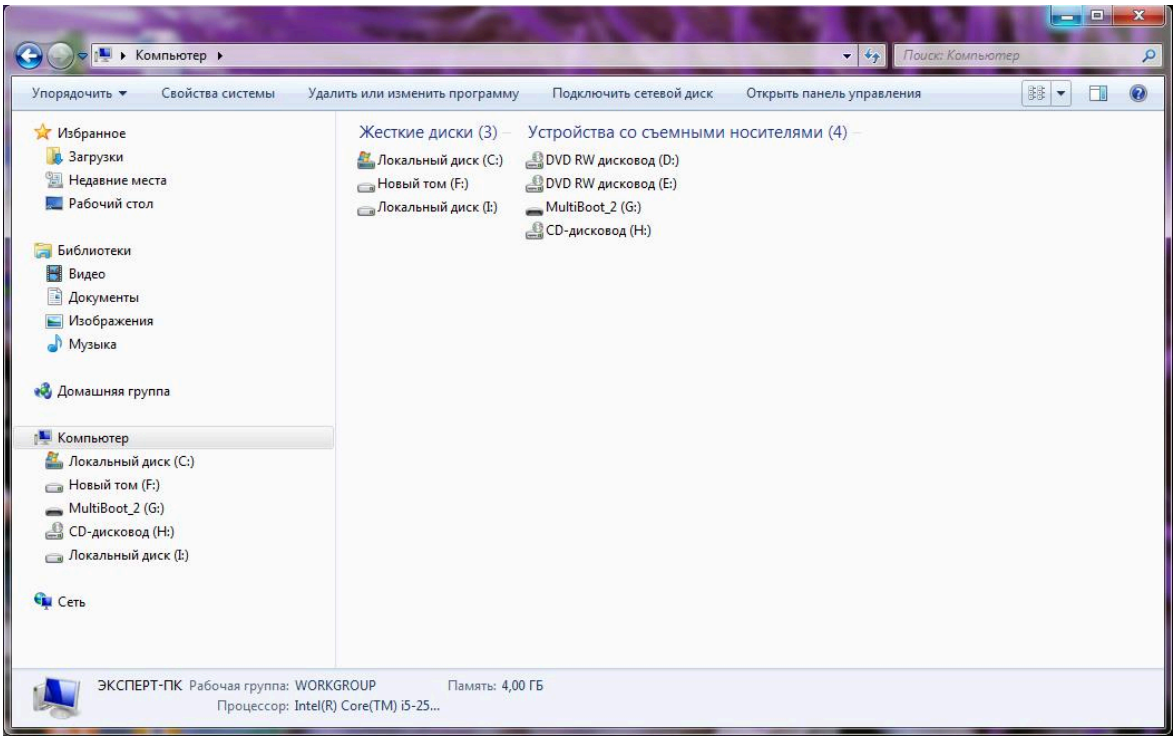


Рис. 6.4.7. Вид подключенного образа в обозревателе дисков

Из рисунка видно, что раздел отражается как логический в проводнике операционной системы, однако отсутствует в разделе «Управление дисками». В этом случае необходимо выяснить причину возникновения такого расхождения и принять неотложные меры к сохранению информации, которая может быть безвозвратно утрачена, если произвести выключение системы. Информацию о процессах, в результате чего произошли расхождения, можно выяснить в «Диспетчере задач». Кроме того, в описанном примере программного обеспечения AccessData FTK Imager будет отражаться в меню «Приложения» диспетчера задач. А, например, при использовании TrueCryp, данные об активации программного обеспечения будут доступны только в меню «Процессы».

Получение данных о сетевых соединениях. Из данных командной строки SYSTEMINFO можно получить сведения о сетевых адаптерах и подключениях. Более подробные сведения о сети можно получить с помощью командной строки IPCONFIG /ALL. Здесь будут содержаться следующие сведения:

– настройка протокола IP для Windows;

– сетевое имя компьютера;

– физические адреса адаптеров.

Если в системе имеется виртуальная машина, то она так же будет отражаться как сетевой адаптер.

Следует обратить внимание, что если в системе используется несколько сетевых адаптеров, то для адаптеров, которые в данный момент неактивны, в строе «состояние среды» будет обозначение «среда передачи недоступна»! Ниже приведены сведения, полученные с помощью данной команды и выгруженные в файл.

Настройка протокола IP для Windows

Имя компьютера . . . . . : DESKTOP-ORIPDGG
Основной DNS-суффикс . . . . . :
Тип узла. . . . . : Гибридный
IP-маршрутизация включена . . . . : Нет
WINS-прокси включен . . . . . : Нет
Порядок просмотра суффиксов DNS . : local.vimvd.ru

Адаптер беспроводной локальной сети Беспроводная сеть:

Состояние среды. . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . . :
Описание. . . . . : Realtek RTL8188SU Wireless LAN 802.11n USB 2.0 Network Adapter
Физический адрес. . . . . : 00-14-D1-D1-50-86
DHCP включен. . . . . : Да

```
   Автонастройка включена. . . . . : Да

Адаптер беспроводной локальной сети Подключение по локальной сети* 9:

   Состояние среды. . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . :
   Описание. . . . . : Microsoft Hosted Network Virtual Adapter
   Физический адрес. . . . . : 00-14-D1-D1-50-86
   DHCP включен. . . . . : Да
   Автонастройка включена. . . . . : Да

Адаптер Ethernet Ethernet:

   DNS-суффикс подключения . . . . . : local.vimvd.ru
   Описание. . . . . : Intel(R) 82579V Gigabit Network Connection
   Физический адрес. . . . . : 50-46-5D-74-0E-2B
   DHCP включен. . . . . : Да
   Автонастройка включена. . . . . : Да
   Локальный IPv6-адрес канала . . . : fe80::f90e:9d63:3960:e405%10(Основной)
   IPv4-адрес. . . . . : 192.168.118.236(Основной)
   Маска подсети . . . . . : 255.255.255.0
   Аренда получена. . . . . : 26 ноября 2021 г. 8:53:48
   Срок аренды истекает. . . . . : 27 ноября 2021 г. 8:53:47
   Основной шлюз. . . . . : 192.168.118.50
   DHCP-сервер. . . . . : 192.168.118.3
   IAID DHCPv6 . . . . . : 105924189
   DUID клиента DHCPv6 . . . . . : 00-01-00-01-28-4B-7B-23-50-46-5D-74-0E-2B
   DNS-серверы. . . . . : 192.168.118.3
   NetBios через TCP/IP. . . . . : Включен

Адаптер PPP VPN:

   DNS-суффикс подключения . . . . . :
   Описание. . . . . : VPN
   Физический адрес. . . . . :
   DHCP включен. . . . . : Нет
   Автонастройка включена. . . . . : Да
   IPv4-адрес. . . . . : 172.16.14.231(Основной)
   Маска подсети . . . . . : 255.255.255.255
   Основной шлюз. . . . . : 0.0.0.0
   DNS-серверы. . . . . : 172.16.14.221
   NetBios через TCP/IP. . . . . : Включен
```

Далее необходимо определить активные подключения, для чего используется команда «NETSTAT». Команда выводит сведения о TCP и UDP-соединений, таблицы маршрутизации, слушаемых портов, статистических данных.

Команда «NBTSTAT–n» отображает таблицу NetBIOS-имен на локальном компьютере. Таблица содержит следующие сведения: «Имя»,

«тип», «Состояние». Состояние «Зарегистрирован» означает, что имя зарегистрировано с использованием широковещательного запроса или с помощью сервера WINS. Также отражается количество локальных подключений.

Команда «NET USE» – отображает список сетевых дисков, подключенных в системе.

Команда «NET SHARE» – отображает список ресурсов, к которым открыт общий доступ.

Команда «NET LOCALGROUP Администраторы» - отображает список пользователей локальной группы «Администраторы» системы.

Команда «NET USER» – отображает список пользователей.

Данные о настройке Dialupass сетевых соединений, в том числе VPN хранятся в файле:

%SystemDrive%\Users\[имя пользователя]\AppData\AppData\Roaming\Microsoft\Network\Connections\Pbk\rasphone.pbk

Фрагмент содержимого файла:

DEVICE=vpn

PhoneNumber=vpn.local.vimvd.ru

Если для данных подключений сохранен пароль, то для его просмотра необходимо специализированное программное обеспечение, например, входящей в комплект «NirLauncher – Nirsoft» утилитой «Dialupass».

Данные о беспроводном подключении wi-fi можно получить командой «NETSH WLAN SHOW PROFILES».

Профили «wi-fi» хранятся в каталоге %ProgramData%\Microsoft\Wlansvc\Profiles\Interfaces в виде файлов *.xml.

Если для данных подключений сохранен пароль, то для его просмотра в явном виде, возможно использовать специализированное программное обеспечение, например, входящей в комплект «NirLauncher – Nirsoft» утилитой «WirelessKeyView».

Информация о всех сетевых подключениях, в том числе о подключениях по локальной сети, хранится в журнале Приложений и служб Microsoft-Windows-NetworkProfile/Operational (выполняется). Файл данного журнала расположен по адресу: «%SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-NetworkProfile%4Operational.evtx». Данным о подключении соответствует код события 1000.

Ниже приведены примеры из журнала для различных подключений.

Подключение для локальной сети:

Сеть подключена

Имя: Сеть

Тип: Неуправляемая

Состояние: Подключен
Категория: Публичная

xmlns="**http://schemas.microsoft.com/win/2004/08/events/event**">
- <System>
<Provider Name="**Microsoft-Windows-NetworkProfile**" Guid="**{fbcfac3f-8459-419f-8e48-1f0b49cdb85e}**" />
<EventID>10000</EventID>
<Version>0</Version>
<Level>4</Level>
<Task>0</Task>
<Opcode>0</Opcode>
<Keywords>0x4000200000000020</Keywords>
<TimeCreated SystemTime="**2021-11-29T12:37:26.0362317Z**" />
<EventRecordID>2794</EventRecordID>
<Correlation />
<Execution ProcessID="**1800**" ThreadID="**628**" />
<Channel>Microsoft-Windows-NetworkProfile/Operational</Channel>
<Computer>DESKTOP-ORIPDGG</Computer>
<Security UserID="**S-1-5-19**" />
</System>
- <EventData>
<Data Name="**Name**">Сеть</Data>
<Data Name="**Description**">Сеть</Data>
<Data Name="**Guid**">{13363522-92d9-4fc4-a151-c083335e02af}</Data>
<Data Name="**Type**">0</Data>
<Data Name="**State**">1</Data>
<Data Name="**Category**">0</Data>
</EventData>
</Event>

Подключение для VPN:

Сеть подключена
Имя: VPN
Описание: VPN
Тип: Неуправляемая
Состояние: Подключен
Категория: Публичная

- <Event xmlns="**http://schemas.microsoft.com/win/2004/08/events/event**">
- <System>
<Provider Name="**Microsoft-Windows-NetworkProfile**" Guid="**{fbcfac3f-8459-419f-8e48-1f0b49cdb85e}**" />
<EventID>10000</EventID>
<Version>0</Version>
<Level>4</Level>
<Task>0</Task>
<Opcode>0</Opcode>
<Keywords>0x4000200000000020</Keywords>
<TimeCreated SystemTime="**2021-11-28T12:27:30.2096527Z**" />
<EventRecordID>2636</EventRecordID>
<Correlation />
<Execution ProcessID="**1744**" ThreadID="**7408**" />
<Channel>Microsoft-Windows-NetworkProfile/Operational</Channel>

<Computer>DESKTOP-ORIPDGG</Computer>
<Security UserID="**S-1-5-19**" />
</System>
- <EventData>
<Data Name="**Name**">VPN</Data>
<Data Name="**Description**">VPN</Data>
<Data Name="**Guid**">{b84cd10d-0a3e-4580-854f-07ccffff8ffd}</Data>
<Data Name="**Type**">0</Data>
<Data Name="**State**">1</Data>
<Data Name="**Category**">0</Data>
</EventData>
</Event>

Подключение для сетей wi-fi:

Сеть подключена
Имя: AndroidAPfc89
Описание: AndroidAPfc89
Тип: Неуправляемая
Состояние: Подключен
Категория: Частная

<Event xmlns="**http://schemas.microsoft.com/win/2004/08/events/event**">
- <System>
<Provider Name="**Microsoft-Windows-NetworkProfile**" Guid="**{fbcfac3f-8459-419f-8e48-1f0b49cdb85e}**" />
<EventID>10000</EventID>
<Version>0</Version>
<Level>4</Level>
<Task>0</Task>
<Opcode>0</Opcode>
<Keywords>0x4000200000000020</Keywords>
<TimeCreated SystemTime="**2021-11-28T14:57:35.5332991Z**" />
<EventRecordID>2686</EventRecordID>
<Correlation />
<Execution ProcessID="**1800**" ThreadID="**7420**" />
<Channel>Microsoft-Windows-NetworkProfile/Operational</Channel>
<Computer>DESKTOP-ORIPDGG</Computer>
<Security UserID="**S-1-5-19**" />
</System>
- <EventData>
<Data Name="**Name**">AndroidAPfc89</Data>
<Data Name="**Description**">AndroidAPfc89</Data>
<Data Name="**Guid**">{3f59751b-de23-444d-a76a-cf87b960ecac}</Data>
<Data Name="**Type**">0</Data>
<Data Name="**State**">1</Data>
<Data Name="**Category**">1</Data>
</EventData>
</Event>

Кроме того информация о VPN соединениях хранится в журналах:

– «Система», код события 20267, источник RasMan;

– «Приложение», код события 20226, источник RasClient.

Информация о wi-fi подключениях хранится в журналах:

– «Система», код события 20267, источник WLAN-AutoConfig;

– «Приложений и служб» -Windows-WLAN-AutoConfig/Operational. Файл данного журнала расположен по адресу: %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-WLAN-AutoConfig%4Operational.evtx.

Из данных представлений можно получить информацию, как о времени подключения, так и об устройствах, с помощью которых данное подключение осуществлялось. В частности, для рассматриваемого wi-fi подключения можно определить источник, предоставляющий доступ к сети - AndroidAPfc89.

Следует обратить внимание, что в журнале WLAN-AutoConfig содержится более подробная информация о wi-fi подключениях. Так, на ниже приведены данные о подключениях, код событий 8001, и об отключениях, код событий 8003, от wi-fi сети.

Служба автонастройки беспроводной сети успешно подключилась к беспроводной сети.
Сетевой адаптер: Realtek RTL8188SU Wireless LAN 802.11n USB 2.0 Network Adapter
GUID интерфейса: {631eb393-ef5a-4d30-9da9-22777c86ddc1}
Режим подключения: Подключение вручную с использованием профиля
Имя профиля: AndroidAPfc89

- <Event xmlns="**http://schemas.microsoft.com/win/2004/08/events/event**">
- <System>
<Provider Name="**Microsoft-Windows-WLAN-AutoConfig**" Guid="**{9580d7dd-0379-4658-9870-d5be7d52d6de}**" />
<EventID>8001</EventID>
<Version>0</Version>
<Level>4</Level>
<Task>24010</Task>
<Opcode>190</Opcode>
<Keywords>0x8000000020000600</Keywords>
<TimeCreated SystemTime="**2021-11-28T14:57:34.3415108Z**" />
<EventRecordID>52</EventRecordID>
<Correlation />
<Execution ProcessID="**2456**" ThreadID="**3660**" />
<Channel>Microsoft-Windows-WLAN-AutoConfig/Operational</Channel>
<Computer>DESKTOP-ORIPDGG</Computer>
<Security UserID="**S-1-5-18**" />
</System>
- <EventData>
<Data Name="**InterfaceGuid**">{631eb393-ef5a-4d30-9da9-22777c86ddc1}</Data>
<Data Name="**InterfaceDescription**">Realtek RTL8188SU Wireless LAN 802.11n USB 2.0 Network Adapter</Data>
<Data Name="**ConnectionMode**">Подключение вручную с использованием

профиля</Data>
<Data Name="**ProfileName**">AndroidAPfc89</Data>
<Data Name="**SSID**">AndroidAPfc89</Data>
<Data Name="**BSSType**">Infrastructure</Data>
<Data Name="**PHYType**">802.11n</Data>
<Data Name="**AuthenticationAlgorithm**">WPA2-Personal</Data>
<Data Name="**CipherAlgorithm**">AES-CCMP</Data>
<Data Name="**OnexEnabled**">0</Data>
<Data Name="**ConnectionId**">0x3</Data>
<Data Name="**NonBroadcast**">false</Data>
</EventData>
</Event>

Служба автонастройки WLAN успешно отключилась от беспроводной сети.

Сетевой адаптер: Realtek RTL8188SU Wireless LAN 802.11n USB 2.0 Network Adapter
GUID интерфейса: {631eb393-ef5a-4d30-9da9-22777c86ddc1}
Режим подключения: Подключение вручную с использованием профиля
Имя профиля: AndroidAPfc89

<Event xmlns="**http://schemas.microsoft.com/win/2004/08/events/event**">
- <System>
<Provider Name="**Microsoft-Windows-WLAN-AutoConfig**" Guid="**{9580d7dd-0379-4658-9870-d5be7d52d6de}**" />
<EventID>8003</EventID>
<Version>0</Version>
<Level>4</Level>
<Task>24010</Task>
<Opcode>192</Opcode>
<Keywords>0x8000000040000600</Keywords>
<TimeCreated SystemTime="**2021-11-28T15:04:41.2671922Z**" />
<EventRecordID>55</EventRecordID>
<Correlation />
<Execution ProcessID="**2456**" ThreadID="**3660**" />
<Channel>Microsoft-Windows-WLAN-AutoConfig/Operational</Channel>
<Computer>DESKTOP-ORIPDGG</Computer>
<Security UserID="**S-1-5-18**" />
</System>
- <EventData>
<Data Name="**InterfaceGuid**">{631eb393-ef5a-4d30-9da9-22777c86ddc1}</Data>
<Data Name="**InterfaceDescription**">Realtek RTL8188SU Wireless LAN 802.11n USB 2.0 Network Adapter</Data>
<Data Name="**ConnectionMode**">Подключение вручную с использованием профиля</Data>
<Data Name="**ProfileName**">AndroidAPfc89</Data>
<Data Name="**SSID**">AndroidAPfc89</Data>
<Data Name="**BSSType**">Infrastructure</Data>
<Data Name="**Reason**">Сеть отключена драйвером.</Data>
<Data Name="**ConnectionId**">0x3</Data>
<Data Name="**ReasonCode**">0</Data>
</EventData>
</Event>

Для определения данных об использовании программных продуктов (на примере Microsoft Office) просматривается следующая информация:

– данные из ветви реестра HKEY_CURRENT_USER\Software;

– данные из ветвей реестра, содержащих сведения об использовании программного обеспечения, например, данные из ветви реестра HKEY_CURRENT_USER\Software\Microsoft\Office\XX.X\Word\File MRU содержат сведения об открытых в приложении файлах;

– данные из файлов журнал системы;

– данные из файлов «Prefetch»;

– данные из файлов гибернации - hiberfil.sys;

– данные из файлов подкачки- pagefile.sys;

– данные из оперативной памяти;

– данные из файлов журналирования;

– данные из файлов ссылок;

– данные из MFT (*Master File Table* - «Главная файловая таблица»);

– данные из директории %SYSTEMDRIVE% \ Users \% USERNAME% \ AppData \ Roaming \ Microsoft \ Windows \ Recent;

– данные из файла реестра Amcache.hve, расположенного %SYSTEMROOT% \appcompat\Programs\;

– данные из файлов переходов – Jump Lists.

Файлы списков переходов «* .automaticDestinations-ms» расположены по следующему пути:

%SYSTEMDRIVE% \ Users \% USERNAME% \ AppData \ Roaming \ Microsoft \ Windows \ Recent \ AutomaticDestinations

Для просмотра файлов можно использовать утилиту «JumpListsView» входящий в комплект «NirLauncher - Nirsoft».

Данные об использовании Microsoft Office (на примере Word) содержатся:

– в файле «WINWORD.EXE-B9C5483D.pf» директории «Prefetch»;

– в журнале приложений – «Microsoft Office Alerts».

Для Windows 7 и выше в директории %SYSTEMDRIVE%\Users\%USERNAME%\AppData\Roaming\Microsoft\ Office\ Последние файлы\

В реестре для каждого компонента «Office»:

HKEY_CURRENT_USER\Software\Microsoft\Office\XX.X\Word\File MRU

И ключе типа:

HKEY_USERS\S-1-5-21-3243842915-810645812-68586957-1000\Software\Microsoft\Office\XX.X\Word\File MRU

– в файлах гибернации – hiberfil.sys;

– в файлах подкачки – pagefile.sys;

– данные из оперативной памяти;

– в данных MFT;

– в данных из директории %SYSTEMDRIVE% \ Users \% USERNAME% \ AppData \ Roaming \ Microsoft \ Windows \ Recent;

– в данных из файлов переходов – Jump Lists.

Причем частично содержимое файлов Microsoft Office сохраняется в файлах гибернации – hiberfil.sys, файлах подкачки – pagefile.sys, в оперативной памяти.

Рассмотрим способ получения данных из MFT. MFT (англ. Master File Table – «Главная файловая таблица») – база данных, в которой хранится информация о содержимом тома с файловой системой NTFS.

Для получения данных из MFT сначала необходимо скопировать сам файл $MFT на доступное специалисту пространство его машинного носителя, т.е. в директорию для исследования. Для этой цели воспользуемся программным продуктом Access Data FTK Imager. С его помощью возможно получать данные из служебных областей диска. После запуска программы необходимо воспользоваться меню Add All Attached Devices  , с помощью чего открываем необходимый раздел диска. Для каждого раздела с файловой системой NTFS имеется свой файл $MFT. Далее открываем раздел root и получаем доступ к содержимому раздела. Для копирования файла активируем меню Export Files. После того как файл будет скопирован, необходимо преобразовать его в табличный вид. Для это воспользуемся программой MFTDump. Программа работает из командной строки. После преобразования создается файл mftdump_localhost.txt, который необходимо открыть в табличном редакторе, например, Exel. При этом для корректного отображения кириллицы необходимо выбрать формат 65001: юникод (UTF-8).

MFTDump предоставляет три формата отчетов; короткие, стандартные и длинные. Если не указать параметр / s (короткий) или / l (длинный) в командной строке, выходной отчет будет в стандартном формате. Пример поля отчета показан на рисунке 6.4.8.

Названия столбцов обозначают следующее: Rename – переименование файла; Local Move – перемещение файла в пределах одной файловой системы; Volume move – перемещение между файловыми системами; Copy – копирование файла; Create – создание файла; Delete – удаление файла; Open – открытие файла; Properties – просмотр свойств файла; Attributes – изменение атрибутов файла; Modify – изменение файла.

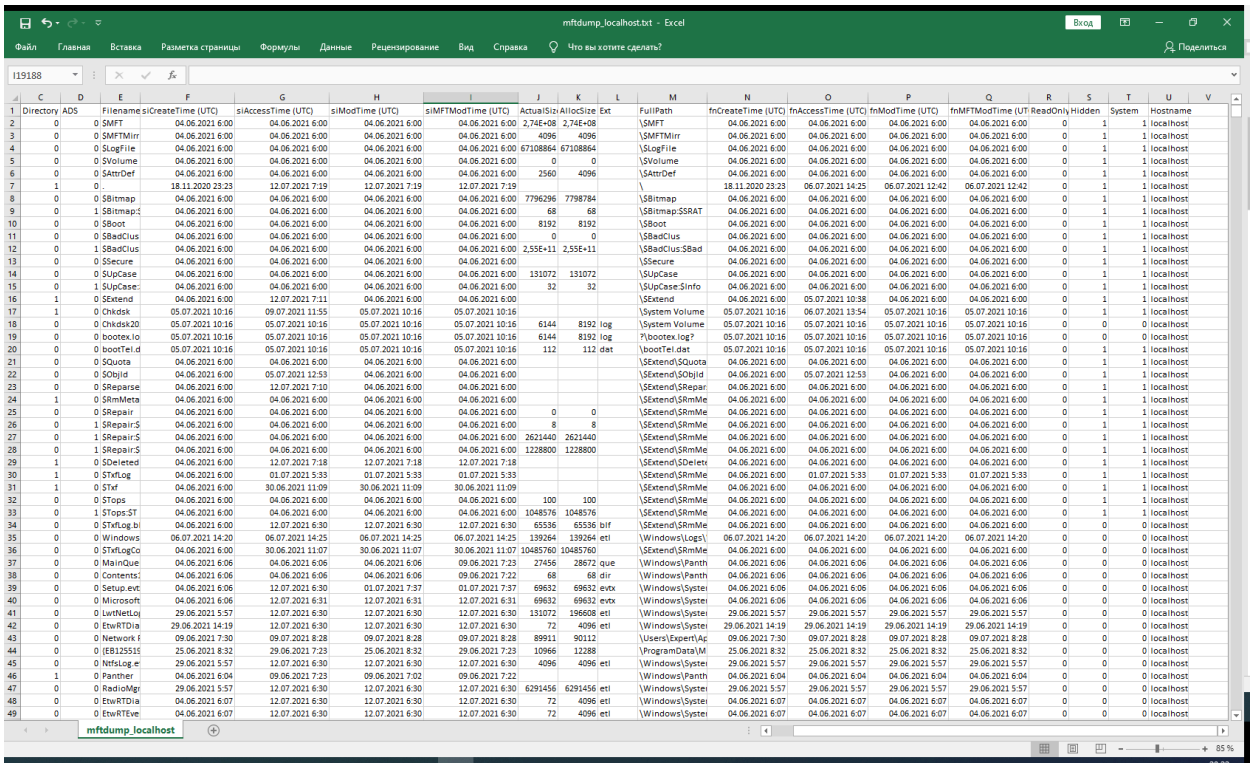


Рис. 6.4.8. Пример поля отчета

Для работы с таблицей необходимо воспользоваться фильтрами. Так, для поиска документов, созданных в Word, в столбце Ext выбираем фильтр по расширению файлов doc и docx.

Данные об удалении файлов находятся в столбце Deleted, значение 1. Следует обратить внимание, что изменения в файл $MFT сохраняются при любом подключении к соответствующему разделу диска. В том числе и при загрузке с внешнего носителя или подключении диска как внешнего.

Соответствующие данные о выявленных программных продуктах целесообразно привести в виде таблицы. Также данные об использовании программных продуктов хранятся в файле Amcache.hve, расположенном по адресу «%SystemRoot%\appcompat\Programs\. Данный файл является файлом реестра, о чем свидетельствует сигнатура файла 72 65 67 66 04 00 в HEX, и regf в ANSI кодировке. Для просмотра файла можно воспользоваться программой Windows Registry Recovery от компании MiTeC. Для копирования файла в активной системе можно воспользоваться программой AccessData FTK Imager. В файле Amcache.hve содержатся сведения о расположении и временных параметрах запуска программных продуктов. Так, для определения данных о программном продукте Word достаточно произвести поиск по данному слову. Результаты приведены на рисунке 6.4.9.

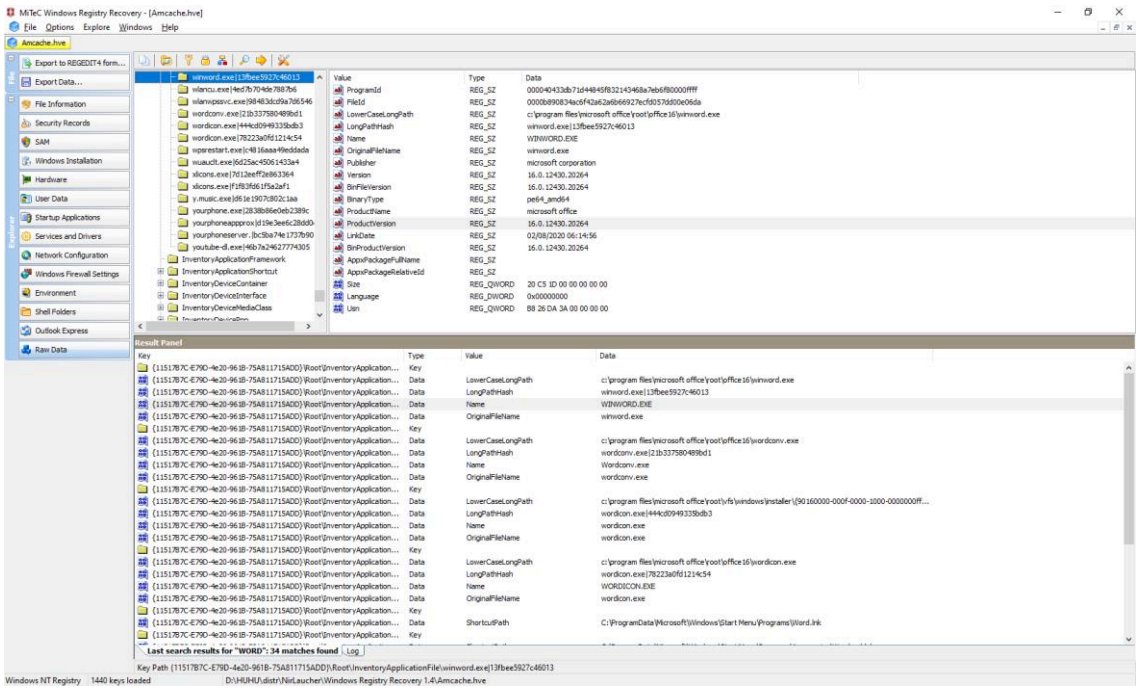


Рис. 6.4.9 Данные о программном продукте Word из файла Amcache.hve

Для получения сведений об использовании Microsoft Office из директории Prefetch, расположенной в директории Windows, целесообразно воспользоваться специализированными утилитами, например, winprefetchview, входящей в комплект «NirLauncher – Nirsoft». Просмотром файла WINWORD с помощью данной утилиты можно определить, какие последние файлы открывались в приложении Microsoft Office и расположение соответствующих временных файлов приложения.

Данные об установленном программном обеспечении Microsoft Office хранятся в ветвях реестра:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\ (далее запись типа: 9140110900063D11C8EF10054038389C)\InstallProperties

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\XX.0\Registration\ (далее запись типа: {90110419-6000-11D3-8CFE-0150048383C9})

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\XX.0\Registration\ (далее запись типа: {90120000-0016-0000-0000-0000000FF1CE})

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\ (далее запись типа: 00002109610000000000000000F01FEC)\InstallProperties,

где XX.0 код программного обеспечения Microsoft Office.

Ниже приведено соответствие кодов программного обеспечения Microsoft Office версии программы:

- Office 2003 Office11
- Office 2007 Office12
- Office 2010 Office14
- Office 2013 Office15
- Office 2016 Office15
- Office 2019 Office15

Данные о подключении USB устройств. Информация о подключенных внешних устройствах хранится:

- в реестре операционных систем;
- журналах событий;
- в файлах журналирования;
- в файлах драйверов программного обеспечения

Рассмотрим более подробно каждое из указанных мест.

Данные из реестра.

Сведения о подключении USB устройств содержатся в следующих ветвях реестра:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB

и

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR.

В данных ветвях содержится информация о типе и виде подключенных устройств, а также их серийный номер и уникальный номер (Globally Unique Identifier – GUID), который идентифицирует устройство для системы.

Причем данные о серийном номере содержатся в имени ветви, например:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USB\Vid_058f&Pid_6387\FKZ9XO6P, где FKZ9XO6P – серийный номер устройства.

В ветви реестра USB устройства обозначаются идентификатором производителя и идентификатором устройства.

В ветви реестра USBSTOR устройства обозначаются по наименованию или типу.

Время подключения устройств определяется из времени изменения соответствующей ветви реестра. Для получения данных о времени подключения можно использовать утилиту «USBDeview», входящую в комплект «NirLauncher – Nirsoft». Если нет возможности использовать сторонне программное обеспечение, то можно произвести экспорт соответствующей ветви реестра в текстовый файл. При этом в файле будут указаны времена подключения соответствующих USB устройств. Ниже на рисунке 6.4.10 приведены данные из реестра о подключении внешних устройств.

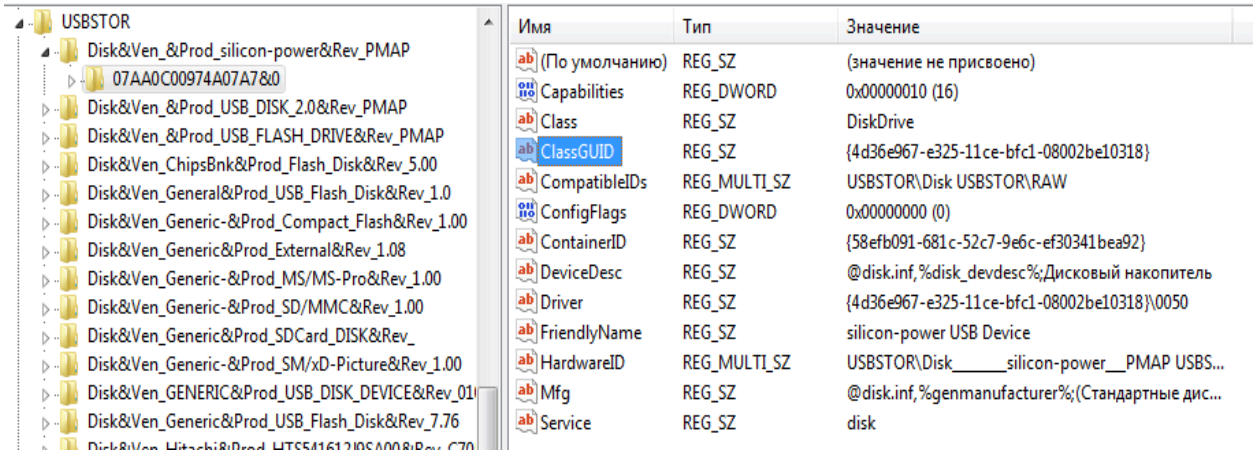


Рис. 6.4.10. Данные из реестра о подключении внешних устройств

Данные журналов событий. Данные о подключенных устройствах отражаются в журналах событий Windows, в частности в журнале «система» и в журналах приложений и служб, в частности в журнале «Конфигурация устройств».

Для журнала «Система» Windows 7 и выше используют следующие коды событий, содержащих информацию о времени подключения внешних устройств:

– «10000» источник «DriverFrameworks-UserMode» содержит сведения о начале установки пакета драйверов;

– «20001», «20003» содержат сведения о завершении установки драйверов.

Данные коды событий можно задать в «фильтре» программы просмотра журналов. Следует помнить, что здесь содержатся данные об установке драйверов USB устройств и что указанное время напрямую зависит от системного времени.

Для просмотра файлов журналов событий можно использовать штатные средства операционной системы, в меню «действия» программного обеспечения «управление компьютером», открыв исследуемый файл. Или воспользоваться специализированным программным обеспечением, например, «Event Log Explorer».

На рисунке 6.4.11 приведено изображение окна просмотра журнала «Система» с выборкой фильтра «10000».

На рисунке 6.4.12 приведены данные из журнала «Microsoft-Windows-Kernel-PnP/Configuration» («Конфигурация устройства»), расположенного по следующему пути: %SystemRoot%\System32\Winevt\Logs\Microsoft-Windows-Kernel-PnP%4Configuration.evtx.

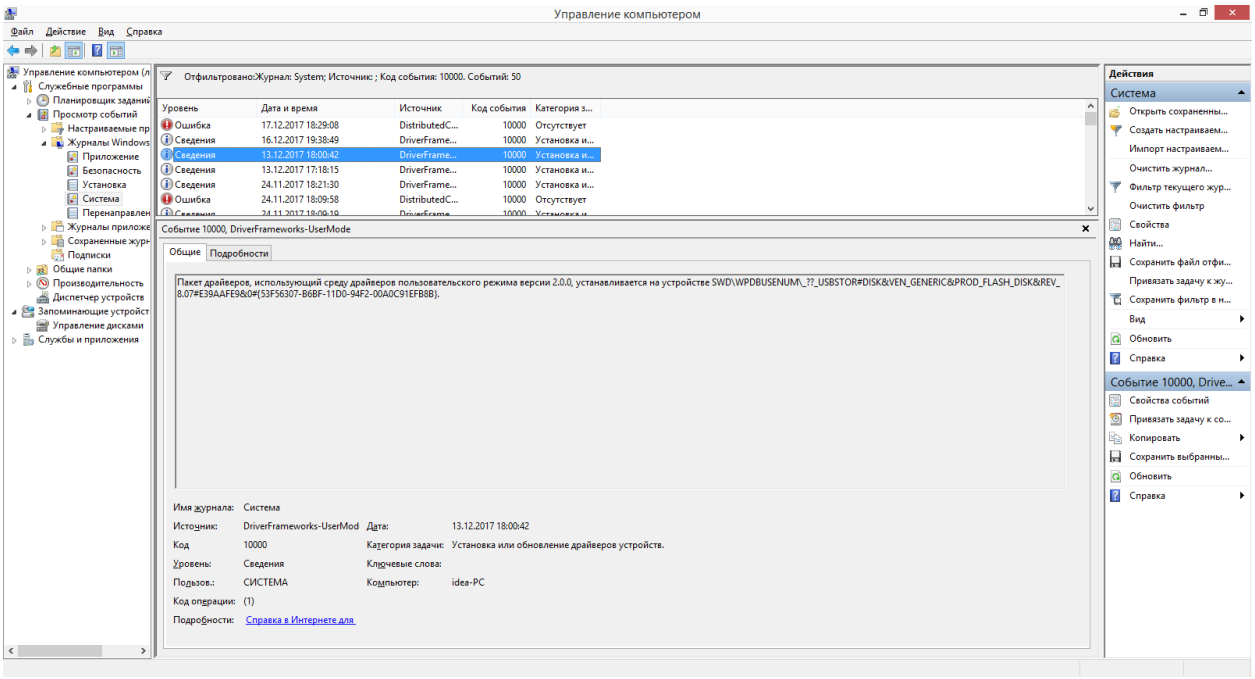


Рис. 6.4.11. Данные из журнала «Система» с выборкой фильтра «10000»

Данный журнал содержит сведения об использовании USB устройств.

Следует помнить, что информация в журналах событий сохраняется только за время ведения журнала.

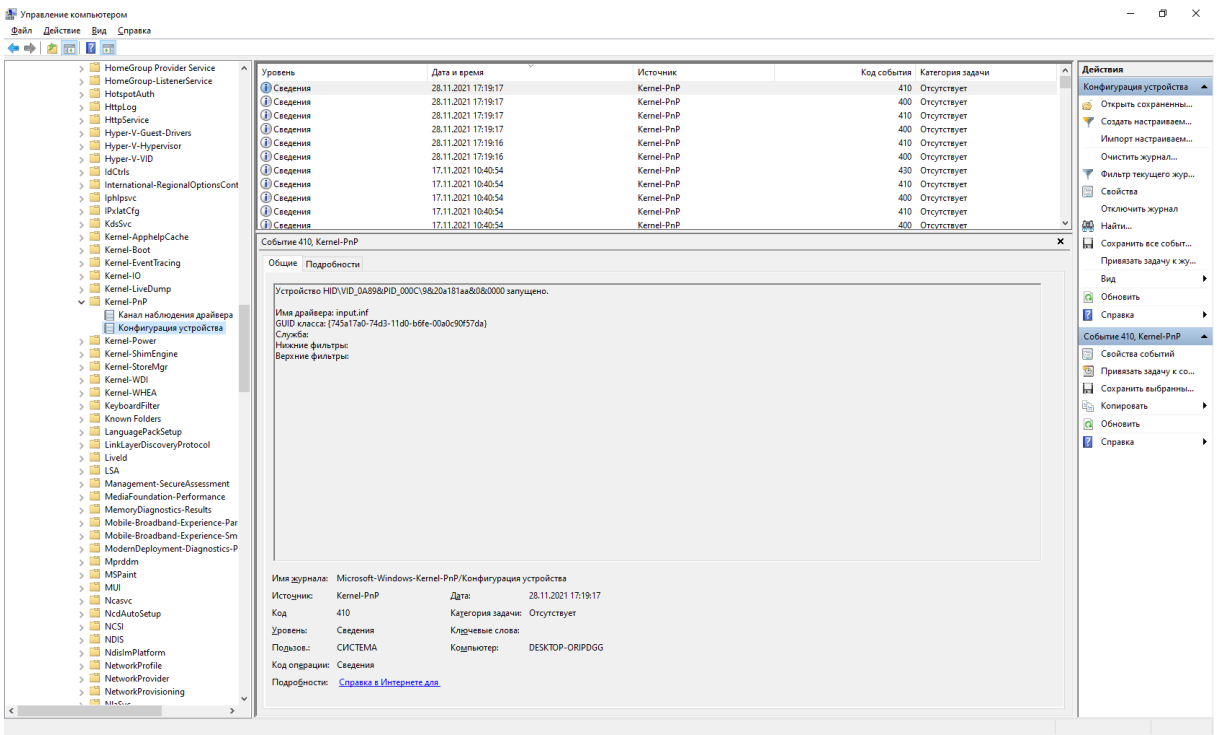


Рис. 6.4.12. Данные из журнала «Microsoft-Windows-Kernel-PnP/Configuration» («Конфигурация устройства»)

Файлы журналирования драйверов программного обеспечения. Данные об использовании USB устройств содержатся в файле «setupapi.dev.log», расположенном в директории \Windows\inf\ для Windows 7 и выше.

В файле «setupapi.dev.log» содержится информация следующего вида:

«… [Device Install (Hardware initiated) – USB\VID_058F&PID_6366\058F63666438]

>>> Section start 2017/12/16 19:41:00.117 …»

То есть имеется информация об идентификаторах производителя и устройства, а также серийный номер устройства. Эта информация содержится в ветви реестра:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB.

В файлах «usb.inf» и «usb.PNF», расположенных в директории \Windows\inf\, содержится информация об установке драйверов для USB устройств.

В файле «usb.inf» содержится информация следующего вида:

«[Version]
Signature="$Windows NT$"
Class=USB
ClassGUID={36FC9E60-C465-11CF-8056-444553540000}
Provider=%Msft%
DriverVer=06/21/2006,6.3.9600.17238

[ControlFlags]
; Exclude USB\COMPOSITE from BasicDriverOK list
BasicDriverOk=USB\CLASS_09&SUBCLASS_01, USB\CLASS_09
ExcludeFromSelect=*»

Получение информации из журналов операционной системы.

Для определения действий, проведенных операционной системой семейства Windows, производится просмотр журналов событий операционной системы.

Для Windows 7 данные файлы по умолчанию расположены в директории %SYSTEMROOT%\System32\Winevt\Logs\ и имеют расширение «.Evtx».

Просмотром данного журнала возможно определить:

- временные рамки работы операционной системы;

- временные рамки запуска ряда программных продуктов, запуск которых отображается в журнале событий операционной системы Windows;

- временные рамки подключения – отключения сетевых ресурсов

(сетевого адаптера), запуск которых отображается в журнале событий операционной системы Windows и ряд других параметров.

6.5. Особенности реагирования на сетевые кибератаки

Реализация большинства сценариев сетевого кибернападения предусматривает наличие определенной инфраструктуры. Данная инфраструктура направлена, как правило, на компрометацию информационных систем для получения над ними контроля с целью включения в ботнет [4], получения несанкционированного доступа к информации, ее шифрование или хищение с целью последующего вымогательства или продажи [5], приведения информационного ресурса в неработоспособное состояние [6]. Указанная инфраструктура предусматривает существование определенных категорий:

- авторов вредоносного программного обеспечения. По данным некоторых исследований [7], часть группировок сосредоточены исключительно на разработке;
- злоумышленников, непосредственно применяющих вредоносное программное обеспечение (ПО) с подконтрольных им информационных систем. Вредоносное ПО может быть применено с ранее скомпрометированных информационных систем – реальных компьютеров, ботнетов, виртуальных машин на публичных хостингах и т.д.;
- каналов доставки вредоносного программного обеспечения в целевые информационные системы. Примерами таких каналов являются: электронная почта, сделанные злоумышленникам копии легитимных web-порталов с созвучными оригинальным доменными именами, уязвимости операционных систем, ошибки конфигурирования сетевого оборудования и др.;
- так называемых C&C серверов (англ. – Communication And Control Servers – серверы управления и контроля), позволяющих осуществлять управление вредоносным программным обеспечением после его закрепления в информационной системе-жертве.

В интересах решения проблемы кибербезопасности информационных систем важным является решение задачи практической оценки эффективности средств киберзащиты. Решение этой задачи может быть получено путем воспроизведения условий информационного взаимодействия, обеспечивающих достаточную, с точки зрения рассматриваемых процессов и явлений, схожесть с реальными условиями работы систем защиты и средств нападения и анализа сценариев развития событий.

В работе [8] сделан вывод о том, что современная преступная интернет-деятельность оставляет за собой материальные следы, идеальные следы в виде показаний потерпевших, свидетелей и подозреваемых

(обвиняемых), виртуальные следы в виде кэш-файлов, IP-адресов, журналов историй, log-файлов и т.п. Отмечается, что одним из важнейших элементов следовой картины рассматриваемой категории преступлений является информация, оставленная преступниками в сети Интернет, в том числе в результате их контакта с жертвой (переписка, фотографии, всевозможные записи и т.п.). Элементами следовой картины, оставляемой интернет-преступлениями, являются традиционные следы (материальные и идеальные), а также новые, малоизученные криминалистикой виды следов – виртуальные и информационные, фиксации и изъятию которых должно быть уделено особое внимание, обусловленное их свойствами. Особая сложность обнаружения следов интернет-преступлений обусловлена особенностями сети Интернет. Подчеркивается, что следы преступных действий могут быть распределены по множеству объектов (компьютерная система жертвы, преступника, провайдера, промежуточные сетевые узлы и т.п.).

В то же время известно, что в сетях информация может быть собрана с помощью предварительно настроенных сетевых протоколов snmp, syslog, IPFIX (Cisco NetFlow) и захватчиков трафика – WireShark, tcpdump и подобных. Существуют комбинированные решения, позволяющие использовать сразу несколько протоколов, инструменты анализа и захвата сетевого трафика. С учетом разнородного характера информации, на основе анализа которой могут быть сделаны выводы о наличии вредоносного кода или вредоносной активности, в сетях средних и крупных масштабов применяют системы управления событиями информационной безопасности, так называемые SIEM. Положительные примеры мировой практики применения подобных систем позволяют говорить о внушительном списке проверенных решений: IBM QRadar Security Intelligence, Splunk Enterprise Security, McAfee Enterprise Security Manager, AlienVault Unified Security Platform, Micro Focus ArcSight Enterprise Security Manager, RSA NetWitness Platform, FireEye Helix Security Platform, Rapid7 insightIDR, Fortinet FortiSIEM, MaxPatrol SIEM, RuSIEM, SIEM KUMA и единая модульная платформа лаборатории Касперского [9] и др. По состоянию на середину 2021 г. на сайте ФСТЭК России в Государственном реестре сертифицированных средств защиты информации имелось порядка 10 продуктов, в составе названий которых фигурировала аббревиатура SIEM.

С учетом приведенных фактов, данных о механизмах следообразования в сети Интернет, а также информации о категориях объектов, вовлекаемых в процесс реализации сетевых кибератак, для исследования систем противодействия сетевым кибератакам может быть использован киберполигон, содержащий:

1. Сегмент информационных систем-жертв. В данном сегменте в соответствии со сценарием кибератаки размещаются информационные

системы, имеющие уязвимости, ошибки конфигурирования, неточности настройки и т.п.

2. Сегмент атакующих. В данном сегменте в соответствии со сценарием кибератаки размещаются атакующие хосты со специальным программным обеспечением, скриптами автоматизации атак и т.д.

3. Ядро маршрутизации и коммутации. Назначение данного сегмента заключается в предоставлении сервисов коммутации и маршрутизации между отдельными сетевыми сегментами киберполигона. В данный сегмент также входит граничный маршрутизатор, отделяющий сетевые сегменты киберполигона от рабочей сети или сети датацентра, в которой он развернут, а также при необходимости обеспечивающий подключение к сети Интернет, и сервисы VPN «сеть-сеть» и «сеть-пользователь» для работы на полигоне с рабочих станций удаленных учебных классов или отдельных удаленных пользователей.

4. Сегмент постоянных сервисов. В данном сегменте размещаются постоянные сервисы, к которым следует отнести компоненты отображения и обработки SIEM, вспомогательные системы мониторинга объектов киберполигона и другие необходимые системы.

Практическое использование полигона предполагает наличие сценариев реализации кибератак, основанное на комбинировании возможных векторов кибератак применительно к рассматриваемой структуре и составу информационных ресурсов, и конкретную реализацию этих атак с одновременным решением задачи защиты, наблюдения и реагирования имеющимися силами и средствами.

С учетом возможностей аппаратных ресурсов современных ЭВМ и преимуществ систем виртуализации [10] схема для реализации сетевого киберполигона принимает вид как показано на рисунке 6.5.1.

В принятых обозначениях сегмент информационных систем-жертв представлен серверами SRV11, SRV12, коммутатором S11 и межсетевым экраном FW11; сегмент атакующих – серверами SRV21, SRV22, коммутатором S22 и маршрутизатором R21; ядро маршрутизации и коммутации представлено «моделью сети Интернет» – маршрутизатором R31 и коммутаторами S31, S32, S33 для подключения к другим сетевым сегментам полигона, а также межсетевым экраном FW51 для подключения к сети организации или датацентра.

В дополнение к уже заявленным функциям составляющих подсистем отметим, что межсетевой экран FW51 в данной схеме предполагает настройку сетевой политики безопасности, запрещающей взаимодействие любого внутреннего узла из состава киберполигона с любым узлом, не входящим в список учебных автоматизированных рабочих мест (АРМ) организации – локальных или удаленных, а реальные физические подключения к сети организации или датацентра есть только у серверов виртуализации, обозначенных на схеме VES1, VES2 и внешнего

интерфейса межсетевого экрана FW51, на котором предполагается настройка механизма трансляции сетевых адресов NAT, причем «внешней» сетью считается сеть организации, а «внутренней» сетью – сетевое соединение между соответствующим интерфейсом маршрутизатора R31 и внутренним интерфейсом межсетевого экрана FW51. При наличии в сети организации сервера авторизации при доступе в сеть Интернет в межсетевой экран FW51 может быть встроено подключаемое клиентское VPN-соединение для обеспечения такого доступа всем узлам из состава киберполигона, например, на период обновления вирусных баз, списков запрещенных узлов, сигнатур сетевых атак и и т.п.

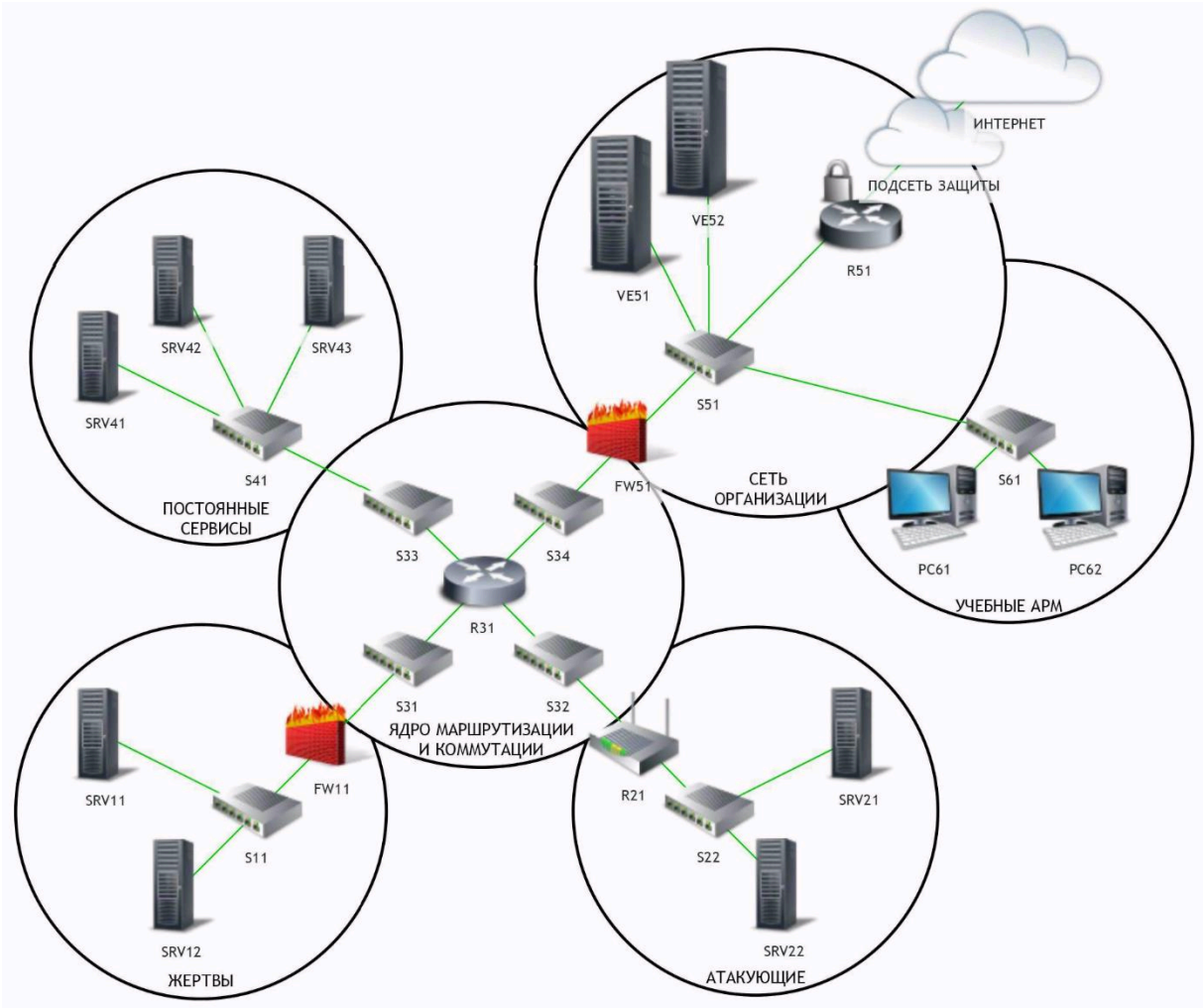


Рис. 6.5.1. Схема сетевого киберполигона для исследования практической эффективности систем противодействия сетевым кибератакам

Кроме этого, с учетом модульности предлагаемого решения, ядро коммутации и маршрутизации может быть дополнено внешним сетевым оборудованием, на котором могут быть смоделированы иные виды атак,

напрямую не относящиеся к сетевым кибератакам, совершаемым удаленно через сеть Интернет – например, «угон» маршрута протокола динамической маршрутизации BGP, отравление записи DNS сервера и т.д. Возможность такой интеграции обеспечивается использованием мостовых соединений канального уровня между физическими интерфейсами или под-интерфейсами, прежде всего, виртуальных или физических коммутаторов S31, S32, S33, физическими интерфейсами или под-интерфейсами серверов виртуализации и физическими интерфейсами или под-интерфейсами исследуемого внешнего сетевого оборудования.

Рассмотрим конкретный пример реализации киберполигона и на нем – конкретный сценарий развития сетевой кибератаки, ее наблюдения и реагирования на нее. В данном примере киберполигон реализован на удаленной технологической площадке с одним физическим сервером с операционной системой Debian Linux 10.10 с установленным средством виртуализации ProxMox VE 6.4-13, размещенным непосредственно за NAT-маршрутизатором с одним общественным IPv4 адресом на его внешнем интерфейсе. При реализации подобного решения для целей поточного удаленного обучения целесообразно предложить подключение удаленных учебных классов к сетевым сегментам полигона через внешний VPN концентратор, по отношению к которому граничный VPN маршрутизатор киберполигона также будет являться клиентом. Это позволит исключить атаки внешних злоумышленников на серверный транспортный VPN порт технологической площадки с киберполигоном, убрав необходимость иметь и использовать такой порт. Основная адресная информация, относящаяся к объектам киберполигона сведена в таблицы 6.5.1–6.5.4, а логика именования узлов сохранена.

Таблица 6.5.1
Сегмент информационных систем-жертв. Подсеть 10.36.15.0/24

№ п/п	Хост	Интерфейс	IPv4 адрес	Сетевой префикс	Шлюз по умолчанию, DNS сервер	Примечание
1.	SRV11	Eth0	10.36.15.3	/24	10.36.15.1, 10.36.15.1	Windows 2012 Server Сетевые сервисы: RDP, zabbix-client
2.	SRV12	Eth0	10.36.15.5	/24	10.36.15.1, 10.36.15.1	CentOS7 Server Сетевые сервисы: PostgreSQL, MySQL, http, https, zabbix-client, ssh, сервер 1С:Предприятие 8
3.	FW11	WAN (vtnet0)	1.1.1.254	/24	1.1.1.1	pfSense 2.5.2 Сетевые сервисы: https, zabbix-client, ssh, NAT, IDS/IPS Suricata
		LAN (vtnet1)	10.36.15.1	/24	-	
4.	S11	-	-	-	-	Неуправляемый коммутатор

Таблица 6.5.2
Сегмент атакующих. Подсеть 10.48.11.0/24

№ п/п	Устройство	Интерфейс	IPv4 адрес	Сетевой префикс	Шлюз по умолчанию, DNS сервер	Примечание
1.	SRV21	Eth0	10.48.11.254	/24	10.48.11.1, 10.48.11.1	Kali Linux Сетевые сервисы: RDP, zabbix-client, ssh Pentest-tools
2.	SRV22	Eth0	10.48.11.253	/24	10.48.11.1, 10.48.11.1	BackBox Linux Сетевые сервисы: RDP, zabbix-client, ssh Pentest-tools
3.	R21	WAN (vtnet0)	2.2.2.254	/24	2.2.2.1	pfSense 2.5.2 Сетевые сервисы: https, zabbix-client, ssh, NAT
		LAN (vtnet1)	10.48.11.1	/24	-	
4.	S21	-	-	-	-	Неуправляемый коммутатор

Таблица 6.5.3
Сегмент маршрутизации и коммутации

№ п/п	Устройство	Интерфейс	IPv4 адрес	Сетевой префикс	Шлюз по умолчанию, DNS сервер	Примечание
1.	R31	VCS	1.1.1.1	/24	-	К жертвам
		ATS	2.2.2.1	/24	-	К атакующим
		SRS	3.3.3.1	/24	-	К постоянным сервисам
		WAN	X.X.X.17	/24	X.X.X.230, 8.8.8.8	К Интернет через реальный NAT маршрутизатор
		tun0	10.177.13.1	/24	-	Для удаленных защищенных подключений «сеть-сеть»
		tun1	10.177.9.1	/24	-	Для удаленных защищенных подключений «сеть-пользователь»
2.	S31	-	-	-	-	Неуправляемый коммутатор
3.	S32	-	-	-	-	Неуправляемый коммутатор
4.	S33	-	-	-	-	Неуправляемый коммутатор
5.	S34	-	-	-	-	Неуправляемый коммутатор

В рассматриваемой реализации функции граничного маршрутизатора FW51 возложены на R31, в результате чего у R31 возникли новые интерфейсы – WAN, tun0, tun1, а сетевой маршрутизатор FW51 отсутствует. Маршрутизатор R31 собран на основе операционной системы CentOS8, служб iptables и OpenVPN, причем зарегистрировано

два серверных процесса VPN: один для обслуживания подключений «сеть-сеть», конфигурация которого оптимизирована под оборудование Mikrotik, а второй для обслуживания подключений «сеть-пользователь» – со стартовым TLS ключом и усиленными параметрами безопасности соединений. Параметры VPN сконфигурированы для работы на основе индивидуальных цифровых сертификатов с возможностью выпуска, отзыва, блокировки на произвольные временные периоды. Для мониторинга сетевых потоков на R31 установлен пакет ipcad 3.7.3-23.3x86-64, который эмулирует работу механизма Cisco NetFlow и программное обеспечение Manage Engine NetFlow Analyzer в варианте «free edition», которое представляет собой коллектор NetFlow трафика и обеспечивает функции отображения витрин данных.

Сегменты информационных систем-жертв и атакующих скрыты за NAT маршрутизаторами, что соответствует реальным типовым настройкам информационных систем малого и среднего масштабов. Для публикации информационных сервисов на межсетевом экране FW11 настроена трансляция сетевых портов, как показано в таблице 6.5.5, а для удаленного доступа и реализации атак с узлов, атакующих на маршрутизаторе R21, настроена трансляция сетевых портов, как показано в таблице 6.5.6. В результате этих настроек обращение к сетевым сервисам сегмента 10.36.15.0/24 становится возможным через IP адрес 1.1.1.254, а удаленное управление узлами в сегменте 10.48.11.0/24 через адрес 2.2.2.254.

Таблица 6.5.4
Сегмент постоянных сервисов

№ п/п	Устройство	Интерфейс	IPv4 адрес	Сетевой префикс	Шлюз по умолчанию, DNS сервер	Примечание
1.	SRV41	Eth0	3.3.3.7	/24	3.3.3.1, 3.3.3.1	CentOS8 Zabbix 5.5 Server
2.	SRV42	Eth0	3.3.3.9	/24	3.3.3.1, 3.3.3.1	CentOS8 ELK Stack 7.16.2 PFELK 22.01
3.	S41	-	-	-	-	Неуправляемый коммутатор

Таблица 6.5.5
Настройка трансляции сетевых портов на FW11

№ п/п	Интер-фейс	Протокол	Адрес источ-ника	Порт источ-ника	Адрес назначе-ния	Порт назначе-ния	NAT IP	NAT ports	Примечание
1.	WAN	TCP	любой	любой	WAN адрес	20-21	10.36.15.5	20-21	FTP на SRV12
2.	WAN	TCP	любой	любой	WAN адрес	9001-9009	10.36.15.5	9001-9009	FTP passive на SRV12

№ п/п	Интер-фейс	Протокол	Адрес источ-ника	Порт источ-ника	Адрес назначе-ния	Порт назначе-ния	NAT IP	NAT ports	Примечание
3.	WAN	TCP	любой	любой	WAN адрес	48050-48051	10.36.15.3	10050-10051	Zabbix agent на SRV11
4.	WAN	TCP	любой	любой	WAN адрес	48389	10.36.15.3	3389	RDP на SRV11
5.	WAN	TCP	любой	любой	WAN адрес	48150-48151	10.36.15.5	10050-10051	Zabbix agent на SRV12
6.	WAN	TCP	любой	любой	WAN адрес	48080	10.36.15.5	80	http на SRV12

Таблица 6.5.6

Настройка трансляции сетевых портов на R21

№ п/п	Интер-фейс	Протокол	Адрес источ-ника	Порт источ-ника	Адрес назначе-ния	Порт назначе-ния	NAT IP	NAT ports	Примечание
1.	WAN	TCP	любой	любой	WAN адрес	49389	10.48.11.254	3389	RDP на SRV21
2.	WAN	TCP	любой	любой	WAN адрес	49022	10.48.11.254	22	ssh на SRV21
3.	WAN	TCP	любой	любой	WAN адрес	49050-49051	10.48.11.254	10050-10051	Zabbix agent на SRV21
4.	WAN	TCP	любой	любой	WAN адрес	45389	10.48.11.253	3389	RDP на SRV22
5.	WAN	TCP	любой	любой	WAN адрес	45022	10.48.11.253	22	ssh на SRV22
6.	WAN	TCP	любой	любой	WAN адрес	45050-45051	10.48.11.253	10050-10051	Zabbix agent на SRV22

Станции атакующих в рассматриваемом варианте реализации киберполигона виртуализованы, к ним настроен удаленный доступ по протоколам RDP и ssh. Это позволяет ограничить перечень программного обеспечения на рабочих станциях учебных классов до графического и консольного тонких клиентов – например, клиента удаленных рабочих столов tsclient и putty для Windows или клиента удаленных рабочих столов rdesktop и клиента putty для Linux.

С учетом содержания приведенной в п. 6.1 цепочки кибератаки рассмотрим сценарий киберинцидента и воспроизведем его. В качестве киберинцидента исследуем получение несанкционированного доступа к серверу удаленных рабочих столов Windows по протоколу RDP за счет использования специального программного обеспечения подбора параметров учетной записи Windows, имеющей права на удаленный вход в систему. Данный вид атаки получил особенно широкое распространение в период пандемии в 2020–2022 гг.

Сформулируем для определенности легенду, в рамках которой совершается киберинцидент. Сотрудники бухгалтерии компании А после

прибытия на работу в очередной рабочий день и входа на сервер удаленных рабочих столов Windows Server до начала работы с системой 1С:Предприятие обнаружили изменение стартового окна входа в систему, на котором появилась информация о том, что система была взломана и данные были зашифрованы. При попытке открытия офисных документов и баз данных системы 1С:Предприятие, связанных с автоматизацией повседневной деятельности из истории файлов, выдавались сообщения, что документы не найдены. Системный инженер развернул поврежденный функционал на резервном сервере, восстановив файлы и базы данных с холодного сервера резервного копирования с потерей данных за последние двое суток (с учетом расписания архивации). Инженер сообщил, что примерно две недели назад он открыл в сети Интернет порт удаленных рабочих столов данного сервера напрямую для обеспечения возможности работы на нем сотрудника, убывшего в зарубежную командировку с планшетом, т. к. тот высказался о неудобстве работы с сервером RDP с предварительной установкой VPN соединения до корпоративной сети.

По ситуации могут быть сформулированы следующие вопросы:

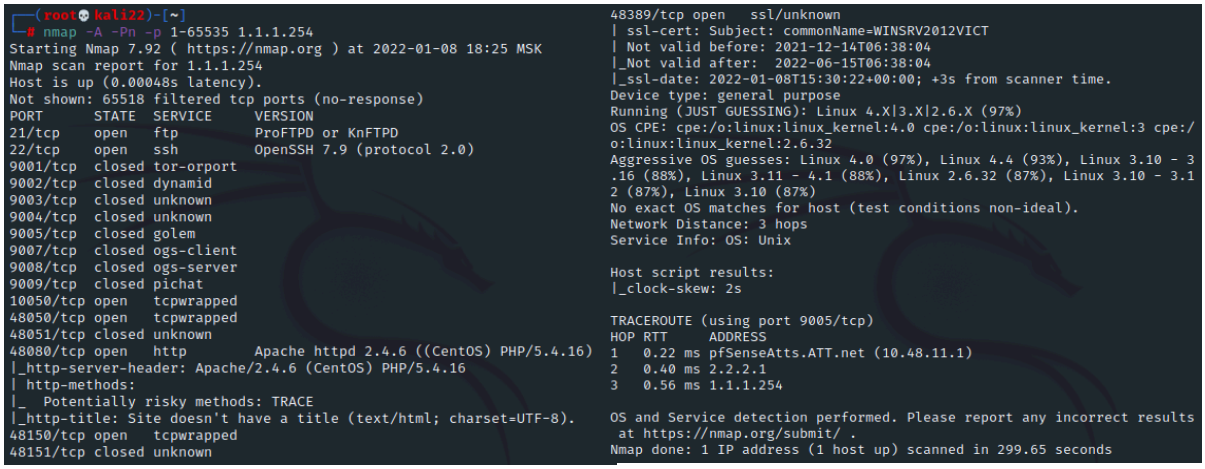
1. Какие сведения имеются о способах реализации несанкционированного доступа?
2. Имеются ли в системе данные о действиях внутренних нарушителей?
3. Имеются ли в системе данные о незаконной модификации или копировании информации на внешние ресурсы?

Смоделируем этап разведки и сбора данных – сканирование внешнего IP адреса корпоративной сети (внешний IP адрес FW11 – 1.1.1.254) с помощью сканера nmap с сервера SRV21, а затем с него же подбор пароля RDP одной из соответствущих программ из инструментария установленной на нем операционной системы (выбор способа атаки; доставка; эксплуатация).

Посмотрим, на каких объектах сформируется следовая картина в результате первого этапа кибератаки. Потенциально, как отмечено в [8], следы могут сформироваться: на атакующем компьютере, на компьютере жертве и на сетевой инфраструктуре. На атакующем компьютере сканирование портов может быть запущено, как показано на рисунке 6.5.2 (выбранные параметры nmap соответствуют «агрессивному» сканированию, не отвечающему на ping узла с IP адресом назначения 1.1.1.254 во всем диапазоне возможных номеров портов 1…65535 с определением версий сетевых служб и сервисов, а также версий операционных систем и имен удаленных хостов).

Если сравнить приведенный результат и строки таблицы 6.5.5, содержащей описание трансляций портов NAT маршрутизатора FW11, замечаем, что 100% открытых портов были обнаружены, причем для некоторых служб были определены их версии, несмотря на то, что часть

служб была опубликована на нестандартных портах. Кроме того, в заключительной части отчета присутствует маршрут до сканируемого узла, который оказался в трех транзитных прыжках от атакующего компьютера. При перенаправлении вывода подобных команд в файлы эти файлы будут содержать информацию о состоявшихся попытках сканирования атакуемого ресурса на атакующем устройстве.



```
┌──(root💀kali22)-[~]
└─# nmap -A -Pn -p 1-65535 1.1.1.254
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-08 18:25 MSK
Nmap scan report for 1.1.1.254
Host is up (0.00048s latency).
Not shown: 65518 filtered tcp ports (no-response)
PORT      STATE  SERVICE     VERSION
21/tcp    open   ftp         ProFTPD or KnFTPD
22/tcp    open   ssh         OpenSSH 7.9 (protocol 2.0)
9001/tcp  closed tor-orport
9002/tcp  closed dynamid
9003/tcp  closed unknown
9004/tcp  closed unknown
9005/tcp  closed golem
9007/tcp  closed ogs-client
9008/tcp  closed ogs-server
9009/tcp  closed pichat
10050/tcp open   tcpwrapped
48050/tcp open   tcpwrapped
48051/tcp closed unknown
48080/tcp open   http        Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
48150/tcp open   tcpwrapped
48151/tcp closed unknown
48389/tcp open   ssl/unknown
| ssl-cert: Subject: commonName=WINSRV2012VICT
| Not valid before: 2021-12-14T06:38:04
|_Not valid after:  2022-06-15T06:38:04
|_ssl-date: 2022-01-08T15:30:22+00:00; +3s from scanner time.
Device type: general purpose
Running (JUST GUESSING): Linux 4.X|3.X|2.6.X (97%)
OS CPE: cpe:/o:linux:linux_kernel:4.0 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: Linux 4.0 (97%), Linux 4.4 (93%), Linux 3.10 - 3.16 (88%), Linux 3.11 - 4.1 (88%), Linux 2.6.32 (87%), Linux 3.10 - 3.12 (87%), Linux 3.10 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 3 hops
Service Info: OS: Unix

Host script results:
|_clock-skew: 2s

TRACEROUTE (using port 9005/tcp)
HOP RTT     ADDRESS
1   0.22 ms pfSenseAtts.ATT.net (10.48.11.1)
2   0.40 ms 2.2.2.1
3   0.56 ms 1.1.1.254

OS and Service detection performed. Please report any incorrect results
 at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 299.65 seconds
```

начало окончание

Рис. 6.5.2. Типовой вариант запуска и вывод команды, использующей сетевой сканер nmap

При данном варианте команды сканирования многократных обращений к серверным службам не происходит, поэтому в журналах событий безопасности соответствующих служб хостов SRV11, SRV12 характерных потоков событий на этом этапе атаки обнаружить не удается.

Однако рассматриваемая сетевая атака происходит через подконтрольный граничный маршрутизатор FW11. В рассматриваемом случае на этом маршрутизаторе, который представляет собой многофункциональный межсетевой экран pfSense [11], установлена IDS/IPS – система обнаружения и предотвращения вторжений Suricata [12] с множественными базами сигнатур атак – см. рис. 6.5.3, которая используется для детектирования атак и фиксации соответствующих следов. Для обеспечения наглядности происходящих событий безопасности на межсетевом устройстве настроена отправка событий безопасности по протоколу syslog на узел с установленным стеком программ Elastic [13]. Разбор приходящих в компонент Logstash логов, формирование нереляционной базы данных документов Elasticsearch, а также формирование витрин данных Kibana реализованы с помощью решения PFELK [14]. Фрагмент панели данных Suricata показан на рисунке 6.5.4.

INSTALLED RULE SET MD5 SIGNATURES

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Emerging Threats Open Rules	978a5674a7985e6140352ad3256e7575	Saturday, 08-Jan-22 17:28:27 MSK
Snort Subscriber Rules	53b1919831432c15bb7fda40b2164433	Saturday, 08-Jan-22 00:15:42 MSK
Snort GPLv2 Community Rules	6fd8bd1527f1e2ee1204b528f3e63304	Saturday, 08-Jan-22 00:15:42 MSK
Feodo Tracker Botnet C2 IP Rules	239ac6aa8e28020e3c4b4584dd496643	Saturday, 08-Jan-22 00:15:37 MSK
ABUSE.ch SSL Blacklist Rules	febbedbafd9f46e5be7ec7051fd72478	Saturday, 01-Jan-22 00:15:42 MSK

Рис. 6.5.3. Базы сигнатур атак модуля Suricata 6.0.3.3 решения pfSense 2.5.2

Рассмотрим содержимое фрагмента панели данных, доступной по адресу http://3.3.3.9:5601 и показанной на рисунке 6.5.4 (слева направо, сверху вниз). В левой верхней части показаны транзитные потоки пакетов. Среди этих потоков можно найти сетевое взаимодействие 2.2.2.254 -> 1.1.1.254, которое, как будет установлено, соответствует процессу сканирования портов внешним нарушителем. Справа имеется блок фильтрации выводимых данных и матричное представление возникающих событий безопасности. В следующем информационном блоке слева имеется протяженная гистограмма событий, она в нашем случае самая информативная. В окрестности момента времени сканирования (18-15) наблюдаем характерный всплеск потока событий, расшифровка элементов которого может быть найдена в нижней, табличной части информационной панели, а также попадает в область выше нижней таблицы справа с указанием типа события (по имеющимся базам сигнатур) и IP адреса источника события. Под временной гистограммой событий безопасности расположены три круговых диаграммы. Первая дает распределение возникающих событий по интерфейсам, вторая – по уровню серьезности и третья – по удельному весу классов событий в общем объеме.

На втором этапе кибератаки в результате применения специального программного обеспечения по подбору пароля гистограмма событий будет аналогична показанной на рисунке 6.5.4 (по этой причине еще раз приводить этот рисунок мы не будем), и обнаружить данную атаку можно будет также по характерному всплеску событий. Однако, поскольку будут происходить повторяющиеся обращения к службе удаленных рабочих столов сервера SRV11, с перебором сочетаний имен пользователей и паролей, в журнале безопасности Windows Server будут появляться характерные события с отказами во входе в систему, как показано на рисунке 6.5.5. Развернув подробности событий, можно уточнить IP адрес атакующего узла. Наличие подобной картины в журнале событий Windows Server указывает на факты возможного использования специального программного обеспечения подбора паролей учетных записей Windows, а детализация IP адреса с привлечением дополнительной информации

позволит заключить, является ли нарушитель внутренним или внешним. Это позволит ответить на первый и второй вопросы, сформулированные относительно возникшей ситуации.

Момент смены событий с аудитом отказа на события с аудитом успеха соответствуют моменту проникновения в систему.

Сетевая атака может быть определена также путем анализа исходных журналов службы системы обнаружения вторжений Suricata на маршрутизаторе pfSensde, в нашем случае здесь: /var/log/suricata/suricata_vtnet053236/eve.json.

Рис. 6.5.4. Фрагмент панели данных Suricata решения PFELK 22.01 в период времени, соответствующей сетевой атаке в виде сканирования портов

Фрагмент одного из событий из этого журнала показан на рисунке 6.5.6. Содержимое данного события говорит о том, что сетевая сессия, зафиксированная под номером 21162720015211153 на интерфейсе vtnet0 распозналась как тревога – «alert», при этом IP адрес источника 2.2.2.254, IP адрес назначения 1.1.1.254, порт источника 64431, порт назначения 48389, а распознанная сигнатура – «ET SCAN MS Terminal Server on Non-standard Port», которая в базе сигнатур имеет идентификационный номер 2023753.

Выгрузки архивов современных БД составляют не менее 2 Гб. Поэтому определить, передавалась ли информация в период совершения киберинцидента, можно, проанализировав сетевые потоки NetFlow с сервера SRV11 в направлении сети Интернет по адресу интерфейса NetFlow коллектора http://1.1.1.1:8080. Рисунки 6.5.7, 6.5.8 позволяют сделать вывод, что такие объемы за указанный период не передавались.

Безопасность Событий: 9 437 (!) Есть новые события

Ключевые слова	Дата и время	Источ...	Код со...	Категория задачи
Аудит успеха	08.01.2022 23:41:27	Micros...	4624	Вход в систему
Аудит успеха	08.01.2022 23:41:27	Micros...	4672	Специальный вход
Аудит успеха	08.01.2022 23:41:27	Micros...	4624	Вход в систему
Аудит успеха	08.01.2022 23:41:26	Micros...	4776	Проверка учетных данных
Аудит успеха	08.01.2022 23:41:26	Micros...	4624	Вход в систему
Аудит отказа	08.01.2022 23:41:26	Micros...	4625	Вход в систему
Аудит отказа	08.01.2022 23:41:25	Micros...	4625	Вход в систему
Аудит отказа	08.01.2022 23:41:25	Micros...	4625	Вход в систему
Аудит отказа	08.01.2022 23:41:25	Micros...	4625	Вход в систему
Аудит отказа	08.01.2022 23:41:25	Micros...	4625	Вход в систему
Аудит отказа	08.01.2022 23:41:25	Micros...	4625	Вход в систему

Рис. 6.5.5. Фрагмент журнала событий безопасности операционной системы Windows Server

eve.json

```
1915  {"timestamp":"2022-01-08T23:49:42.216789+0300","flow_id":2116272001521153,"in_iface":
      "vtnet0","event_type":"alert","src_ip":"2.2.2.254","src_port":64431,"dest_ip":"1.1.1.254",
      "dest_port":48389,"proto":"TCP","alert":{"action":"allowed","gid":1,"signature_id":2023753,
      "rev":2,"signature":"ET SCAN MS Terminal Server Traffic on Non-standard Port","category":
      "Attempted Information Leak","severity":2,"metadata":{"affected_product":[
      "Microsoft_Terminal_Server_RDP"],"attack_target":["Server"],"created_at":["2017_01_23"],
      "deployment":["Perimeter"],"performance_impact":["Low"],"signature_severity":["Major"],
      "updated_at":["2017_02_23"]}},"app_proto":"failed","flow":{"pkts_toserver":14,
      "pkts_toclient":6,"bytes_toserver":2365,"bytes_toclient":2157,"start":
      "2022-01-08T23:49:42.005633+0300"},"payload_printable":"...-(......Cookie:
      mstshash=company\r\n.....2......%.X...u..h.B....../@.9.>q....A{G
      ...=&G':......u?ZX^.XwU.....j....>......,.0.........+./...$.(.k.#.'.g.\n...9.....3.....=.<.5
```

Рис. 6.5.6. Фрагмент зафиксированного события безопасности службы Suricata на межсетевом маршрутизаторе FW11

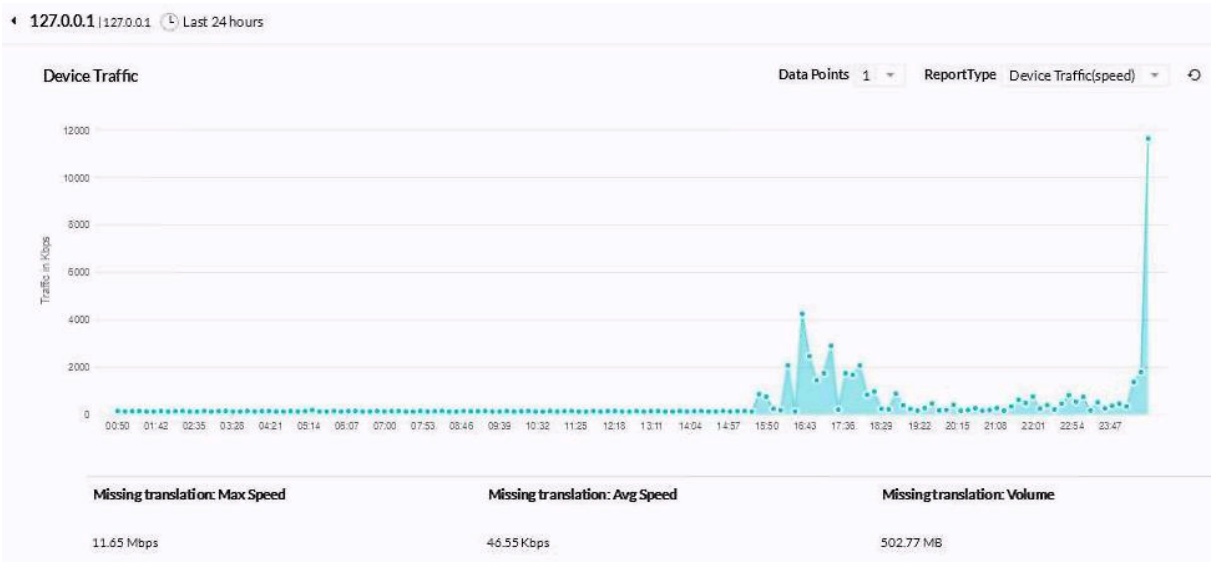


Рис. 6.5.7. Распределение скорости передачи данных на интерфейсе VCS маршрутизатора R31 от времени суток, включая период киберинцидента

Рис. 6.5.8. Распределение объемов переданной информации по видам приложений

Таким образом, на все вопросы, сформированные по инциденту, получены аргументированные ответы.

Контрольные вопросы:

1. Приведите этапы алгоритма совершения типового киберпреступления.
2. Приведите основные этапы алгоритма реагирования на инциденты информационной безопасности.
3. Перечислите и охарактеризуйте особенности выявления и фиксации следов киберпреступления.
4. Что составляет правовые основы участия специалиста при проведении следственных действий при осмотре средств вычислительно техники?
5. Каким образом могут быть получены сведения о работе операционной системы компьютера и его подсистем?
6. Каким образом можно получить сведения о сетевых соединениях, настроенных на компьютере?
7. Охарактеризуйте программы и утилиты, наиболее часто применяемые при извлечении следовой информации из персонального компьютера.
8. Где расположены файлы журналов работы основных служб персонального компьютера?
9. Каким образом с высокой степенью точности на практике могут быть смоделированы сетевые кибератаки?
10. Какие сетевые сервисы и службы могут подвергнуться сетевой атаке?
11. На каком уровне модели OSI могут быть реализованы сетевые атаки?
12. Каким образом в системе обнаружения сетевых атак или сетевых злоупотреблений может быть использован протокол snmp?
13. Каким образом в системе обнаружения сетевых атак или сетевых злоупотреблений может быть использован протокол syslog?
14. Каким образом в системе обнаружения сетевых атак или сетевых злоупотреблений может быть использован протокол Cisco NetFlow (IPFIX)?
15. Какую информацию позволяют получить в процессе расследования сетевого киберинцидента захватчики сетевого трафика (WireShark, tcpdump и др.)?

Литература к главе 6

1. Руководство по реагированию на инциденты информационной безопасности. URL : https://media.kasperskycontenthub.com/wpcontent/uploads/sites/58/2017/08/12170645/Incident_Response_Guide_rus_2021.pdf, свободный. – Загл. с экрана. – Текст : электронный.

2. Уголовный кодекс Российской Федерации: от 13.06.1996 № 63-ФЗ (ред. от 07.04.2020) // Собрание законодательства Российской Федерации. – 17.06.1996. – № 25. – Ст. 2954. – Текст : непосредственный.

3. Уголовно-процессуальный кодекс Российской Федерации: от 18.12.2001 г. № 174-ФЗ // Собрание законодательства Российской Федерации. – 24 декабря 2001 г. – № 52 (часть I). – Ст. 4921. – Текст : непосредственный.

4. Wazzan, M., Algazzawi, D., Bamasaq, O., Albeshri, A., Cheng, L. Internet of Things Botnet Detection Approaches: Analysis and Recommendations for Future. Research. Appl. Sci. 2021, 11, 5713. URL : https://www.researchgate.net/publication/352566503_Internet_of_Things_Botnet_Detection_Approaches_Analysis_and_Recommendations_for_Future_Research, свободный. – Текст : электронный.

5. Berrueta, E., Morato, D. A Survey on Detection Techniques for Cryptographic Ransomware October 2019 IEEE Access PP(99):1-1, DOI: 10.1109/ACCESS.2019.2945839. URL : https://www.researchgate.net/publication/336339807_A_Survey_on_Detection_Techniques _for_Cryptographic_Ransomware, свободный. – Загл. с экрана. – Текст : электронный.

6. Dayal, N. Srivastava, S. Analyzing behavior of DDoS attacks to identify DDoS detection features in SDN. In 2017 9th International Conference on Communication Systems and Networks (COMSNETS), IEEE, jan 2017, pp 274 –281. URL : https://www.researchgate.net/publication/354857618_Matrix_profile_for_DDoS_attacks_detection, свободный. – Загл. с экрана. – Текст: электронный.

7. HI-TECH CRIME TRENDS 2020/2021. Отчет компании Group-IB об изменении вектора кибератак в 2020/2021 гг. Доступен на официальном сайте компании по запросу. URL : https://www.group-ib.ru/resources/threat-research/2020-report.html, свободный. – Загл. с экрана. – Текст : электронный.

8. Введенская, О. Ю. Особенности следообразования при совершении преступлений посредством сети интернет / О. Ю. Введенская – Текст : непосредственный // Юридическая наука и правоохранительная практика, 2015, № 4, Т. 34, С. 209–216.

9. Обзор мирового и российского рынка SIEM-систем. URL : https://www.antimalware.ru/analytics/Market_Analysis/overview-global-and-russian-market-siem, свободный. – Загл. с экрана. – Текст: электронный.

10. Романова, А. О. Виртуализация в высокопроизводительных вычислительных системах / А. О. Романова – Текст: электронный // «Наука и образование» : Электронное научно-техническое издание. – 2011. – №3. – С.1–29. URL : https://www.elibrary.ru/download/elibrary_15633744_15203072.pdf, свободный. – Загл. с экрана.

11. pfSense. Open Source Security. Secure networks start here. URL : https://www.pfsense.org/, свободный. – Загл. с экрана. – Текст : электронный.

12. Suricata. Community Driven. Always Alert. URL : https://suricata.io, свободный. – Загл. с экрана. – Текст : электронный.

13. The Elastic Stack. Grab and go integrations. URL : https://www.elastic.co, свободный. – Загл. с экрана. – Текст : электронный.

14. PFELK. pfSense/OPNsense + Elastic Stack. URL : https://github.com/pfelk/pfelk, свободный. – Загл. с экрана. – Текст : электронный.

ЗАКЛЮЧЕНИЕ

В учебнике значительное внимание уделено терминологии, раскрывающей базовые аспекты в сфере обеспечения компьютерной безопасности современных организаций. В необходимом объеме рассмотрены понятия системы и системного подхода, процесса и процессного подхода к управлению таким сложнообусловленным явлением, как компьютерная безопасность.

Авторами с необходимой степенью детальности проведен анализ и рассмотрены практические вопросы применения национальных и международных нормативных правовых актов.

С целью максимального приближения теоретических материалов учебника к практическим проблемам обеспечения компьютерной безопасности приведены принципы обеспечения кибербезопасности устройств на базе различных операционных систем, сетевой инфраструктуры. Проанализированы кибератаки на сетевые ресурсы и основы безопасной работы с мобильными устройствами. Обсуждена политика информационной безопасности в аспекте компьютерной безопасности – от основных понятий, причин, требований и принципов ее разработки и внедрения, до частных аспектов ее построения и реализации.

В последней главе учебника на основе ранее изученных в нем вопросов рассматривается реагирование на инциденты кибербезопасности.

Для более глубоко понимания и освоения изложенного материала к каждой главе сформулированы вопросы для самоконтроля и приведен детальный список нормативной правовой и научной литературы.

Приложение

Основные документы, регламентирующие сферу информационной безопасности в целом и кибербезопасности в частности в Российской Федерации:

- Конституция РФ от 12 декабря 1993 г.;
- Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»;
- Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи»;
- Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности»;
- Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
- Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»;
- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Федеральный закон от 3 апреля 1995 г. № 40-ФЗ (ред. от 07.03.2018) «О федеральной службе безопасности»;
- Федеральный закон от 10 июля 2002 г. № 86-ФЗ (ред. от 28.11.2018) «О Центральном банке Российской Федерации (Банке России)»;
- Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»;
- Кодекс Российской Федерации об административных правонарушениях (Федеральный закон от 30 декабря 2001 г. № 195-ФЗ);
- Уголовный Кодекс Российской Федерации (Федеральный закон от 13 июня 1996 г. № 63-ФЗ);
- Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ;
- Трудовой кодекс Российской Федерации (Федеральный закон от 30 декабря 2001 г. № 197-ФЗ), в части персональных данных;
- Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ от 5 декабря 2016 г. № 646);

- Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
- Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации»;
- Указ Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации»;
- Указ Президента РФ от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;
- Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы»
- Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с Национальной стратегией развития искусственного интеллекта на период до 2030 года);
- Указ Президента РФ от 16 августа 2004 г. № 1085 (ред. от 08.05.2018) «Вопросы Федеральной службы по техническому и экспортному контролю»;
- Указ Президента РФ от 11 августа 2003 г. № 960 (ред. от 03.07.2018) «Вопросы Федеральной службы безопасности Российской Федерации»;
- Указ Президента РФ от 14 апреля 2022 г. № 203 «О Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации» (вместе с Положением о Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации);
- Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утв. Президентом РФ 12.12.2014 № К 1274);
- Указ Президента РФ от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;

- Постановление Правительства РФ от 2 июня 2008 г. № 418 «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации»;
- Постановление Правительства РФ от 16 марта 2009 г. № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (вместе с Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций);
- Постановление Правительства РФ от 26 июня 1995 г. № 608 (ред. от 21.04.2010) «О сертификации средств защиты информации»;
- Постановление Правительства РФ от 18 мая 2009 г. № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям»;
- Постановление Правительства РФ от 8 сентября 2010 г. № 697 «О единой системе межведомственного электронного взаимодействия»;
- Постановление Правительства РФ от 8 июня 2011 г. № 451 «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме»;
- Постановление Правительства РФ от 26 июня 2012 г. № 644 «О федеральной государственной информационной системе учета информационных систем, создаваемых и приобретаемых за счет средств федерального бюджета и бюджетов государственных внебюджетных фондов»;
- Постановление Правительства РФ от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;
- Постановление Правительства РФ от 18 сентября 2012 г. № 940 «Об утверждении Правил согласования проектов решений ассоциаций, союзов и иных объединений операторов об определении дополнительных угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю»;
- Постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения

обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

- Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Минкомсвязи России от 25 августа 2009 г. № 104 «Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования»;
- Приказ Минкомсвязи России от 22 августа 2013 г. № 220 «Об утверждении методических рекомендаций для исполнительных органов государственной власти субъектов Российской Федерации по осуществлению учета и классификации информационных систем и компонентов информационно-телекоммуникационной инфраструктуры, создаваемых и приобретаемых за счет средств бюджетов субъектов Российской Федерации, а также по составу сведений, размещаемых в системе учета информационных систем»;
- Приказ Минкомсвязи России от 23 июня 2015 г. № 210 «Об утверждении Технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия» (Зарегистрировано в Минюсте России 25.08.2015 № 38668);
- Приказ ФСБ РФ № 416, ФСТЭК РФ № 489 от 31 августа 2010 г. «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования» (Зарегистрировано в Минюсте РФ 13.10.2010 N 18704);
- Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (Зарегистрировано в Минюсте России 31.05.2013 № 28608);
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 № 28375);
- Методический документ «Меры защиты информации в государственных информационных системах» (утв. ФСТЭК России 11.02.2014);

- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. заместителем директора ФСТЭК России 14.02.2008);
- Приказ ФСБ России от 24 июля 2018 г. № 366 «О Национальном координационном центре по компьютерным инцидентам» (вместе с Положением о Национальном координационном центре по компьютерным инцидентам) (Зарегистрировано в Минюсте России 06.09.2018 N 52109);
- Приказ ФСБ России от 24 июля 2018 г. № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (Зарегистрировано в Минюсте России 06.09.2018 № 52108);
- Приказ ФСБ России от 24 июля 2018 г. № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» (Зарегистрировано в Минюсте России 06.09.2018 № 52107);
- Приказ ФСБ России от 6 мая 2019 г. № 196 «Об утверждении требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» (Зарегистрирован 31.05.2019 № 54801);
- Приказ ФСБ России от 19 июня 2019 г. № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации» (Зарегистрировано в Минюсте России 16.07.2019 № 55285);

- Приказ ФСБ России от 19 июня 2019 г. № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации» (Зарегистрировано в Минюсте России 16.07.2019 № 55284);
- Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (Зарегистрировано в Минюсте России 18.08.2014 № 33620)
- Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности» (утв. ФСБ России 31.03.2015 № 149/7/2/6-432
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК РФ 15.02.2008);
- Приказ Роскомнадзора от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (вместе с Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ) (Зарегистрировано в Минюсте России 10.09.2013 № 29935);
- Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (утв. Роскомнадзором 13.12.2013);
- ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;
- ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хеширования»;
- ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры»;

- ГОСТ Р 34.13-2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров»;
- ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;
- ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»;
- ГОСТ Р 56205-2014 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели»;
- ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей»;
- ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем»;
- Рекомендации по стандартизации Р 50.1.053-2005 «Информационные технологии. Основные термины и определения в области технической защиты информации»;
- Рекомендации по стандартизации Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения».