**Федеральное государственное казенное образовательное
учреждение высшего образования
«Уральский юридический институт
Министерства внутренних дел Российской Федерации»**

Кафедра информационного обеспечения органов внутренних дел

**А. П. Леонов
А. В. Копеина
А. В. Макшанцева**

Основы кибербезопасности

Курс лекций

**Екатеринбург
2022**

ББК 66.4(0),304.1
Л476

Леонов А. П.

Л476 ***Основы кибербезопасности:*** *курс лекций* / А. П. Леонов, А. В. Копеина, А. В. Макшанцева. – Екатеринбург: Уральский юридический институт МВД России, 2022. – 176 с.

ISBN 978-5-88437-906-0

Коллектив авторов

А. П. Леонов, кандидат юридических наук (введение, лекции 1, 3–6, заключение);
А. В. Копеина (лекция 2, вопросы 1–2);
А. В. Макшанцева (лекция 2, вопросы 3–4)

Рецензенты: **Н. В. Коробов**, доцент кафедры математики и информатики Санкт-Петербургского университета МВД России, кандидат технических наук, доцент;
А. Ю. Коптяев, начальник кафедры информационно-аналитического и документационного обеспечения деятельности органов внутренних дел Тюменского института повышения квалификации сотрудников МВД России, кандидат юридических наук

Курс лекций направлен на формирование у обучающихся знаний, умений, навыков и опыта деятельности (профессиональных компетенций) в области методов, способов и средств обеспечения кибербезопасности.

Учебное пособие предназначено для профессорско-преподавательского состава, курсантов и слушателей образовательных организаций системы МВД России, обучающихся по специальностям 38.05.01 Экономическая безопасность, 40.05.01 Правовое обеспечение национальной безопасности, 40.05.02 Правоохранительная деятельность, направлениям подготовки 40.03.01 Юриспруденция, 40.03.02 Обеспечение законности и правопорядка.

Обсужден на заседании кафедры информационного обеспечения органов внутренних дел УрЮИ МВД России (протокол № 14 от 27 октября 2022 г.).

Рекомендован для использования в образовательном процессе методическим советом УрЮИ МВД России (протокол № 5 от 14 ноября 2022 г.).

ISBN 978-5-88437-906-0 ББК 66.4(0),304.1

Введение

Мы живем в удивительное время бурного научно-технического прогресса, когда за бесконечно короткий по меркам развития нашей цивилизации миг – всего одно столетие, время жизни трех-четырех поколений – человек достиг большего, чем за многие тысячелетия до этого. Большая часть того, о чем раньше можно было прочесть лишь в книгах писателей-фантастов, стало обыденностью. Человек спустился в глубины океана и вышел в космос. Реальностью стали лазерные технологии, радиосвязь и телевидение. На предприятиях человека все больше и больше вытесняет искусственный интеллект, выполняющий ту же работу гораздо быстрее, качественнее и, самое главное – дешевле, чем человек. Безусловно, искусственный интеллект пока еще может называться «интеллектом» весьма и весьма условно, но определяющим здесь является слово «пока еще». Современная молодежь вряд ли способна представить себе жизнь без компьютеров и Интернета, без разнообразных гаджетов и социальных сетей, без виртуальной реальности и киберспорта. Однако их родители прекрасно помнят те совсем не далекие времена, когда не то, что мобильный телефон, но даже обычный стационарный домашний аппарат, который сегодня уже стал редкостью в наших домах, был своего рода предметом роскоши, очереди на установку которого люди ждали годами. Ну а глобальная информационно-телекоммуникационная сеть «Интернет», сегодня известная всем от мала до велика и активно используемая как отдельными людьми для личных нужд, так и государствами для решения стратегических задач развития, еще два десятка лет назад для 99,9 % населения планеты представляла собой всего лишь непонятный набор букв, за которыми ничего не стояло.

Наше время примечательно еще и тем, что мы имеем возможность собственными глазами наблюдать все последствия научно-технического прогресса, в том числе и не самые правильные с точки зрения законодательства любого государства. Лавинообразное развитие информационных технологий в последние годы XX века и приход этих технологий в каждый дом, в каждую семью, естественно не могли оставить равнодушными к такой, прямо скажем, золотой жиле в плане сравнительно безопасного отъема денег у населения, представителей криминального мира. Компьютеры, построенные на их основе гаджеты, а также сеть «Интернет» наряду с катастрофической цифровой безграмотностью подавляющего количества их пользователей, оказались весьма удобными средствами для совершения различного рода преступлений – от банальных краж до террористических актов.

Для устранения указанных проблем, а также в целях подготовки высококвалифицированных специалистов для системы МВД России, способных на научной основе противодействовать преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, в образовательных организациях МВД России введена для изучения специальная учебная дисциплина «Основы кибербезопасности».

Курс лекций «Основы кибербезопасности» подготовлен в соответствии с рабочими программамиодноименной учебной дисциплины, предназначен для обучающихся по специальностям 38.05.01 Экономическая безопасность, 40.05.01 Правовое обеспечение национальной безопасности, 40.05.02 Правоохранительная деятельность, направлениям подготовки 40.03.01 Юриспруденция, 40.03.02 Обеспечение

законности и правопорядка, 40.04.01 Юриспруденция и направлен на формирование следующих компетенций:

1) *для обучающихся по специальности 38.05.01 Экономическая безопасность:*

– способности использовать современные информационные технологии и программные средства при решении профессиональных задач (ОПК-6);

– способности понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности (ОПК-7);

2) *для обучающихся по специальности 40.05.01 Правовое обеспечение национальной безопасности:*

– способности понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности (ОПК-9);

– способности использовать в профессиональной служебной деятельности компьютерную технику, справочно-правовые информационные системы, учеты и автоматизированные информационно-поисковые системы, в том числе с учетом требований информационной безопасности (ПК-14);

3) *для обучающихся по специальности 40.05.02 Правоохранительная деятельность:*

– способности понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности (ОПК-13);

– способности использовать компьютерную технику, справочно-правовые информационные системы, учеты и автоматизированные информационно-поисковые системы при осуществлении служебной деятельности, в том числе с учетом требований информационной безопасности (ПК-23);

4) *для обучающихся по направлению подготовки 40.03.01 Юриспруденция:*

– способности понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности (ОПК-9);

– способности использовать в профессиональной служебной деятельности компьютерную технику, справочно-правовые информационные системы, учеты и автоматизированные информационно-поисковые системы, в том числе с учетом требований информационной безопасности (ПК-14);

5) *для обучающихся по направлению подготовки 40.03.02 Обеспечение законности и правопорядка:*

– способности понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности (ОПК-12);

– способности использовать в профессиональной служебной деятельности компьютерную технику, специализированное программное обеспечение, в том числе для работы с банками данных МВД России (информационно-правовыми, автоматизированными, информационными и иными системами), выполнять требования информационной безопасности (ПК-12).

Лекция 1. Общие вопросы обеспечения кибербезопасности

В июле 2020 года в цифровом пространстве произошел один из многих, но при этом очень показательный инцидент. Представители одной из хакерских групп осуществили взлом целого ряда аккаунтов в социальной сети Twitter, являющейся одной из самых популярных в мире.

Безусловно, взлом был осуществлен вовсе не для демонстрации квалификации хакеров, а с вполне конкретными и откровенно противозаконными целями. Суть заключалась в том, что на страницах пользователей сети появились крайне заманчивые сообщения о том, что производится «бесплатная» раздача биткоинов всем желающим – для этого необходимо было всего лишь перевести собственные средства на определенный кошелек, ну а «меценаты» гарантировали удвоение каждого входящего платежа. Такое предложение, очевидно слишком заманчивое, чтобы быть правдой, у многих пользователей Twitter не вызвало никаких подозрений. Причиной является тот факт, что сообщение было размещено не на страницах условных Джонов и Джеков, никому не известных и никому не интересных, а, напротив, на страницах множества очень известных и популярных во всем мире людей. В частности, бесплатную раздачу биткоинов со своей страницы обещал подписчикам экс-президент США Барак Обама. Не отставали от него и не менее известные люди, например экс-глава корпорации Microsoft Билл Гейтс и предприниматель, глава компаний SpaceX и Tesla, миллиардер Илон Маск.

Итогом данной аферы стал ущерб на общую сумму как минимум 120 тысяч американских долларов. На первый взгляд – не такая уж и большая сумма. Однако не стоит забывать о том, что это всего лишь один инцидент из множества происходящих ежедневно. Что касается данного случая, то он стал возможен в результате фишинговой атаки, совершенной злоумышленниками в отношении ряда сотрудников Twitter, что было официально признано компанией сразу после выявления инцидента. Тот факт, что киберпреступникам удалось достаточно легко организовать и, самое главное, осуществить подобную кибератаку, лишний раз доказывает, что методы социальной инженерии, несмотря на активную деятельность государства, его специальных служб, различных коммерческих организаций по повышению уровня цифровой грамотности населения, все еще остаются крайне действенными в арсенале киберпреступников. Именно по этой причине в современном мире на первый план выходит знание элементарных основ кибербезопасности.

1. Кибербезопасность: современные киберугрозы

В общем случае под кибербезопасностью сегодня понимают совокупность различных концепций, доктрин, стратегий, методов и средств защиты от атак злоумышленников (хакеров) на компьютеры, серверы, информационные системы, сети передач данных, мобильные устройства и т. д.

Очевидно, что прежде чем изучать эти стратегии, методы и средства кибербезопасности, необходимо хорошо представлять, от каких явлений и угроз нужно в принципе защищаться (киберпреступность, кибертерроризм, кибершпионаж, кибер-разведка), нужно хорошо знать основные концепции и методы применения современного кибероружия, нужно знать все типовые уязвимости в системах киберзащиты, через которые проникают компьютерные вирусы, программные и аппаратные

трояны, а также типовые и перспективные средства защиты от них – антивирусные программы, средства проактивной антивирусной защиты, перспективные кибериммунные и киберфизические операционные системы, методы и средства киберразведки и киберконтрразведки, методы и средства обеспечения кибербезопасности конечных точек (оконечных устройств) и многое другое. В свою очередь сегодня активно развиваются многочисленные направления обеспечения безопасности, как самих сетей, так и различных приложений. Например, под безопасностью сетей понимают действия по защите компьютерных сетей от различных угроз (целевых атак, вредоносных программ и т. д.). Под безопасностью приложений понимают методы, программные и аппаратные средства защиты от угроз, которые злоумышленники могут «спрятать» в различных прикладных программах. Такое «заряженное» приложение может открыть злоумышленнику доступ к данным, которые это приложение по определению должны защищать от несанкционированного доступа, поэтому безопасность таких приложений должна обеспечиваться еще на стадии разработки, до появления приложения в открытых источниках. То же самое можно сказать и о «безопасности информации» – обеспечении целостности и конфиденциальности данных как в процессе их передачи, так и во время их хранения.

К вопросам кибербезопасности также относятся и методы аварийного восстановления – оперативное автоматические реагирование систем защиты на любые инциденты (действия злоумышленников), которые могут нарушить работу системы или привести к утечке или потере данных.

Еще одно относительно новое направление кибербезопасности – кибербезопасность оконечных устройств – обеспечение безопасности разных устройств (планшеты, ноутбуки, мобильные телефоны, рабочие станции), находящихся в оконечных точках корпоративных и промышленных сетей. Особое место в проблеме обеспечения кибербезопасности занимают стандарты кибербезопасности. Это вообще особая тема – мало того, что существует великое множество различных международных стандартов, так еще практически у каждой страны (государства) имеются свои собственные многостраничные стандарты, определяющие типовые процедуры и сценарии сбора и обработки информации, оценки рисков, типовых решений и действий.

Современная кибербезопасность как новая отрасль науки стремительно развивается. Например, еще в 2014 году в работе «Network Scienceand Cybersecurity»[1] было предсказано, что эта область науки начнет активно использовать теоретические положения теории игр, криптографии, машинного интеллекта, обфускации, высокоуровневого компьютерного моделирования, и сегодня это можно наблюдать на практике.

Особое место в проблеме обеспечения кибербезопасности всегда занимало «военное» направление, в связи с чем этот момент надо рассмотреть более детально. Как известно, средством ведения любых боевых действий (войн) является оружие, под которым обычно понимаются многообразные устройства, средства и системы, которые применяются либо для непосредственного (физического) уничтожения живой силы противника, либо в целях повреждения и уничтожения принадлежащих ему технических средств, различного рода сооружений, коммуникационных и логистических линий.

[1] См.: *Robinson E. Pino.* Network Science and Cybersecurity. New York: Springer, 2014.

История развития человеческой цивилизации по своей сути представляет собой непрерывную эволюцию средств вооружения. И как бы странно это ни звучало, но именно необходимость развивать оружие, создавать новые, все более совершенные и смертоносные его образцы, являлась и продолжает являться основным двигателем прогресса. Именно военная отрасль практически всегда становилась полигоном для создания и апробирования новых технологий, именно в ней в полной мере проявлялась человеческая конструкторская мысль, именно для ее производственных нужд синтезируются новые и усовершенствуются существующие материалы, появляются новые профессии. Любые технологии и открытия – химические, бактериологические, атомные, оптические, космические, основанные на использовании энергии волн сверхвысокой частоты и на гиперзвуке – все это изначально находит применение в области развития оружия и лишь затем адаптируется под возможности использования в мирных целях. Вряд ли это можно считать поводом для гордости, но к настоящему времени человечество разработало невероятное количество видов и разновидностей оружия – холодного и огнестрельного, предназначенного для самообороны или для нападения, представляющего опасность для ограниченного количества целей и способного уничтожать целые города. Более того, некоторые виды современного оружия способны с легкостью уничтожить всю человеческую цивилизацию и даже целиком нашу планету.

Справедливости ради стоит отметить, что у человечества хватает ума для того, чтобы понять простую вещь – применение сверхмощных видов оружия в реальных войнах равносильно попытке самоубийства экзотическим, но, при этом, весьма действенным способом, поскольку победителей в такой войне не будет. Однако человек не был бы человеком, если бы не нашел выход и из этой ситуации. Он просто научился использовать в качестве оружия то, что таковым по определению не является.

В настоящее время одним их наиболее опасных видов оружия является так называемое кибероружие. По своей сути оно представляет собой, всего лишь, определенного рода информацию (поражающий элемент), а также технические средства и информационно-коммуникационные технологии, используемые как средства доставки этого поражающего элемента к цели. Однако, несмотря на такую простоту, это оружие по степени опасности сопоставимо, например, с ядерным оружием, обладая при этом огромными преимуществами перед ним. Оно несопоставимо дешевле в производстве, не требует специализированной промышленной и производственной базы, не способно уничтожить планету или превратить ее в непригодный для жизни кусок камня. И, самое главное, это оружие может быть применено (и чаще всего именно так и применяется) скрытым образом, когда объект, в отношении которого применяется кибероружие, не имеет представления о субъекте его применения. Естественно, при этом практически сводится к нулю возможность так называемого «удара возмездия», неминуемого в случае применения обычных сверхмощных видов вооружений.

Базисом (технологической платформой) современного кибероружия являются многочисленные вирусы, черви, программные и аппаратные трояны, шпионские программы, использующие различные уязвимости в системах киберзащиты (уязвимости в микросхемах, криптографических алгоритмах, стандартах, протоколах, уязвимости программного обеспечения и т. д.).

Перечисленные виды вредоносного программного и аппаратного обеспечения представляют серьезную опасность для любых объектов, входящих в инфраструктуру современного государства. Под угрозой находятся объекты топливно-энергетического комплекса, банковские системы, связь и навигация, объекты военного и оборонного назначения, системы управления транспортными потоками и т. д. Независимо от того, как именно реализована угроза – путем программного трояна или при помощи закладки, внедренной непосредственно в аппаратную часть технического устройства (например, в микросхему), результат ее работы может быть катастрофическим. Подчиняясь воле своего «хозяина» и реализуя скрытые от пользователя (а иногда и от разработчика) аппаратуры функции и алгоритмы работы, подобные программные или аппаратные закладки способны получать доступ к защищаемой информации и, без ведома владельца, передавать ее злоумышленнику. Они способны полностью или частично менять функциональные и электрические режимы работы оборудования, отключать или блокировать как отдельные модули (например, систему защиты информации), так и полностью всю информационную систему, выводить ее из-под управления законного пользователя и передавать под управление злоумышленника, а также выполнять множество других недекларированных (скрытых от пользователя) вредоносных функций, направленных на причинение физического, экономического, репутационного и других видов ущерба интересам законного пользователя.

Отметим интересный факт – исторически первыми начали применять на практике программные и аппаратные закладки вовсе не специальные государственные службы, что кажется очевидным и логичным. Первопроходцами в этом нелегком деле были те, кто находится по другую сторону баррикад на поле борьбы с преступностью, а именно представители национальной организованной преступности ряда экономически и технически развитых стран. Безусловно, организованная преступность в данном случае преследовала исключительно противозаконные цели – достижение своих преступных интересов относительно «бескровными» способами, для совершения, например, незаконных банковских операций, уничтожения собранных следственными органами улик, находящихся в банках данных, в целях промышленного шпионажа и сбора конфиденциальной информации и т. д. Достаточно быстро представители специальных служб и вооруженных сил таких стран как Китай, Россия, Израиль и США поняли и оценили все перспективы и возможности использования подобных подходов и технологий в своей деятельности, что привело к появления в их составе специальных подразделений, выполняющих оперативно-служебные и боевые задачи исключительно в киберпространстве. В настоящее время такие подразделения, получившие условное название «кибервойска», есть в составе специальных служб и вооруженных сил практически всех развитых государств мира.

2. Методы совершения киберпреступлений

Итак, в общем случае кибербезопасность – это совокупность различных концепций, доктрин, стратегий, методов и средств защиты от атак злоумышленников (хакеров) на компьютеры, серверы, информационные системы, сети передач данных, мобильные устройства и т. д. Второй вариант определения звучит следующим образом – это комплекс мероприятий, направленных на обеспечение защищенности

той или иной информационной (компьютерной) системы от внешних и внутренних угроз, реализуемых злоумышленниками при помощи специальных познаний в области современных компьютерных технологий и навыков использования этих технологий.

Совершенно логичным является следующий за формулировкой указанного определения шаг, а именно определение тех воздействий, от которых, собственно, должна защищаться информационная система. Такие воздействия принято называть общим собирательным термином «киберугрозы». Итак, что понимают под киберугрозами? На самом деле существует множество определений этого понятия, и, как это часто бывает, в большинстве случаев авторы говорят об одном и том же, используя разные слова. В целом же киберугроза может быть обозначена как совокупность факторов и условий, создающих опасность нарушения информационной безопасности[1].

Киберугрозы, как правило, рассматривают с точки зрения действий злоумышленников в киберпространстве, направленных на проникновение в информационную систему с целью кражи данных, денежных средств или с иными намерениями, которые потенциально ведут к негативным последствиям для государства, бизнеса или частных лиц[2]. При этом киберугрозы могут быть представлены в двух основных формах: кибертерроризм и киберпреступность.

Традиционно все киберугрозы принято делить на две группы по месту возникновения: внутренние и внешние.

Если говорить о внешних киберугрозах, то они, как нетрудно догадаться, проникают в защищаемую систему извне, тогда как угрозы внутренние проистекают из действий владельца или пользователя технического устройства, а также от используемого для организации функционирования системы программного и аппаратного обеспечения.

Внешние угрозы исключительно многообразны, но в целом в их структуре можно выделить несколько наиболее часто встречающихся, которые будут кратко охарактеризованы ниже.

Первыми в списке внешних киберугроз заслуженно располагаются **вирусы,** которые представляют собой вредоносное программное обеспечение, специально разработанное для скрытного проникновения внутрь компьютера для осуществления деструктивного воздействия. Характерной особенность вирусов является то, что противодействовать их разрушительному воздействию можно только при наличии достаточно эффективной специализированной системы защиты. Заражение компьютера вирусом может быть осуществлено разными способами. Например, заражение возможно через съемные носители информации – флэш-накопители, внешние жесткие диски и т. д. Частой причиной заражений является посещение пользователем сайтов в сети Интернет, распространяющих «пиратское» программное обеспечение. Не менее часто заражение происходит при открытии пользователем электронного письма, содержащего зараженное вложение.

---

[1] См.: *Лобач Д. В.* Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам. Территория новых возможностей // Вестник Владивостокского государственного университета экономики и сервиса. 2019. Т. 11. № 4. С. 25.

[2] Там же.

Опасность вирусов заключается в том, что они специально разрабатываются для оказания деструктивного воздействия на компьютерную систему и содержащуюся в ней информацию. Они способны вывести из строя аппаратную часть компьютера, модифицировать, заблокировать или уничтожить файлы или иным образом нарушить работу системы.

Еще одним крайне распространенным видом киберугроз является **спам,** представляющий собой массовую рассылку «мусорных» сообщений посредством СМС, электронной почты, социальных сетей, интернет-мессенджеров и т. д. Опасность спама на первый взгляд может показаться неочевидной, но ее нельзя недооценивать. Спам не только заваливает пользователей валом «мусорных» писем, заставляя в этом потоке выискивать действительно важные сообщения, но и является одним из основных каналов, через которые происходит заражение компьютеров вредоносным программным обеспечением.

В нашем кратком списке наиболее распространенных киберугроз нельзя обойти вниманием такое явление, как **фишинг**, суть которого заключается в том, чтобы заставить пользователя выполнить действия, ведущие к заражению компьютера вредоносным программным обеспечением. В отличие от спама фишинг нацелен, как правило, на узкие группы пользователей или на отдельных людей, при этом он широко использует методы социальной инженерии для того, чтобы заставить потенциальную жертву выполнить те действия, которые позволят злоумышленнику достичь своей цели.

Четвертым в нашем списке наиболее распространенных киберугроз отметим **удаленный взлом компьютеров**. Суть явления заключается в том, что злоумышленник, используя специальные знания и навыки, получает скрытый от законного пользователя доступ к информационной системе, благодаря чему может распоряжаться этой системой, ее ресурсами, аппаратными средствами, входящими в ее состав, а также содержащейся в ней информацией по своему усмотрению. Крайняя степень опасности данной киберугрозы заключается именно в ее скрытности, поскольку законный пользователь системы в этом случае даже не подозревает о том, что подвергся кибератаке.

Развитие информационно-коммуникационных технологий идет семимильными шагами, а их широкое внедрение в нашу повседневную жизнь не осталось незамеченным представителями криминального мира, которые, как уже отмечалось ранее, также очень активно осваивают и используют новейшие достижения научно-технического прогресса в собственных целях. Это закономерно привело к появлению новых видов преступлений, а традиционная контактная преступность, когда преступник и потерпевший взаимодействуют в физическом пространстве, в настоящее время активно вытесняется преступностью бесконтактной, когда преступник осуществляет свою деятельность исключительно в рамках киберпространства, без необходимости даже минимального физического взаимодействия с потерпевшим.

В настоящее время существует достаточно много видов преступлений, совершаемых с использованием компьютерных технологий. В частности, таким образом могут совершаться хищения и присвоения цифровых активов (денежных средств или информации), компьютеры могут использоваться для совершения вымогательств (равно как и цифровые активы могут быть предметом вымогательства), пре-

ступники для достижения своих целей активно (и главное – неправомерно) получают доступ к компьютерной информации[1], создают, используют и распространяют вредоносное программное обеспечение[2], нарушают правила эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей[3] и совершают еще целый ряд различных действий, которые также образуют составы компьютерных преступлений. В целом же, всю совокупность преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, в зависимости от целей, которые перед собой ставят преступники и от методов, которые они используют для достижения этих целей, принято обозначать собирательными названиями «киберпреступность» и «кибертерроризм».

Сегодня можно встретить несколько классификаций компьютерных преступлений, однако ни одна из них, по мнению авторов данного курса лекций не может претендовать на то, чтобы считаться всеобъемлющей. Вероятно, именно с этим связан тот факт, что национальные уголовные законодательства разных стран мира содержат в своем составе разное количество видов компьютерных преступлений и используют разные формулировки для их обозначения. При этом до сих пор не существует единого межгосударственного подхода к этой проблематике.

Так, например, на X Конгрессе ООН в 2000 году была предложена следующая классификация компьютерных преступлений[4] (рис. 1):

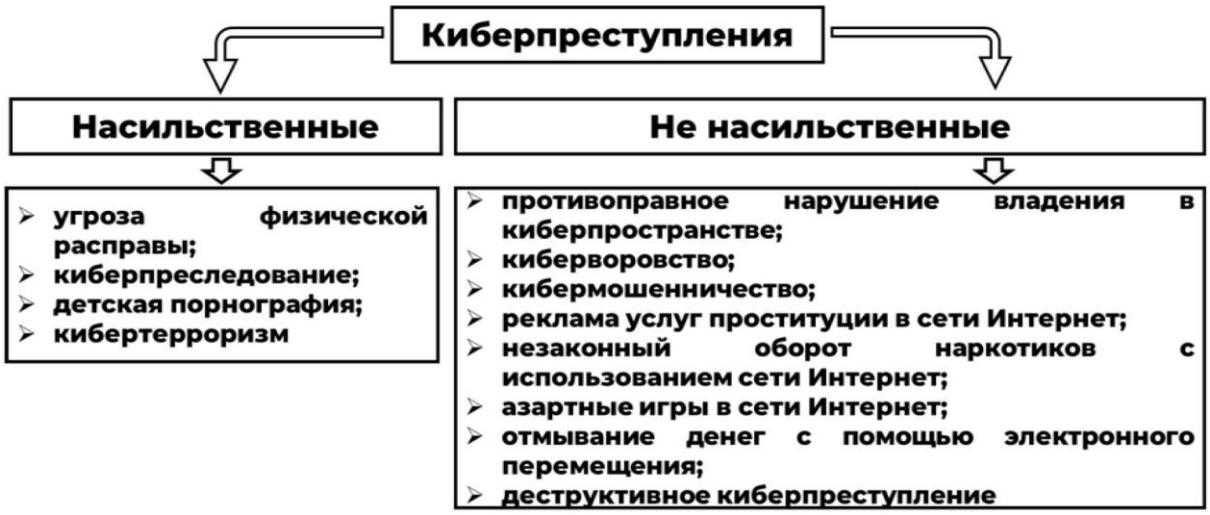


Рис. 1.

Европейская конвенция о преступности в сфере компьютерной информации в 2001 году предложила несколько иную классификацию[5]:

---

[1] Уголовный кодекс Российской Федерации. Ст. 272 // СПС «Консультант-Плюс».
[2] Там же. Ст. 273.
[3] Там же. Ст. 274.
[4] Доклад X Конгресса Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями. Вена, 10–17 апреля 2000 г. URL: https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/030_ACONF.187.15_Report_of_the_Tenth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders_R.pdf
[5] Конвенция о преступности в сфере компьютерной информации (ETS N 185): заключена в г. Будапеште 23.11.2001 // СПС «КонсультантПлюс».

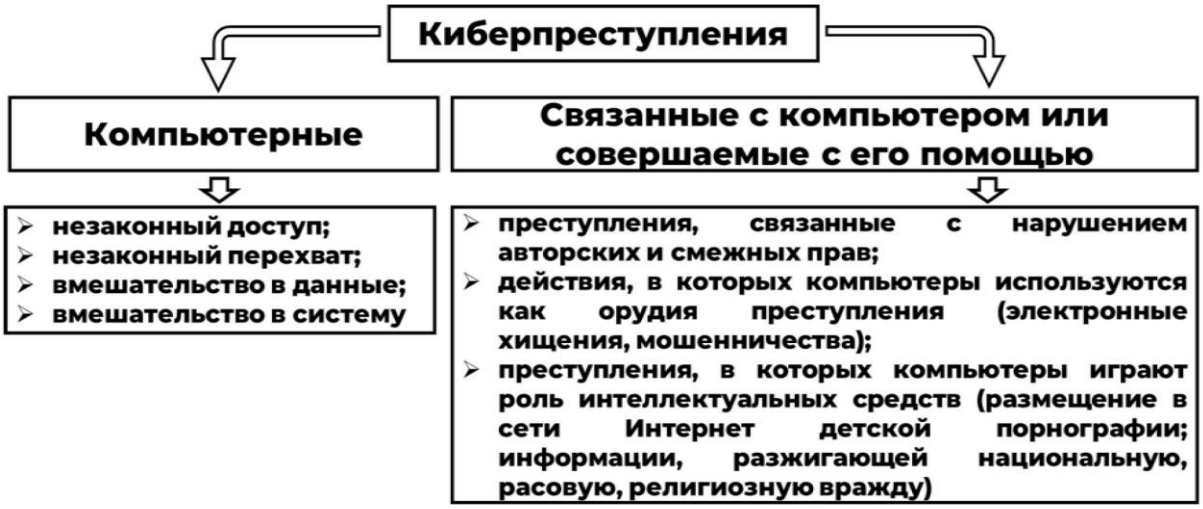


Рис. 2.

Очевидно, что подобный подход представляет собой серьезную проблему и создает существенные трудности в раскрытии и расследовании киберпреступлений. Некоторые их виды, такие как, например, кибермошенничества, вымогательства или кражи, признаются практически всеми странами мира и, соответственно, включены в состав национальных уголовных законодательств. Однако киберпреступность – это чрезвычайно специфическое явление, которое носит виртуальный характер, не признает государственных границ, зачастую выходит за рамки привычных составов преступлений (или вообще не охватывается ими). Стоит отметить, что в настоящее время механизм межгосударственного взаимодействия при расследовании компьютерных преступлений фактически отсутствует, чем успешно пользуются преступники, которые физически могут находиться на территории одного государства, используемые ими для совершения преступлений сервера – на территории другого государства, а само киберпреступление вполне может совершаться на территории третьего государства. В такой ситуации отсутствие единого подхода у разных государств в деле определения и формулирования составов киберпреступлений, отсутствие ратифицированных договоров и соглашений о международном взаимодействии в части борьбы с киберпреступностью, позволяет злоумышленникам зачастую оставаться безнаказанными, поскольку в подобных случаях обеспечить всестороннее и объективное расследование преступления и привлечение виновных к ответственности силами одного государства практически невозможно.

Отметим, что наличие данной проблемы осознается во всем мире и страны предпринимают определенные меры для ее урегулирования. В частности, одним из наиболее серьезных шагов в этой области, стало принятие уже упомянутой выше Европейской конвенции о преступности в сфере компьютерной информации 2001 года. Указанный документ по своей сути представляет собой первое международное соглашение, устанавливающее нормативные и процессуальные особенности выявления, пресечения, раскрытия и расследования киберпреступлений. К сожалению, несмотря на очевидную важность данной конвенции, далеко не все страны мира к ней присоединились. По состоянию на декабрь 2020 года конвенцию ратифицировали 65 государств, из 195 признаваемых Организацией Объединенных Наций. Еще 4 государства данную конвенцию подписали, но не ратифицировали. Что касается

нашей страны, то конвенция была подписана (но не ратифицирована) на основании распоряжения Президента Российской Федерации 15.11.2005 № 557-рп, однако в 2008 году, распоряжением Президента от 22.03.2008 № 144-рп, подпись Российской Федерации под данной конвенцией была отозвана.

Если с киберпреступностью как таковой все относительно просто, то такому явлению, как кибертерроризм, считаем необходимым уделить особое внимание. Кибертерроризм представляет собой наиболее опасную разновидность киберпреступности. Преследуя те же цели, от традиционного терроризма он отличается в методах их достижения. Здесь нет смертников с поясами шахидов и нет захватов заложников в школах и театрах, зато используются новейшие достижения науки и техники, самые современные информационные и компьютерные технологии. И, безусловно, огромную помощь кибертеррористам в достижении их преступных целей оказывает все тот же Интернет. Проанализировав деятельность наиболее известных террористических организаций, можно выделить ряд основных направлений, в которых ими используется глобальная информационно-коммуникационная сеть:

1. Любая террористическая организация жизненно заинтересована в привлечении новых членов. Современные информационные технологии позволяют делать это значительно более массовым и безопасным способом, чем традиционные виды вербовки. Таким образом, Интернет – это прекрасная площадка для своеобразной «рекламы» террористической организации, ее целей, задач и т. д. путем создания и продвижения сайтов соответствующего содержания.

2. Интернет дает возможность вовлекать в террористическую деятельность участников, не разделяющих идеологию террористической организации. Например, хакер, которому заплатили за выполнение конкретной задачи, может не иметь представления о том, что является звеном в цепочке осуществления террористического акта.

3. Террористические организации заинтересованы те только в привлечении новых членов в свои ряды, но и в их обучении. И здесь опять на смену традиционным методам контактной работы приходят методики дистанционного обучения. Для этих целей в сети Интернет в огромных количествах размещаются сайты, содержащие информацию о наиболее опасных видах оружия, каких как взрывные устройства и взрывчатые вещества, боевые отравляющие вещества, яды и т. д. Здесь же дается исчерпывающая информация о способах их самостоятельного изготовления и наиболее эффективного применения.

4. Терроризм – недешевое явление. Деньги требуются на приобретение или изготовление оружия, вербовку новых членов и оплату действующих, их обучение, осуществление разведывательных мероприятий, подготовку и проведение непосредственно террористических актов и т. д. И здесь снова на помощь приходит Интернет с предоставляемой им возможностью осуществления трудно отслеживаемых платежей и переводов. Таким образом, осуществляется финансирование террористических организаций, причем зачастую это делают люди, не имеющие отношения к терроризму, не разделяющие их идеологии и свято верящие в то, что их деньги пойдут на благое дело. Но всегда ли можно быть уверенным в том, что тысяча рублей, переведенная нами, например, на лечение больного ребенка по объявлению в Ин-

тернете, действительно будет использована именно для этой цели, а не для организации взрыва нашего собственного дома?

5. Добровольные пожертвования не всегда способны перекрыть потребности террористических организаций. В этом случае Интернет используется как площадка для вымогательства денежных средств у различных (как правило – крупных) финансовых институтов. Не секрет, что большинство игроков на финансовом рынке всегда, так или иначе, нарушают закон, обманывают конкурентов и потребителей и прочими способами не совсем честно ведут бизнес. Этим и пользуются террористические организации, выдвигая требования под лозунгом: «хотите сохранить свою репутацию или не подвергаться актам кибертерроризма, платите». Как правило, платят.

6. Любая террористическая организация должна не только декларировать свои цели, но и доводить до своих сторонников информацию о том, как они осуществляются. В данном случае Интернет используется как своеобразное средство коммуникации террористов с массовой аудиторией для извещения о планируемых акциях или об уже осуществленных.

7. Интернет в силу распространенности и доступности для всех возрастов и слоев населения является прекрасной площадкой для информационно-психологического влияния на органы государственной власти и население любой страны.

Исходя из приведенного анализа, можно сделать вывод о том, что для современных террористических организаций Интернет представляет интерес в первую очередь как инструмент для вербовки новых сторонников и коммуникации. Термин «кибертерроризм» существует с 80-х годов XX века, но, к счастью, до настоящего времени мир не видел ни одного сколь либо серьезного кибертеракта. К сожалению, никто не может гарантировать того, что подобное не случится завтра.

В качестве примера можно привести успешную реальную атаку, которая была осуществлена в отношении самолета Boeing 757. Информация об этом инциденте была доведена министерством внутренней безопасности США на ежегодной конференции CyberSat. К счастью, трагедии в этом случае не произошло. Но только потому, что атаку осуществляли не кибертеррористы, а, напротив, специалисты в области кибербезопасности. Осуществленная ими атака не давала возможности совершить угон самолета (хотя при должной квалификации злоумышленников и с учетом того, что современные самолеты представляют собой один большой компьютер, это тоже вполне возможно), но она должна была привести к отказу двигателей и системы аварийного выпуска шасси при взлете самолета, что непременно привело бы к аварии лайнера и гибели пассажиров и экипажа.

Самолет – далеко не единственная возможная цель кибертеррористов. Ваш автомобиль также вполне может оказаться в поле их преступных интересов. Ни для кого не секрет, что современный автомобиль – это чрезвычайно сложное и высокотехнологичное устройство, подавляющая часть функций которого управляется при помощи компьютера. К сожалению, все эти системы уязвимы перед взломами, и может быть выделено как минимум 12 возможных направлений кибератак на бортовые системы управления – от систем управления тормозами и рулевым устройством до электронной системы управления двигателем. Стоит отметить, что взломать

можно не только самые современные автомобили, но и достаточно старые. В качестве примера можно привести ситуацию с уязвимостью, еще в 2014 году выявленной так называемыми «белые» или «этичные» хакерами в мультимедийной системе Uconnect, которая в качестве штатной устанавливалась на автомобили, производимые такими автомобильными гигантами как Jeep, Ram, Chrysler и Dodge. Эксплуатация этой уязвимости могла дать злоумышленникам возможность получить полный контроль над управлением автомобилем. В качестве демонстрации специалисты по кибербезопасности осуществили дистанционный взлом автомобиля JeepCherokee, в результате чего получили контроль над всеми его системами, а в итоге даже успешно направили автомобиль в кювет[1]. Результат этого эксперимента привел к экстренному отзывы в США более 1,4 миллиона автомобилей с аналогичной мультимедийной системой. Да, это пример всего лишь на одном автомобиле. Но что, если нечто подобное случится одновременно с сотнями и тысячами автомобилей по всей стране?

Безусловно, когда речь идет о кибертерроризме, дело не обходится одними самолетами и автомобилями. Целью преступников могут стать любые автоматизированные системы, выход из строя которых или потеря управления которыми могут привести к катастрофическим последствиям. В зоне потенциального риска – объекты атомной энергетики и топливно-энергетического комплекса, системы управления транспортом, медицинские компьютеры, компьютеры государственных служб и органов, системы управления вооружением, в том числе – высокоточным и массового поражения.

3. Уязвимости «Интернета вещей»

«Интернет вещей» (IoT, InternetofThings) представляет собой разнообразные технические устройства, имеющие возможность подключаться к Интернету и объединяться в единую сеть посредством проводных или беспроводных технологий, обмениваясь между собой данными в режиме реального времени. Устройства, которые относятся к категории IoT, могут как работать в полностью автоматическом режиме, так и поддерживать протоколы прямого или дистанционного управления пользователем.

«Интернет вещей» развивается очень стремительно. Еще совсем недавно возможность подключения к Интернету имели только компьютеры. Затем такую возможность получили телефоны. Чуть позже к Интернету научились подключать часы. Сегодня же с трудом можно представить себе какое-либо устройство, не обладающее подобным функционалом. Как правило, все такие устройства в своем названии имеют слово «смарт», что в прямом переводе с английского означает «умный» или «интеллектуальный». Многие из них действительно полезны. «Умный» браслет или «умные» часы на вашей руке анализируют частоту и силу ваших сердечных сокращений, насыщенность вашей крови кислородом, дают рекомендации об уровне вашей физической активности, принимают и отправляют для вас и вместо вас различного рода сообщения и т. д. «Умный» чайник к нужному времени до нужной температуры согреет воду для того, чтобы вы могли взбодриться чашечкой кофе перед рабочим днем или расслабиться за чашкой чая по его окончании. «Умный» телевизор, подстраиваясь под ваши интересы, предложит, что посмотреть вечером, а

[1] URL: https://book.cyberyozh.com/ru/kibervojna-kiberdiversii-i-kiberterrorizm/

«умный» холодильник, проанализировав, какие продукты и как часто вы в него ставите и из него достаете – сам сделает необходимый заказ к удобному для вас времени. Польза и необходимость других весьма и весьма сомнительна (пример – «умные» носки, способные уведомить своего владельца о том, что их необходимо постирать, что они прохудились и требуют замены, о том, является ли второй носок парой для первого, и если нет, то где находится потерявшийся парный) и объясняется скорее желанием производителя максимально заработать на современных тенденциях превращать в «умные» любые вещи вокруг нас. Однако, независимо от споров о полезности или бесполезности того или иного «умного» устройства, ключевым признаком того, что оно относится к категории IoT, является способность устройства самостоятельно подключаться к сети Интернет, либо связываться в общую сеть с другими устройствами подобного рода, передавая им и получая от них необходимые данные. Таким образом, именно связанность является важнейшей отличительной чертой «Интернета вещей».

Как нетрудно убедиться, в состав «Интернета вещей» входит огромное количество разнообразных технических устройств, из которых многие действительно полезны и призваны сделать жизнь современного человека более комфортной и безопасной. Однако, несмотря на очевидные плюсы, которые «Интернет вещей» дает своему пользователю, он обладает рядом серьезных уязвимостей, успешная эксплуатация которых киберпреступниками и кибертеррористами может привести к очень серьезным последствиям. Рассмотрим и кратко охарактеризуем основные уязвимости «Интернета вещей».

1. ***Недостатки в организации физической безопасности устройства.*** В данном случае речь идет о том, что большинство пользователей не уделяют должного внимания физической защищенность устройств IoT от несанкционированного доступа. Зачастую компоненты, входящие в состав пользовательской экосистемы, размещаются открыто, за пределами контролируемой зоны, что дает потенциальному злоумышленнику возможность получить контроль над устройством и использовать его для доступа к сети пользователя.

2. Использование устройств с небезопасными либо неизменяемыми настройками.

Речь идет о том, что большая часть современных устройств поставляется пользователю полностью готовыми к работе, что называется «из коробки». При этом подавляющее большинство пользователей на протяжение всего цикла эксплуатации пользуется данными устройствами с теми настройками, которые были установлены изготовителем, даже не задумываясь о том, что они совершенно небезопасны. Например, как много пользователей может похвастаться тем, что они, купив и установив в домашней сети новый Wi-Fi-роутер, сразу же изменили логин и пароль администратора для доступа к панели настройки роутера? Опыт подсказывает, что таковых единицы. Все остальные используют стандартный логин «admin» и аналогичный стандартный пароль, не задумываясь о том, что эти данные указываются изготовителем на корпусе устройства и одинаковы для всех устройств без исключения. Можно ли в данном случае говорить о безопасности сети, построенной на базе такого роутера? Очевидно, нет.

Более того, многие производители в принципе не предоставляют пользователю возможности для изменения каких-либо настроек безопасности. Задумайтесь – у многих из вас на запястьях надеты «умные» часы или «умные» браслеты. А многие могут сказать, что знают, как менять в них настройки безопасности и есть ли там вообще такая возможность? У дорогих и известных брендов такие возможности, безусловно, есть. У дешевых и неизвестных – в большинстве случаев нет. Между тем «умные» часы – это такой же компьютер, со своей операционной системой, своим «администратором», знающий все о вашей жизни, распорядке дня, круге общения, снабженный микрофоном и, зачастую, видеокамерой. Представьте, что злоумышленник получил к ним удаленный доступ. Теперь он знает все о вас, о вашей работе, о вашем окружении. Слышит все, о чем вы говорите. Видит все, что происходит вокруг вас. И все это потому, что вы не изменили настройки по умолчанию, либо приобрели устройство, не предоставляющее такие возможности обычному пользователю. Обратили внимание на слово «обычному»?

3. Уязвимости в парольной защите.

Очевидная, всем хорошо известная, на протяжение десятилетий занимающая верхние строчки в топах проблема, которая, тем не менее, и в настоящее время остается крайне актуальной. Заключается она в том, что огромное, без преувеличения – подавляющее большинство пользователей либо не имеет представления о необходимости использования сложных и разнообразных паролей для доступа к своим устройствам, либо не считает это необходимым.

Ситуация парадоксальна – никому и в голову не придет выйти из дома и оставить незапертой дверь, наоборот, мы ставим мощные замки, современные системы сигнализации и иными способами защищаем свое жилище от посторонних. Но при этом очень многие из нас не задумаются и на секунду, установив на всех своих устройствах один и тот же пароль «1234», и будут свято верить в то, что теперь они защищены от всех бед. Вот только получив доступ к вашему устройству или к вашей сети злоумышленник в большинстве случаев может причинить ущерб намного больший, чем если бы он проник в вашу квартиру. Для того, чтобы получить доступ в вашу квартиру злоумышленник должен взломать замок в том время как подъезды зачастую оборудованы камерами видеонаблюдения, бдительные соседи могут поинтересоваться, что он делает возле вашей двери или просто вызвать полицию, да и вы можете не вовремя вернуться домой. То есть вскрыть сложный замок преступник должен в максимально некомфортных для себя условиях. Между тем, ломая двери в ваш цифровой дом, он может не опасаться камер, бдительных соседей и полиции. Да и ваше присутствие ему не сильно помешает. Как думаете, долго ли в таких условиях будет сопротивляться вскрытию «супер»пароль «1234»?

4. *Использование небезопасных сетевых сервисов.*

Суть данной проблемы заключается в том, что на устройстве зачастую оказывается запущено множество сетевых сервисов. Пари этом постоянная фоновая работа большинства из них вовсе не нужна для корректной работы устройства, а некоторые являются откровенно опасными, особенно если имеют подключение к сети Интернет.

Именно сетевые службы и сервисы обеспечивают подключение устройства к сети, обмен данными с серверами и другими устройствами, но они же позволяют получить несанкционированный доступ к устройству, если не обеспечен должный

уровень безопасности. Именно сетевые службы и сервисы, запущенные на устройстве, становятся первыми целями злоумышленников при проведении киберразведки и осуществлении первых этапов кибератаки. Простой пример – прежде чем провести кибератаку, злоумышленник должен четко понимать, что за устройства вы используете, какое на нем установлено программное обеспечение, какие присутствуют уязвимости в программном и аппаратном обеспечении вашей системы и как их можно эксплуатировать для достижения нужных ему целей. При этом огромный объем необходимой информации киберпреступник может получить простым сканированием открытых на устройстве портов.

5. Отсутствие механизмов обновления или использование небезопасных.

Суть проблемы заключается в том, что многие устройства «Интернета вещей», в первую очередь из категории недорогих, вообще не имеют встроенных механизмов обновления, по сути, являясь устройствами без технической поддержки разработчиком. При этом нужно понимать, что любое программное обеспечение, в том числе и то, которое управляет работой устройства, априори не лишено множества недоработок, ошибок и уязвимостей, многие из которых относятся к категории критических. Безусловно, такие устройства нужно обходить стороной даже в том случае, если вопрос цены является определяющим при проектировании системы.

Не менее распространена проблема, когда формально механизм обновления управляющего программного обеспечения, так называемой прошивки, разработчиком устройства предусмотрен, но в реальности новые версии прошивки или просто не разрабатываются, или устройство снимается с поддержки, а значит и с обновления, через непродолжительный срок с момента его запуска в производство. Такой подход, к сожалению, можно встретить у многих разработчиков, в том числе у тех, которые позиционируются как дорогие устройства «премиум» класса.

Третий вариант этой проблемы заключается в том, что механизм обновления предусмотрен, обновления разрабатываются и получаются устройством, но сам механизм является небезопасным. Например, при передаче обновления могут использоваться незашифрованные каналы, файл прошивки может передаваться в незашифрованном виде, в прошивке может быть не предусмотрен механизм верификации (проверки целостности), может отсутствовать функционал аварийного отката к предыдущей версии при ошибках обновления или обнаружении поврежденных или подмененных файлов, могут отсутствовать уведомления пользователя об изменениях настроек системы безопасности по итогам обновления и т. д. Все это, очевидно, способно предоставить злоумышленнику даже не лазейку в заборе, а широко распахнутые ворота в вашу систему.

6. Использование небезопасных механизмов передачи и хранения данных.

Крайне серьезная проблема, суть которой заключается в том, что многие устройства « Интернета вещей» не используют в работе с принимаемыми и передаваемыми данными механизмы шифрования и контроля доступа к данным.

Не является секретом, что устройства «Интернета вещей» собирают, обрабатывают, передают и хранят огромное количество личной и конфиденциальной информации обо всем, что происходит вокруг них (вспомните пример с «умными» часами). Очевидно, что такие данные должны быть надежно защищены от несанкционированного доступа. Самими распространенными и, при этом, наиболее эффектив-

ными механизмами защиты признаются контроль доступа к данным и их криптографическая защита – шифрование – на всех этапах работы. К сожалению, далеко не все устройства «Интернета вещей» способны похвастаться наличием и качественной реализацией данных механизмов. Если же на устройстве не реализованы такие механизмы, и оно имеет подключение к сети Интернет, то при передаче данных по сети они могут легко быть перехвачены злоумышленниками и использованы для достижения их преступных целей.

4. Центры мониторинга и управления безопасностью как составляющие системы борьбы с киберпреступлениями

Многие значимые расследования хакерских атак ведутся в центрах мониторинга и управления безопасностью. Главная задача таких центров заключается в том, чтобы в непрерывном режиме мониторить работу всех систем безопасности компании для того, чтобы максимально оперативно реагировать на инциденты информационной безопасности, устранять их и профилактировать появление новых инцидентов.

Рассмотрим элементарный пример: у многих на домашних компьютерах установлены антивирусные программные продукты, призванные защищать систему от вирусов. Наверняка вам приходилось видеть сообщение антивируса о том, что обнаружен вирус. Но дальнейшие действия системы зависят от ее настройки – вирус может быть удален в автоматическом режиме, а может быть выведено сообщение пользователю о его обнаружении с предложением самостоятельно принять решение о дальнейших действиях. И до тех пор, пока вы не дадите антивирусному ПО команду на удаление вируса, он будет продолжать жить в системе. Да, он будет заблокирован и не сможет (в большинстве случаев) причинить системе вред, но жить он будет. Другой пример: возможно, вы уже знаете, что далеко не все вирусы успешно «отлавливаются» антивирусным ПО. В частности, печально известные вирусы-шифровальщики, эпидемия которых накрыла российский сегмент Интернета в 2016–2017 годах (Petya, NotPetya, WannaCry) большинством антивирусных продуктов не замечались, что и позволило им реализовать такую массовую атаку. Почему так происходило? На самом деле все просто – эти вирусы использовали уязвимости в операционных системах таким образом, что антивирус находится в полной уверенности, что система находится в своем стандартном состоянии и все, что в ней происходит, является легитимным. Именно в таких ситуациях, как в описанных нами двух примерах (равно как и в десятках и сотнях других подобных), необходима качественная работа специалистов центров мониторинга и управления безопасностью: чем быстрее они заметят, что в системе, несмотря на отсутствие тревоги от штатных средств защиты, происходят аномалии, тем меньший ущерб будет причинен в конечном итоге.

Аномалии могут быть разными. Например, наличие в системе слишком большого количества файлов, подвергшихся изменениям за небольшой промежуток времени, является одним из явных признаков работы вируса-шифровальщика, который в самое ближайшее время обрадует вас требованием заплатить определенную сумму за восстановление доступа к вашим файлам. Потребление системой слишком большого количества системных ресурсов, явно не соответствующих выполняемым за-

дачам – признак, характерный для заражения вирусом-майнером, использующим ресурсы вашей системы для добычи криптовалюты. Нетипичный интернет-траффик к неизвестным интернет-ресурсам с высокой степенью вероятности может свидетельствовать о том, что ваша система стала частью бот-сети и используется для организации DDoS-атак. Естественно, возможны и многие другие виды аномалий, указывающих на другие виды проблем. Но, какими бы они ни были, задача специалистов центров мониторинга и управления безопасностью заключается в том, чтобы максимально оперативно их выявить, локализовать, минимизировать их последствия, не допустить повторного появления.

Безусловно, специалист центра не работает сам по себе. В принятии решений он опирается на информацию, поступающую от различных специализированных систем, таких, например, как, SIEM-системы (системы управления информацией о безопасности и событиями информационной безопасности) назначение и принцип работы которых будут более подробно рассмотрены в рамках одной из следующих тем.

Выделяют два типа центров мониторинга и управления безопасностью – внутренние центры и внешние. С внутренним центром все достаточно просто – он создается в том случае, если руководство организации считает необходимым в режиме реального времени реагировать на возможные инциденты кибербезопасности, но уже имеющихся ресурсов подразделений информационной безопасности или технической службы для данных целей недостаточно. В подобной ситуации создается внутренний центр, в состав которого набирают наиболее квалифицированных специалистов в области информационной безопасности из числа уже имеющегося персонала компании, либо нанимают новых. Внешний центр – это организация внешняя и самостоятельная по отношению к организации, заинтересованной в оперативном реагировании на киберинциденты, и оказывающая соответствующие услуги по договору с ней.

Данные, поступающие во внешний центр, непрерывно обрабатываются и анализируются сотрудниками дежурной смены, в состав которой входят, как правило, следующие специалисты:

Системный администратор или инженер – специалист, который обеспечивает настройку внутренних систем самого центра, используемых при обработке данных, получаемых от заказчика. Кроме того, системный администратор или инженер несет ответственность за то, чтобы данные от заказчика поступали стабильно. Сотрудник центра, работающий на данной должности, обязан быть специалистом в области установки и настройки различных операционных систем, прикладного программного обеспечения, а также всевозможных систем информационной защиты и безопасности.

Специалист по настройке правил – сотрудник, который получает сведения о том, как и в каких режимах работают его информационные системы, и, основываясь на этих сведениях, разрабатывает правила выявления инцидентов кибербезопасности и реагирования на них при помощи инфраструктуры центра.

Аналитик 1-го уровня – специалист, который отвечает за первоначальный анализ входящей от заказчика информации. Он осуществляет распределение киберинцидентов и отсев так называемых ложноположительных срабатываний, то есть

ситуаций, когда система явно ошибочно приняла то или иное событие за киберинцидент. Как правило, этот специалист работает на основании заранее разработанных в центре алгоритмов и сценариев действий, в которых подробно расписаны все шаги, которые необходимо предпринять для устранения того или иного киберинцидента. В том случае, если самостоятельно выполнить все необходимые шаги и устранить киберинцидент аналитик 1-го уровня не в состоянии, он передает его аналитику 2-го уровня.

Аналитик 2-го уровня – специалист более высокого класса, который при реагировании на инцидент, выявленный на 1 уровне, опирается уже не на типовые, заранее разработанные шаги, а решает стоящую перед ним задачу «с листа», опираясь только на собственный опыт и навыки. В том случае, если в ходе его работы выяснится, что данный киберинцидент спровоцирован применением неизвестного, ранее не применявшегося вредоносного программного обеспечения или ситуация такова, что невозможно сделать однозначный вывод о том, что и как именно произошло, инцидент передается на 3-й уровень, где с ним работают специалист по реверс-инжинирингу или форензик-эксперт.

Специалист по реверс-инжинирингу – специалист высочайшего уровня, как правило, являющийся профессиональным программистом. Специалист по реверс-инжинирингу должен изучить вредоносное программное обеспечение, ставшее причиной киберинцидента, и понять, как оно устроено и что именно делает. Для этого вирус запускается в специальной изолированной среде (так называемой песочнице), анализируется его поведение и производится процедура так называемой обратной разработки, когда из имеющегося в распоряжении вируса специалист получает его исходный код для дальнейшего анализа, выявления особенностей работы и поиска методов наиболее эффективного противодействия.

Форензик-эксперт – специалист по компьютерной криминалистике, в задачу которого входит установление всех изменений в системе, подвергшейся киберинциденту, выявление удаленных или измененных файлов, определение того, что именно было похищено при помощи вредоносного программного обеспечения, какие еще системы были подвергнуты атаке, а также выявление того, как именно происходила атака, то есть установление ее полного пути от момента проникновения угрозы в систему (как и откуда) до момента ее локализации (что делала, какой ущерб был причинен в итоге).

Специалист по киберразведке – его зона ответственности лежит в поиске внутри системы заказчика нового, ранее не выявленного вредоносного программного обеспечения, например, так называемых вирусов – логических бомб, которые начинают свою деятельность только при выполнении определенных условий в атакуемой системе, а до этого момента никак себя не проявляют, оставаясь незаметными для систем защиты. Кроме того, в обязанности данного специалиста входит поиск в Интернете, в том числе на специализированных форумах, информации о новых киберугрозах, о планируемых кибератаках, о методах противодействия им, а также о наличии интереса к компании-заказчику.

5. Понятие критической информационной инфраструктуры

Критическая информационная инфраструктура – это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, а также сети электросвязи, используемые для организации их взаимодействия. Ключевым условием отнесения системы к КИИ является ее использование государственным органом или учреждением, либо российской компанией в следующих сферах: здравоохранение, наука, транспорт, связь, энергетика, банковский (финансовый) сектор, топливно-энергетический комплекс, атомная энергетика, оборонная промышленность, ракетно-космическая промышленность, горнодобывающая промышленность, металлургическая промышленность, химическая промышленность.

Также к КИИ будут относиться системы, которые на праве собственности, аренды или на ином законном основании принадлежат российской компании или ИП, и обеспечивают взаимодействие указанных выше систем или сетей.

Понятие критической информационной инфраструктуры раскрыто в Федеральном законе от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры». Согласно ему, все критически важные структуры обязаны встроиться в Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также обезопасить свои системы от киберпреступников. Предполагается, что новые правила заработают с 1 января 2023 года для софта и с 2024 года – для оборудования. За несоответствие требований к безопасности критически важных объектов компаниям грозит административная и даже уголовная ответственность.

Несмотря на то, что сети КИИ, как правило, закрыты и отделены от публичного сегмента Сети, их владельцы ошибочно считают, что такой изоляции достаточно для защиты от кибератак. Но это не так, показало исследование компании «Ростелеком-Солар». Согласно его результатам, каждая десятая критически важная IT-система в России оказалась заражена вредоносными программами. От хакерских атак не удалось защититься ни банкам, ни госорганам, ни оборонным и транспортным объектам. Аналитики предупредили, что потенциально уязвимых инфраструктур может быть гораздо больше, а нанести удар сейчас способны даже хакеры-дилетанты без должного опыта, поскольку подавляющее большинство компаний забывают вовремя обновлять свой софт.

Интересно, что затраты российских предприятий на переход на отечественное программное обеспечение оценили в 1 трлн рублей. Сейчас таких денег у бизнеса нет, поэтому Российский союз промышленников и предпринимателей попросил исключить из требования по обязательному импортозамещению софта хотя бы некритические объекты, включая банки.

Вопросы и задания для самоконтроля

1. Сформулируйте определение термина «безопасность».
2. Дайте определение термину «кибербезопасность».
3. Назовите основные направления кибербезопасности.
4. Сформулируйте понятие «кибербезопасность оконечных устройств».
5. Что является технологической платформой современного кибероружия?

6. Дайте определение понятию «киберугроза».

7. Перечислите и кратко охарактеризуйте основные виды киберугроз.

8. Назовите и кратко охарактеризуйте основные уязвимости «Интернета вещей».

9. Перечислите основные должности специалистов, входящих в состав дежурной смены центров мониторинга и управления безопасностью.

10. Сформулируйте определение понятия «критическая информационная инфраструктура» согласно действующему законодательству.

Лекция 2. Нормативно-правовое обеспечение кибербезопасности

В современных условиях повсеместной цифровизации проблема кибербезопасности становится крайне актуальной. Различные государственные, муниципальные и коммерческие структуры владеют огромными массивами информации. В условиях научно-технического прогресса в геометрической прогрессии изменяется в сторону увеличения количество и качество цифровых средств, которые способны считывать, анализировать, передавать и т. д. полученные данные с большой скоростью. Вслед за усилением интеграции между работой государственных и коммерческих учреждений и цифровых технологий появляются угрозы, которые открывают все больше новых путей для образования новых мошеннических схем, совершения новых видов киберпреступлений. Обостряется также проблема защиты персональных данных в связи с тотальной цифровизацией общества.

Огромный объем информации ежедневно, ежеминутно и ежесекундно попадает в Интернет и хранится в различных облачных хранилищах вечно. Количество гаджетов, подключенных к Интернету, как уже отмечалось, с каждым годом увеличивается в геометрической прогрессии. Многие программы получают у неискушенных и не подготовленных пользователей разрешение на использование данных и тем самым в процессе использования собирают не только основную информацию, необходимую для работы приложения, но и множество других персональных сведений.

В этой связи, такое важнейшее такое направление как кибербезопасность нуждается в целостной нормативной базе. Необходимо совершенствовать законодательство в этой области и своевременно актуализировать принятые нормы. Очевидно, что это возможно только при условии привлечения к такого рода деятельности компетентных специалистов, способных реализовывать законодательную функцию на стыки двух профессий: юриста и IT-специалиста.

1. Законодательство Российской Федерации в области защиты информации

В рамках первой темы курса был сделан вывод, что понятие «кибербезопасность» является более узким по отношению к понятию «информационная безопасность». Отсюда напрашивается вполне, казалось бы, логичный и очевидный вывод о том, что действующее законодательство в области защиты информации должно регулировать, в том числе, и вопросы, связанные именно с кибербезопасностью. Однако на самом деле все не совсем так, как кажется на первый взгляд.

Для того чтобы разобраться в этой проблеме и понять ее причины, рассмотрим в целом действующее законодательство в области информационной безопасности, а

затем дополнительно рассмотрим вопросы непосредственно кибербезопасности и ее правового регулирования.

Правовое обеспечение процессов информатизации представляет собой совокупность нормативных правовых актов, принимаемых на различных уровнях власти и управления, регулирующих комплекс общественных отношений, связанных с созданием и использованием информации и перспективных информационных технологий.

В условиях формирования информационного общества в России конституционное закрепление информационных прав имеет большое политическое и юридическое значение.

Конституция Российской Федерации[1] закрепляет основные, базовые положения для всех отраслей права. Она содержит основополагающие нормы и в отношении информации. В Основном законе информации посвящено несколько статей (ст. 24, 29, 42, 71).

Ст. 24: «1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом».

Ст. 29: «каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» (п. 4); «гарантируется свобода массовой информации. Цензура запрещается» (п. 5).

Конституционные положения, закрепляющие основные информационные права и свободы, развиваются и детализируются в федеральном законодательстве. Рассматривая уровень федеральных законов, следует выделить следующие:

1. **Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»**[2]**.** Данный нормативный правовой акт может быть обозначен как основной закон РФ, посвященный защите информации. В сферу его нормативного регулирования входят вопросы, связанные с поиском информации, ее получением и передачей, производством, распространением, защитой, а также применением информационных технологий. Закон устанавливает понятийный аппарат, который впоследствии используется иными нормативными правовыми актами. В частности, именно он определяет такие ключевые термины, как информации, информационные технологии, электронное сообщение, сайт, поисковая система и т. д. Рассматриваемый нормативный правовой акт определяет, что информации подразделяется на общедоступную и на такую, доступ к которой ограничен действующим законодательством.

Анализ данного нормативного правового акта позволяет выделить его ключевые моменты:

– Сбор и распространение информации о частной жизни человека без его прямого на то согласия запрещены.

– Информация подразделяется на свободно распространяемую и ограниченного доступа.

---

[1] Собрание законодательства РФ (далее – СЗ РФ). 2014. № 31. Ст. 4398.

[2] СЗ РФ. 2006. № 31 (ч. 1). Ст. 3448.

– Доступ к определенного рода информации (например, к информации о правах, свободах и обязанностях человека и гражданина, о состоянии окружающей среды, о деятельности государственных органов и органов местного самоуправления) не может быть ограничен ни при каких обстоятельствах.

– Информация определенного рода (например, пропагандирующая войну, разжигающая национальную, расовую или религиозную ненависть и вражду) запрещена к распространению и предоставлению на территории Российской Федерации.

– Лицо, осуществляющее хранение информации, обязано предпринимать исчерпывающие меры по ее защите.

– В Российской Федерации ведется Единый реестр интернет-ресурсов, содержащих информацию, запрещенную к распространению на территории государства.

– Интернет-ресурс, доступ к которому заблокирован в связи с включением в Единый реестр как содержащий информацию, распространение которой запрещено на территории Российской Федерации, может быть разблокирован и доступ к нему может быть восстановлен в случае удаления указанной информации, запрещенной к распространению.

2. **Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»**[1]. Этот нормативный правовой акт регулирует отношения, связанные с обработкой государственными органами власти, юридическими и физическими лицами персональных данных, которые не составляют государственную тайну. Сфера нормативного регулирования закона, как следует из его названия, ограничена персональными данными, то есть личными данными конкретных физических лиц. Действие закона распространяется на всех без исключения физических и юридических лиц, органы государственной власти и местного самоуправления, которые собирают и используют в своей деятельности персональные данные.

Анализ данного нормативного правового акта позволяет обозначить его ключевые моменты:

– Сбор и обработка персональных данных допускаются только при получении прямого согласия их владельца.

– Персональные данные не могут собираться «просто так», это допускается только с конкретными, заранее определенными и законными целями и только в объеме, соответствующем заявленным целям.

– Оператор персональных данных обязан обеспечивать их защиту от доступа посторонних лиц.

– Владелец персональных данных вправе в любой момент отозвать у оператора право на их сбор, хранение и обработку. Оператор персональных данных обязан удовлетворить требование их владельца.

– Оператор персональных данных обязан хранить их на серверах, расположенных на территории Российской Федерации. При этом, в случае необходимости, персональные данные (при соблюдении ряда условий) могут передаваться за переделы Российской Федерации, так как закон не содержит запрета на их трансграничную передачу.

[1] СЗ РФ. 2006. № 31 (ч. 1). Ст. 3451.

3. **Федеральный закон от 21 июля 1993 г. № 5485–1 «О государственной тайне»[1].** Этот нормативный правовой акт регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации. Он определяет полномочия государственных органов и должностных лиц по обеспечению сохранности и защиты государственной тайны, содержит перечень сведений, составляющих государственную тайну. Требования этого закона обязаны соблюдать все, кто по роду деятельности имеет допуск к сведениям, составляющим государственную тайну, например сотрудники отдельных подразделений и служб МВД, отдельные категории военнослужащих, а также лица, занимающие некоторые категории должностей государственной или муниципальной гражданской службы.

Ключевые моменты закона:

– Засекречиваться могут не любые сведения, а только те, которые относятся к военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности государства, и распространение которых может нанести ущерб безопасности Российской Федерации.

– Некоторые сведения не подлежат засекречиванию ни при каких обстоятельствах. Это сведения о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях; о состоянии здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности; о фактах нарушения прав и свобод человека и гражданина; о размерах золотого запаса и государственных валютных резервах Российской Федерации и некоторые другие.

– В Российской Федерации существует три грифа секретности сведений, составляющих государственную тайну: секретно, совершенно секретно и особой важности.

– Должностные лица и граждане, виновные в нарушении законодательства Российской Федерации о государственной тайне, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством.

4. **Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»[2].** Данный нормативный правовой акт в сферу своего нормативного регулирования включает все вопросы, связанные с таким правовым явлением как коммерческая тайна. Закон дает определение этому понятию, определяет порядок ее охраны, а также устанавливает ответственность за ее разглашение или передачу посторонним лицам. Согласно определению, данному в законе, коммерческая тайна представляет собой такую информацию, которая способна помочь компании избежать неоправданных расходов, а также увеличить доходы или получить иную коммерческую выгоду.

Анализ норм закона позволяет выделить его ключевые моменты:

---

[1] СЗ РФ. 1997. № 41. Ст. 8220–8235.

[2] СЗ РФ. 2004. № 32. Ст. 3283.

– В отличие от государственной тайны, когда требования о засекречивании той или иной информации устанавливаются государством и не зависят от воли владельца информации, в случае коммерческой тайны именно ее владелец (и только он) вправе определить, будет ли данная информация относиться к коммерческой тайне или нет. Для этого, в каждой организации, работающей с коммерческой тайной, определяется перечень и состав такой информации.

– Существует определенного рода информация, которая ни при каких обстоятельствах не может быть отнесена к коммерческой тайне, например сведения из учредительных документов юридического лица, сведения о численности работников, системе оплаты труда, условиях труда и некоторые другие.

– Государство имеет право получитьу компании информацию, отнесенную к коммерческой тайне, то только на основании мотивированного требования, с указанием целей и правового основания затребования такого рода информации. Компания в этом случае обязана на безвозмездной основе предоставить такую информацию.

– Компания обязана принимать исчерпывающие меры по охране конфиденциальности информации, отнесенной к коммерческой тайне, в частности определять перечень и состав такой информации, ограничивать доступ к ней, вести учет лиц, имеющих право доступа к такого рода информации и т. д.

– Разглашение сведений, составляющих коммерческую тайну, влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность.

5. **Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»**[1]**.** Данный нормативный правовой акт устанавливает на территории Российской Федерации правила использованияэлектронной подписи, являющейся цифровым аналогом обычной собственноручной физической подписи. Суть цифровой подписи заключается в том, чтобы обеспечить возможность подтверждения подлинности той или иной информации, а также невозможность ее подделки или искажения. Этот закон касается электронной подписи – цифрового аналога физической подписи, который помогает подтвердить подлинность информации и избежать ее искажения и подделки. Закон дает определение электронной подписи, определяет ее юридическую силу и устанавливает правовой режим ее использования.

Анализ данного нормативного правового акта позволяет выделить его ключевые моменты:

– Закон не устанавливает обязанности использования какого-либо специализированного программного обеспечения или технических средств для создания электронной подписи. Пользователь вправе самостоятельно определять, какое именно ПО он будет использовать для данной цели при условии, что оно обеспечивает необходимый уровень надежности создаваемой электронной подписи.

– Закон устанавливает три вида электронных подписей: простые, усиленные неквалифицированные и усиленные квалифицированные. Все указанные виды электронных подписей имеют разный правовой режим и используются для разных целей.

[1] СЗ РФ. 2011. № 15. Ст. 2036.

– Полным аналогом собственноручной физической подписи является усиленная квалифицированная электронная подпись. В этой связи те лица, которые работают с такого рода подписью, обязаны хранить в тайне ключ подписи.

– Формирование и выдача электронных подписей и сертификатов, подтверждающих их действительность, осуществляется исключительно специализированными удостоверяющими центрами.

6. **Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[1].** Данный нормативный правовой акт распространяет свое действие на компании и организации, осуществляющие свою деятельность в сферах, имеющих критически важное значение для жизни государства и общества, то есть таких, сбой в работе которых негативно повлияет на безопасность и здоровье населения страны. В этой связи к информационной инфраструктуре таких организаций и ее безопасности предъявляются особые требования.

Закон содержит исчерпывающий перечень таких сфер и к ним относятся, здравоохранение, наука, транспорт, связь, энергетика, банковская сфера и иные сферы финансового рынка, топливно-энергетический комплекс, атомная энергетика, оборонная, ракетно-космическая, горнодобывающая, металлургическая и химическая промышленность. Кроме того, закон определяет, что к критической информационного инфраструктуре государства, помимо компаний и организаций, непосредственно работающих в указанных сферах деятельности, относятся также и обеспечивающие их деятельность организации, например предоставляющие в аренду оборудование или разрабатывающие для них программное обеспечение. Также сюда относят компании, которые обеспечивают работу предприятий из этих сфер, например, предоставляют оборудование в аренду или разрабатывают для них ПО. Если на предприятии из этой сферы будет простой, это негативно отразится на жизни всего государства.

Анализ рассматриваемого нормативного правового акта позволил выделить его ключевые моменты:

– В Российской Федерации, в целях учета значимых объектов критической информационной инфраструктуры, ведется реестр значимых объектов критической информационной инфраструктуры.

– Для защиты объектов критической информационной инфраструктуры в Российской Федерации создана специализированная Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

– Субъекты критической информационной инфраструктуры непрерывно взаимодействовать с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак, в том числе обязаны в установленном порядке предоставлять сведения о компьютерных инцидентах.

– Для каждого значимого объекта критической информационной инфраструктуры, в целях его защиты, должна быть создана система безопасности, обеспечивающая предотвращение несанкционированного доступа к информации, обрабатываемой данным объектом, недопущение воздействия на его технические средства

[1] СЗ РФ. 2017. № 31 (ч. I). Ст. 4736.

обработки информации, восстановление его функционирования в случае необходимости, а также непрерывное взаимодействие с ГосСОПКА.

– На значимых объектах критической информационной инфраструктуры должны быть установлены специальные технические, программные, программно-аппаратные и иные средства для обнаружения, предупреждения, ликвидации последствий компьютерных атак, обмена информацией, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и ликвидации последствий компьютерных атак, а также криптографические средства защиты такой информации.

– Государству в лице федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, предоставлено право проверки значимых объектов критической информационной инфраструктуры. Такие проверки могут проводиться как по установленному и утвержденному плану, так и внепланово, например в случае возникновение компьютерного инцидента, повлекшего негативные последствия, на значимом объекте критической информационной инфраструктуры.

Эти перечисленные шесть федеральных законов можно уверенно относить к категории основных нормативных правовых актов Российской Федерации в области информационной безопасности и защиты информации.

Безусловно, это далеко не все нормативные правовые акты Российской Федерации, регламентирующие правоотношения, возникающие в области информационной безопасности. Среди прочих НПА, имеющих определенное отношение к этой области, можно выделить, например, следующие:

– Гражданский кодекс Российской Федерации[1] (осуществляет правовое регулирование создания и использования программ для ЭВМ и баз данных: ст. 1261, 1262, 1280 и др.);

– Кодекс Российской Федерации об административных правонарушениях[2] (закрепляет ответственность за нарушение норм в сфере обработки персональных данных (ст. 13.11), нарушение правил защиты информации (ст. 13.12)и др.);

– Уголовный кодекс Российской Федерации[3] (содержит статьи, определяющие ответственность за неправомерный доступ к компьютерной информации (ст. 272); создание, использование и распространение вредоносных компьютерных программ (ст. 273); Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274) и др.);

– Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»[4] (регулирует отношения, связанные с обеспечением доступа пользователей к сведениям о деятельности государственных органов и органов местного самоуправления, определены принципы и способы обеспечения доступа к информа-

[1] СЗ РФ. 2006. № 52 (ч. 1). Ст. 5496.
[2] СЗ РФ. 2002. № 1 (ч. 1). Ст. 1.
[3] СЗ РФ. 1996. № 25. Ст. 2954.
[4] СЗ РФ. 2009. № 7. Ст. 776.

ции, формы ее предоставления, права и обязанности пользователей информации, органов власти, их должностных лиц, установлена ответственность за нарушение порядка доступа к информации).

– Указ Президента РФ от 9 мая 2017 г. № 203 «О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»[1];

– Постановление Правительства РФ от 18 мая 2009 г. № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям»[2] (установило требования по обеспечению защиты информации, содержащейся в информационных системах общего пользования);

– 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»[3] (определяет для государственных и муниципальных органов, обрабатывающих персональные данные, необходимость обязательного принятия ряда документов, обеспечивающих выполнение законодательства в области персональных данных);

– Постановление Правительства РФ от 25 апреля 2012 г. № 394 «О мерах по совершенствованию использования информационно-коммуникационных технологий в деятельности государственных органов»[4] (скорректированы акты Правительства РФ по вопросам совершенствования использования информационно-коммуникационных технологий в деятельности государственных органов);

– Постановление Правительства РФ от 6 сентября 2012 г. № 890 «О мерах по совершенствованию электронного документооборота в органах государственной власти»[5] (принят ряд мер по совершенствованию электронного документооборота в органах государственной власти, а также установлен срок (до 31 декабря 2017 г.) перехода к электронному взаимодействию федеральных органов исполнительной власти между собой и с Правительством РФ);

– Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»[6] (пересмотрены требования по защите этих данных при их обработке в соответствующих информационных системах. За безопасность персональных данных отвечает оператор системы, который их обрабатывает, или уполномоченное им лицо. Оператор системы выбирает средства защиты информации в соответствии с нормативными актами ФСБ России и ФСТЭК России).

[1] СЗ РФ. 2017. № 20. Ст. 2901.
[2] СЗ РФ. 2009. № 21. Ст. 2573.
[3] СЗ РФ. 2012. № 14. Ст. 1626.
[4] СЗ РФ. 2012. № 19. Ст. 2419.
[5] СЗ РФ. 2012. № 38. Ст. 5102.
[6] СЗ РФ. 2012. № 45. Ст. 6257.

– Постановление Правительства РФ от 24 июля2021 г. № 1264 «Об утверждении Правил обмена документами в электронном виде при организации информационного взаимодействия»[1](определило правила обмена документами в электронном виде).

Безусловно, и это далеко не все нормативные правовые акты Российской Федерации, которые, так или иначе, имеют отношение к вопросам информационной безопасности государства. Однако даже простое перечисление полного перечня такого рода нормативных правовых актов заняло бы несколько часов, поэтому для нужд данного вопроса были рассмотрены только самые основные НПА.

Если же от общих вопросов нормативного правового обеспечения информационной безопасности на общегосударственном уровне перейти к аналогичным частным вопросам на уровне Министерства внутренних дел Российской Федерации, то здесь можно отметить следующие нормативные правовые акты, часть из которых уже была обозначена выше при рассмотрении данного вопроса.

Правовой основой реализации Министерством своих полномочий в установленной сфере являются Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»[2], 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 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»[3], Федеральный закон от 7 февраля 2011 г. №3-ФЗ «О полиции»[4], Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи», Указ Президента Российской Федерации от 1 марта 2011 г. № 248 «Вопросы Министерства внутренних дел Российской Федерации»[5], Указ Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы», а также нормативные правовые акты МВД России, регулирующие вопросы развития информационных технологий, связи и защиты информации.

2. Основы государственной политики Российской Федерации в области международной информационной безопасности[6]

Международная информационная безопасность трактуется, прежде всего, исходя из характера угроз. Традиционно выделялась «триада угроз» международной информационной безопасности – использование информационно-коммуникационных технологий в террористических, преступных и военно-политических целях (под военно-политическими целями понимается использование ИКТ в межгосударственных

[1] СЗ РФ. 2021. № 31. Ст. 5927.
[2] СЗ РФ. 1995. № 33. Ст. 3349.
[3] СЗ РФ. 2010. № 31. Ст. 4179.
[4] СЗ РФ. 2011. № 7. Ст. 900.
[5] СЗ РФ. 2011. № 10. Ст. 1334.
[6] В основу данного учебного вопроса положены следующие материалы: *Зиновьева Е. С.* Анализ внешнеполитических инициатив РФ в области международной информационной безопасности // Вестник МГИМО Университета. 2014. № 6 (39). С. 47–52; *Ее же*. Информационная безопасность Российской Федерации на современном этапе развития международных отношений // СМИ mgimo.ru (МГИМО-Университет): [сайт]. 2014. 23 июля. URL: https://mgimo.ru/about/news/experts/258416/

конфликтах). В частности, подобный подход к определению угроз был закреплен в ряде резолюций Генеральной Ассамблеи ООН, посвященных проблематике информационной безопасности.

Россия в 2013 году в документе «Основы государственной политики в области международной информационной безопасности на период до 2020 года» добавила к триаде угроз опасность вмешательства во внутренние дела суверенного государства посредством ИКТ, нарушение общественной стабильности, разжигание межэтнической, межнациональной розни. По сути, это стало реакцией России на события «арабской весны», когда социальные сети и блоги активно использовались для координации протестного движения.

Как отмечалсь при рассмотрении второго учебного вопроса, относительно терминологии нет единства мнений – ведутся дискуссии между государствами, придерживающимися различных толкований понятия «международная информационная безопасность». Россия выступает за широкий подход к определению содержания понятия «международная информационная безопасность», включая в нее как технические аспекты (безопасность информационных сетей и систем), так и обширный круг политико-идеологических аспектов (манипулирование информацией, пропаганда посредством глобальных информационных сетей, информационное воздействие). Страны Запада, прежде всего США, придерживаются узкого подхода, ограничиваясь техническими аспектами, и используют иную терминологию – «кибербезопасность».

Значимость национальных интересов России в области обеспечения информационной безопасности и управления сетью Интернет особо подчеркивает тот факт, что они упоминаются в целом ряде официальных документов последних лет, среди которых Стратегия национальной безопасности Российской Федерации, Стратегия развития информационного общества Российской Федерации, Концепция внешней политики Российской Федерации, Основы государственной политики Российской Федерации в области международной информационной безопасности и др. В Стратегии национальной безопасности Российской Федерации информационная безопасность рассматривается в качестве одной из важнейших составляющих национальной безопасности страны.

На сегодняшний день Россия является одним из наиболее динамичных и устойчиво растущих ИКТ-рынков в мире. Вместе с тем, как показывают результаты исследований, Российский сектор Интернета (ру-нет) сталкивается со значительным числом киберугроз, как внутренних, так и внешних. Это также актуализирует необходимость международного сотрудничества по обеспечению информационной безопасности, за что выступает Россия.

Россия исходит из потребности выработки определенных правил поведения государств в информационном пространстве. Это предполагает заключение международных договоренностей, на основании которых государства отказались бы от использования, передачи и применения средств информационного воздействия, то есть осуществления любых возможных агрессивных действий в информационном пространстве. Кроме того, обеспечение международной информационной безопасности предполагает противодействие международной информационной преступности и терроризму.

Россия активно участвует в международных переговорах по обеспечению информационной безопасности, что является практическим воплощением официальной позиции нашей страны, изложенной как в Стратегии развития информационного общества Российской Федерации, так и в Концепции внешней политики Российской Федерации, в соответствии с которыми перед российской дипломатией ставится задача обеспечить эффективное вхождение страны в глобальное информационное общество.

Анализ документов и выступлений официальных лиц позволяет сделать вывод, что Россия выступает за демилитаризацию информационного пространства, т. к. гонка вооружений в информационной сфере способна расшатать сложившиеся договоренности о разоружении и международной безопасности. Согласно Основам государственной политики в области международной информационной безопасности Россия ставит целью государственной политики в области международной информационной безопасности содействие установлению международного правового режима, направленного на создание условий для формирования системы международной информационной безопасности; достижению этой цели, среди прочего, будет способствовать создание условий, обеспечивающих снижение риска использования информационных и коммуникационных технологий для осуществления враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности. В Концепции внешней политики Российской Федерации указано, что Россия будет добиваться выработки под эгидой ООН правил поведения в области обеспечения международной информационной безопасности.

С 1998 года Россия выступает за развитие и углубление международного сотрудничества по обеспечению информационной безопасности, как на глобальном, так и на региональном уровне, и в рамках двусторонних отношений.

Договоренности о сотрудничестве по международной информационной безопасности были достигнуты с рядом государств, в том числе со странами ШОС, Белоруссией, Кубой. В 2013 году был заключен ряд важных договоренностей с США, направленных на формирование мер укрепления доверия в глобальном информационном пространстве. По инициативе России проблематика международной информационной безопасности рассматривалась на высоком политическом уровне и многосторонней основе, в рамках ОБСЕ, ШОС, ОДКБ, Международного союза электросвязи (МСЭ), в ходе Всемирной встрече на высшем уровне по вопросам информационного общества (ВВУИО), в рамках СНГ и Регионального содружества в области связи (РСС).

Сегодня более 130 государств развивают программы ведения кибервойн, что создает серьезные угрозы информационной стабильности: отследить источник информационной атаки сложно, последствия ее могут быть разрушительными и стать причиной ответного удара, в том числе с использованием обычных вооружений. В этой ситуации подход России, выступающей за выработку правил поведения государств в информационном пространстве с целью обеспечить его безопасность, представляется актуальным и соответствующим международной ситуации.

3. Международные стандарты в области обеспечения кибербезопасности[1]

В рамках изучения первой темы нашего курса говорилось о том, что существует великое множество различных международных стандартов в области кибербезопасности, так еще практически у каждой страны (государства) имеются свои собственные многостраничные стандарты, определяющие типовые процедуры и сценарии сбора и обработки информации, оценки рисков, типовых решений и действий.

В настоящий момент существует большое количество подходов к обеспечению и управлению информационной и кибербезопасностью. Наиболее эффективные из них формализованы в стандарты.

Международные стандарты и методологии являются ориентиром при построении информационной и кибербезопасности, а также помогают в решении связанных с этой деятельностью задач всех уровней, как стратегических и тактических, так и операционных. Попробуем разобраться в идеях популярных зарубежных стандартов и в том, как они могут применяться в российской практике.

Сначала ответим на вопрос, зачем вообще нужны подобные стандарты.

Каждому специалисту, имеющему отношение к информационной и кибербезопасности, желательно ознакомиться с наиболее известными методологиями в соответствующей области, а также научиться применять их на практике. Изучение лучших практик дает возможность узнать:

– терминологию в сфере КБ;
– общие подходы к построению КБ;
– общепринятые процессы КБ и рекомендации по их выстраиванию;
– конкретные меры защиты – контроли КБ;
– роли и зоны ответственности при построении процессов КБ;
– подходы к измерению зрелости процессов КБ;
– и многое другое.

Международные КБ-стандарты развиваются годами, и за это время успели усовершенствоваться и вобрать в себя лучший опыт практикующих специалистов, в том числе лучшие практики в области развития КТ.

Еще одним преимуществом изучения стандартов является возможность продуктивного взаимодействия в сообществе КБ-специалистов – общепризнанные стандарты международного уровня позволяют им общаться между собой и с внутренними подразделениями компании на одном языке с использованием устоявшихся терминов и определений. В том числе это помогает обосновывать руководству необходимость тех или иных КБ-мер формулировками, понятными бизнесу. Стоит отметить, что КБ всегда идет бок о бок с информационными технологиями, и для повышения эффективности работы очень важно уметь устанавливать коммуникации с ними. В этом КБ-специалисту помогает изучение таких стандартов, как ITIL и COBIT.

[1] В основу данного учебного вопроса положены следующие материалы: Обзор международных стандартов в области ИБ // Интернет-портал «Безопасность пользователей в сети Интернет»: [сайт]. 2020. 7 мая. URL: https://safe-surf.ru/specialists/article/5259/644530/

Какие же бывают КБ-стандарты? На самом деле существует множество систем взглядов и разных способов группировки стандартов. Методы классификации различаются по целям и задачам применения.

Рассмотрим стандарты с прикладной и процессной точек зрения. Стандарты можно поделить:

– на технические или контрольные, регламентирующие различные аспекты реализации мер защиты,

– процессно-ориентированные, описывающие поход к выстраиванию процессов и построению КБ в целом.

Технические стандарты помогают провести выстраивание технической защиты информации – выбрать необходимый комплекс защитных мер и провести их грамотную настройку.

Процессно-ориентированные стандарты описывают поход к выстраиванию отдельных процессов.

Если процессно-ориентированные стандарты позволяют ответить на вопросы «что делать?», то технические дают практические рекомендации и отвечают на вопрос «как это реализовать?».

К процессно-ориентированным стандартам относятся: серия ISO/IEC 27XXX, руководство ITIL, методология COBIT и так далее.

В части технических стандартов стоит отметить проект OWASP top 10, CIS Controls, а также CIS Benchmarks, которые содержат детальную информацию по обеспечению безопасности ИТ-элементов инфраструктуры, что помогает противодействовать широкому спектру угроз.

Тем не менее, не всегда стоит однозначно делить стандарты на категории. Один стандарт может агрегировать в себе информацию по нескольким направлениям. Так, например, стандарт PCI DSS (стандарт безопасности данных индустрии платежных карт) отражает комплексный подход к обеспечению КБ и содержит как требования к управлению безопасностью, правилам и процедурам, так и большой перечень технических требований к критически важным мерам защиты.

Кратко рассмотрим основные международные стандарты в области информационной и кибербезопасности.

Методология COBIT.

Международная ассоциация ISACA (Information Systems Auditand Control Association), известная разработкой стандартов по управлению ИТ в корпоративной среде и проводимыми сертификациями (например, CISA, CISM, CRISC), и Институт руководства ИТ (IT Governance Institute – ITGI) совместно разработали подход к управлению информационными технологиями. В 1996 году на его основе организация ISACA выпустила первую версию стандарта COBIT. С течением времени и с развитием подходов к управлению ИТ концепция COBIT пересматривалась и расширялась. Сегодня самой новой версией методологии является COBIT 2019, ставшая продуктом эволюции пятой версии стандарта (пересмотр состоялся в декабре 2018 года). COBIT 2019 описывает набор процессов, лучших практик и метрик для выстраивания эффективного управления и контроля, а также достижения максимальной выгоды от использования ИТ.

Основой стандарта являются 40 высокоуровневых целей контроля, сгруппированных в четыре домена, два из которых посвящены информационной и кибербезопасности):

– «COBIT 2019 Framework: IntroductionandMethodology» – «COBIT 2019 Бизнес-модель: Введение и методология».

– «COBIT 2019 Framework: Governance and Management Objectives» – «COBIT 2019 Бизнес-модель: Задачируководстваиуправления.

– «COBIT 2019 DESIGN GUIDE: Designing an Information and Technology Governance Solution – «Проектирование решения по руководству информацией и технологиями».

– «COBIT 2019 IMPLEMENTATION GUIDE: Implementing and Optimizing an Information and Technology Governance Solution» – «Внедрение и оптимизация решения по руководству информацией и технологиями».

Таким образом, стандарт охватывает всю деятельность компании и позволяет широко взглянуть на управление информационными технологиями и информационной и кибербезопасностью. Стандарт носит высокоуровневый характер, то есть говорит, что должно быть достигнуто, но не объясняет, как. С помощью принципов COBIT 2019 можно минимизировать риски и контролировать возврат инвестиций в информационные технологии и средства информационной защиты.

Руководство ITIL.

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

ITIL можно рассматривать в том числе с точки зрения информационной и кибербезопасности, так как для успешного использования ИТ и поддерживаемых услуг необходимо обеспечивать доступность, целостность и конфиденциальность ИТ-инфраструктуры. Это достигается правильным управлением ИТ-безопасностью. Библиотека содержит раздел, посвященный вопросам безопасности в структуре процессов ITIL. В материалах ITIL не прописаны конкретные требования к средствам защиты, а лишь дается описание общей организации безопасной работы ИТ-сервисов. В библиотеке можно найти как основные принципы выстраивания самого процесса управления ИБ, так и ключевые рекомендации по поддержанию СУИБ – Системы управления информационной безопасностью (Information Security Management System или ISMS). Если COBIT определяет ИТ-цели, то ITIL указывает шаги на уровне процессов. Кроме того, библиотека содержит рекомендации по выстраиванию смежных процессов, например, по управлению инцидентами, что позволяет комплексно взглянуть на выстраивание процессов и их интеграцию в ИТ-среду. Библиотека ITIL полезна специалистам, в задачи которых входит выстраивание процесса управления ИТ-услугами и интеграция ИБ в этот подход. Знание документа позволяет им разговаривать с ИТ-службой на одном языке – языке ИТ-сервисов.

Стандарты ISO.

Серия ISO/IEC 27XXX

Наиболее известным и популярным набором стандартов среди как зарубежных, так и российских КБ-специалистов, к которому обращаются в первую очередь при внедрении СУИБ, являются документы из серии КБ-стандартов ISO/IEC 27XXX.

Самый известный стандарт серии – ISO/IEC 27001:2013, был разработан для предоставления сообществу обобщенной модели создания, реализации, мониторинга, проверки, обслуживания и улучшения Системы управления информационной безопасностью (СУИБ). На разработку и внедрение СУИБ применительно к нуждам каждой конкретной организации влияют их конкретные цели, специфические требования безопасности, используемые ими технологические процессы, а также организационная структура организации. Понятно, что эти цели и требования к безопасности со временем изменяются. Надо отметить, что этот международный стандарт использует комплексный подход для создания, внедрения, эксплуатации, мониторинга, анализа, обслуживания и улучшения ISMS конкретной организации (предприятия). Системный подход к управлению информационной безопасностью, представленный в этом международном стандарте, исходит из соображений:

– понимания руководством компании необходимости соблюдения требований обеспечения информационной безопасности организации и необходимости определять свою конкретную политику и свои цели обеспечения информационной безопасности;

– управления всеми возможными средствами снижения рисков информационной безопасности организации, в том числе – применение процедур мониторинга и анализа производительности и эффективности СУИБ.

Этот международный стандарт использует классическую модель «Plan-Do-Check-Act» (PDCA/планирование-исполнение-проверка-принятие мер), которая обычно применяется для структурирования всех процессов управления СУИБ. На рис. 3 показано, как СУИБ решает задачу обеспечения информационной безопасности конкретного производственного объекта.

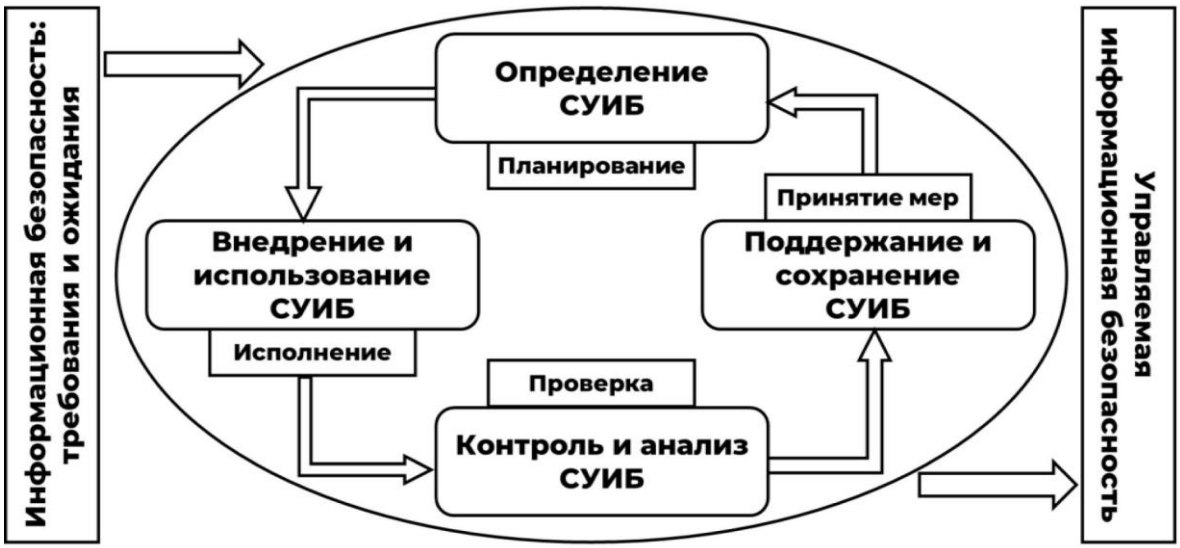


Рис. 3.

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

Также специалисты часто обращаются к стандарту ISO/IEC 27002:2013, который сегодня повсеместно заменяет предыдущий стандарт ISO/IEC 17799 и формулирует конкретные рекомендации по использованию современных методов и практик управления информационной безопасностью для тех специалистов и менеджеров, кто непосредственно отвечает на предприятии за запуск, внедрение или обслуживание СУИБ.

Информационная безопасность в этом стандарте определяется как сохранение конфиденциальности (обеспечение доступности информация только для тех, у кого есть доступ), целостности (защита точности и полноты информации и методов обработки) и доступности (обеспечение возможности того, чтобы авторизованные пользователи имели оперативный и защищенный доступ к любой необходимой им информации при необходимости). Этот стандарт содержит следующие двенадцать основных разделов.

1. Оценка риска.

2. Политика безопасности: основные направления управления политикой.

3. Управление информационной безопасностью.

4. Управление имущественными объектами: инвентаризация и классификация информационных активов.

5. Обеспечение безопасности человеческих ресурсов: конкретные аспекты обеспечения безопасности для абсолютно всех сотрудников, как вступающих (принимаемых на работу), перемещающихся внутри организации, так и покидающих организацию.

6. Физическая и экологическая безопасность: защита вычислительной техники.

7. Управление коммуникациями и операциями: управление средствами технической безопасности в системах и сетях.

8. Контроль доступа: ограничение прав доступа к сетям, системам, приложениям, функциям и данным.

9. Приобретение, разработка и сопровождение информационных систем: обеспечение безопасности приложений.

10. «Управление» инцидентами в сфере информационной безопасности: предвидение (прогнозирование) и адекватное реагирование на факты нарушения информационной безопасности.

11. Управление непрерывностью бизнеса: защита, поддержка и восстановление критически важных бизнес-процессов и систем.

12. Соответствие: здесь имеется в виду обеспечение полного соответствия методикам, стандартам, законам и нормам информационной безопасности каждого конкретного объекта (предприятия).

Внутри каждого раздела этого стандарта указаны конкретные принимаемые меры безопасности и их цели. Для каждого элемента системы управления безопасностью предоставляется руководство по внедрению.

Безусловно, это далеко не все международные стандарты в области информационной и кибербезопасности. В рамках рассмотрения данного учебного вопроса мы остановились лишь на некоторых, наиболее важных из них.

4. Противодействие преступлениям и правонарушениям в сфере компьютерной информации[1]

Анализ законодательства Российской Федерации позволяет сделать вывод о том, что ответственность за совершение правонарушений в сфере компьютерной информации в нашей стране установлена Уголовным кодексом Российской Федерации и, в значительно меньшей степени, Кодексом Российской Федерации об административных правонарушениях.

Перечень административных правонарушений в области компьютерной информации, ответственность за совершение которых установлена главой 13 «Административные правонарушения в области связи и информации» КоАП РФ, достаточно мал и включает в себя всего 3 состава:

– статья 13.12 «Нарушение правил защиты информации»;

– статья 13.12.1 «Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации»;

– статья 13.13 «Незаконная деятельность в области защиты информации».

Однако если рассматривать проблему с точки зрения уголовного права, то перечень компьютерных преступлений будет значительно более широким.

Компьютерная преступность – это совокупность преступлений, где компьютерная информация является предметом преступных посягательств.

Одновременно с пониманием большой ценности информации возникает им потребность в ее защите. Проблема защиты компьютерной информации сейчас является во всем мире одной из самых актуальных. Новые возможности, предоставляемые информационными технологиями, их широкая распространенность и доступность делают это направление крайне привлекательным для представителей криминальной среды. Быстрое развитие информационно-телекоммуникационных сетей, создание многочисленных информационных систем, разработка более совершенных технических устройств – все это создает условия, облегчающие совершение преступлений в этой сфере, вследствие чего с каждым годом растет количество подобных деяний и в России, и за рубежом.

Эксперты в области информации отмечают, что «информационное общество» не имеет экономических, политических и социальных границ. Если раньше информация или ее носители физически перемещались из одной географической точки в другую, то теперь при сборе доказательств, необходимым условием является использование возможностей компьютерных технологий, особенно по уголовным делам о так называемых компьютерных преступлениях. С 80-х годов прошлого века во многих странах пришли к выводу, что правовая защита компьютерных данных с помощью общих положений уголовного и иных отраслей права является недостаточной. Для борьбы с новыми видами правонарушений, которые связаны с использованием компьютерной техники, многие государства разработали новое законодательство об ответственности за компьютерные преступления.

---

[1] В основу данного учебного вопроса положены следующие материалы: *Лямцев А. Н.* Некоторые проблемы российского законодательства в сфере компьютерных преступлений // Вопросы современной науки и практики. Университет им. В. И. Вернадского. 2013. № 1 (45). С. 232–237.

Сейчас во всех телекоммуникационных системах доступа к спутниковым каналам, сотовых системах мобильной связи, системах передачи изображений и других используются цифровые технологии, что обеспечивает создание открытых сетей. Одной из таких сетей является Интернет, который включает в себя разветвленную систему серверов, поставляющих информацию, тем самым создавая мировое информационное пространство. Через открытые информационные сети иногда возможен доступ к национальным, в том числе специально защищаемым, информационным ресурсам различных государств. Именно эти сети, чаще всего, являются каналом, который используется для совершения различных противоправных деяний. В силу этого компьютерная преступность становится одним из наиболее опасных видов преступных посягательств.

В Российской Федерации с 1997 года уголовно-наказуемыми были признаны определенные деяния в сфере компьютерной информации. Нормы о данных преступлениях зафиксированы в четырех статьях УК РФ, которые выделены в самостоятельную главу 28 УК РФ, которая так и называется – «Преступления в сфере компьютерной информации». К ним относятся: статья 272 УК РФ «Неправомерный доступ к компьютерной информации», статья 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ», статья 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» и статья 274.1 УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

29 ноября 2012 г. был принят Федеральный закон №207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации», который впервые в российской законотворческой практике выделил различные виды мошенничеств в отдельные составы преступлений в зависимости от того, в какой сфере они совершены. Благодаря данному закону появились ст. 159.3 УК РФ «Мошенничество с использованием электронных средств платежа» и ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации». Безусловно, это не все составы преступлений, которые могут быть отнесены к преступлениям в сфере компьютерной информации. Здесь также можно упомянуть п. «г» ч. 3 ст. 158 УК РФ (речь идет о краже, совершенной с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3 УК РФ), п. «б» ч. 2 ст. 228.1 УК РФ (речь идет о сбыт наркотических средств, психотропных веществ или их аналогов, совершенном с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет») и другие.

Таким образом, по тем изменениям, которые законодатель вносит в УК РФ, можно проследить общую тенденцию к увеличению составов преступлений в сфере компьютерной информации и конкретизации наказаний за их совершение.

В настоящее время все меры противодействия компьютерным преступлениями можно подразделить на технические, организационные и правовые.

К правовым исследует отнести: совершенствование действующих норм уголовного законодательства, устанавливающих ответственность за преступления в сфере

компьютерной информации; разработку новых норм, устанавливающих ответственность за преступления в этой сфере; защиту авторских прав создателей программного обеспечения. К правовым мерам также можно отнести вопросы общественного контроля за разработчиками компьютерных систем и принятие соответствующих международных правил. Весьма важным представляется расширение правовой и законодательной информированности специалистов и должностных лиц, осуществляющих борьбу с компьютерными преступлениями. При этом при борьбе с компьютерными преступлениями необходимо обеспечивать свободу пользования информационно-коммуникационными средствами и свободу развития данных технологий. Помимо этого, необходимо гарантировать свободу выражения мнений. Следует увеличить количество специальных подразделений по борьбе с компьютерными преступлениями. В данные подразделения должны привлекаться люди, обладающие обширными познаниями в данной области. Множество молодых специалистов в технической и правовой сферах могли бы внести необходимый вклад в борьбу с компьютерной преступностью. В некоторых случаях такие люди не находят применения своим познаниям в рамках закона и преступают его. Поэтому привлечение подобных специалистов может стать одной из мер по борьбе с компьютерными преступлениями.

Что касается международных документов, связанных с компьютерной преступностью, то основополагающим международным нормативным актом в сфере компьютерных технологий является Конвенция об компьютерных преступлениях СЕД № 185, открытая к подписанию в Будапеште 23.11.2001 года. Данная Конвенция стала первым в истории международным договором о преступлениях, совершаемых через сеть Интернет и иные коммуникационные сети. Она устанавливает принципы уголовной ответственности за мошенничество с использованием электронно-вычислительных машин, нарушение авторского права, а также за нарушение безопасности компьютерных сетей. Приоритетная цель Конвенции состоит в определении общей политики в сфере уголовного права, направленной на защиту общества от компьютерных преступлений. На настоящий момент Конвенция ратифицирована 53 странами, из которых 30 стран из числа членов Совета Европы, а также США. Российская Федерация несколько раз рассматривала вопрос о подписании Конвенции, но отрицательное решение было принято из-за несогласия российских спецслужб предоставить иностранными правоохранительным органам возможность технического перехвата российского интернет-трафика.

К сожалению, российское законодательство в настоящее время не отвечает жестким мировым требованиям по борьбе с компьютерной преступностью. Необходимо устранение недочетов в законодательстве, наказания должны соответствовать совершенным деяниям. Недостаток судебной практики должен быть восполнен, основываясь на международном опыте. Многие страны, ратифицировавшие Конвенцию об компьютерных преступлениях СЕД № 185, гораздо успешнее ведут борьбу с компьютерными преступниками, так как имеют в своем распоряжении больше возможностей для этого. Ратификация Конвенции позволила бы повысить эффективность борьбы с компьютерной преступностью в России. Конечно, только этого будет недостаточно, но серьезный шаг к затруднению деятельности преступников будет сделан.

Вопросы и задания для самоконтроля

1. Назовите и охарактеризуйте основополагающие положения Конституции РФ в области информации.

2. Охарактеризуйте с точки зрения защиты информации Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Охарактеризуйте с точки зрения защиты информации Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

4. Охарактеризуйте с точки зрения защиты информации Федеральный закон от 21 июля 1993 г. № 5485-1 «О государственной тайне».

5. Охарактеризуйте с точки зрения защиты информации Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».

6. Охарактеризуйте с точки зрения защиты информации Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

7. Охарактеризуйте с точки зрения защиты информации Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

8. Дайте краткую характеристику государственной политики Российской Федерации в области международной информационной безопасности.

9. Сформулируйте основную цель создания международных стандартов в области кибербезопасности и защиты информации.

10. Приведите классификацию международных стандартов в области кибербезопасности и защиты информации с прикладной и процессной точек зрения.

11. Кратко охарактеризуйте стандарт ISO/IEC 27001:2013.

12. Приведите краткую характеристику принимаемых в Российской Федерации мер по противодействию преступлениям и правонарушениям в сфере компьютерной информации.

Лекция 3. Принципы обеспечения компьютерной безопасности

Число кибератак по всему миру возрастает в геометрической прогрессии. По прогнозу одной из крупнейших мировых аналитических компаний Juniper Research, только в 2023 году будет украдено более 33 миллиарда учетных записей пользователей. По итогам 2018 г. число скомпрометированных записей оценивается в 12 миллиардов; таким образом, увеличение с 2018 по 2023 г. составит 175 %. Отсюда следует вполне логичный вывод о том, что вопросам кибербезопасности следует уделять самое серьезное внимание.

Однако, несмотря на, казалось бы, совершенно очевидные вещи, в целом, владельцы бизнеса, равно как и государственные организации, редко задумываются о защите своих сетей от кибератак, пока не станут жертвой такой атаки. Между тем, по оценкам аналитиков, 95 % случаев утечки информации можно было предотвратить при помощи простых мер кибербезопасности и применения надежных решений, основанных на использовании сведений об угрозах.

1. Обеспечение кибербезопасности оконечных устройств (сетевые камеры видеонаблюдения, сетевые контроллеры, компьютеры, серверы, ноутбуки, смартфоны)[1]

Оконечные устройства – это наиболее уязвимые элементы корпоративных сетей. Удивительно, но этого часто не замечают даже профессионалы в сфере IT-безопасности. Учитывая рост числа утечек данных, в рамках данного учебного вопроса уделим внимание безопасности оконечных устройств, чтобы обсудить всеобъемлющую защиту информационных активов, как частного лица, так и государственной или коммерческой организации. При этом определим, что такое вообще оконечное устройство, а также рассмотрим способы совершения кибератак на средства хранения, обработки и передачи данных и простейшие, но от этого не менее эффективные способы защиты от вредоносного программного обеспечения.

Оконечные устройства – это все машины, соединенные через Интернет в сеть, которая является техническим центром вашей информационной системы. У обычного человека, не являющегося специалистом в области защиты информации и кибербезопасности, может возникнуть резонный на первый взгляд вопрос – о какой информационной системе идет речь, если у меня нет никакой сети? Между тем ответ на этот вопрос достаточно прост.

---

[1] В основу данного учебного вопроса положены следующие материалы: Вирусы-вымогатели (шифровальщики) Ransomware // Интернет-портал и аналитическое агентство TAdviser: [сайт]. 2022. 26 авг. URL: https://www.tadviser.ru/index.php/Статья:Вирусы-вымогатели_ (шифровальщики)_Ransomware; Компьютерный вирус // Интернет-портал и аналитическое агентство TAdviser: [сайт]. 2010. 29 апр. URL: https://www.tadviser.ru/index.php/Статья:Компьютерный_вирус; Отказ от обслуживания // Интернет-портал и аналитическое агентство TAdviser: [сайт]. 2022. 18 марта. URL: https://www.tadviser.ru/index.php/Статья:Distributed_Denial-of-Service,_DDoS_(отказ_от_обслуживания); Трояны // Интернет-портал и аналитическое агентство TAdviser: [сайт]. 2022. 20 авг. URL: https://www.tadviser.ru/index.php/Статья:Трояны; Фишинг // Интернет-портал и аналитическое агентство TAdviser: [сайт]. 2022. 14 апр. URL: https://www.tadviser.ru/index.php/Статья: Фишинг_(phishing).

Мы давно уже живем в окружении разного рода сетей и информационных систем, и у каждого из нас есть собственные сети, объединяющие все наши умные устройства воедино. У каждого из нас есть стационарный компьютер или ноутбук (а у кого-то есть и то и другое, да и не в единственном экземпляре), есть смартфоны, умные часы и фитнес-браслеты, электронные книги и планшетные компьютеры, умные телевизоры и умные колонки от Яндекса, Гугла или других производителей, есть IP-камеры и множество других устройств, которые имеют подключение к сети Интернет и общаются между собой в рамках единой домашней сети. Ну и, конечно, мы ежедневно работаем с ведомственными сетями, в состав которых входят все те же настольные компьютеры, ноутбуки, смартфоны, POS-терминалы, принтеры, сканеры и планшеты – то есть все, что мы сами или наши сотрудники используют для коммуникаций друг с другом и обмена данными. Все эти устройства и называются оконечными устройствами и, к сожалению, все они также могут быть уязвимыми перед киберугрозами.

Управление безопасностью оконечных устройств – это политика, которую каждый человек, являющийся их владельцем, создает для обеспечения определенного уровня безопасности для всех оконечных устройств в его сети. В равной степени это относится и к организациям, разве что там эта политика определяется руководителем. Это часть комплексной программы безопасности, и это требование времени и для отдельного человека, и для малого бизнеса и огромных международных корпораций. И здесь необходимо понимать, что это не своеобразный страховой полис, который позволит вам компенсировать потери от киберугроз, а, скорее, хорошо оснащенная система сигнализации, которая должна остановить хакеров, которые охотятся за вашими ценными данными.

В наши дни оконечные устройства – это самое слабое звено в сети каждого человека и каждой организации и предприятия. Чтобы разобраться, почему это так, давайте разберемся с причинами утечек данных. Некоторые компании, даже можно утверждать, что их подавляющее большинство устанавливают на компьютеры в своих офисах антивирусы и какие-либо защитные решения. Но что насчет мобильных устройств? А здесь как раз в большинстве случаев наличествует явный пробел в системах защиты, хотя давно известно, что в первую очередь следует опасаться не потенциального разведчика, сидящего под кустом и в подзорную трубу наблюдающего за вашими окнами, в надежде понять, что там происходит и какие секреты вы скрываете. В первую очередь необходимо опасаться халатности и злонамеренных действий ваших собственных сотрудников, а они получают доступ в сеть как раз с оконечных устройств, в том числе – мобильных.

Вы можете спросить, а как же насчёт хакеров и фишинговых атак и так далее? Но на самом деле реальность такова, что программисты, которые стремятся эксплуатировать слабые места в системах, выбирают самую легкую уязвимость с самой высокой вероятностью успешной эксплуатации. В настоящее время, особенно в условиях пандемии, все больше компаний работают удаленно, и это означает, что используется все больше оконечных устройств, и возрастает вероятность, что на каком-то этапе что-то пойдет не так, и в первую очередь это, опять же, касается мобильных устройств, хотя, конечно, и все другие виды оконечных устройств тоже могут быть подвержены уязвимостям, и они совершенно не являются безопасными.

Эффективная защита представляет собой достаточно большую сложность. Программы киберзащиты становятся все сложнее и сложнее, поскольку все больше оконечных устройств становится частью корпоративных сетей. Их мобильность или легкость коммуникации повышают эффективность работы, но в то же время такие устройства могут вызывать сложности при обеспечении защиты.

Для эффективной защиты оконечных устройств частные лица, руководители государственных организаций и владельцы бизнеса должны создать политику, которая покрывает сеть, не имеющую географических границ. И здесь есть много проблем. Может оказаться экономически нерационально иметь собственный сервер с центральным управлением, который будет проверять сотрудников и подрядчиков перед тем, как предоставить им доступ к данным в вашей сети. Сотрудники, работающие на удаленных системах, могут не всегда обновлять ПО, могут не всегда аккуратно обращаться с подозрительными электронными письмами и загружаемыми файлами. Поэтому неудивительно, что существует расширяющийся список лучших практик, касающихся систем управления безопасностью оконечных решений. Важный первый шаг – это установить требование, чтобы все устройства использовали одобренную операционную систему и VPN-соединение. Если устройство нарушает эту политику, существуют способы ограничить доступ к важным данным. Собственно, именно таким образом реализован доступ сотрудников к ведомственной единой системе информационно-аналитического обеспечения деятельности МВД РФ, которую чаще называют сокращенно – ИСОД МВД России. Здесь для того, чтобы получить доступ к системе на оконечном устройстве (для примера рассмотрим стационарный компьютер или ноутбук) должна быть установлена одна из разрешенных операционных систем, обязательно наличие установленного и настроенного специального программного обеспечения КриптоПРО и VIPNet, обязательно использование только разрешенного антивирусного программного обеспечения и еще целый ряд требований должен быть выполнен.

Но мы, естественно, не будем ограничиваться исключительно системой МВД России, а поговорим о вопросах обеспечения безопасности оконечных устройств в целом, и в первую очередь рассмотрим основные способы совершения кибератак на средства хранения, обработки и передачи данных.

Итак, кибератаки могут воздействовать на информационное пространство компьютера, в котором находятся сведения, хранятся материалы физического или виртуального устройства. Атака, обычно, поражает носитель данных, специально предназначенный для их хранения, обработки и передачи личной информации пользователя.

По способу распространения кибератаки можно поделить на массовые и целенаправленные.

Массовые кибератаки направлены на глобальное распространение вредоносных программ, способных нарушить работоспособность компьютера, удалить важные файлы или повредить их. Примерами подобных программ являются: программа-шутка (вызывает отображение изображений и окон на мониторе), руткиты (устанавливают и выполняют в системе код без согласия или оповещения пользователя), вирусы («троянский конь», сетевые и т. д.), прочие.

Таргетированные (или целенаправленные) атаки – их особенность заключается в том, что злоумышленников интересует конкретная компания или государственная организация. Это отличает данную угрозу от массовых хакерских атак, когда одновременно атакуется большое число целей, и наименее защищенные пользователи становятся жертвой. Целенаправленные атаки обычно хорошо спланированы и включают несколько этапов – от разведки и внедрения до уничтожения следов присутствия. Как правило, в результате целенаправленной атаки злоумышленники закрепляются в инфраструктуре жертвы и остаются незамеченными в течение месяцев или даже лет – на протяжении всего этого времени они имеют доступ ко всей корпоративной информации.

На рис. 4 отображена типовая схема таргетированной кибератаки.

Рис. 4.

Давайте рассмотрим основные инструменты кибератак.

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

Хакеры использовали электронные письма для осуществления подобного рода атак, но благодаря широкому распространению социальных сетей и смартфонов с доступом в Интернет стали множится и типы фишинговых атак.

Данные электронные письма содержат ссылку, которая якобы ведет пользователя на сайт какой-то компании с высоким уровнем конфиденциальности, хотя, на самом деле, такой сайт – это всего лишь имитация оригинального сайта без какой-либо конфиденциальности. Таким образом, самоуверенный пользователь, у которого нет надежной антивирусной защиты, может стать жертвой атаки, предназначенной для кражи персональных данных.

Фишинг – одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности: в частности, многие не знают

простого факта: сервисы не рассылают писем с просьбами сообщить свои учётные данные, пароль и прочее.

Для защиты от фишинга производители основных интернет-браузеров договорились о применении одинаковых способов информирования пользователей о том, что они открыли подозрительный сайт, который может принадлежать мошенникам. Новые версии браузеров уже обладают такой возможностью, которая соответственно именуется «антифишинг».

Большинство киберпреступников полагается не только на технологию, но и на человеческую беспечность и доверчивость. Еще в 2011 году в отчете компании Cisco были перечислены семь человеческих слабостей, эксплуатируемых преступниками, которые используют психологические методы воздействия на людей через электронную почту, социальные сети и телефонную связь. Речь идет о сексуальности, алчности, тщеславии, чрезмерной доверчивости, лени, сострадании и поспешности в принимаемых решениях.

Коротко обозначим, как выглядит типичное фишинговое письмо:

Отправители:

– органы исполнительной власти;
– крупные телекоммуникационные операторы;
– профильные интернет-форумы;
– кредитно-финансовые организации;
– организации-партнеры;
– организации-клиенты.

Содержание:

– требование, поступившее от органов исполнительной власти;
– рассылка изменений в нормативных актах;
– взыскание/погашение задолженности/штрафа, оплата услуг;
– поиск документов для проверки.

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

Большинство троянских программ предназначено для сбора конфиденциальной информации. Их задача, чаще всего, состоит в выполнении действий, позволяющих получить доступ к данным, которые не подлежат широкой огласке. К таким данным относятся пользовательские пароли, регистрационные номера программ, сведения о банковских счетах и т. д. Остальные троянцы создаются для причинения прямого ущерба компьютерной системе, приводя ее в неработоспособное состояние.

Все «троянские кони» имеют две части: клиент и сервер. Клиент осуществляет управление серверной частью программы по протоколу TCP/IP. Клиент может иметь графический интерфейс и содержать в себе набор команд для удалённого администрирования.

Серверная часть программы – устанавливается на компьютере жертвы и не содержит графического интерфейса. Серверная часть предназначена для обработки (выполнения) команд от клиентской части и передаче запрашиваемых данных злоумышленнику.

3. DDoS-атаки. DistributedDenial-of-Service, или по-русски – отказ от обслуживания. Поток ложных запросов, который пытается блокировать выбранный ресурс либо путем атаки на канал связи, который «забивается» огромной массой бесполезных данных, либо атакой непосредственно на сервер, обслуживающий данный ресурс. Такие действия используются в целях конкурентной борьбы, прямого шантажа компаний, а также для отвлечения внимания системных администраторов от иных противоправных действий.

Атаки DoS и DDoS часто встречаются в мире интернет-безопасности. Во-первых, они не направлены на уязвимости, которые могут быть исправлены; во-вторых, каждый отдельный пакет является вполне легитимным – лишь их совокупность приводит к разрушительным последствиям, и, в-третьих, такие атаки носят продолжительный характер – они длятся несколько часов или дней, вместо нескольких секунд или минут.

4. Ботнет – это компьютерная сеть, состоящая из некоторого количества хостов, с запущенным автономным программным обеспечением. Ботом в составе такой сети является сам компьютер с вредоносным ПО, дающим возможность злоумышленнику выполнять некие действия с использованием ресурсов заражённого ПК. Ботнеты используются для атак на сервера, подбора паролей на удаленной машине или рассылки спама.

5. Backdoor – бэкдор, (от англ. backdoor, чёрный ход) – программа или набор программ, которые устанавливает взломщик (хакер) на взломанном им компьютере после получения первоначального доступа с целью повторного получения доступа к системе. При подключении предоставляет какой-либо доступ к системе (как правило, это командный интерпретатор: в GNU/Linux – Bash, в Microsoft Windows– cmd).

Существует два вида предоставления shell-доступа: «BindShell» и «Back Connect»:

– «BindShell» – самый распространённый, работает по архитектуре «клиент-сервер», то есть бэкдор ожидает соединение.

– «Back Connect» – применяется для обхода брандмауэров, бэкдор сам пытается соединиться с компьютером хакера.

Известные бэкдоры заносятся в базы антивирусных систем. Хакеры высокого класса используют собственноручно написанные либо модифицированные бэкдоры и руткиты, что делает их обнаружение и удаление затруднительным.

6. Классические файловые вирусы – разновидность компьютерной программы, способной создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения.

Определение компьютерного вируса – исторически проблемный вопрос, поскольку достаточно сложно дать четкое определение вируса, очертив при этом свойства, присущие только вирусам и не касающиеся других программных систем. На-

оборот, давая жесткое определение вируса как программы, обладающей определенными свойствами, практически сразу же можно найти пример вируса, таковыми свойствами не обладающего. Поэтому сегодня под вирусом чаще всего понимается не «традиционный» вирус, а практически любая вредоносная программа, хотя это абсолютно неверный подход.

В настоящее время не существует единой системы классификации и именования вирусов, и в различных источниках можно встретить разные классификации. Приведем некоторые из них:

Классификация вирусов по степени воздействия

– Безвредные. Вирусы, никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);

– Неопасные. Вирусы, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах;

– Опасные. Вирусы, которые могут привести к различным нарушениям в работе компьютера;

– Очень опасные. Их действие может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

Классификация вирусов по способу маскировки (при создании копий для маскировки могут применяться следующие технологии):

– Шифрование – вирус состоит из двух функциональных кусков: собственно вирус и шифратор. Каждая копия вируса состоит из шифратора, случайного ключа и собственно вируса, зашифрованного этим ключом.

– Метаморфизм – создание различных копий вируса путем замены блоков команд на эквивалентные, перестановки местами кусков кода, вставки между значащими кусками кода «мусорных» команд, которые ничего не делают.

Шифрованный вирус – это вирус, использующий простое шифрование со случайным ключом и неизменный шифратор. Такие вирусы легко обнаруживаются по сигнатуре шифратора.

Вирус-шифровальщик. Попав на компьютер-«жертву», вирусы-шифровальщики шифруют информацию наиболее распространённых форматов – офисные, медиафайлы, архивы, то есть то, что представляет собой наиболее чувствительные для пользователя данные – это либо «работа», либо «жизнь». Как они попадают в компьютер? Существует несколько основных способов.

Почта. При отсутствии эффективного спам-фильтра в вашу почту будет сыпаться огромное количество спама. Да, большая часть таких писем будет просто неуместной и навязчивой рекламой, но некоторые могут оказаться весьма «интересными». Сообщения о сборах на лечение больных детей, к которым приложены «подтверждающие медицинские документы», уведомления из налоговой инспекции и Ростелекома с требованиями оплатить налог, прочитать приложенную повестку в суд или срочно оплатить приложенный счет за услуги связи – самые частые уловки злоумышленников. Что интересно, зачастую в поле «От» у этих писем стоят реальные адреса налоговой инспекции или действующих сотрудников Ростелекома – это означает, что рассылка ведется со взломанных аккаунтов без ведома их владельцев. Изначальный «кредит доверия» этим компаниям вкупе с низкой осведомленностью

подавляющего большинства офисных сотрудников о киберугрозах делает такие атаки весьма эффективными. Ну а приложенные к таким письмам «документы» оказываются троянами, которых пользователь запускает при открытии архивов.

Вложения вредоносных писем чаще всего бывают в архивах .zip, .rar, .7z. И если в настройках системы компьютера отключена функция отображения расширения файлов, то пользователь (получатель письма) увидит лишь файлы вида «Документ.doc», «Акт.xls» и тому подобные. Другими словами, файлы будут казаться совершенно безобидными. Но если включить отображение расширения файлов, то сразу станет видно, что это не документы, а исполняемые программы или скрипты, имена файлов приобретут иной вид, например, «Документ.doc.exe» или «Акт.xls.js». При открытии таких файлов происходит не открытие документа, а запуск вируса-шифровальщика. Вот лишь краткий список самых популярных «опасных» расширений файлов: .exe, .com, .js, .wbs, .hta, .bat, .cmd.

Вредоносные сайты. Тут есть два варианта. В первом случае пользователь, скачивая приложения или другие файлы с фишинговых, взломанных или просто никем не контролируемых ресурсов (файлообменники, торренты и т. д.), сам запускает их, даже не подозревая, что вместе с полезным материалом получил вредоносный «довесок». Второй вариант развития событий еще хуже: достаточно бывает просто зайти на зараженный сайт, чтобы запустившийся скрипт загрузил на ПК троянца и активизировал его. К счастью, это возможно только при совершенно «небезопасных» настройках браузера и операционной системы. К несчастью, именно такие настройки и имеет большинство пользователей...

Сменные носители информации. Это основной путь заражения компьютеров, либо вообще не имеющих сетевых подключений, либо являющихся частью небольших локальных сетей без выхода в Интернет. Если сменный носитель, будь то флешка или съемный жесткий диск, заражен, а на компьютере не отключена функция автозапуска и нет антивирусной программы, то велик риск, что для активации троянца будет достаточно просто вставить устройство в USB-разъем.

Эти три пути являются основными и составляют 90 % «собственноручных» заражений. Остальные 10 % приходятся на «вирусные эпидемии», а также различные диверсии и саботаж, удаленную установку и запуск троянцев. При открытии вложения происходит моментальный запуск вируса-шифровальщика, который незаметно зашифрует все документы. Пользователь обнаружит заражение, увидев, что все файлы станут отображаться иконками неизвестного типа. За расшифровку преступником будут затребованы деньги. Но, зачастую, даже заплатив злоумышленнику, шансы восстановить данные ничтожно малы.

Теперь давайте коротко поговорим о том, как, собственно, можно от всего этого безобразия защититься.

Лучший способ не допустить заражения оборудования – это придерживаться нескольких простых правил:

– необходимо проверять внешние носители информации, прежде чем начать им пользоваться;

– создавать и использовать надежные пароли;

– регулярно сканировать оборудование на наличие вредоносных программ с помощью антивирусов;

– не устанавливать программы от неизвестного поставщика или скачанные с подозрительных сайтов;

– регулярно осуществлять резервное копирование важных данных.

Один из самых надежных способов обезопасить свою систему от кибератак, это использование виртуализации.

Виртуализация – эта практика использования виртуальных вычислительных сред с собственными операционными системами, абстрагированных от аппаратного обеспечения устройств. Виртуализация позволяет запускать на одном устройстве несколько виртуальных машин с собственной ОС у каждой виртуальной машины. Эксперты по безопасности давно интересуются виртуализацией как способом защитить устройства от угроз, особенно в условиях, когда все больше сотрудников используют свои личные устройства для работы. С виртуализацией пользователь может запустить на одном устройстве одну виртуальную машину для рабочих приложений и еще одну виртуальную машину для личных и развлекательных приложений.

Основное преимущество виртуализации для безопасности – это то, что каждая виртуальная машина изолирована от других ВМ. Вредоносное ПО не может распространяться от одной виртуальной машины к другой. Эта изоляция рабочих задач помогает защитить важную рабочую информацию, позволяя при этом сотрудникам использовать устройства как для профессиональных, так и для личных целей.

Однако есть и минусы у такого рода решений. И самый главный из них, это вычислительные ресурсы. Дело в том, что виртуальные машины представляют собой, по сути, виртуальный аналог настоящего компьютера, для работы которого необходим центральный процессор, оперативная память, видеокарта, носитель информации и т. д. И все эти ресурсы виртуальная система получает из системы реальной. То есть виртуальная система по определения не может быть мощнее, чем реальное железо, на котором она запущена, и более того, большинство производителей программ виртуализации позволяют создавать далеко не самые мощные по нынешним временам виртуальные машины.

Своеобразной разновидностью виртуализации является использование так называемых «песочниц» как средств проактивной защиты от киберугроз. Песочница – это специально выделенная (изолированная) среда для безопасного исполнения компьютерных программ. Обычно представляет собой жёстко контролируемый набор ресурсов для исполнения гостевой программы – например, место на диске или в памяти. Доступ к сети, возможность сообщаться с главной операционной системой или считывать информацию с устройств ввода обычно либо частично эмулируют, либо сильно ограничивают.

Повышенная безопасность исполнения кода в песочнице зачастую связана с большой нагрузкой на систему – именно поэтому некоторые виды песочниц используют только для неотлаженного или подозрительного кода.

Как правило, песочницы используют для запуска непроверенного кода из неизвестных источников, как средство проактивной защиты от вредоносного кода, а также для обнаружения и анализа вредоносных программ.

Применение песочниц связано с тем, что в связи с большим распространением вредоносных программ, а также применением вирусописателями специальных технологий (например, полиморфизм), классические сигнатурные сканеры уже не мо-

гут эффективно противостоять новым угрозам. Поэтому многие разработчики антивирусного программного обеспечения используют в своих продуктах песочницу как средство проактивной защиты пользователей от ещё неизвестных угроз.

Перейдем к более подробному рассмотрению антивирусов. Существует достаточно большое количество программ, предупреждающих и обезвреживающих кибератаки, которые имеют общее родовое название антивирусы. Каждая из этих программ выполняет свои собственные функции. Различают такие антивирусные программы, как:

– программы-детекторы (анализируют систему, сравнивая цифровые отпечатки программ с собственной базой);

– программы-доктора (не только ищут, но и удаляют вредоносную программу, не повредив при этом зараженные файлы);

– программы-ревизоры (сравнивают исходные состояния программ, файлов и т. д. с текущим их состоянием);

– программы-фильтры (обнаруживают подозрительные действия, характерные для вирусов);

– программы-вакцины (изменяют программу или систему так, что вредоносная программа воспринимает оборудование уже зараженным и не внедряется в него).

Все это хорошо работает для массовых атак. Но выявить таргетированные атаки гораздо сложнее. Для этого необходимы особые методы. Основными методами обнаружения подобных атак являются: сигнатурный анализ, эвристический анализ, файрволлы (брандмауэры), белый список.

Сигнатурный анализ.

Осуществление сигнатурного анализа предполагает, что аналитики имеют файл, зараженный вирусом. Изучив данную вредоносную программу, можно снять с нее сигнатуру (цифровой отпечаток). После занесения отпечатка в базу можно проверять файл на наличие этого вируса в оборудовании, сравнивая сигнатуры. Сигнатурный анализ обладает рядом преимуществ:

– используется не только для поиска вирусов, но и для фильтрации системного трафика;

– позволяет достаточно точно проводить испытания противостояния атакам.

Минусом сигнатурного анализа является потребность в постоянном обновлении сигнатурной базы.

Эвристический анализ

Роль эвристического анализа заключается в проверке кода на наличие свойств, характерных для вирусов. То есть данный метод заключается в проверке программ на наличие соответствий с поведением известных вирусов. Для этого антивирусная программа должна полностью контролировать работу, выполняемую программой. Этот способ хорош тем, что не зависит от актуальности баз. Минусом данного вида анализа является наличие ложных реагирований на безопасные файлы.

Файрволлы.

Метод выявления целенаправленных атак предполагает использование файрволлов (брандмауэров), позволяющих фильтровать трафик. Они действуют согласно определенным правилам, построенным по принципу «условие – действие». Трафик

пройдет проверку, если к нему найдется соответствующее правило. Недостатком данного метода является большое число лжесрабатываний.

Белый список.

Данный метод защиты используется для запуска приложений. Суть заключается в том, что станция может запустить только определенные приложения, находящиеся в этом списке. Помимо защиты от кибератак, он запрещает установку нежелательных программ, которые могут мешать или отвлекать от рабочего процесса. Минус заключается в том, что «белый список» должен включать все приложения, которые нужны пользователю. Такой способ является достаточно надежным, но неудобным, так как замедляет рабочие процессы оборудования.

Следует заметить, что данные виды анализа применяются и для обнаружения массовых атак, и многие из них, например сигнатурный анализ и брандмауэры, входят в пакет современных антивирусных программ.

2. Система обнаружения вторжений на объекты критической информационной инфраструктуры[1]

Глобальный рынок продуктов информационной безопасности развивается под воздействием быстро растущего многообразия сложных и комплексных угроз, что приводит к непосредственному влиянию на деятельность органов государственной власти и на бизнес, в результате чего данные продукты становятся востребованными не только для крупных и средних, но и для малых организаций. В настоящее время ситуация обстоит таким образом, что традиционные средства защиты, такие как межсетевой экран и антивирус, не способны обеспечить надлежащий уровень защиты внутренней сети организации, поскольку вредоносное программное обеспечение может «замаскироваться» и отправлять пакеты, которые с точки зрения межсетевого экрана выглядят полностью легитимными. Существует множество коммерческих решений, способных обеспечить надлежащий уровень защиты внутренней сети организации, однако в рамках рассмотрения данного учебного вопроса остановимся на таком классе решений, как системы обнаружения вторжений и системы предотвращения вторжений. Ванглоязычнойлитературеониназываются Intrusion Detection Systems (IDS) и Intrusion Prevention Systems (IPS). Различия между ними заключаются лишь в том, что одна может автоматически блокировать атаки, а другая просто предупреждает об этом.

Система обнаружения вторжений – это устройство или программный продукт, обеспечивающий наблюдение за сетевой и системной активностью и обнаружение вредоносных действий и нарушений политики безопасности. Примерами нарушения политики безопасности могут быть: атаки на сетевые сервисы, атаки, направленные на повышение привилегий, неавторизованный доступ к файлам и т. п. СОВ делятся на несколько типов и подходят к решению задачи обнаружения вредоносного трафика по-разному. Более подробно о системах обнаружения вторжений остановимся в рамках изучения шестой темы курса. Пока же ограничимся самыми общими сведениями о подобных системах. Существует два основных типа СОВ – сетевые и уз-

[1] В основу данного учебного вопроса положены следующие материалы: *Шарыпин Е. М.* Системы обнаружения вторжений // Образовательный интернет-портал StudyLib: [сайт]. URL: https://studylib.ru/doc/4374337/sharypin-e.m.-sistemy-obnaruzheniya-vtorzhenij.

ловые. Некоторые СОВ могут попытаться пресечь попытку несанкционированного доступа, но это не является ни необходимой ни основной задачей системы обнаружения. Основными задачами систем обнаружения и предотвращения вторжений (СОПВ) является обнаружение возможных инцидентов, хранение информации о них и составление отчетов о попытках взлома. Кроме того, предприятия и организации используют СОПВ и в других целях, например аудит систем безопасности, документирование возможных уязвимостей, а также в качестве «пугала», предотвращающего нарушения политики безопасности пользователями внутри системы.

Как правило, СОПВ записывают информацию, непосредственно относящуюся к наблюдаемым событиям, уведомляют администратора сети в случае потенциального вторжения и составляют отчеты о событиях. Многие СОПВ также могут противостоять обнаруженным угрозам, пытаясь предотвратить успех атаки. Например, СОПВ может сама остановить атаку, изменить настройки брандмауэра или изменить содержание атаки.

Обычно архитектура СОВ включает:

– сенсорную подсистему, предназначенную для сбора событий, связанных с безопасностью защищаемой системы;

– подсистему анализа, предназначенную для выявления атак и подозрительных действий на основе данных сенсоров;

– хранилище, обеспечивающее накопление первичных событий и результатов анализа;

– консоль управления, позволяющая конфигурировать СОВ, наблюдать за состоянием защищаемой системы и СОВ, просматривать выявленные подсистемой анализа инциденты.

Системы обнаружения вторжений можно разделить на несколько видов:

– сетевые СОВ, обычно представляют собой устройство, устанавливаемое в сети;

– узловые СОВ, обычно представляют собой программу-агент, устанавливаемую на устройства в сети;

– протокол-ориентированные СОВ: системы, анализирующие данные, передаваемые определенными протоколами;

– гибридные СОВ, совмещающие два и более подхода.

Кроме того, системы обнаружения вторжений можно разделить по характеру ответной реакции:

– пассивные или системы обнаружения, в которых после обнаружения и опознания подозрительного трафика СОВ только уведомляет пользователя или администратора;

– активные или системы предотвращения, противостоящие вторжениям, путем сброса соединения либо перепрограммирования правил брандмауэра с целью блокировки подозрительного траффика;

– гибридные, осуществляющие и обнаружение, и противостояние вторжениям в автоматическом режиме.

Системы обнаружения вторжений также можно классифицировать по методикам анализа:

– эвристические (статистические) СОВ;

– сигнатурные СОВ;

– гибридные СОВ.

Рассмотрим обозначенные нами типы систем обнаружения вторжений немного более подробно. Начнем с сетевых и узловых СОВ.

Сетевые системы обнаружения вторжений.

ССОВ обычно устанавливаются в стратегически важных точках внутри сети и как правило представляют из себя устройства, подключаемые к сети организации. Они анализируют весь проходящий траффик во всей подсети, работая в неразборчивом режиме, а затем сравнивают проходящий траффик с базой уже известных атак. Когда атака обнаружена и опознана, уведомление об этом отсылается администратору. Примером конфигурации ССОВ является, например установка ее в одной подсети с брандмауэрами в целях обнаружения попыток их обхода. В идеальном случае ССОВ сканирует весь входящий и исходящий траффик, но на практике это может привести к созданию «узкого места», тем самым снижается производительность сети в целом.

Узловые системы обнаружения вторжений.

Узловые системы обнаружения вторжений (УСОВ) работают на отдельных устройствах и рабочих станциях сети. УСОВ анализирует траффик только одного устройства, и предупреждает администратора или пользователя в случае тревоги. Кроме того, УСОВ при установке, как правило, создает резервную копию системных файлов и периодически сравнивает ее с текущим состоянием этих файлов. В случае их изменения или отсутствия, она немедленно уведомляет администратора для последующего расследования ситуации. Часто такая система устанавливается на критически важных узлах, на которых не предусмотрено изменение системных установок.

Кроме того, УСОВ могут использовать системно-зависимые средства и так называемые ханипоты (honeypots), то есть специально сконфигурированные системы, с минимальной защитой, призванные приманивать злоумышленников.

Рассмотрим основные методы анализа, используемые СОВ. Двумя основными подходами к анализу сетевой активности, на сегодняшний день являются эвристический (еще его иногда называют статистическим) и сигнатурный. Современные системы обнаружения вторжений используют как правило комбинацию этих методов.

Эвристические СОВ.

Системы обнаружения вторжений, использующие эвристический подход после установки «обучаются» администратором, который задает политику СОВ, соответствующую нормальной активности в сети – типы траффика, соединения между узлами, используемые протоколы и порты. При обнаружении аномалий в работе сети или статистически значимых отличий траффика от типичного в данной сети, СОВ оповещает об этом администратора. Основной проблемой такого подхода является сложность в настройке и большое количество ложноположительных тревог в случае некорректно заданных правил.

Сигнатурные СОВ.

Сигнатурные системы обнаружения вторжений анализируют проходящий траффик в сети и сравнивают пакеты с базой данных сигнатур (известных атрибутов атак). Такой подход схож с тем, как работает большинство антивирусного ПО. При

таком подходе основной проблемой является устаревание баз сигнатур – между появлениями новых типов атак и обновлением баз сигнатур может пройти достаточное количество времени, в течение которого СОВ будет не способна обнаружить такую угрозу.

Мы рассмотрели основные виды систем обнаружения и предотвращения вторжений. На первый взгляд может показаться, что это идеальная система, которая гарантированно сможет защитить вас и ваши оконечные устройства от киберугроз. Однако, на самом деле все далеко не так радужно. Системы обнаружения и предотвращения вторжений имеют ряд серьезных проблем, затрудняющих их использование. Коротко обозначим недостатки и проблемы СОВ:

– Информационный шум может серьезно повлиять на эффективность работы СОВ. Пакеты, ошибочно сгенерированные недочетами в разработке ПО, поврежденные данные службы доменных имен могут создать довольно высокий коэффициент ложных тревог.

– Довольно часто случается так, что количество настоящих атак гораздо меньше количества ложных тревог. Иногда разница настолько велика, что настоящая атака может быть проигнорирована или вообще не замечена.

– Как отмечалось раньше, серьезной проблемой является устаревание библиотек сигнатур, что может серьезно сказаться на эффективности обнаружения и предотвращения атак.

– Система обнаружения вторжений не может компенсировать недочеты в проектировании инфраструктуры безопасности, уязвимости протоколов как таковых или слабые методы аутентификации. Если атакующий получает доступ, используя уязвимости слабого метода аутентификации, то СОВ не сможет предотвратить ущерб.

– Зашифрованные пакеты не обрабатываются системами обнаружения вторжений. Таким образом, атака с использованием зашифрованных пакетов может привести к успешному вторжению, не обнаруженному СОВ, пока злоумышленник не начнет предпринимать действия внутри сети, обнаруживаемые системой.

– Системы обнаружения вторжений предоставляют информацию об атаках, используя сетевой адрес, содержащийся в IP-пакетах, проходящих в сети. Это эффективно только если сетевой адрес в пакете настоящий, так как адрес в пакете может быть искажен или сфальсифицирован.

Таким образом, из материала двух рассмотренных нами вопросов можно сделать важный вывод: ни один из известных на сегодняшний день методов защиты от киберугроз не способен самостоятельно обеспечить полноценную защиту. Любые заверения производителей о том, что их система является лучшей из представленных на рынке и способна защитить вас от любых видов киберугроз, на самом деле, являются не более, чем маркетинговым ходом. Для полноценной же защиты необходимо использование комплексных решений, состоящих из нескольких аппаратных и программных средств, дополняющих и усиливающих друг друга. При этом необходимо понимать, что идеал в принципе недостижим, и можно лишь максимально затруднить злоумышленнику возможность получения доступа к охраняемым данным.

3. Управление рисками[1]

В рамках изучения второй темы курса были рассматрены нормативные документы в области защиты информации и кибербезопасности в Российской Федерации. Если внимательно изучить эти документы, то можно увидеть, что ряд из них содержит в себе ссылки на методологии оценки и управления рисками информационной безопасности. В целом необходимо отметить, что управление информационной безопасностью является дочерним процессом более широкого процесса управления рисками: если компания после анализа и оценки всех своих бизнес-рисков делает вывод об актуальности рисков ИБ, то в игру вступает уже непосредственно защита информации как способ минимизации некоторых рисков. Управление рисками позволяет эффективно и рационально выстраивать процессы ИБ и распределять ресурсы для защиты активов компании, а оценка рисков позволяет применять целесообразные меры по их минимизации: для защиты от существенных и актуальных угроз логично будет применять более дорогостоящие решения, чем для противодействия незначительным или труднореализуемым угрозам.

Кроме этого, выстроенный процесс управления рисками ИБ позволит разработать и в случае необходимости применить чёткие планы обеспечения непрерывности деятельности и восстановления работоспособности организации: глубокая проработка различных рисков поможет заранее учесть, например, внезапно возникшую потребность в удаленном доступе для большого количества сотрудников, как это может произойти в случае эпидемий или коллапса транспортной системы. В рамках рассмотрения данного учебного вопроса познакомимся с основами управления рисками информационной безопасности. Сразу отметим, что сама по себе эта тема очень объемна, и в полной мере рассмотреть ее в рамках одного учебного вопроса не представляется возможным, поэтому ограничимся лишь рассмотрением общей концепции управления рисками информационной безопасности.

Под риском информационной безопасности, или киберриском, понимают потенциальную возможность использования уязвимостей активов конкретной угрозой для причинения ущерба организации. Под величиной риска условно понимают произведение вероятности негативного события и размера ущерба. В свою очередь под вероятностью события понимается произведение вероятности угрозы и опасности уязвимости, выраженные в качественной или количественной форме. Условно можно выразить это логической формулой:

ВеличинаРиска=ВероятностьСобытия*РазмерУщерба, где
ВероятностьСобытия=ВероятностьУгрозы*ВеличинаУязвимости

Существуют также условные 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

[1] В основу данного учебного вопроса положены следующие материалы: *Рахметов Р. Г.* Анализ международных документов по управлению рисками информационной безопасности. Часть 1 // Интернет-портал Habr: [сайт]. 2020. 2 апр. URL: https://habr.com/ru/post/495236/.

активы, репутация, бизнес-процессы); по продолжительности влияния (операционные, тактические, стратегические).

Если говорить о целях анализа рисков ИБ, то всего их принято выделять четыре:

– Идентификация активов и оценка их ценность.

– Идентификация угроз активам и уязвимостей в системе защиты.

– Просчитывание вероятностей реализации угроз и их влияния на бизнес.

– Соблюдение баланса между стоимостью возможных негативных последствий и стоимостью мер защиты, предоставление рекомендаций руководству компании по обработке выявленных рисков.

Этапы с 1-го по 3-й являются оценкой риска и представляют собой сбор имеющейся информации. Этап 4 представляет из себя уже непосредственно анализ рисков, т. е. изучение собранных данных и выдачу результатов (указаний) для дальнейших действий. При этом важно понимать собственный уровень уверенности в корректности проведенной оценки. На этапе 4 также 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 компании уровень рисков, установить минимально возможный уровень безопасности, 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 компании, такие как утеря прав интеллектуальной собственности, разглашение секретов производства, снижение стоимости активов или их частичное или полное разрушение, судебные издержки и выплата штрафов и компенсаций и т. д.

Непрямой ущерб может означать качественные или косвенные потери.

Качественными потерями могут являться приостановка или снижение эффективности деятельности компании, потеря клиентов, снижение качества производимых товаров или оказываемых услуг. Косвенные потери – это, например, недополученная прибыль, потеря деловой репутации, дополнительно понесенные расходы. Кроме этого, в зарубежной литературе встречаются также такие понятия, как тотальный риск, который присутствует, если вообще никаких мер защиты не внедряется, а также остаточный риск, который присутствует, если угрозы реализовались, несмотря на внедренные меры защиты.

Анализ рисков может быть как количественным, так и качественным.

В рамках данного вопроса очень коротко рассмотрим один из способов количественного анализа рисков. Основными показателями будем считать следующие величины:

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

SLE – singlelossexpectancy, ожидаемые разовые потери, т. е. «стоимость» одного инцидента.

EF – exposurefactor, фактор открытости перед угрозой, т. е. какой процент актива разрушит угроза при её успешной реализации.

ARO – annualizedrateofoccurrence, среднее количество инцидентов в год в соответствии со статистическими данными.

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 поможет проранжировать риски – риск с высоким ALE будет самым критичным. Далее рассчитанное значение ALE можно будет использовать для определения максимальной стоимости реализуемых мер защиты, поскольку, согласно общепринятому подходу, стоимость защитных мер не должна превышать стоимость актива или величину прогнозируемого ущерба, а расчетные целесообразные 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 внедрения мер защиты, а также вычтя ежегодные затраты на реализацию этих мер. Условно записать это выражение можно следующим образом:

(Ценность мер защиты для компании) = (ALE до внедрения мер защиты) – (ALE после внедрения мер защиты) – (Ежегодные затраты на реализацию мер защиты)

Примерами качественного анализа рисков могут быть, например, метод Дельфи, в котором проводится анонимный опрос экспертов в несколько итераций до достижения консенсуса, а также мозговой штурм и прочие примеры оценки т. н. «экспертным методом».

4. Принципы обеспечения сетевой безопасности

Число случаев нарушения безопасности с каждым годом увеличивается все большими темпами. А поскольку угрозы безопасности становятся все более изощренными, соответствующего усложнения требуют и меры по защите сетей. Операторы, сетевые администраторы и другие специалисты, работающие в центрах обработки данных, должны четко понимать основные принципы безопасности, чтобы безопасно осуществлять развертывание и управление сетями в сегодняшних условиях.

В рамках рассмотрения данного учебного вопроса обозначим и коротко охарактеризуем самые основные принципы обеспечения сетевой безопасности.

Принцип знания сети.

Нельзя обеспечить защиту чего бы то ни было, если неизвестно, что именно нужно защищать. Организации любого размера должны обладать рядом документированных ресурсов, материальных объектов и систем. Каждому из этих элементов должно быть задано относительное значение, назначенное в соответствии с его важностью для организации. Примерами элементов, которые должны учитываться, являются серверы, рабочие станции, системы хранения данных, маршрутизаторы, коммутаторы, концентраторы, сети и телекоммуникационные соединения, а также любые другие сетевые элементы, например: принтеры, системы ИБП и т. д. Другими

важными аспектами этой задачи являются документирование местоположения оборудования и примечания о существующих взаимосвязях.

Принцип физической безопасности сети.

Большинство экспертов сходятся во мнении, что любая система обеспечения безопасности начинается с организации физической безопасности. Контроль физического доступа к компьютерам и точек подключения в сети является, пожалуй, более важным, чем любые другие аспекты безопасности. При любом типе физического доступа к внутреннему узлу возникает большая угроза для этого узла. Защита файлов, паролей, сертификатов и всех прочих типов данных обычно требуется, если возможен физический доступ к ним. К счастью, существуют различные типы устройства контроля доступа и защитные шкафы, которые могут помочь в решении этой проблемы.

Принцип секционирование сетей и защиты их границ с помощью межсетевых экранов.

Помимо элементарной физической защиты объекта другим наиболее важным аспектом обеспечения безопасности является контроль доступа к вычислительным сетям в сети организации и за ее пределами. В большинстве случаев это означает контроль точек подключения к внешнему миру, как правило, через Интернет. Как правило, такой контроль осуществляется при помощи межсетевых экранов (файрволлов, брандмауэров).

Межсетевые экраны могут быть как очень простыми, так и очень сложными. Так же, как и в случае с другими аспектами обеспечения безопасности, решение о том, какой межсетевой экран использовать, будут определять такие факторы как уровень трафика, нуждающиеся в защите службы и сложность требуемых правил.

Очень важно использовать межсетевые экраны не только на серверах сети, но и на всех рабочих станциях. Межсетевые экраны на рабочих станциях могут блокировать доступ ко всем портам на вход и на выход для отдельных хостов, если такие запросы не являются обычными требованиями этого хоста. Кроме того, все системы должны иметь возможность заблокировать все порты, которые не требуются для использования.

Принцип строгой изоляции портов и сокращения числа выполняемых служб.

На многих сетевых устройствах и хостах различные сетевые службы запускаются по умолчанию. Каждая из таких служб может стать возможностью для атаки злоумышленника, проникновения червя или троянской программы. Очень часто все эти запускаемые по умолчанию службы просто не нужны. Блокирование портов путем отключения служб сокращает эту потенциальную угрозу. Для решения этой задачи чаше всего используются программные продукты, выполняющие функции межсетевых экранов.

Принцип управления именами пользователей и паролями.

Как многим известно, неправильное управление именами пользователей и паролями является обычной проблемой в большинстве корпоративных сетей. Хотя применение сложных, централизованных систем аутентификации может значительно сократить число проблем, вполне возможно достичь отличных результатов, про-

сто соблюдая простейшие базовые принципы. Необходимо придерживаться следующих четырех основных правил в отношении имен пользователей и паролей.

1. Нельзя использовать очевидные пароли, такие как имя супруга, название любимой команды, день рождения, кличка домашнего питомца и т. д.

2. Необходимо использовать длинные пароли, состоящие из смеси чисел и буквенных символов.

3. Необходимо регулярно менять пароли.

4. Никогда нельзя оставлять реквизиты доступа, заданные для сетевого оборудования по умолчанию.

Принцип списочного контроля доступа.

Большое число различных типов оборудования или хостов могут быть настроены с помощью списков доступа. В этих списках определяются имена хостов или IP-адреса, для которых разрешен доступ данного устройства. Обычно, например, это используется в корпоративной сети, для ограничения доступа к сетевому оборудованию изнутри. Таким методом обеспечивается защита от любого вида доступа, который может нарушить работу внешнего межсетевого экрана. Подобные списки видов доступа служат в качестве последнего важнейшего рубежа защиты и могут быть очень эффективны при работе с некоторыми устройствами, когда для различных протоколов доступа используются разные правила.

Принцип аутентификация пользователей для сетевых устройств.

Аутентификация необходима, когда требуется контроль за доступом к сетевым элементам, в особенности к устройствам сетевой инфраструктуры. Аутентификация раскладывается на две подзадачи: аутентификация общего доступа и функциональная авторизация. Общий доступ означает возможность контроля за тем, имеет или нет определенный пользователь какие-либо права доступа к рассматриваемому элементу сети. Обычно эта информация рассматривается в виде «учетной записи пользователя». Авторизация связана с отдельными «правами» пользователя. Например, что пользователь может делать после его аутентификации? Может ли он настраивать устройство или только просматривать данные?

Для обеспечения безопасности все сетевые устройства должны иметь механизм аутентификации с именем пользователя и нетривиальным паролем (достаточно длинным, включающим комбинацию букв, цифр и символов). Пользователи должны быть ограничены как по числу, так и по типу авторизаций. Необходимо предпринимать меры предосторожности при использовании методов удаленного доступа, которые не безопасны, например, когда имя пользователя или пароль передаются в незашифрованном виде по сети. Пароли также необходимо менять с определенной разумной периодичностью.

Принцип защиты данных в сетях с помощью шифрования.

В некоторых случаях необходимо уделить внимание неразглашению информации, обмен которой происходит между элементами сети, компьютерами или системами. Если требуется избежать разглашения отправляемых по сети данных, необходимо использовать методы шифрования, которые сделают передаваемые данные недоступными для чтения кем-либо, кто мог каким-нибудь образом перехватить их во время передачи по сети.

5. Особенности подсистем обеспечения безопасности и журналирования в операционных системах Windows, Linux. Компоненты системы журналирования в операционных системах семейства Windows

Основная часть системы журналирования в операционных системах семейства Windows это служба журнала событий. Этот классический механизм, используемый со времен Windows NT. Служба обеспечивает поддержку нескольких стандартных журналов. Через специальный API система или приложения могут записывать сообщения в эти журналы.

Крайне важным, с точки зрения автоматизации, расширением стала встроенная возможность автоматического сбора данных журналов событий с удаленных компьютеров. Для этих целей предусмотрена служба Windows Event Collector, которая создает и поддерживает подписки на события, регистрируемые на других компьютерах сети. Существует несколько типов подписок, которые определяют способ сбора данных:

Source-initiatedsubscriptions – события отправляются источником. Позволяет создавать подписки на машине, которая будет собирать данные с удаленных источников. Удаленные машины требуют такой настройки глобальной политики, которая позволит им отправлять данные о событиях в единую точку. Этот тип подписки может использоваться для работы как с доменными машинами, так и с машинами, не входящими в домен.

Collector-initiatedsubscriptions – события собираются приемником. Если список систем, с которых собираются события, известен, то можно настроить компьютер, для сбора данных с систем в домене. В этом случае приемник самостоятельно опрашивает системы и собирает данные. Этот тип подписки реализуется только внутри домена.

Администрирование систем Linux. Журналирование событий.

Linux предлагает необычный метод журналирования, а также позволяет конфигурировать составные части журналов. В Linux журналы представляют собой обычный текст, так что вы можете исследовать и читать их, не применяя специальных средств. Вы также можете написать скрипт для просмотра журналов и автоматического выполнения каких-либо функций на основе их содержимого.

Linux-журналы хранятся в каталоге /var/log. Здесь содержится несколько файлов, которые поддерживаются системой. Другие сервисы и программы также могут размещать здесь свои log-файлы. Большинство журналов доступны для чтения только суперпользователю root, но это можно легко изменить, скорректировав права доступа к файлам.

Журнал /var/log/messages – журнал сообщений – основной системный log-файл. Он содержит сообщения о ходе загрузки системы, а также другие сообщения о статусе работающей системы. В этом файле накапливаются сообщения об ошибках ввода/вывода (IO), проблемах с сетью и другие сообщения о системных ошибках. Кроме того, здесь хранится и другая информация, например, о том, в какое время какой-нибудь пользователь стал root'ом. Если запущен какой-либо сервис, например DHCP-сервер, в этом файле вы можете наблюдать за его деятельностью. С изучения файла /var/log/messages обычно начинают выявление и устранение неполадок.

Журнал /var/log/XFree86.0.log – этот журнал содержит информацию о последнем запуске сервера Xwindow Xfree86. В случае возникновения проблем с запуском графической сессии в этом файле обычно можно найти причину неудачи.

Другие журналы. В каталоге /var/log могут быть и другие log-файлы в зависимости от того, какой дистрибутив Linux используется и какие сервисы и приложения запущены. Например, они могут быть связаны с запуском почтового сервера, распределением ресурсов, автоматическим выполнением задач и т. д.

Архивы Rotate В каталоге /var/log вы можете видеть несколько файлов, имена которых оканчиваются цифрой. Это «rotated» архивы. Log-файлы могут быть довольно большими и громоздкими. В Linux имеется команда для ротации этих файлов, за счет чего текущая информация не смешивается с устаревшими, уже не нужными данными. Команда logrotate обычно запускается автоматически через определенные промежутки времени, но ее можно запустить и вручную. Команда logrotate берет текущую версию log-файла и добавляет в конец имени файла «.1». Затем все предыдущие такие файлы нумеруются последовательно: «.2,» «.3,» и так далее. Чем больше число в конце имени файла, тем файл старше.

Из всего сказанного можем сделать вывод о том, что одним из наиболее важных аспектов в управлении любой системой является контроль за системными событиями. ОС Linux предлагает необычный метод журналирования, а также позволяет конфигурировать составные части журналов. В Linux журналы представляют собой обычный текст, так что вы можете исследовать и читать их, не применяя специальных средств.

Подход операционной системы Windows в данном вопросе одновременно похож и в то же время сильно отличается от того, что видно в Linux. Основное различие заключается в работе через API и графические оболочки, что позволяет пользоваться подобным инструментом рядовым пользователям, но в то же время сильно уменьшает гибкость подобной системы.

Вопросы и задания для самоконтроля

1. Сформулируйте определения терминов «оконечное устройство» и «безопасность оконечных устройств». Определите причины, по которым оконечные устройства являются самыми слабыми звеньями любой сети.

2. Дайте определение массовых и таргетированных (целенаправленных) кибератак. Приведите примеры кибератак такого рода.

3. Фишинг – в чем заключается суть атаки, как выглядит типичное фишинговое письмо?

4. Что такое атака типа «троянский конь»? Принцип работы «троянского коня» и наиболее распространенные виды троянов.

5. Что представляет из себя DDoS-атака?

6. Бэкдоры – что из себя представляют и как могут использоваться на практике?

7. Что представляет из себя атака в виде классического файлового вируса?

8. Определите основные способы заражения оконечного устройства вредоносными программами.

9. Виртуализация как один из наиболее эффективных способов противодействия киберугрозам. Плюсы и минусы виртуализации.

10. Использование «песочниц» как один из способов противодействия кибератакам.

11. Антивирусные программы и файрволлы – назначение и отличия. Основные типы антивирусных программ.

12. Что представляют из себя сигнатурный и эвристический анализ киберугроз?

13. Дайте определение системы обнаружения вторжений. В чем заключается различие между системами обнаружения вторжений и системами предотвращения вторжений?

14. Определите элементы и подсистемы, входящие в состав классической системы обнаружения вторжений.

15. Опишите принцип работы сетевых систем обнаружения вторжений.

16. Раскройте принцип работы узловых систем обнаружения вторжений.

17. Перечислите основные недостатки и проблемы систем обнаружения вторжений.

18. Укажите основные способы обхода защиты систем обнаружения и предотвращения вторжений.

Лекция 4. Источники и каналы утечки информации. Основы технической защиты информации[1]

Современный этап развития общества характеризуется существенным возрастанием роли и актуальности проблем обеспечения безопасности всех сфер жизнедеятельности. Особенно показателен этот процесс для безопасности информационной сферы, которая за последние два десятилетия вышла из области компетенции специальных служб госструктур на уровень взаимоотношений в обществе.

Один из основных источников угроз информационной безопасности – противозаконная деятельность зарубежных разведок, конкурентов, преступных сообществ, организаций, групп, формирований и отдельных лиц, направленная на сбор или хищение ценной (конфиденциальной, секретной) информации, закрытой для доступа посторонних лиц.

Для несанкционированного добывания информации в настоящее время используется широкий арсенал технических средств, из которых малогабаритные технические средства отражают одно из направлений в развитии современных разведывательных технологий. Выполняемые в портативном, миниатюрном и сверхминиатюрном виде, эти средства аккумулируют в себе новейшие научные, технические и технологические достижения электроники, акустики, оптики, радиотехники и других наук. Такие средства находят широкое применение, в деятельности как правоохранительных органов, так и иностранных технических разведок, в подпольном информационном обеспечении незаконных экономических, финансовых и криминальных организаций. В условиях рыночной экономики в последние годы приоритеты подобной деятельности смещаются и в экономическую область.

Главной причиной возникновения промышленного (экономического) шпионажа является стремление к реализации конкурентного преимущества – важнейшего

---

[1] В данной лекции использованы следующие материалы: *Ахмаджонов А.* Технические каналы утечки и защиты информации от перехвата // Информационное противодействие угрозам терроризма. 2013. № 21. С. 42–46.; *Башлы П. Н.* Информационная безопасность: учеб.-метод. пособие для студентов высш. учеб. заведений, обуч. по спец. 080801 «Прикладная информатика» и другим междисциплинар. специальностям. М.: Изд. центр ЕАОИ, 2011; *Бузов Г. А.* Практическое руководство по выявлению специальных технических средств несанкционированного получения информации. М.: Горячая линия – Телеком, 2010; *Галкин А. П.* Защита учреждений и предприятий от несанкционированного доступа к информации в технических каналах связи: дис. ... д-ра техн. наук. Владимир, 2003; *Голиков А. М.* Защита информации от утечки по техническим каналам: учеб. пособие. Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2015; *Еськов А. В.* Физические основы технической защиты информации: учеб. пособие. Краснодар: Краснодар. ун-т МВД России, 2020; *Зайцев А. П.* Технические средства и методы защиты информации: учеб. пособие для вузов. М.: Горячая линия – Телеком, 2012; *Креопалов В. В.* Технические средства и методы защиты информации: учеб.-практ. пособие. М.: Евразийский открытый ин-т, 2011; *Малюк А. А.* Введение в информационную безопасность: учеб. пособие для вузов. М.: Горячая линия – Телеком, 2011; *Скрипник Д. А.* Общие вопросы технической защиты информации: учеб. пособие. М., Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020; *Соколов А.И.* Технические средства защиты информации: технические каналы утечки информации: учеб. пособие. Владимир: Владимир. гос. ун-т, 2007; *Титов А. А.* Технические средства защиты информации: учеб. пособие. Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2010; *Торокин А.А.* Инженерно-техническая защита информации: учеб. пособие для студентов, обуч. по спец. в области информ. безопасности. М.: Гелиос АРВ, 2005.

условия достижения успеха в рыночной экономике. Охота за чужими секретами позволяет компаниям экономить собственные средства на ведение НИОКР и фундаментальные исследования, быть в курсе дел конкурентов, использовать их научно-технические достижения, овладевать рынками сбыта, подделывать товары, дискредитировать или устранять (экономически или физически подавлять) конкурентов, срывать переговоры по контрактам и т. д.

На рынке России представлен арсенал самых современных технических средств, предназначенных для негласного получения информации, которые находят все более широкое применение на практике. К ним относятся: визуально-оптические, фотографические, телевизионные, тепловизионные (инфракрасные), акустические, радио-, радиотехнические и другие средства разведки.

Для организации защиты конфиденциальной информации необходимо знать возможности технических средств, предназначенных для негласного получения информации, способы их применения и, в первую очередь, представлять себе каналы, по которым ценная информация потенциально может быть перехвачена, то есть возможна ее утечка.

1. Понятие о технических каналах утечки информации: состав и характеристики

Утечка информации означает несанкционированный перенос информации от ее источника к злоумышленнику по каналу утечки информации. Всего можно выделить четыре основные формы утечки информации (рис. 5):

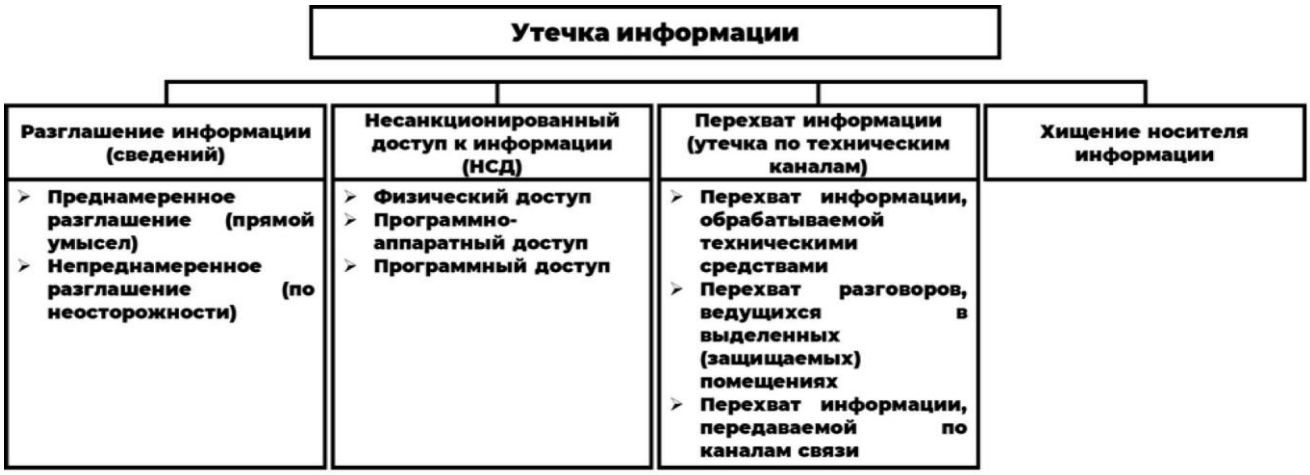


Рис. 5.

1. Разглашение информации (сведений) – такое противоправное предание огласке защищаемых сведений, при котором они стали достоянием посторонних лиц (при этом посторонним признается любое лицо, которое по характеру выполняемой работы или служебных обязанностей не имеет права доступа к данным сведениям). Осуществляется в двух формах – преднамеренное разглашение (прямой умысел) и непреднамеренное разглашение (по неосторожности);

2. Несанкционированный доступ к информации (НСД) – доступ к информации, осуществляемый с нарушением установленных прав и (или) правил доступа к ней с применением штатных средств, предоставляемых СВТ или АС, или средств, аналогичных им по своему функциональному предназначению и техническим характери-

стикам. Осуществляется в трех формах – физический доступ, программно-аппаратный доступ, программный доступ;

3. Перехват информации (утечка по техническим каналам) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов – осуществляется в трех формах – перехват информации, обрабатываемой техническими средствами и системами; перехват разговоров, ведущихся в выделенных (защищаемых) помещениях; перехват информации, передаваемой по каналам связи;

4. Хищение носителя информации.

Если утечка информации происходит с помощью технических средств, то соответствующий канал называется техническим каналом утечки информации.

Технический канал утечки информации – совокупность объекта разведки (источник информации), технического средства разведки (средство перехвата информации), с помощью которых добывается информация об этом объекте, и физической среды, в которой распространяется информационный сигнал (канал связи).

По сути, под техническим каналом утечки информации понимают способ получения разведывательной информации об объекте с помощью технических средств, а под разведывательной информацией – обычно сведения или совокупность данных об объекте разведки независимо от формы их представления.

Материальными носителями информации являются сигналы – некоторые физические процессы, с помощью которых передаются информационные сообщения. По своей физической природе сигналы могут быть электрическими, электромагнитными, акустическими и т. д. То есть сигналы, как правило, – это электромагнитные, механические и другие виды колебаний, в которых информация записана на изменяемых ею параметрах, например, в амплитуде, частоте, фазе, длине волны и т. д.

Сигналы распространяются в определенных физических средах. В общем случае средой распространения могут быть воздушные, жидкостные и твердые среды, например, воздушное пространство, конструкции зданий, соединительные линии, токопроводящие элементы, грунт (земля) и т. п.

Технические средства разведки служат для приема сигналов в каналах утечки информации и выделения из них информационных параметров, а также создания самих технических каналов утечки информации.

В рамках изучения данной темы мы, в ходе ближайших двух лекций, дадим классификацию и рассмотрим характеристики технических каналов утечки информации, обрабатываемой техническими средствами, передаваемой по каналам связи, а также акустической (речевой), видовой (оптической) и материально-вещественной информации.

Информация, записанная на распространяющихся в пространстве носителях, может быть перенесена этими носителями от источника к несанкционированному получателю. В таком случае говорят об утечке информации по аналогии с утечкой жидких или газообразных веществ. Однако по сравнению с ними утечка информации имеет ряд особенностей.

Под утечкой информации понимается несанкционированный процесс переноса информации от источника к злоумышленнику (зарубежной разведке, конкурентам, криминалу, террористам и т. д.).

Понятие «утечка» широко распространено. Говорят об утечке воды, газа, материальных ценностей со склада, информации из различных структур и т. п. Утечка информации возможна путем ее разглашения людьми, утерей последними носителей с информацией, а также при ее переносе с помощью полей, потоков элементарных частиц, веществ в газообразном, жидком или твердом виде. Например, желание сотрудников поделиться последними новостями о работе с родными или близкими создает возможности (предпосылки) утечки конфиденциальной информации. Переносчиками информации могут быть любые ее носители.

Часто под утечкой понимают случайный процесс, вроде вытекания воды из неисправного крана. Но такой подход представляется несколько упрощенным. В криминальной практике известны факты организации утечки, например бензина с последующим списыванием его на случайную неисправность в нефтепроводе или хранилище. В политической жизни общества практикуется «организация утечки» информации из правительственных структур с целью зондирования или подготовки общественного мнения перед принятием непопулярных решений.

Утечка информации по сравнению с утечкой (хищением) материальных объектов имеет ряд особенностей, которые надо учитывать при организации защиты информации:

– утечка информации может происходить только при попадании ее к заинтересованному в ней несанкционированному получателю (злоумышленнику), в отличие, например, от утечки воды или газа;

– при утечке информации происходит ее тиражирование, которое не изменяет характеристики исходного носителя информации (не уменьшается количество листов документа, не сокращается число пикселей изображения, не меняются размеры, цвет и другие демаскирующие признаки продукции и т. д.);

– цена информации при ее утечке уменьшается за счет тиражирования;

– утечка возникает, если принятые меры по обеспечению безопасности информации недостаточны, неэффективны или несвоевременны, а факт утечки информации, как правило, обнаруживается спустя некоторое время, по последствиям.

Первая особенность имеет существенное значение для безопасности информации, так как сами по себе факты утери документа, разглашения сведений, распространения носителей за пределы контролируемой зоны и другие действия далеко не всегда приводят к утечке информации. Например, если конфиденциальный разговор во время совещания в кабинете руководителя организации слышен в приемной из-за неплотно закрытой двери, а в приемной нет людей, то утечки информации нет, хотя носитель информации (акустическая волна) выходит за пределы контролируемой зоны – помещения, где проводится совещание. Если в приемной находится добросовестно выполняющий свои обязанности секретарь руководителя, который после совещания будет оформлять его результаты, то утечка информации также отсутствует, так как информация не попадет к злоумышленнику. Только в том случае, когда в приемной будет находиться сотрудник организации или посетитель, который воспользуется информацией из услышанного разговора в личных целях или поделится ею с другими заинтересованными в ней людьми, происходит утечка информации из кабинета руководителя. То есть можно говорить об утечке информации как факте нарушения ее безопасности только тогда, когда она попадает к злоумышленнику не-

зависимо от того, знает или не знает об этом владелец информации. Если по какой-либо причине на этом пути передачи информации происходит разрыв в цепочке и информация исчезает на носителе или вместе с ее носителем, то утечки информации не происходит.

Следовательно, под утечкой следует понимать не процесс распространения носителя информации за пределы определенной области пространства вообще, а частный случай распространения, когда информация попадает к злоумышленнику. Выход же носителя за пределы заданной области создает предпосылки для утечки информации и повышает угрозу ее безопасности.

Замечание о несанкционированности получателя имеет принципиальное значение. Если получатель информации санкционирован, то речь идет не об утечке, а о передаче информации по так называемому функциональному каналу связи, специально создаваемому для обеспечения коммуникаций в человеческом обществе.

Физический путь переноса информации от ее источника к несанкционированному получателю называется каналом утечки. Если запись информации на носитель канала утечки и съем ее с носителя осуществляется с помощью технических средств, то такой канал называется техническим каналом утечки.

Несанкционированный перенос информации полями различной природы, макро- и микрочастицами выполняется в рамках технических каналов утечки информации.

Давайте рассмотрим основные характеристики технических каналов утечки информации.

Для передачи информации носителями в виде полей и микрочастиц по любому техническому каналу (функциональному или каналу утечки) последний должен содержать три основных элемента: источник сигнала, среду распространения носителя и приемник. Обобщенная типовая структура канала передачи информации приведена на рис. 6.

Рис. 6.

На вход канала поступает информация в виде первичного сигнала. Первичный сигнал представляет собой носитель с информацией от ее источника или с выхода предыдущего канала. В качестве источника сигнала могут выступать:

– объект наблюдения, отражающий электромагнитные и акустические волны;

– объект наблюдения, излучающий собственные (например, тепловые) электромагнитные волны или побочные электромагнитные излучения;

– приемо-передатчик функционального канала связи и сам канал связи;

– закладное устройство;

– источник опасного сигнала;

– источник акустических волн, модулированных информацией.

Указанные на предыдущем рисунке стрелками пути входа и выхода информации обозначают вход и выход первичных сигналов с информацией. Так как информация от источника поступает на вход канала на языке источника (в виде буквенно-цифрового текста, символов, знаков, звуков, сигналов и т. д.), то передатчик преобразует эту форму представления информации в форму, обеспечивающую ее запись на носитель информации, соответствующий среде распространения. Кроме того, он выполняет следующие функции:

– создает (генерирует) поля (акустическое, электромагнитное) или электрический ток, которые переносят информацию;

– осуществляет запись информации на носитель (модуляцию информационных параметров носителя);

– усиливает мощность сигнала (носителя с информацией);

– обеспечивает передачу (излучение) сигнала в среду распространения в заданном секторе пространства.

Информация записывается путем изменения параметров носителя в соответствии с уровнем первичного сигнала, поступающего на вход. Если носителями информации являются субъекты и материальные тела (макрочастицы), то передатчик соответствует первоначальному смыслу этого слова – передавать или переносить, т. е. выполняет функцию носителя. В случае, когда информацию переносят сигналы (поля, электрический ток и элементарные частицы), передатчики являются их источниками.

Источниками сигналов могут быть как источники функциональных каналов связи, так и опасных сигналов. К последним относятся сигналы с конфиденциальной информацией, появление которых является для источника информации случайным событием и им не контролируется.

Среда распространения носителя – часть пространства, в которой перемещается носитель. Она характеризуется набором физических параметров, определяющих условия перемещения носителя информации. Из них основными параметрами, которые надо учитывать при анализе среды распространения носителя, являются следующие:

– физические препятствия для субъектов и материальных тел;

– мера ослабления (или пропускания энергии) сигнала на единицу длины;

– частотная характеристика (неравномерность ослабления частотных составляющих спектра сигнала);

– вид и мощность помех для сигнала.

Приемник выполняет функции, обратные функциям передатчика. Он осуществляет:

– выбор (селекцию) носителя с нужной получателю информацией;

– усиление принятого сигнала до значений, обеспечивающих съем информации;

– съем информации с носителя (демодуляцию, декодирование);

– преобразование информации в форму сигнала, доступную получателю (человеку, техническому устройству), и его усиление до значений, необходимых для безошибочного восприятия информации получателем.

Канал утечки информации отличается от функционального канала передачи получателем информации. Если получатель санкционированный, то канал функциональный, в противном случае – канал утечки. Классификация каналов утечки информации дана на рис. 7.

Рис. 7.

Физическая природа носителя является основным классификационным признаком технических каналов утечки информации. По этому признаку они делятся:

– на оптические;

– радиоэлектронные;

– акустические;

– материально-вещественные.

Носитель информации в оптическом канале – электромагнитное поле в диапазоне 0,46–0,76 мкм (видимый свет) и 0,76–13 мкм (инфракрасные излучения).

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток, распространяющийся по проводникам из меди, железа, алюминия. Диапазон колебаний этого вида носителя чрезвычайно велик: от звукового диапазона до десятков ГГц. Часто этот канал называют электромагнитным, что представляется недостаточно корректным, так как носителями информации в оптическом канале являются также электромагнитные поля, но в более высокочастотном диапазоне. Кроме того, широко используется в качестве носителя информации модулированный поток электронов (электрический ток). Объединяя эти два носителя информации в канале одного вида, целесообразно назвать его «радиоэлектронный» (электромагнитное поле в радиодиапазоне и электроны электрического тока).

Носителями информации в акустическом канале являются механические акустические волны в инфразвуковом (менее 16 Гц), звуковом (16–20 кГц) и ультразвуковом (свыше 20 кГц) диапазонах частот, распространяющиеся в атмосфере, воде и твердой среде.

В материально-вещественном канале утечка информации возможна через несанкционированное распространение за пределы организации вещественных носителей с секретной или конфиденциальной информацией, прежде всего выбрасываемых черновиков документов и использованной копировальной бумаги, забракованных деталей и узлов, демаскирующих веществ. Последние в виде твердых, жидких и газообразных отходов или промежуточных продуктов содержат химические элемен-

ты, по которым в принципе можно определить состав, структуру и свойства новых материалов или восстановить технологию их получения.

Когда речь идет о распространении за пределы организации отходов производства в широком смысле, то следует отличать технический канал утечки от агентурного, в рамках которого носитель с информацией выносится проникшим к источнику злоумышленником, завербованным сотрудником организации или сотрудником, стремящимся продать информацию любому ее покупателю. Граница между каналами достаточно условна, однако при утечке информации в агентурном канале переносчиком информации является лицо, сознающее противоправные действия, а в техническом материально-вещественном канале носители вывозятся из организации с целью освобождения ее от отходов или отходы распространяются в результате действия природных сил. В качестве таких сил могут быть воздушные потоки, разносящие газообразные отходы, или водные потоки рек или водоемов, куда сбрасываются недостаточно очищенные жидкие или взвешенные в воде твердые частицы демаскирующих веществ.

Каждый из технических каналов имеет свои особенности, которые необходимо знать и учитывать для обеспечения эффективной защиты информации от утечки или ее предпосылок.

По информативности каналы утечки делят на информативные, малоинформативные и неинформативные (информативность канала оценивается ценностью передаваемой по нему информации). По времени проявления – на постоянные, периодические и эпизодические. В постоянном канале утечка информации носит достаточно регулярный характер. Например, наличие в кабинете источника опасного сигнала может привести к передаче из кабинета речевой информации до момента обнаружения этого источника. Периодический канал утечки может возникнуть во время пролетов разведывательных космических аппаратов, при условии, например, размещения во дворе неукрытой продукции, демаскирующие признаки которой составляют тайну. К эпизодическим относят каналы, утечка информации в которых имеет разовый, случайный характер.

Канал утечки информации, состоящий из передатчика, среды распространения и приемника, является одноканальным. Однако возможны варианты, когда утечка информации происходит более сложным путем – по нескольким последовательным или параллельным каналам. При этом используется свойство информации переписываться с одного носителя на другой. Например, если в кабинете ведется конфиденциальный разговор, то утечка возможна не только по акустическому каналу через стены, двери, окна, но и по оптическому – путем съема информации лазерным лучом со стекла окна или по радиоэлектронному с использованием установленной в кабинете радиозакладки. В двух последних вариантах образуется составной канал, образованный из последовательно соединенных акустического и оптического (на лазерном луче) или акустического и радиоэлектронного (радиозакладка – среда распространения – радиоприемник) каналов. Для повышения дальности канала утечки может также использоваться ретранслятор, совмещающий функции приемника одного канала утечки информации и передатчика следующего канала. Например, для повышения дальности подслушивания с использованием радиозакладки можно раз-

местить ретранслятор в портфеле, сдаваемом в камеру хранения закрытого предприятия.

Как любой канал связи, канал утечки информации характеризуется следующими основными показателями:

– пропускной способностью;

– дальностью передачи информации.

Пропускная способность канала связи оценивается количеством информации, передаваемой по нему в единицу времени с определенным качеством. В теории связи пропускная способность канала в бодах (битах в секунду) определяется по формуле Шеннона:

$$C = \Delta F \times \log_2(1 + \frac{P_с}{P_п}),$$

где ΔF – ширина полосы пропускания канала связи; $P_с$ и $P_п$ – мощность сигнала и помехи (в виде белого шума) в полосе пропускания канала соответственно.

Следовательно, пропускная способность канала связи является интегральной характеристикой, учитывающей как ширину полосы частот сигнала, которую пропускает канал, так и его энергетику. Чем меньше отношение мощностей сигнала и помехи, тем больше ошибок в принятом сообщении и тем меньше количество переданной информации.

По ширине полосы частот пропускания каналы делят на узко- и широкополосные. Стандартный телефонный канал для передачи речевой информации имеет полосу 300–3400 Гц и относится к узкополосным, а канал для передачи телевизионных сигналов шириной 8 МГц – к широкополосным. Чем шире канал, тем больше информации можно передать за единицу времени. Так как для добывания информации с требуемым качеством необходимо обеспечить на входе приемника канала минимально допустимое для каждого вида информации и носителя отношение сигнал/помеха, то это отношение достигается на различном удалении от источника сигнала в зависимости от мощности сигнала и помехи, а также величины (коэффициента) ослабления (затухания) сигнала в канале. Носители информации существенно отличаются по величине затухания в среде распространения: в наибольшей степени уменьшается энергия акустической волны, в наименьшей – электромагнитная волна в длинноволновом диапазоне частот.

2. Основные и вспомогательные технические средства и системы

Для начала отметим, что для информации, обрабатываемой средствами вычислительной техники, актуальны все перечисленные нами в первом учебном вопросе формы утечки. Например:

– разглашение информации: передача носителя информации постороннему лицу (преднамеренное) или обработка информации ограниченного доступа на СТВ в присутствии постороннего (непреднамеренное);

– НСД к информации: вскрытие системного блока СВТ и изъятие накопителя информации для физического копирования (физический); сброс установленных параметров BIOS и изменение приоритета загрузки носителей с последующей загрузкой альтернативной операционной системы и копирования информации на съемный

накопитель (программно-аппаратный); внедрение в СВТ вредоносных программ для осуществления НСД к информации или ее копирования (программный);

– хищение носителей информации;

– утечка информации по техническим каналам.

Технические средства и системы приема, обработки, хранения, отображения и передачи информации (ТСПИ) по отношению к информации ограниченного доступа подразделяются на основные и вспомогательные.

Под основными техническими средствами и системами (ОТСС) понимают технические средства и построенные на их базе системы, непосредственно обрабатывающие (принимающие, хранящие, обрабатывающие и передающие) секретную или конфиденциальную информацию. К таким средствам относятся: электронно-вычислительная техника, режимные АТС, системы оперативно-командной и громкоговорящей связи, звукоусиления, звукового сопровождения и звукозаписи, и другие, предназначенные для ведения конфиденциальных переговоров и обработки иной защищаемой информации.

При выявлении технических каналов утечки информации, ОТСС необходимо рассматривать как систему, включающую основное, а также каналообразующее, коммуникационное (стационарное или мобильное) оборудование, оконечные устройства, соединительные линии (совокупность проводов и кабелей, прокладываемых между отдельными ОТСС и их элементами), распределительные и коммутационные устройства.

Часто вместе с ОТСС устанавливаются технические средства и системы, непосредственно не участвующие в обработке защищаемой информации, но использующиеся совместно с основными техническими средствами. Такие технические средства и системы называются вспомогательными техническими средствами и системами (ВТСС). К ним относятся: технические средства и линии открытой телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, системы электропитания, электроосвещения, заземления, радиофикации, электробытовые и электроизмерительные приборы и т. д. При этом всегда возникает задача защиты информации – разместить ВТСС по отношению к ОТСС так, чтобы информационные наводки электромагнитного поля ОТСС на ВТСС были минимальными и безопасными. В свою очередь, информация в ОТСС защищается инженерно-техническими, программно-аппаратными, криптографическими, режимными и другими мерами.

Для создания технических каналов утечки информации наибольший интерес представляют соединительные линии ОТСС и 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.

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, подверженные информационным наводкам ПЭМИ ОТСС, называются посторонними проводниками, или распределенными антеннами, и также подлежат защите от утечки.

В зависимости от физической природы образования информационного сигнала технические каналы утечки информации можно разделить на естественные и специально создаваемые.

Естественные каналы утечки информации образуются за счёт побочных электромагнитных излучений, возникающих при обработке информации СВТ (электромагнитные каналы утечки информации), а также вследствие наводок информативных сигналов в линиях электропитания и заземления СВТ, соединительных линиях ВТСС и посторонних проводниках (электрические каналы утечки информации). К числу естественных ТКУИ также относят вибрационные каналы.

К специально создаваемым каналам утечки информации относятся каналы, создаваемые путём внедрения в СВТ электронных устройств перехвата информации, на специальном сленге имеющих название «закладных устройств» или просто «закладок» (электрические ТКУИ) и путём «высокочастотного облучения» СВТ (параметрические ТКУИ).

На рис. 8 приведена классификация технических каналов утечки информации, обрабатываемой основными техническими средствами и системами.

Рис. 8.

Характеристику технических каналов утечки информации, обрабатываемой основными и вспомогательными техническими средствами и системами, начнем с **электромагнитных ТКУИ**, к которым относятся каналы утечки информации, возникающие за счет различного вида побочных электромагнитных излучений (ПЭМИ) основных технических средств и систем:

– элементов ОТСС;

– на частотах работы высокочастотных генераторов ОТСС и ВТСС;

– на частотах самовозбуждения усилителей низкой частоты ОТСС.

Все электромагнитные ТКУИ относятся к категории естественных технических каналов утечки информации. Обобщенная структурная схема любого технического канала утечки информации, обрабатываемой средствами вычислительной техники (ОТССТ и ВТСС) приведена на рис. 9.

Рис. 9.

1. Электромагнитные излучения элементов ОТСС. В ОТСС носителем информации является электрический ток, параметры которого (амплитуда, частота и фаза) изменяются по закону информационного сигнала. При прохождении электрического тока по токоведущим элементам ОТСС вокруг них (в окружающем пространстве) возникают электрическое и магнитное поля. В силу этого элементы ОТСС можно рассматривать как излучатели электромагнитного поля, модулированного информационным сигналом. Такого рода электромагнитные излучения в теории защиты информации получили название побочных электромагнитных излучений (ПЭМИ) и представляют собой нежелательные (паразитные) электромагнитные излучения, возникающие при функционировании технических средств обработки информации, и приводящие к утечке обрабатываемой информации. Все ПЭМИ условно делятся на два типа – информативные и неинформативные. С точки зрения защиты информации опасность представляют информативные ПЭМИ, содержащие в себе признаки обрабатываемой информации.

Информативными ПЭМИ называются сигналы, представляющие собой ВЧ-несущую, модулированную информацией, обрабатываемой на СВТ (например, изображением, выводимым на монитор, данными, обрабатываемыми на устройствах ввода-вывода и т. д.).

Неинформативными ПЭМИ называются сигналы, анализ которых может дать представление только о режиме работы СВТ и никак не раскрывает характер информации, обрабатываемой на СВТ.

ПЭМИ возникают при различных режимах обработки информации средствами вычислительной техники:

– вывод информации на монитор;
– ввод данных с клавиатуры;
– запись информации на накопители;
– чтение информации с накопителей;
– передача данных в каналы связи;
– вывод данных на печатные устройства;

– запись данных от сканера и т. д.

При каждом режиме работы СВТ возникают ПЭМИ, имеющие свои характерные особенности. Диапазон возможных частот ПЭМИ зависит от типа СВТ и может составлять от сотен Гц до десятков ГГц.

2. Электромагнитные излучения на частотах работы высокочастотных генераторов ОТСС и ВТСС. 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.

В результате внешних воздействий информационного сигнала (например, электромагнитных колебаний) на элементах высокочастотных генераторов наводятся электрические сигналы. Наведенные электрические сигналы могут вызвать непреднамеренную модуляцию собственных высокочастотных колебаний генераторов. Эти промодулированные высокочастотные колебания излучаются в окружающее пространство. 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 ВТСС и ОТСС.

3. Электромагнитные излучения на частотах самовозбуждения усилителей низкой частоты ОТСС. К усилителям низкой частоты в ОТСС относят усилители систем звукоусиления и звукового сопровождения, магнитофонов, систем громкоговорящей связи и т. п. Их самовозбуждение 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 усилителей низкой частоты (например, полупроводниковых приборов, электровакуумных ламп и т. п.). Сигнал на частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом. Самовозбуждение наблюдается, в основном, при переводе усилителя в нелинейный режим работы, т. е. в режим перегрузки.

Перехват побочных электромагнитных излучений ОТСС осуществляется средствами радио-, радиотехнической разведки, размещенными в том числе 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), в специальной литературе называется опасной зоной 2.

Структурная схема электромагнитных каналов утечки информации представлена на рис. 10.

Рис. 10.

На рис. 11 представлен принцип перехвата ПЭМИ СВТ.

Рис. 11.

Мы закончили краткое ознакомление с электромагнитными техническими каналами утечки информации и переходим к следующему типу, а именно к электрическим ТКУИ.

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 линии электропитания ОТСС;

– просачивание информационных сигналов в систему заземления ОТСС;

– использование закладных устройств.

Первые три канала относятся к категории естественных ТКУИ, а четвертый – использование закладных устройств – к категории специально создаваемых ТКУИ.

1. Как уже было отмечено, одной из причин возникновения электрических ТКУИ являются **наводки электромагнитных излучений ОТСС**, под которыми понимаются токи и напряжения в токопроводящих элементах, вызванные побочными электромагнитными излучениями, ёмкостными и индуктивными связями. Таким образом, электромагнитная наводка, это 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. Наводки возникают при излучении элементами ОТСС 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.

В зависимости от физических причин возникновения наводки информативных сигналов можно разделить:

– на наводки информативных сигналов в электрических цепях ТСОИ, вызванные информативными ПЭМИ ТСОИ;

– наводки информативных сигналов в соединительных линиях ВТСС и посторонних проводниках, вызванные информативными ПЭМИ ТСОИ;

– наводки информативных сигналов в электрических цепях ТСОИ, вызванные внутренними ёмкостными и индуктивными связями («просачивание» информативных сигналов в цепи электропитания через блоки питания ТСОИ);

– наводки информативных сигналов в цепях заземления ТСОИ, вызванные информативными ПЭМИ ТСОИ, а также гальванической связью схемной (рабочей) земли и блоков ТСОИ.

Пространство вокруг ОТСС, в пределах которого на случайных антеннах наводится информационный сигнал выше допустимого (нормированного) уровня, в специальной литературе называется **опасной зоной 1.**

Случайной антенной является цепь ВТСС или посторонние проводники, способные принимать побочные электромагнитные излучения элементов ОТСС. Различают сосредоточенные и распределенные случайные антенны.

Сосредоточенная случайная антенна представляет собой компактное техническое средство, например, телефонный аппарат, громкоговоритель радиотрансляционной сети и т. д.

К распределенным случайным антеннам относят случайные антенны с распределенными параметрами: кабели, провода, металлические трубы и другие токопроводящие коммуникации.

Общая схема возникновения и перехвата ПЭМИН отражена на рис. 12.

Рис. 12.

2. Просачивание информационных сигналов в линии электропитания. Это возможно при наличии магнитной связи между выходным трансформатором усилителя (например усилителя низкой частоты) и трансформатором блока питания. 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.

3. Просачивание информационных сигналов в систему 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: нулевой провод сети электропитания, экраны (металлические оплетки и 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, в которую могут просачиваться 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 ОТСС, ВТСС и посторонним проводникам, проходящим через помещения, где установлены ОТСС, а также к их системам электропитания и заземления. Для этих целей используются специальные средства радио- и радиотехнической разведки, а также специальная измерительная аппаратура.

На рисунках ниже приведен ряд схем, иллюстрирующих электрические каналы утечки информации. Так, на рис. 13 представлена структурная схема электрического ТКУИ при помощи перехвата ПЭМИН СВТ с соединительных линий ВТСС и посторонних проводников.

Рис. 13.

На рис. 14 изображен принцип перехвата наводок информационных сигналов с соединительных линий ВТСС и посторонних проводников.

Рис. 14.

На рис. 15 представлена структурная схема электрического ТКУИ при помощи перехвата ПЭМИН СВТ по цепям электропитания.

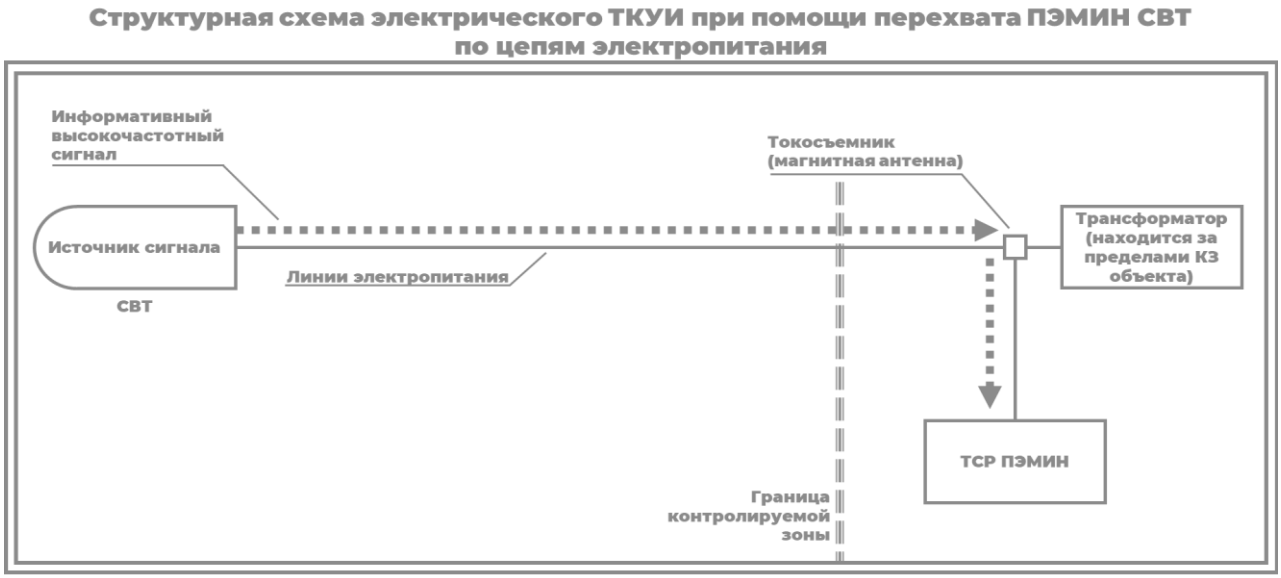


Рис. 15.

На рис. 16 представлена структурная схема электрического ТКУИ при помощи перехвата ПЭМИН СВТ по цепям заземления.

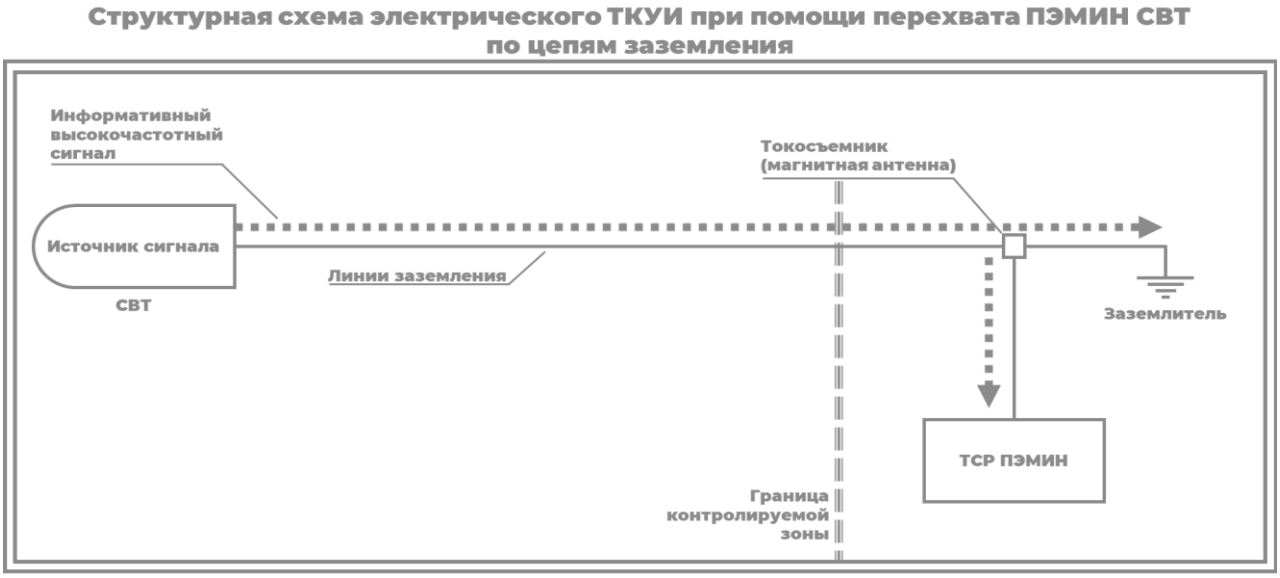


Рис. 16.

На рис. 17 изображен принцип перехвата информационных сигналов с цепей заземления и электропитания.

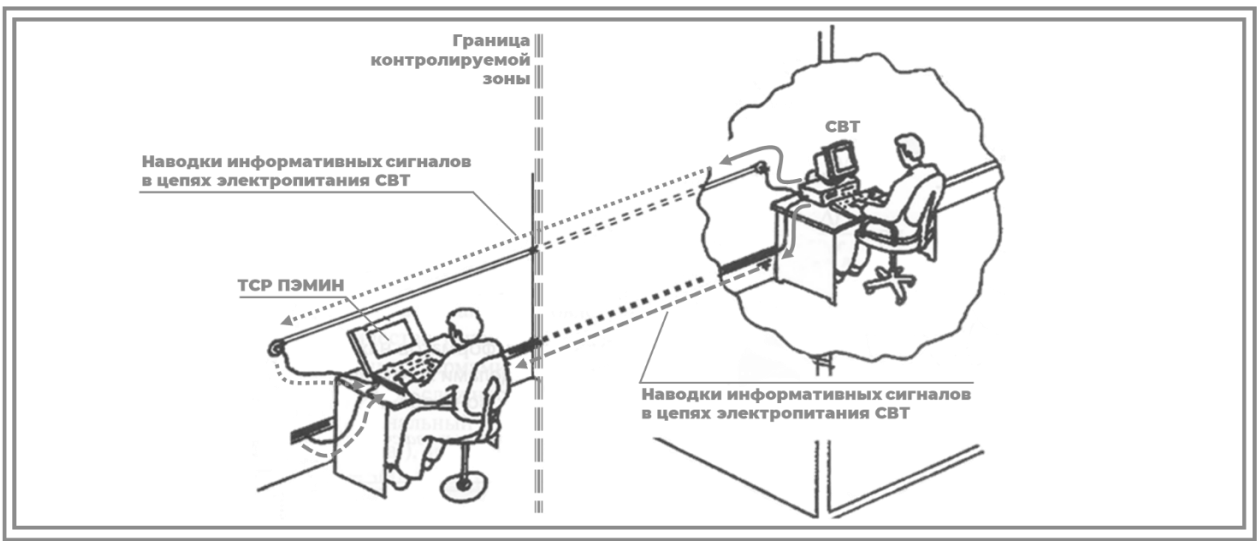


Рис. 17.

4. Съем информации с использованием аппаратных закладок. На практике достаточно широко используется способ съема информации, обрабатываемой в ОТСС, путем установки в них электронных устройств перехвата информации – закладных устройств. Как уже было отмечено, этот канал утечки информации, единственный из группы электрических каналов, относится к категории специально создаваемых ТКУИ, тогда как все остальные являются естественными.

Под аппаратной закладкой понимают электронное устройство, скрытно устанавливаемое (внедряемое) в СВТ (ОТСС) с целью обеспечить утечку информации, нарушение ее целостности или блокирование. Они представляют собой мини-передатчики, излучение которых модулируется информационным сигналом. Наиболее часто закладки устанавливаются в технические средства иностранного производства, однако возможна их установка и в отечественных средствах.

Аппаратная закладка, как правило, состоит:

– из блока перехвата;

– блока передачи информации (или модуля записи информации);

– блока ДУ (при необходимости);

– блока питания.

Блок перехвата подключается к информационным кабелям или к платам блоков СВТ и осуществляет перехват информационных сигналов, их обработку и преобразование в вид, удобный для записи или передачи на приемный пункт.

Перехватываемая аппаратными закладками информация может записываться в память ЗУ (например, на flash-память) или передаваться на приемный пункт по радиоканалу, электросети, выделенной линии, оптическому каналу (при использовании ИК-порта) и т. п.

С помощью системы ДУ осуществляется включение/выключение устройства (запуск программы перехвата информации), включение/выключение режима передачи информации, установка параметров процесса съема и передачи информации.

Перехваченная с помощью закладных устройств информация или непосредственно передается по радиоканалу, или сначала записывается на специальное запоминающее устройство, а уже затем по команде передается на запросивший ее объект.

Все разнообразие закладных устройств, применяемых для перехвата информации, обрабатываемой в СВТ (ОТСС), условно можно классифицировать по следующим основаниям (табл. 1.).

Таблица 1

Показатель классификации	**Значения**
По виду перехватываемой информации	1. Видеоизображение, выводимое на экран монитора. 2. Информация, вводимая с клавиатуры. 3. Информация, выводимая на принтер. 4. Информация, записываемая на внутренний накопитель (HDD, SSD). 5. Информация, записываемая на внешние накопители (flash-память, CD, DVD, USB-накопители). 6. Информация, передаваемая по каналу связи.
По месту установки	1. В корпусе системного блока. 2. Подключаемые к внешним разъемам системного блока (например, USB). 3. Подключаемые в виде переходных элементов в разрыв информационных кабелей, соединяющих системный блок с оконечными устройствами, например клавиатурой, принтером и т. д. 4. В корпусе монитора. 5. В корпусе клавиатуры. 6. В корпусе принтера и т. д.
По способу передачи информации	1. Без передачи информации (перехваченная информация записывается на специальные цифровые накопители, например, на flash-память). 2. По радиоканалу. 3. По сети 220 В. 4. По выделенной линии. 5. По оптическому каналу.
По средству передачи информации	1. Специальное радиопередающее устройство. 2. ИК-порт. 3. Устройство типа Bluetooth. 4. Устройство типа Wi-Fi, WiMAX и т. д.
По типу источника питания	1. От низковольтных источников питания. 2. От сети 220 В.
По виду исполнения	1. Обычные (отдельные модули). 2. Камуфлированные под типовые элементы электронных устройств.

По способу управления передатчика	1. Неуправляемые (с включением передатчика при включении СВТ). 2. Дистанционно управляемые.
По способу накопления информации	1. Без накопления. 2. С промежуточным накоплением (с коротким и длинным временем накопления).
По способу кодирования информации	1. Без кодирования информации. 2. С цифровым кодированием информации.

Структурная схема ТКУИ, создаваемого путем установки в СВТ специальных закладных устройств представлена на рис. 18.

Рис. 18.

Принцип перехвата информации, путем установки в СВТ аппаратных закладок, представлен на рис. 19.

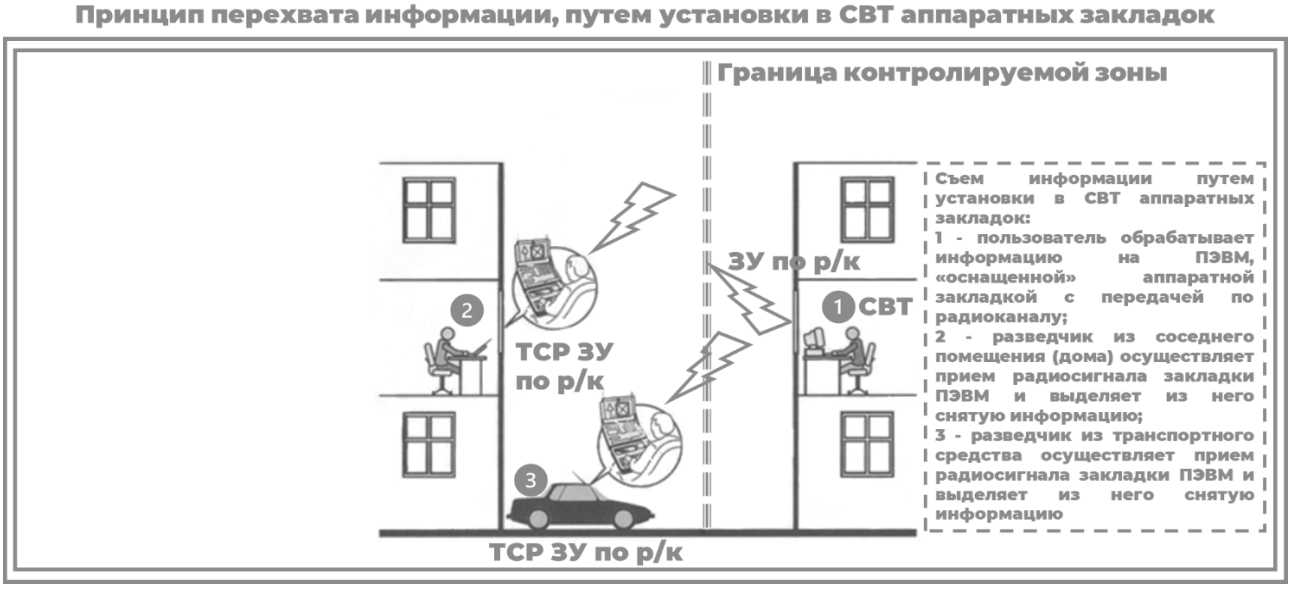


Рис. 19.

Мы закончили краткое ознакомление с электрическими техническими каналами утечки информации и переходим к третьему типу каналов утечки, которые в теории защиты информации получили название параметрических ТКУИ. Параметрические каналы относятся к категории специально создаваемых ТКУИ.

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 возможно применение импульсных сигналов.

При переизлучении параметры исходного облучающего сигнала изменяются модулирующими информационными сигналами ОТСС. Поэтому данные каналы утечки информации часто называют параметрическими.

Для перехвата информации по данным каналам необходимы специальные высокочастотные генераторы с антеннами, имеющими узкие диаграммы направленности и специальные радиоприемные устройства. Структурная схема параметрического ТКУИ, создаваемого методом высокочастотного облучения СВТ, представлена на рис. 20.

Рис. 20.

Принцип перехвата информации, обрабатываемой СВТ, методом высокочастотного облучения, представлен на рис. 21.

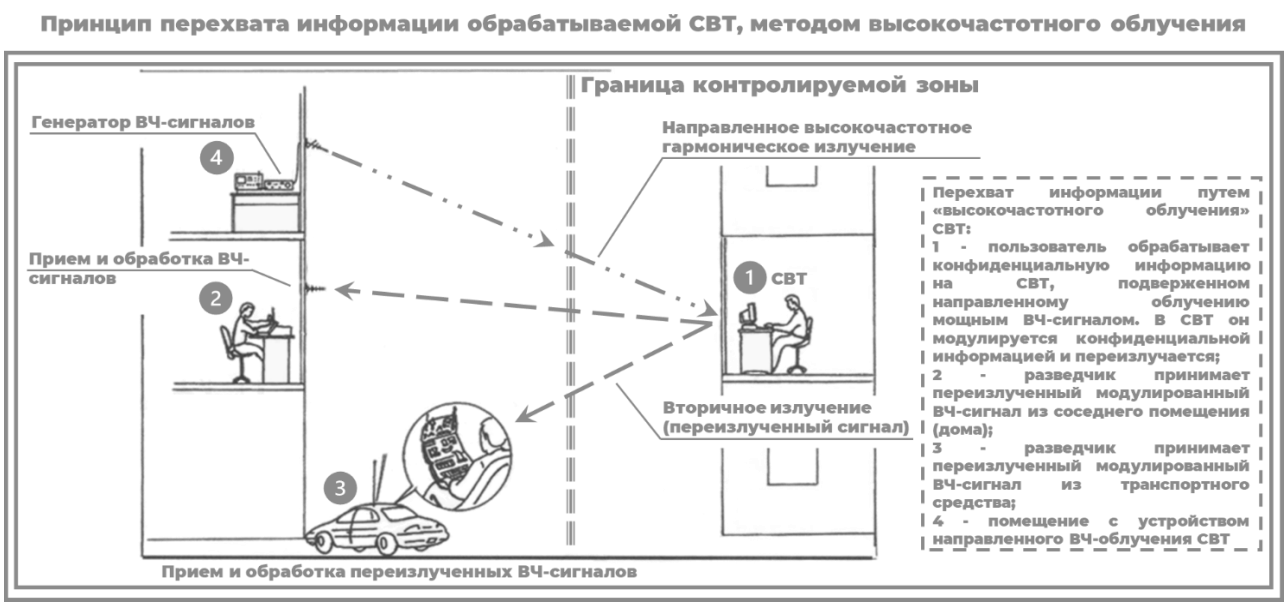


Рис. 21.

3. Технические каналы утечки информации при ее передаче по каналам связи

Информация после обработки в ОТСС может передаваться по каналам связи, где также возможен ее перехват.

При перехвате решаются следующие основные задачи:

– поиск в пространстве и по частоте сигналов с нужной информацией;

– 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.

В настоящее время для передачи информации используют в основном КВ, УКВ, радиорелейные, тропосферные и космические каналы связи, а также кабельные и волоконно-оптические линии связи. В зависимости от вида каналов связи технические каналы перехвата информации можно разделить на электромагнитные, электрические и индукционные. Классификация указанных каналов перехвата информации приведена на рис. 22.

Рис. 22.

Кратко охарактеризуем три выделенных вида каналов перехвата информации и начнем с **электромагнитного канала**.

Высокочастотные электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться портативными средствами радиоразведки и при необходимости передаваться в центр обработки для их раскодирования. Принцип перехвата информации, передаваемой по каналам радиосвязи, приведен на рис. 23.

Рис. 23.

Упрощенная структура типового комплекса средств перехвата приведена на рис. 24.

Рис. 24.

Типовой комплекс включает в себя: приемные антенны, радиоприемник, анализатор технических характеристик сигналов, радиопеленгатор, регистрирующее устройство.

Антенна предназначена для пространственной селекции и преобразования электромагнитной волны в электрические сигналы, амплитуда, частота и фаза которых соответствуют аналогичным характеристикам электромагнитной волны.

Радиоприемник служит для поиска и селекции радиосигналов по частоте, усиления и демодуляции (детектирования) выделенных сигналов, усиления и обработки демодулированных (первичных) сигналов: речевых, цифровых данных, видеосигналов и т. д.

Для анализа радиосигналов после частотной 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) или его координат.

Регистрирующее устройство обеспечивает запись сигналов для документирования и последующей обработки.

Данный канал перехвата информации наиболее широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или радиорелейным и спутниковым линиям связи.

Перейдем к рассмотрению **электрического канала перехвата информации**. Электрический канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение аппаратуры перехвата к кабельным линиям связи.

Подключение средства перехвата электрических сигналов к электрическим проводам кабеля может быть последовательным или параллельным. При последовательном подключении в разрыв провода линии включается элемент приемника перехвата – сопротивление, сигнал с которого усиливается и воспроизводится в форме, доступной для человека, анализа или записи на аудио- или видеоноситель. При параллельном способе средство перехвата подключается к проводам линии параллельно.

Наиболее простым средством перехвата сигнала с целью подслушивания речевой информации в телефонных линиях связи является телефонная трубка, которая

подключается к проводам со снятой изоляцией телефонной линии с помощью контактов типа «крокодил».

Принцип перехвата информации по электрическому каналу приведен на рис. 25.

Рис. 25.

Электрический канал наиболее часто используется для перехвата телефонных разговоров. Устройства, подключаемые к телефонным линиям связи и совмещенные с устройствами передачи информации по радиоканалу, обычно называют телефонными закладками.

Мы закончили рассмотрение электрического канала перехвата информации, и теперь перейдем к краткой характеристике следующего вида каналов, а именно **индукционного**.

В случае применения сигнальных устройств контроля целостности линии связи, факт контактного подключения к ней аппаратуры разведки будет обнаружен. Поэтому спецслужбы наиболее часто используют индукционный канал перехвата информации, не требующий подключения к каналам связи. В данном канале используется эффект возникновения вокруг кабеля связи электромагнитного поля при прохождении по нему информационных электрических сигналов, которые перехватываются специальными индукционными датчиками (см. рис. 25).

Бесконтактные средства подключения (датчики) перехватывают сигналы, которые излучают провода при протекании по ним электрического тока. В этом случае средства перехвата не отбирают у сигналов энергию и обнаруживаются существенно хуже, только по изменению индуктивности и емкости линии за счёт своих индуктивности и емкости, а также по изменению волнового сопротивления линии.

4. Технические каналы утечки акустической информации: воздушные, вибрационные, параметрические, электроакустические, оптико-электронные

Под акустической понимается информация, носителем которой являются акустические сигналы. Если источник информации – человеческая речь, акустическая информация называется речевой.

Совершенно очевидно, что наивысшую ценность представляет информация, передаваемая устно. Это объясняется рядом специфических особенностей, свойственных речи. Устно сообщают сведения, которые не могут быть доверены техническим средствам передачи. Информация, полученная в момент ее озвучивания, является самой оперативной. Живая речь, несущая эмоциональную окраску личностного отношения к сообщению, позволяет составить психологический портрет человека. Кроме того, современные методы дают возможность однозначно идентифицировать личность говорящего.

Эти особенности объясняют неослабевающий интерес противоборствующих сторон к непосредственному прослушиванию речи, циркулирующей в помещениях, по виброакустическому и акустическому (воздуховоды, окна, потолки, трубопроводы) каналам. Поэтому при решении вопросов по защите от утечки информации по техническим каналам защите речевой информации уделяется первоочередное внимание.

Акустический сигнал представляет собой возмущения упругой среды, проявляющиеся в возникновении акустических колебаний различной формы и длительности. Механические колебания частиц упругой среды, распространяющиеся от источника колебаний в окружающее пространство в виде волн различной длины, называются акустическими.

В зависимости от формы акустических колебаний различают тональные и сложные сигналы. Тональный – это сигнал, вызываемый колебанием, совершающимся по синусоидальному закону. Сложный сигнал включает в себя целый спектр гармонических составляющих.

Речевой сигнал является сложным акустическим сигналом в диапазоне частот от 200–300 Гц до 4–6 кГц.

Теперь давайте перейдем непосредственно к техническим каналам утечки акустической информации (ТКУАИ). В данном случае под каналом утечки информации понимают совокупность объекта разведки (выделенного помещения), технического средства акустической (речевой) разведки (ТСАР), с помощью которого перехватывается речевая информация, и физической среды, в которой распространяется информационный сигнал.

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, виброакустические, электроакустические, оптико-электронные и параметрические (см. табл. 2).

Таблица 2

Тип канала	**Каналы утечки**
Воздушные	1. Перехват акустических сигналов микрофонами в комплексе с портативными звукозаписывающими устройствами. 2. Перехват акустических сигналов направленными микрофонами.

	3. Перехват акустических сигналов в комплексе с устройствами передачи информации по радиоканалу. 4. Перехват акустических сигналов микрофонами в комплексе с устройствами передачи информации по сети электропитания. 5. Перехват акустических сигналов микрофонами в комплексе с устройствами передачи информации по телефонной линии. 6. Перехват акустических сигналов микрофонами в комплексе с устройствами их подключения к телефонной линии по сигналам вызова от внешнего телефонного абонента. 7. Перехват акустических сигналов микрофонами в комплексе с устройствами передачи информации по трубам водоснабжения, отопления, металлоконструкциям.
Виброакустические	1. Перехват акустических сигналов электронными стетоскопами. 2. Перехват акустических сигналов стетоскопами в комплексе с устройствами передачи информации по оптическому каналу в ИК-диапазоне. 3. Перехват акустических сигналов стетоскопами в комплексе с устройствами передачи информации по трубам водоснабжения, отопления, металлоконструкциям.
Параметрические	1. Перехват акустических сигналов путем приема и детектирования побочных ЭМИ ОТСС и ВТСС, модулированных информационным сигналом. 2. Перехват акустических сигналов путем высокочастотного облучения специальных полуактивных закладных устройств.
Оптико-электронный	Перехват акустических сигналов путем лазерного зондирования оконных стекол.
Электроакустические	1. Перехват акустических колебаний через ВТСС, обладающих микрофонным эффектом путем подключения к их соединительным линиям. 2. Перехват акустических колебаний через ВТСС путем высокочастотного навязывания.

Первая группа акустических каналов, которую мы рассмотрим, получила название **воздушных технических каналов утечки информации**. В такого рода каналах утечки средой распространения акустических сигналов является воздух, и для их перехвата используются миниатюрные высокочувствительные и специальные направленные микрофоны. Схемы воздушных технических каналов утечки информации показаны на рис. 25–30.

Миниатюрные микрофоны объединяются с портативными звукозаписывающими устройствами (диктофонами) или специальными миниатюрными передатчиками. Автономные устройства, конструкционно объединяющие миниатюрные микрофоны и передатчики, называют закладными устройствами перехвата речевой информации, или акустическими закладками.

Перехваченная закладными 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 закладными устройствами, осуществляется, как правило, на специальные приемные устройства, работающие в соответствующем диапазоне длин волн. Однако встречаются закладные устройства, принимать информацию с которых можно 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 конструкционно объединяет миниатюрный микрофон и специальный блок коммутации и обычно 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.

Перехват акустических сигналов микрофонами, комплексированными с портативными устройствами звукозаписи

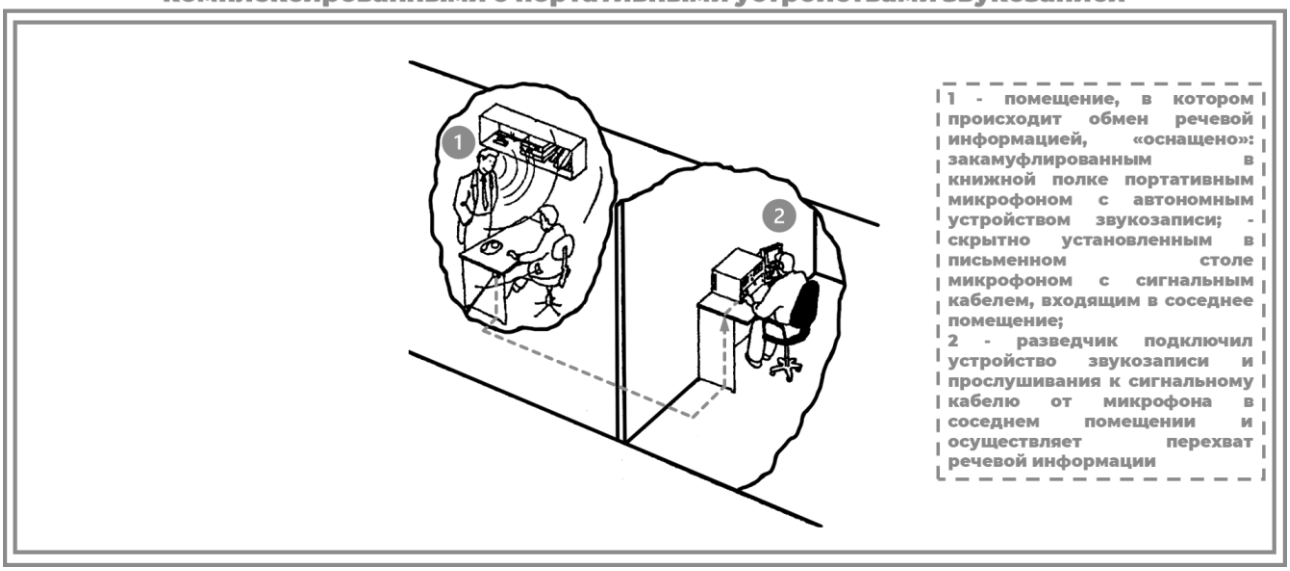


Рис. 26.

Перехват акустических сигналов направленными микрофонами

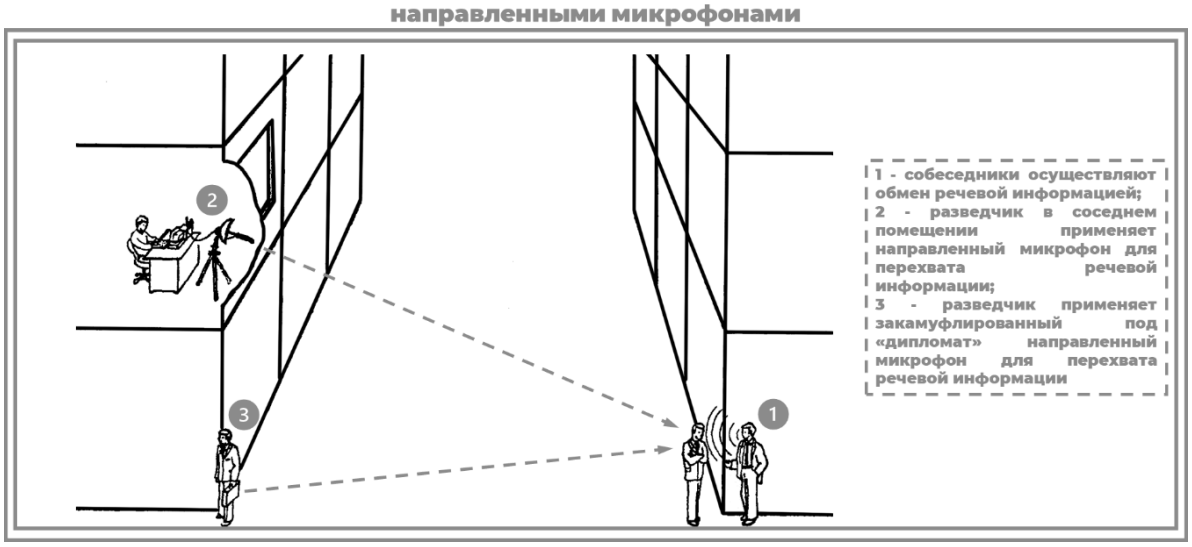


Рис. 27.

Перехват акустических сигналов микрофонами, комплексированными с устройствами передачи информации по радиоканалу

Рис. 28.

Перехват акустических сигналов микрофонами (в том числе контактными), комплексированными с устройствами передачи информации по оптическому каналу

Рис. 29.

Рис. 30.

Рис. 31.

Теперь давайте перейдем к краткой характеристике **второй группы каналов утечки акустической информации, а именно к виброакустических каналов.**

В виброакустических (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). Схемы виброакустических технических каналов утечки информации представлены на рис. 31 и 32.

Контактные микрофоны, соединенные с электронным усилителем, называют электронными стетоскопами.

По виброакустическому каналу также возможен перехват информации с использованием закладных устройств. В основном для передачи информации используется радиоканал, поэтому такие устройства часто называют радиостетоскопами.

Возможно использование закладных устройств с передачей информации по оптическому каналу в ближнем инфракрасном диапазоне длин волн, а также по ультразвуковому каналу (по металлоконструкциям здания).

Рис. 32.

Рис. 33.

Третья группа акустических каналов утечки информации имеет название электроакустических (или акустоэлектрических).

Электроакустические технические каналы утечки информации возникают за счет электроакустических преобразований акустических сигналов в электрические и включают перехват электроакустических сигналов из ВТСС, обладающих собственным «микрофонным эффектом» (рис. 34), а также получивших его путем «высокочастотного навязывания» (рис. 35).

Некоторые элементы ВТСС, в том числе трансформаторы, катушки индуктивности, электромагниты звонков телефонных аппаратов, дроссели ламп дневного

света, электрореле 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.

Рис. 34.

Рис. 35.

ВТСС кроме указанных элементов могут содержать непосредственно электроакустические преобразователи. К таким ВТСС относятся некоторые типы датчиков охранной и пожарной сигнализации, громкоговорители ретрансляционной сети и т. д. Эффект акустоэлектрического преобразования в специальной литературе называют «микрофонным эффектом». Причем из ВТСС, обладающих «микрофонным эф-

фектом», наибольшую чувствительность к акустическому полю имеют абонентские громкоговорители и некоторые датчики пожарной сигнализации.

Перехват электроакустических колебаний в данном канале утечки информации осуществляется путем непосредственного подключения к соединительным линиям ВТСС специальных высокочувствительных низкочастотных усилителей. Например, подключая такие средства к соединительным линиям телефонных аппаратов с электромеханическими вызывными звонками, можно прослушивать разговоры, ведущиеся в помещениях, где установлены эти аппараты.

Технический канал утечки информации путем «высокочастотного навязывания» может быть осуществлен несанкционированным контактным введением токов высокой частоты от соответствующего генератора в линии (цепи), имеющей 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 применяются специальные приемники с достаточно высокой чувствительностью. Для исключения влияния зондирующего и переотраженного сигналов могут использоваться импульсные сигналы «высокочастотного навязывания».

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.

Теперь рассмотрим четвертый вид каналов утечки акустической информации. Он называется оптико-электронным каналом.

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. п.). 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 (рис. 36). Причем лазерные приемники 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.

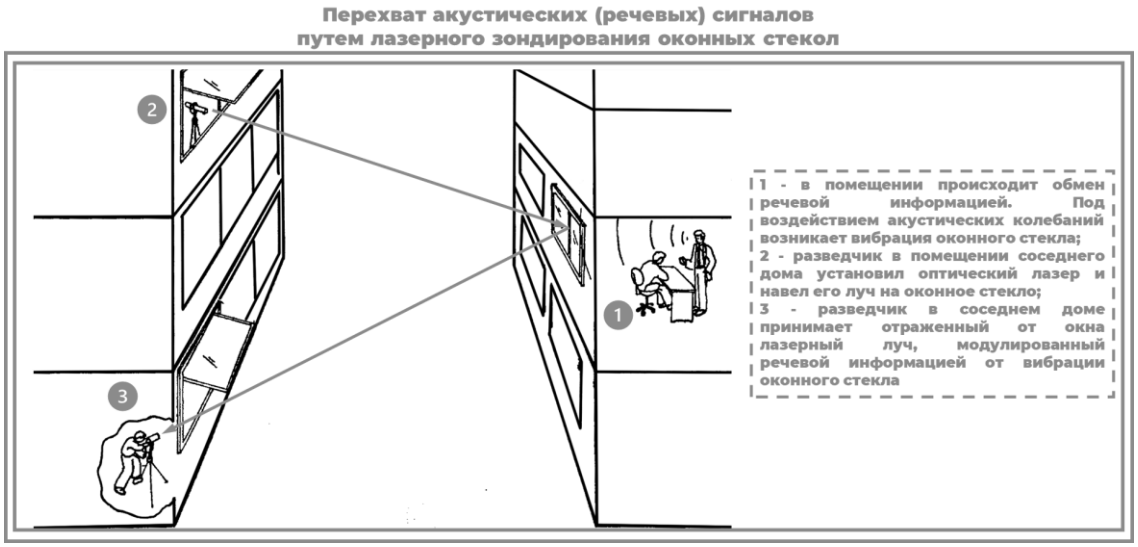


Рис. 36.

Перейдем к рассмотрению следующего и последнего вида каналов утечки акустической информации – параметрического.

В результате воздействия акустического сигнала 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 собственных высокочастотных сигналов ОТСС и ВТСС, например, к модуляции воздействующим информационным акустическим сигналом.

Поэтому такой 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, изменению его емкости, что, в свою очередь, также приводит к частотной модуляции высокочастотного сигнала генератора. Промодулированные информационным сигналом высокочастотные колебания излучаются в окружающее пространство и могут быть перехвачены и детектированы средствами радиоразведки (рис. 37).

Рис. 37.

Параметрический канал утечки информации может быть реализован и путем «высокочастотного облучения» помещения, где установлены полуактивные переизлучающие закладные устройства, имеющие элементы, некоторые параметры которых изменяются по закону изменения воздействующего акустического (речевого) сигнала (рис. 38).

При облучении мощным высокочастотным сигналом помещения, в котором установлено такое закладное устройство, в последнем при взаимодействии облучающего электромагнитного поля со специальными элементами закладки происходит образование вторичных радиоволн, т. е. переизлучение электромагнитного поля. Специальное устройство в закладке обеспечивает амплитудную, фазовую или частотную модуляцию переизлученного сигнала под воздействием акустической волны речевого сигнала. Подобного вида закладки иногда называют полуактивными.

Для перехвата информации по данному каналу кроме закладного устройства необходимы специальный передатчик с направленным излучением и приемник.

Рис. 38.

5. Технические каналы утечки видеоинформации

Наряду с информацией, обрабатываемой в ТСПИ, и речевой информацией важную роль играет видовая (оптическая) информация, получаемая техническими средствами перехвата в виде изображений объектов или документов.

В зависимости от характера информации можно выделить следующие способы ее получения:

– наблюдение за объектами;

– съемка объектов;

– съемка (снятие копий) документов.

Классификация способов скрытого видеонаблюдения и съемки приведена в табл. 3.

Таблица 3

Вид канала утечки	Время суток	Способ реализации
Наблюдение за объектами	День	Наблюдение за объектами с использованием оптических приборов (монокуляров, подзорных труб, биноклей, телескопов)
		Наблюдение за объектами с использованием телевизионных систем, в т. ч. комплексированных с устройствами передачи изображений по радиоканалу
	Ночь	Наблюдение за объектами с использованием приборов ночного видения
		Наблюдение за объектами с использованием телевизионных систем, в т. ч. комплексированных с приборами ночного видения
		Наблюдение за объектами с использованием телевизионных систем
Съемка объектов	День	Съемка объектов с использованием фотоаппаратов
		Съемка объектов с использованием телевизионных систем, комплексированных с портативными устройствами видеозаписи или передачи изображения по радиоканалу
	Ночь	Съемка объектов с использованием фотоаппаратов, комплексированных приборами ночного видения
		Съемка объектов с использованием телевизионных систем, в т. ч. комплексированных с приборами ночного видения и портативными устройствами видеозаписи или передачи изображения по радиоканалу
		Съемка объектов с использованием телевизионных систем, комплексированных с портативными устройствами видеозаписи
Съемка (снятие копий) документов	В любое время	Съемка (снятие копий) документов с использованием портативных (в т. ч. камуфлированных) фотоаппаратов

В общем случае источником оптического сигнала является объект наблюдения, который излучает сигнал или переотражает свет другого, внешнего источника.

Кратко охарактеризуемканалы утечки, то есть те способы, которые позволяют несанкционированно получить видовую информацию.

1. Наблюдение за объектами.

В зависимости от условий наблюдения и освещения для наблюдения за объектами могут использоваться различные технические средства: днем – оптические приборы (монокуляры, подзорные трубы, бинокли, телескопы и т. д.), телевизионные камеры; ночью – приборы ночного видения, телевизионные камеры, тепловизоры.

Так как физическая природа носителя информации в видимом и инфракрасном диапазонах одинакова, то различные средства наблюдения, применяемые для добывания информации в этом диапазоне, имеют достаточно общую структуру, которая включает в себя внешний источник света, объект наблюдения (источник сигнала), среду распространения, оптический приемник и воздействующую на сигнал помеху.

Большинство средств наблюдения представляют собой оптический приемник, содержащий оптическую систему, светоэлектрический элемент, усилитель и индикатор. В зависимости от вида светочувствительного элемента оптические приборы делят на визуально-оптические, фотографические и оптико-электронные. В визуально-оптических средствах наблюдения светочувствительным элементом является сетчатка глаза человека, в традиционных фото- и киноаппаратах – фотопленка, а в оптико-электронных приборах – мишень светоэлектрического преобразователя (СЭП).

Для наблюдения с большого расстояния используются средства с длиннофокусными оптическими системами, а при наблюдении с близкого расстояния – камуфлированные скрытно установленные телевизионные камеры. При этом изображение с телевизионных камер может передаваться на мониторы, как по кабелю, так и по радиоканалу.

2. Съемка объектов.

Съемка объектов проводится для документирования результатов наблюдения и более подробного изучения объектов. Для съемки объектов используются телевизионные и фотографические средства.

При съемке объектов, так же, как и при наблюдении за ними, использование тех или иных технических средств обусловлено условиями съемки и временем суток. Для съемки объектов днем с большого расстояния используются фотоаппараты и телевизионные камеры с длиннофокусными объективами или совмещенные с телескопами.

Для съемки объектов днем с близкого расстояния применяются портативные камуфлированные фотоаппараты и телекамеры, совмещенные с устройствами видеозаписи или передачи изображений по радиоканалу.

Съемка объектов ночью проводится, как правило, с близкого расстояния. Для этих целей используются портативные фотоаппараты и телевизионные камеры, совмещенные с приборами ночного видения, или тепловизоры, а также портативные закамуфлированные телевизионные камеры высокой чувствительности, совмещенные с устройствами передачи информации по радиоканалу.

Съемка документов осуществляется, как правило, с использованием портативных фотоаппаратов.

Вопросы и задания для самоконтроля

1. Дайте определение технического канала утечки информации.
2. Назовите характеристики и дайте классификацию каналов утечки информации.
3. Дайте определение основным и вспомогательным техническим средствам и системам (ОТСС и ВТСС). Определите ключевое различие между этими системами.
4. Дайте определение понятиям «контролируемая зона (КЗ)», «опасная зона 1 (зона R1)», «опасная зона 2 (зона R2)».
5. Дайте определение понятию «случайная антенна». Укажите, что может пониматься как сосредоточенная случайная антенна, а что – как распределенная случайная антенна?
6. Сформулируйте понятие опасного сигнала, назовите и охарактеризуйте основные виды опасных сигналов.
7. Перечислите основные источники опасных сигналов.
8. Назовите основные виды каналов утечки информации, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации (ТСПИ).
9. Объясните физическую сущность возникновения побочных электромагнитных излучений (ПЭМИ).
10. Назовите и охарактеризуйте основные виды каналов утечки акустической информации.
11. Назовите и охарактеризуйте основные электромагнитные технические каналы утечки информации (ТКУИ).
12. Назовите и охарактеризуйте основные электрические ТКУИ.
13. Как создаются составные каналы утечки информации?
14. Метод «высокочастотного навязывания»: как и в каком виде ТКУИ реализуется.
15. Метод «высокочастотного облучения»: как и в каком виде ТКУИ реализуется.
16. Использование лазерного луча является реализацией какого ТКУИ? Как именно осуществляется доступ злоумышленника к защищаемой информации с использованием лазерного луча?

Лекция 5. Основы криптографической защиты информации[1]

Проблема защиты информации путем преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с древних времен. История криптографии – ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. Классическим примером являются, например, священные книги Древнего Египта, Древней Индии и других народов.

Криптографические методы защиты информации – это специальные методы шифрования, кодирования или иного преобразования информации, в результате которого ее содержание становится недоступным для посторонних лиц без предъявления ключа криптограммы и обратного преобразования. Криптографический метод защиты, безусловно, самый надежный метод защиты, так как охраняется непосредственно сама информация, а не доступ к ней (например, зашифрованный файл нельзя прочесть даже в случае кражи носителя). Данный метод защиты информации реализуется в виде программ или пакетов программ.

Актуальность темы лекции совершенно очевидна, т. к. информация в современном обществе представляет собой одну из высших ценностей, требующую защиты от несанкционированного доступа посторонних лиц, а известное выражение, авторство которого приписывают банкиру, основателю одноименной династии, Натану Майеру Ротшильду – «кто владеет информацией, тот владеет миром», на сегодняшний день становится актуальной как никогда.

1. Роль криптографии в глобальной задаче защиты коммуникаций. Криптология, криптография, криптоанализ

Криптография (греч. kryptos – тайный, скрытый и graho – пишу) – наука о методах защиты информации на основе ее преобразования с помощью различных шифров и сохранением достоверности семантического содержания. Криптография также представляет собой отрасль науки палеографии (а также египтологии), изучающей графику систем тайнописи. Исходя из современных позиций теории передачи информации и теории кодирования, криптография определяется как отрасль научных знаний о методах обеспечения секретности и достоверности данных при передаче по каналам связи и хранении в устройствах оперативной и долговременной памяти.

Криптография является одной из трех составных частей криптологии (kryptos – тайный, logos – наука) – науки о передаче информации в виде, защищенном от не-

[1] В данной лекции использованы следующие материалы: *Бахаров Л. Е.* Информационная безопасность и защита информации (разделы криптография и стеганография): практикум. М.: Изд. дом МИСиС, 2019*; Фороузан Б. А.* Управление ключами шифрования и безопасность сети: курс лекций. М.: Интуит НОУ, 2016; *Его же.* Криптография и безопасность сетей: учеб. пособие. М.: Интернет-Университет Информ. Технологий: БИНОМ. Лаб. знаний, 2010; Руководство по безопасности в Lotus Notes: курс: учеб. пособие. М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2008; *Салий В. Н.* Криптографические методы и средства защиты информации: учеб. пособие. Саратов: СГУ, 2017; *Сухов А. Н.* Реальная социальная психология: учеб.-метод. пособие. М.: Моск. психолого-социальный ин-т, 2004; *Шолин И. М.* Алгоритм переносной шифровальной машины Энигма // Форум молодых ученых. 2018. № 10 (26). С. 1352–1356.

санкционированного доступа. Криптография, как было сказано, занимается шифрованием и дешифрованием сообщений с помощью секретных ключей.

Другая часть криптологии (с прямо противоположными целями) – криптоанализ (греч. kryptos – тайный, скрытый и analysis – разложение) – представляет собой теорию и практику извлечения информации из криптограммы без использования ключа. Основной принцип криптоанализа сформулировал один из его основоположников, английский криптолог нидерландского происхождения Огюст Керкгоффс (1835–1903) в 1883 году в книге «Военная криптография»: «При оценке надежности шифра следует допустить, что противнику известно о нем все, кроме ключа».

Третья часть криптологии – аутентификация – объединяет в себе совокупность приемов, позволяющих проверять подлинность источника информации и полученных сообщений.

Изначально криптография изучала методы шифрования информации – обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или ключа в шифрованный текст (шифротекст). Современная криптография включает в себя четыре крупных раздела:

– симметричные криптосистемы;

– криптосистемы с открытым ключом;

– системы электронной подписи;

– управление ключами.

В криптографии используется определенная терминология, при этом нужно понимать, что в качестве информации, подлежащей шифрованию и дешифрованию, рассматриваются тексты, построенные на некотором алфавите.

Алфавит – конечное множество используемых для кодирования информации знаков.

Текст – упорядоченный набор из элементов алфавита, например, 32 буквы русского алфавита и пробел.

Шифрование – преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом.

Дешифрование – обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

Ключ – информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

Криптографическая система представляет собой семейство T [T1, T2, ... Tk] преобразований открытого текста. Члены этого семейства индексируются, или обозначаются символом k; параметр k является ключом. Пространство ключей К – это набор возможных значений ключа. Обычно ключ представляет собой последовательный ряд символов (букв алфавита). Криптосистемы разделяются на симметричные и с открытым ключом.

В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ.

В системах с открытым ключом используются два ключа – открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Термины **распределение ключей** и **управление ключами** относятся к процессам системы обработки информации, содержанием которых является составление и распределение ключей между пользователями.

Электронной (цифровой) подписью называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т. е. криптоанализу). Имеется несколько показателей криптостойкости, среди которых: количество всех возможных ключей и среднее время, необходимое для криптоанализа.

Преобразование Tk определяется соответствующим алгоритмом и значением параметра k. Эффективность шифрования с целью защиты информации зависит от сохранения тайны ключа и криптостойкости шифра.

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: достаточно высокая производительность, простота, защищенность и т. д. Программная реализация, в свою очередь, более практична, допускает известную гибкость в использовании.

Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:

– зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

– число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного сообщения и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;

– число операций, необходимых для расшифровывания информации путем перебора всевозможных ключей, должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютеров (с учетом возможности использования сетевых вычислений);

– знание алгоритма шифрования не должно влиять на надежность защиты;

– незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения даже при использовании одного и того же ключа;

– структурные элементы алгоритма шифрования должны быть неизменными;

– дополнительные биты, вводимые в сообщение в процессе шифрования, должен быть полностью и надежно скрыты в шифрованном тексте;

– длина шифрованного текста должна быть равной длине исходного текста;

– не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования;

– любой ключ из множества возможных должен обеспечивать надежную защиту информации;

– алгоритм должен допускать как программную, гак и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрования.

Пробуждение значительного интереса к криптографии и ее развитие началось с XIX века, что связано с зарождением электросвязи. В XX столетии секретные службы большинства развитых стран стали относится к этой дисциплине как к обязательному инструменту своей деятельности. Наряду с развитием криптографических систем совершенствовались и методы, позволяющие восстанавливать исходное сообщение, исходя только из шифртекста (криптоанализ). Успехи криптоанализа приводили к ужесточению требований к криптографическим алгоритмам.

Уже упоминавшийся нами Огюст Керкгоффс впервые сформулировал правило: стойкость шифра, т. е. криптосистемы как набора процедур, управляемых некоторой секретной информацией небольшого объема, должна быть обеспечена в том случае, когда криптоаналитику противника известен весь механизм шифрования за исключением секретного ключа – информации, управляющей процессом криптографических преобразований. Видимо, одной из задач этого требования было осознание необходимости испытания разрабатываемых криптосхем в условиях более жестких по сравнению с условиями, в которых мог бы действовать потенциальный нарушитель. Это правило стимулировало появление более качественных шифрующих алгоритмов. Можно сказать, что в нем содержится первый элемент стандартизации в области криптографии, поскольку предполагается разработка открытых способов преобразований. В настоящее время это правило интерпретируется более широко: все долговременные элементы системы защиты должны предполагаться известными потенциальному злоумышленнику. В последнюю формулировку криптосистемы входят как частный случай систем защиты. В этой формулировке предполагается, что все элементы систем защиты подразделяются на две категории – долговременные и легко сменяемые. К долговременным элементам относятся те элементы, которые относятся к разработке систем защиты и для изменения требуют вмешательства специалистов или разработчиков. К легко сменяемым элементам относятся элементы системы, которые предназначены для произвольного модифицирования или модифицирования по заранее заданному правилу, исходя из случайно выбираемых начальных параметров. К легко сменяемым элементам относятся, например, ключ, пароль, идентификатор и т. п. Рассматриваемое правило отражает тот факт, что надлежащий уровень секретности может быть обеспечен только по отношению к легко сменяемым элементам.

Подведем итог сказанномувыше и определим, как применяется криптография в настоящее время. Значение криптографии выходит далеко за рамки обеспечения секретности данных. По мере все большей автоматизации процессов передачи и обработки информации и интенсификации информационных потоков ее методы приобретают уникальное значение. Если говорить о тех задачах, для решения которых может применяться (и применяется) криптография в настоящее время, то их будет достаточно большое количество. Выделим только основные, наиболее важные задачи криптографии:

1. Обеспечение конфиденциальности данных (предотвращение несанкционированного доступа к данным). Это одна из основных задач криптографии, для ее решения применяется шифрование данных, т. е. такое их преобразование, при котором прочитать их могут только законные пользователи, обладающие соответствующим ключом

2. Обеспечение целостности данных – гарантии того, что при передаче или хранении данные не были модифицированы пользователем, не имеющим на это права. Под модификацией понимается вставка, удаление или подмена информации, а также повторная пересылка перехваченного ранее текста.

3. Обеспечение аутентификации. Под аутентификацией понимается проверка подлинности субъектов (сторон при обмене данными, автора документов, и т. д.) или подлинности самой информации. Во многих случаях субъект X должен не просто доказать свои права, но сделать это так, чтобы проверяющий субъект (Y) не смог впоследствии сам использовать полученную информацию для того, чтобы выдать себя за X. Подобные доказательства называются «доказательствами с нулевым разглашением».

Обеспечение невозможности отказа от авторства, то есть предотвращение возможности отказа субъектов от совершенных ими действий (обычно – невозможности отказа от подписи под документом). Эта задача неотделима от другой задачи, а именно от обеспечения невозможности приписывания авторства. Наиболее яркий пример ситуации, в которой стоит такая задача – подписание договора двумя или большим количеством лиц, не доверяющих друг другу. В такой ситуации все подписывающие стороны должны быть уверены в том, что в будущем, во-первых, ни один из подписавших не сможет отказаться от своей подписи и, во-вторых, никто не сможет модифицировать, подменить или создать новый документ (договор) и утверждать, что именно этот документ был подписан. Основным способом решения данной проблемы является использование цифровой подписи.

2. Исторические примеры шифрования: шифр Сциталя, шифр Цезаря, шифр Виженера, EnigmaMachine. Подстановочные, перестановочные, многоалфавитные шифры

За всю историю человечества было изобретено огромное количество шифров. Однако внимательное изучение показало, что подавляющее их число укладывается во вполне обозримое множество теоретических схем, важнейшие из которых будут рассмотрены нами в рамках изучения данного учебного вопроса лекции.

1. Перестановочные шифры.

Шифр называется перестановочным, если все связанные с ним криптограммы получаются из соответствующих открытых текстов перестановкой букв. Способ, каким при шифровании переставляются буквы открытого текста, и является ключом шифра. Как запомнить (и передать другому лицу) выбранный способ перестановки? Рассмотрим два широко распространенных метода.

а) маршрутное шифрование.

Этот способ шифрования изобрел выдающийся французский математик и криптограф Франсуа Виет (1540–1603). Пусть m и n – некоторые натуральные (т. е. целые положительные) числа, каждое больше 1. Открытый текст последовательно разбивается на части (блоки) с длиной, равной произведению mn (если в последнем блоке не хватает букв, можно дописать до нужной длины произвольный их набор). Блок вписывается построчно в таблицу размерности m×n (т. е. m строк и n столбцов). Криптограмма получается выписыванием букв из таблицы в соответствии с некоторым маршрутом. Этот маршрут вместе с числами m и n составляет ключ

шифра. Чаще всего буквы выписывают по столбцам, которые упорядочиваются в соответствии с паролем: под таблицей подписывается слово, состоящее из n неповторяющихся букв, и столбцы таблицы нумеруются по алфавитному порядку букв пароля. Например, для шифрования открытого текста, выражающего один из главных принципов криптологии: «нельзя недооценивать противника», добавим к его 29 буквам еще одну, скажем а, возьмем m=5, n=6, впишем текст в таблицу 5×6 и выберем в качестве пароля слово «пароль» (рис. 39):

н	е	л	ь	з	я
н	е	д	о	о	ц
е	н	и	в	а	т
ь	п	р	о	т	и
в	н	и	к	а	а
п	а	р	о	л	ь

Рис. 39.

Выписывая теперь буквы по столбцам в соответствии с алфавитным порядком букв в пароле, получаем следующую криптограмму: ЕЕНПНЗОАТАЬОВОКННЕЬВЛДИРИЯЦТИА (истинные пробелы в криптографии не выставляются).

Рассмотренный способ шифрования (столбцовая перестановка) в годы первой мировой войны использовала легендарная немецкая шпионка Мата Хари;

b) шифрование с помощью решеток.

Этот способ шифрования предложил в 1881 году австрийский криптограф Эдуард Флейснер.

Выбирается натуральное число k>1, и квадрат размерности k×k построчно заполняется числами 1, 2, …, k^2. Для примера возьмем k = 2. Квадрат поворачивается по часовой стрелке на 90° и размещается вплотную к предыдущему квадрату. Аналогичные действия совершаются еще два раза, так чтобы в результате из четырех малых квадратов образовался один большой с длиной стороны 2k (рис. 40).

1	2	3	1
3	4	4	2
2	4	4	3
1	3	2	1

Рис. 40.

Далее из большого квадрата вырезаются клетки с числами от 1 до k^2, для каждого числа одна клетка. Процесс шифрования происходит следующим образом. Сделанная решетка (квадрат с прорезями) накладывается на чистый квадрат 2k×2k и в прорези по строчкам (т. е. слева направо и сверху вниз) вписываются первые буквы открытого текста. Затем решетка поворачивается на 90° по часовой стрелке и накладывается на частично заполненный квадрат, вписывание продолжается. После третьего поворота, наложения и вписывания все клетки квадрата будут заполнены.

Правило выбора прорезей гарантирует, что при заполнении квадрата буква на букву никогда не попадет. Из заполненного квадрата буквы можно выписать по столбцам, выбрав подходящий пароль. Например, с использованием изображенной выше решетки и пароля «шифр» открытый текст «договор подписали» переводится в криптограмму за пять шагов (рис. 41):

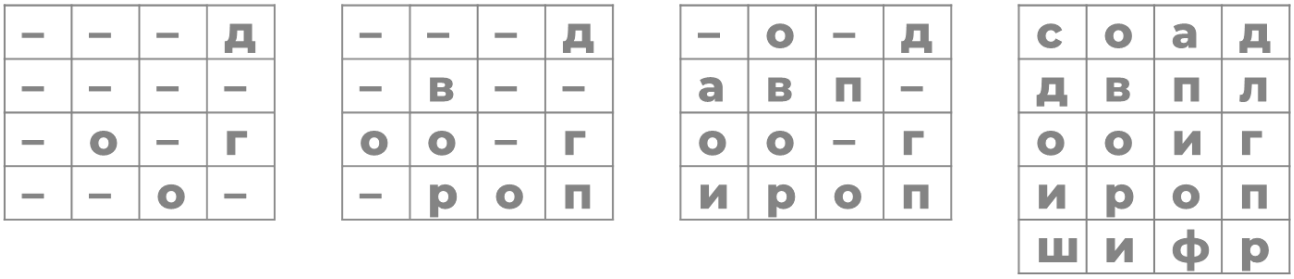


Рис. 41.

Итоговая криптограмма: ОВОРДЛГПАПИОСДОИ.

Шифрование с помощью решеток в первой половине 1917 года германская армия использовала на Восточном (против России) фронте. В 1982 году его применяли британские войска в вооруженном конфликте с Аргентиной за Фолклендские острова.

2. Подстановочные шифры (шифры замены).

Класс шифров замены выделяется тем свойством, что для получения криптограммы отдельные символы или группы символов исходного алфавита заменяются символами или группами символов шифроалфавита. В шифре простой замены происходит замена буквы на букву, т. е. устанавливается попарное соответствие символов исходного алфавита с символами шифроалфавита. Например, в рассказе Эдгара По «Золотой жук» пиратский капитан Кидд в своей шифровке вместо букв a, b, c, d, e, f, g, h, i писал соответственно 5, 2, -, +, 8, 1, 3, 4, 6, 0, 9. В «Пляшущих человечках» Артура Конан-Дойла бандит Слени использовал шифр, где буквы заменялись схематическими человеческими фигурками в разных позах.

Одним из древнейших вариантов практической реализации подобного шифрования можно уверенно называть шифр Сцитала. Сцитала или иногда говорят Скитала (от греч. «жезл») – инструмент, используемый для осуществления перестановочного шифрования, в криптографии известный также как шифр Древней Спарты. Представляет собой цилиндр и узкую полоску пергамента, на которой писалось сообщение, обматывавшуюся вокруг него по спирали. Античные греки и спартанцы, предположительно, использовали этот шифр для обмена сообщениями во время военных кампаний.

Для шифрования сообщения использовались пергаментная лента и палочка цилиндрической формы с фиксированной длиной и диаметром. Пергаментная лента

наматывалась на палочку так, чтобы не было ни просветов, ни нахлёстов. Написание сообщения производилось по намотанной пергаментной ленте по длинной стороне цилиндра. После того, как достигался конец намотанной ленты, палочка поворачивалась на часть оборота и написание сообщения продолжалось. После разматывания ленты на ней оказывалось зашифрованное сообщение. Расшифрование выполнялась с использованием палочки таких же типоразмеров.

Сам процесс шифрования заключался в перестановке символов исходного текста в соответствии с длиной окружности палочки. Например, используется палочка, по длине окружности которой помещается 4 символа (число строк в таблице), а длина самой палочки позволяет записать 5 символов (число столбцов в таблице), исходный текст: «это шифр древней Спарты». Схематически это можно изобразить так (рис. 42):

Рис. 42.

После разматывания ленты шифротекст будет следующим «ЭФВПТРНАОДЕРШРЙТИЕСЫ».

В практической криптографии при создании шифра простой замены в качестве шифроалфавита берется исходный алфавит с измененным порядком букв (алфавитная перестановка). Чтобы запомнить новый порядок букв, перемешивание алфавита осуществляют с помощью пароля – слова или нескольких слов с неповторяющимися буквами. Шифровальная таблица состоит из двух строк. В первой записывается стандартный алфавит открытого текста, во второй же строке, начиная с некоторой позиции, размещается пароль (без пробелов, если они есть), а после его окончания перечисляются в обычном алфавитном порядке буквы, в пароль не вошедшие. Если начало пароля не совпадает с началом строки, процесс после ее завершения циклически продолжается с первой позиции. Ключом шифра служит пароль вместе с числом, указывающим место начальной буквы пароля. Например, таблица шифрования на ключе «7полярник» имеет вид (рис. 43):

а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
щ	ъ	ы	ь	э	ю	п	о	л	я	р	н	и	к	а	б	в	г	д	е	ё	ж	з	й	м	с	т	у	ф	х	ц	ч	ш

Рис. 43.

При шифровании каждая буква открытого текста заменяется на стоящую под ней букву. В рассматриваемом примере указание «никогда не рассекречивай открытый текст в его истинной формулировке» можно представить в виде криптограммы

КЛРАЬ ЭЩКЮВ ЩГГЮР ВЮМЛЫ ЩЯАДР ВФДФЯ ДЮРГД ЫЮЬАЛ ГДЛКК АЯЖАВ ИЕНЛВ АЫРЮУ.

Здесь, как это часто делается, текст разбит на пятибуквенные блоки, в конце, для завершенности, добавлена незначащая буква.

Криптоанализ шифров простой замены осуществляется с помощью частотных характеристик языка открытых текстов. Известно, что в русском тексте длиной 10.000 знаков буква О встречается в среднем 1047 раз, Е – 836, А – 808, Н – 723, И – 700, Т – 625, Р – 584, В – 569, С – 466. Поэтому, если в достаточно длинной криптограмме какая-то буква оказывается безусловным лидером по числу вхождений, есть основание предполагать, что она заменяет О. Блестящим примером частотного криптоанализа являются рассуждения Леграна, героя рассказа «Золотой жук», прочитавшего шифрованное указание о месте сокрытия пиратского клада, и выводы (в подлиннике) Шерлока Холмса в Деле Пляшущих Человечков. Заметим, что в английских текстах самыми частыми являются (в порядке убывания) буквы e, t, a, o, i, n, s, r.

Для увеличения стойкости подстановочных шифров используют различные методы, скрывающие частотные соотношения языка. Рассмотрим несколько известных приемов. Шифры названы историческими именами использовавших их агентов:

a) шифр «Дора» (рис. 44).

	1	2	3	4	5	6	7	8	9
4, 5, 6, 7, 8, 9,	a	s	i	n	t	o	e	r	
2, 3,	b	c	d	f	g	h	j	k	l
1,	m	p	q	u	v	w	x	y	z

Рис. 44.

Во второй строке таблицы записаны самые частые английские буквы (65 % всех букв в текстах) в виде мнемонической (для запоминания) фразы «asintoer(r)» – «грех ошибаться». Далее оставшиеся буквы перечисляются в алфавитном порядке с пропуском букв из второй строки. Заметим, что, за счет только изменения порядка букв во второй строке, можно получить 40320 различных таблиц. Шифрование производится заменой каждой буквы на двузначное число, составленное из номера строки и номера столбца, где находится эта буква. При этом буква может выступать в криптограмме в нескольких вариантах. Например, 41, 51, 61, 71, 81, 91 – образы одной и той же буквы а. Понятно, что, глядя на криптограмму, невозможно установить, как же в ней «спрятана» та или иная из самых частых букв;

b) шифр «Марк» (рис. 45).

	1	2	3	4	5	6	7	8	9	0
	с	е	н	о	в	а	л			
8	б	г	д	ж	з	и	й	к	м	п
9	р	т	у	ф	х	ц	ч	ш	щ	ъ
0	ы	ь	э	ю	я	.	/			

Рис. 45.

Буквы, стоящие во второй строке таблицы (они дают 45 % букв в русских текстах), при шифровании заменяются стоящими над ними цифрами, остальные буквы – двузначными числами «строка-столбец». Косая черта – знак начала и окончания числового массива в открытом тексте (цифры при шифровании сохраняются);

c) шифр «Рамзай» (рис. 46).

s	u	b	w	a	y
0	82	87	91	5	97
c	d	e	f	g	h
80	83	3	92	95	98
i	j	k	l	m	n
1	84	88	93	96	7
o	p	q	r	t	v
2	85	89	4	6	99
x	z	.	/		
81	86	90	94		

Рис. 46.

3. Многоалфавитные шифры.

Полиалфавитный шифр (многоалфавитный шифр) – это совокупность шифров простой замены, которые используются для шифрования очередного символа открытого текста согласно некоторому правилу.

Суть полиалфавитного шифра заключается в циклическом применении нескольких моноалфавитных шифров к определённому числу букв шифруемого текста. Предположим, что имеется некоторое сообщение $x_1, x_2, x_3, \ldots, x_n, \ldots, x_{2n}, \ldots$, которое необходимо зашифровать, а также для использования полиалфавитного шифра взяли n моноалфавитных шифров. В данном случае к первой букве применяется первый моноалфавитный шифр, ко второй букве — второй, к третьей – третий, …, к n-ой букве — n-ый, а к (n+1)-ой вновь первый, и так далее, пока все сообщение не будет зашифровано. Таким образом, получается довольно-таки сложная последовательность, вскрыть которую сложнее, нежели моноалфавитный шифр. Важным эффектом, достигаемым при использовании полиалфавитного шифра, является маскировка частот появления тех или иных букв в тексте, чего лишены шифры простой замены.

Одним из примеров практической реализации подобного шифра, причем реализации аппаратной, можно считать известную переносную шифровальную машину «Энигма», которая использовалась для шифрования и расшифрования секретных сообщений. Первую версию роторной шифровальной машины запатентовал в 1918 году Артур Шербиус. На основе конструкции первоначальной модели «Энигмы» было создано целое семейство электромеханических роторных машин под тем же названием, применявшихся с 1920-х годов в сфере коммерческой и военной связи во многих странах мира, но наибольшее распространение получили в гитлеровской

Германии во время Второй мировой войны. Именно германская военная модель чаще всего подразумевается при упоминании «Энигмы».

Впервые шифр «Энигмы» удалось дешифровать в польском Бюро шифров в декабре 1932 года. Четверо сотрудников разведки – Мариан Реевский, Ежи Ружицкий, Генрих Зыгальский и Иоганн Ревклид – с помощью данных французской разведки, математической теории и методов обратной разработки смогли разработать и построить специальное устройство для дешифровки закодированных сообщений, которое назвали «криптологической бомбой». После этого немецкие инженеры усложнили устройство «Энигмы» и в 1938 году выпустили обновлённую версию, для дешифровки которой требовалось построить более сложные механизмы.

9 мая 1941 года при захвате силами Великобритании подводной лодки U-110 в руки союзников впервые попала шифровальная машина Энигма вместе с кодами, радиограммами и другими связанными документами. С помощью полученных материалов английские криптографы начали чтение сообщений немецких подлодок, использовавших «Дельфин» на трёхроторной «Энигме».

В августе 1941-го англичане создали более совершенные «Бомбы», позволившие им оперативно расшифровывать немецкие радиограммы. Через два месяца немцы ввели новый код для подлодок, но Блетчли-парк сумел взломать и его.

Англичане читали вражеские шифрограммы до февраля 1942-го, когда немецкий флот начал использовать новую четырёхроторную «Энигму». Ситуацию удалось исправить только когда 30 октября 1942 года противолодочный корабль Petard захватил модернизированную «Энигму» и документацию к ней с подводной лодки U-559. Это позволило расшифровывать немецкие сообщения до самого конца войны.

Во время Второй мировой войны в Англии для расшифровки сообщений, зашифрованных с помощью «Энигмы», была создана машина с кодовым названием «TuringBombe», оказавшая значительную помощь антигитлеровской коалиции. С целью сохранения секретности вся информация, полученная криптоанализом с её помощью, получила кодовое название «Ultra» и предназначалась для распространения среди очень ограниченного круга лиц. Утверждалось, что это достижение являлось решающим фактором в победе союзников.

Несмотря на то, что с точки зрения современной криптографии шифр «Энигмы» был слаб, на практике только сочетание этого фактора с другими (такими как ошибки операторов, процедурные изъяны, заведомо известный текст сообщений (например, при передаче метеосводок), захваты экземпляров «Энигмы» и шифровальных книг) позволили взломщикам шифров разгадывать шифры «Энигмы» и читать сообщения.

Как и другие роторные машины, «Энигма» состояла из комбинации механических и электрических систем. Механическая часть включала в себя клавиатуру, набор вращающихся дисков – роторов, – которые были расположены вдоль вала и прилегали к нему, и ступенчатого механизма, двигающего один или несколько роторов при каждом нажатии на клавишу. Электрическая часть, в свою очередь, состояла из электрической схемы, соединяющей между собой клавиатуру, коммутационную панель, лампочки и роторы.

Конкретный механизм работы мог быть разным, но общий принцип был таков: при каждом нажатии на клавишу самый правый ротор сдвигается на одну позицию,

а при определённых условиях сдвигаются и другие роторы. Движение роторов приводит к различным криптографическим преобразованиям при каждом следующем нажатии на клавишу на клавиатуре.

Механические части двигались, замыкая контакты и образуя меняющийся электрический контур (то есть, фактически, сам процесс шифрования букв реализовывался электрически). При нажатии на клавишу клавиатуры контур замыкался, ток проходил через различные цепи и в результате включал одну лампочку из набора, отображающую искомую букву кода. (Например: при шифровке сообщения, начинающегося с ANX.., оператор вначале нажимал на клавишу A – загоралась лампочка Z – то есть Z и становилась первой буквой криптограммы. Далее оператор нажимал N и продолжал шифрование таким же образом далее). Таким образом, постоянное изменение электрической цепи, через которую шёл ток вследствие вращения роторов, позволяло реализовать многоалфавитный шифр подстановки, что давало высокую, для того времени, устойчивость шифра.

4. Блочные шифры.

В самом общем виде идеология блочного шифрования выглядит так: открытый текст разбивается на блоки различной длины, каждый блок шифруется по особому методу, полученные блоки криптограммы после некоторой перестановки «сшиваются» в единый массив. На практике же все блоки открытого текста имеют одинаковую длину, все шифруются по одному и тому же способу и преобразуются в той же длины блоки криптограммы, которые последовательно выстраиваются в порядке соответствующих исходных блоков:

а) шифр Уитстона-Плейфера.

Исторически первым блочным шифром был шифр, разработанный английским физиком и криптографом Чарлзом Уитстоном (1802–1875) и представленный лордом Плейфером министру иностранных дел Великобритании Палмерстону в 1854 году. Английский алфавит (с j=i) обычным приемом парольного перемешивания вписывается в таблицу 5×5 (рис. 47).

p	**a**	**l**	**m**	**e**
r	**s**	**t**	**o**	**n**
b	c	d	f	g
h	i	k	q	u
v	w	x	y	z

Рис. 47.

Открытый текст разбивается на блоки длины 2. Если обе буквы блока стоят в одной строке (в одном столбце) таблицы, они заменяются их правыми (нижними) соседями. Если же буквы блока стоят в разных строчках и разных столбцах, то каждая из них заменяется на букву, стоящую в той же строке, но в столбце другой буквы блока. Примеры соответствий: cf→DG, wz→XV, oq→FY, ez→NE, su→NI. Если в тексте рядом стоят две одинаковые буквы, между ними вставляется x, так что

«lesson for missDolly» предстанет в виде «lesxson for misxsDolxly». Шифр Уитстона-Плейфера использовался в ходе Первой мировой войны британской дипломатией, а во Второй мировой войне – в соединениях германской армии на Западном фронте (и его читали союзники);

b) шифр Виженера.

Французский криптограф Блез Виженер (1523–1596) опубликовал свой метод в «Трактате о шифрах» в 1585 году. С тех пор на протяжении трех столетий шифр Виженера считался нераскрываемым, пока с ним не справился австриец Фридрих Казиски (в 1863 году). При этом способе шифрования открытый текст разбивается на блоки некоторой длины n. Задается ключ – последовательность из n натуральных чисел: a_1, a_2,…,a_n. Затем в каждом блоке первая буква циклически сдвигается вправо по алфавиту на a_1 позиций, вторая буква – на a_2 позиций, …, последняя – на a_n шагов.

Пример криптограммы, зашифрованной шифром Виженера:

ЭОАЯКНЪЫЩЦГ (ключ 25, 9, 21, 17)

Для лучшего запоминания, в качестве ключа обычно берут осмысленное слово, и алфавитные номера составляющих его букв используют для вычислений, связанных со сдвигами. Так, указанный в приведенном примере ключ имеет буквенную форму «шифр» (в русском алфавите ш – двадцать пятая буква, и – девятая, ф – двадцать первая, р – семнадцатая). Для дальнейшего нам понадобится знать номера всех букв русского алфавита (рис. 48):

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я

Рис. 48.

и латинского (рис. 49):

1	2	3	4	5	6	7	8	9	10	11	12	13
a	b	c	d	e	f	g	h	i	j	k	l	m
14	15	16	17	18	19	20	21	22	23	24	25	26
n	o	p	q	r	s	t	u	v	w	x	y	z

Рис. 49.

Из-за нехватки опытных шифровальщиков шифр Виженера с длиной блока, равной всего лишь 3, применялся в низовых звеньях русской армии в 1916 году, во время наступления Юго-Западного фронта против австро-венгерской армии в ходе знаменитого брусиловского прорыва. Противник легко читал русские оперативные шифровки, что, в конце концов, и не позволило генералу Брусилову добиться стратегического успеха в блестяще задуманной операции;

c) шифр Цезаря.

Очень частный случай конструкции Виженера использовал римский полководец и император Гай Юлий Цезарь: он каждую букву открытого текста циклически сдвигал на три позиции вправо. Знаменитая фраза «Пришел, увидел, победил», под-

водившая итог битвы при Зеле в августе 47 года до н.э., в шифрованном письме Цезаря выглядела как ZHQM ZMGM ZMFM.

5. Поточные шифры.

В шифре Виженера длина ключа может оказаться равной длине открытого текста. Шифры, обладающие этим свойством, называют поточными. Можно представить себе, что имеются два синхронизированных потока: буква за буквой поступающий открытый текст и параллельный с ним ключевой поток над тем же алфавитом. Шифрование осуществляется методом Виженера – путем побуквенного сложения этих двух потоков по модулю алфавитной мощности. Рассмотрим наиболее известные поточные шифры:

a) книжный шифр.

В качестве ключа выбирается какая-либо книга с идентификатором некоторого стартового места в тексте (например, «третья буква в пятом абзаце второй главы»). Под открытым текстом подписывается текст книги, начиная с ключевого места. В следующем примере для удобства выставлены номера участвующих букв (рис. 50).

18	13	6	14	9	19	6	25	9	21	17	14	1	18	24	9	19	1	31	19
с	*м*	*е*	*н*	*и*	*т*	*е*	*ш*	*и*	*ф*	*р*	*н*	*а*	*с*	*ч*	*и*	*т*	*а*	*ю*	*т*
у	**л**	**у**	**к**	**о**	**м**	**о**	**р**	**ь**	**я**	**д**	**у**	**б**	**з**	**е**	**л**	**е**	**н**	**ы**	**й**
20	12	20	11	15	13	15	17	29	0	5	20	2	8	6	12	6	14	28	10
6	25	6	25	24	0	21	10	6	21	22	2	3	26	30	21	25	15	27	29
Е	Ш	Щ	Ш	Ч	Я	Ф	Й	Е	Ф	Х	Б	В	Щ	Э	Ф	Ш	О	Ъ	Ь

Рис. 50.

Во второй строке таблицы записан открытый текст, в третьей – ключ (А. С. Пушкин «Руслан и Людмила», Песнь Первая, с первой буквы), в шестой – криптограмма. В первой строке стоят номера букв открытого текста, в четвертой – номера букв ключа, в пятой – сумма по модулю 32 соответствующих букв открытого текста и ключа, т. е. номер получившейся буквы криптограммы;

b) шифры с автоключами.

Первая буква ключа выбирается случайно, а далее он состоит из открытого текста (рис. 51):

Открытый текст:	*с*	*м*	*е*	*н*	*и*	*т*	*е*	*ш*	*и*	*ф*	*р*
Ключ:	**к**	**с**	**м**	**е**	**н**	**и**	**т**	**е**	**ш**	**и**	**ф**
Криптограмма:	Ь	Ю	Т	У	Ц	Ы	Ш	Ю	Б	Э	И

Рис. 51.

или из получающейся буква за буквой криптограммы (рис. 52):

Открытый текст:	*с*	*м*	*е*	*н*	*и*	*т*	*е*	*ш*	*и*	*ф*	*р*
Ключ:	**к**	**ь**	**й**	**п**	**э**	**ж**	**щ**	**я**	**ш**	**б**	**ц**
Криптограмма:	Ь	Й	П	Э	Ж	Щ	Я	Ш	Б	Ц	З

Рис. 52.

Эти способы генерации ключевого потока предложил в своем упоминавшемся трактате Виженер;

c) шифр Вернама.

В 1917 году американский инженер Гилберт Вернам (1890–1960) осуществил, казалось бы, несбыточную мечту криптографов: он предложил шифр, в принципе не раскрываемый. Это поточный шифр над двоичным алфавитом с буквами 0 и 1. Открытый текст представляется в двоичном виде (например, согласно телеграфному коду Бодо, где каждая буква заменяется двоичной последовательностью длины 5), ключом является случайная двоичная последовательность той же длины, которая используется только один раз – для шифрования данного текста. Криптограмма получается посимвольным сложением открытого текста и ключа по модулю 2. Заметим, что поскольку по модулю 2 вычитание совпадает со сложением, для дешифрования криптограмма посимвольно складывается с ключом. Пусть, например, открытым текстом является «white» (белый). В кодовой таблице Бодо находим: e – 00001, h – 10100, i – 00110, t – 10000, w – 10011, так что шифроваться будет двоичная последовательность (длины 25) 1001110100001101000000001. В качестве ключа возьмем двоичную запись цифр после запятой в числе π=3,1415926536… .Для двоичного представления любого числа от 0 до 15 достаточно четырех цифр: 0 – 0000, 1 – 0001, 2 – 0010, 3 – 0011, 4 – 0100, 5 – 0101, 6 – 0110, 7 – 0111, 8 – 1000, 9 – 1001, …, 15 – 1111. Выбирая первые 25 двоичных знаков, кодирующих последовательность 1415926, находим ключ: 0001010000010101100100100. Для получения криптограммы посимвольно складываем по модулю 2 двоичные коды открытого текста и ключа (рис. 53):

```
    1 0 0 1 1 1 0 1 0 0 0 0 1 1 0 1 0 0 0 0 0 0 0 0 1
+2
    0 0 0 1 0 1 0 0 0 0 0 1 0 1 0 1 1 0 0 1 0 0 1 0 0
-------------------------------------------------------
=   1 0 0 0 1 0 0 1 0 0 0 0 1 1 0 0 0 1 0 0 1 0 0 1 0 1
```

Рис. 53.

Обратим внимание на то, что при суммировании (снизу вверх) криптограммы и ключа в самом деле получается открытый текст. Почему же шифр Вернама не раскрываем? Дело в том, что, если известна криптограмма, и ее длина равна n двоичных разрядов (битов), то, перебирая все возможные ключи (т. е. все возможные двоичные последовательности длины n битов) и складывая их посимвольно по модулю 2 с криптограммой, можно получить все возможные двоичные тексты длины n битов. Какой из них был подлинным сообщением, установить невозможно. Так, в рассмотренном примере, зная криптограмму 1000100100011000100100101 и не зная ключа, взломщик шифра попробует испытать все 2^{25}=33.554.432 возможных ключей, т. е. двоичных последовательностей длины 25 битов. На каком-то шаге он наткнется на истинный ключ и получит, складывая с ним криптограмму, «white». Не зная, в самом ли деле это подлинный открытый текст, он в процессе дальнейшего перебора дойдет до ключа 0100010110011110011101010 и, сложив его по Виженеру с криптограммой, получит 1100110010000110111001111, что по таблице Бодо дает «black» (черный). Далее ему попадется в качестве возможного ключа последова-

тельность 01011011100110101000010 01 и в качестве возможного открытого текста он увидит 11010010100000100001011 00 – «green» (зеленый) и т. д.

Абсолютно стойкий шифр Вернама, к сожалению, мало пригоден для повседневной практики, поскольку с каждым открытым текстом нужно связать индивидуальную случайную двоичную последовательность той же длины. Где взять столько случайных двоичных последовательностей? Современные компьютеры генерировать их не способны. Поэтому шифр Вернама применяется только в особо важных случаях. Например, он служит для обмена секретной информацией между руководителями Российской Федерации и США. Заметим, что тому, кто не имеет возможности использовать шифр Вернама, вполне доступны другие приемы надежной криптографической защиты информации. Последовательное применение трех разных шифров – один из них.

3. Алгоритмы симметричного и асимметричного шифрования

Прежде чем говорить о конкретных алгоритмах и техниках шифрования, давайте еще раз вспомним, что же такое криптография.

Криптография, берем самое простое определение, – это искусство или наука сохранения информации в секрете. Хотя для новичков она кажется формой искусства, граничащей с магией, тем не менее, в реальности это наука для действительно высококвалифицированных компьютерных специалистов и математиков. (Надо сказать, что для тех, кто желает глубоко погрузиться в то, как построены шифры и как они работают, серьезная ученая степень в математике была бы большим плюсом.)

Криптография обеспечивает конфиденциальность шифрованием информации, используя алгоритм и один или более ключей. Вы можете добиться базовой криптографии и без ключей, но то, что обычно требуется, – сохранение в секрете самого алгоритма – нечто достаточно трудное в наши дни. Если используются ключи, зашифрованная версия сообщения может быть расшифрована кем-то еще, у кого есть соответствующий шифровальный ключ. Если это тот же самый ключ, то он должен держаться в секрете между двумя сторонами. В зависимости от метода шифрования, как будет видно позже, это может быть и другой ключ. Самая центральная проблема большинства криптографических приложений – управление этими ключами и содержание их в секрете.

Алгоритмы, формирующие базу криптографии, – это шифры. Шифр – это:

– Криптографическая система, в которой элементы открытого текста заменяются согласно предопределенному ключу.

– Любая криптографическая система, в которой произвольные символы или группы символов представляют элементы открытого текста стандартной длины, обычно отдельные буквы; или в которой элементы открытого текста реорганизованы; или и то и другое в зависимости от неких предопределенных правил.

Выражаясь проще, шифры – это замена одного блока текста другим согласно некоторым общеприменимым правилам. Простой шифр произвольно заменял бы каждую букву другой.

Шифры определяются либо как симметричные, либо как асимметричные в зависимости от того, используют ли они один и тот же ключ для шифрования и де-

шифрования (симметричные шифры) или два разных ключа (асимметричное шифрование).

Люди по своему обыкновению склонны путать симметричное и асимметричное шифрование. Главная причина этого в том, что симметричное обычно ассоциируется с четными числами (т. е. два), а асимметричное, естественно, с нечетными (т. е. один).

Если применять такую логику (а так обычно и происходит), то люди получают неправильное представление. По ходу лекции будут приведен достаточно легкий способ запомнить, что есть что на самом деле.

1. Алгоритмы с симметричным ключом.

Алгоритмы с симметричным ключом – это «взрослая» версия того типа секретного кода, которым большинство из нас время от времени играло в детстве. Обычно в них используется простой алгоритм замены символов; если вы хотите зашифровать текст, то просто заменяете каждую букву алфавита другой. Например (рис. 54):

Оригинал:	A	B	C	D	E	F	G	H	I	G	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Замена:	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	I	F

Рис. 54.

В этом случае буквы в алфавите были просто сдвинуты на семь позиций влево, таким образом, фраза «HELLO WORLD» транслировалась бы как «NKRRU CUXRJ». Предпосылкой, на которой основан этот код, является знание и отправителем, и получателем исходного ключа, количества позиций для смещения букв в нашем случае.

Этот общий секрет позволяет получателю сообщения провести процесс шифрования в обратном направлении и прочитать зашифрованное сообщение.

Симметричное шифрование получило свое название из того факта, что один и тот же ключ используется как для шифрования открытого текста, так и для расшифровки соответствующего зашифрованного. Алгоритмы симметричного шифрования, используемые компьютерами, имеют те же самые составляющие, как и вышеприведенный пример, а именно механизм для шифровки/расшифровки сообщения (известный также как шифр) и общий секрет (ключ), который позволяет получателю расшифровать зашифрованное сообщение.

Очень важным вопросом является определение надежности симметричного шифра. Надежность шифра с симметричным ключом подобного типа диктуется целым рядом факторов. Первый из них – эффективная рандомизация выхода, чтобы два связанных сообщения с открытым текстом не давали после зашифровывания похожих результатов. Степень рандомизации на криптографическом языке обычно называется энтропией.

Наш детский пример в этом плане совершенно неудачен, поскольку каждая буква при шифровании всегда преобразуется в один и тот же результат, и еще потому, что он совершенно не шифрует пробелы. Даже детсадовский криптоаналитик способен достаточно легко расколоть этот код, зная, что любое однобуквенное слово, вероятнее всего, «А».

Еще одна причина, по которой наш пример столь неудачен, состоит в том, что, если по каким-либо причинам алгоритм известен (в нашем случае алгоритм это

«сдвинуть каждую букву на семь позиций вправо»), человек, знающий его, легко может расшифровать каждое последующее сообщение.

Именно здесь мы подошли к важности концепции ключа. В алгоритмах, основанных на ключе, для его защиты предпринимаются определенные усилия. Такой подход вполне допускает рассмотрение и изучение криптографического алгоритма посторонними. Хороший алгоритм – это такой алгоритм, который можно понять, который эффективен и который нельзя использовать для шифрования без соответствующего ключа. Алгоритмы, о которых речь пойдет далее, все обладают этими чертами.

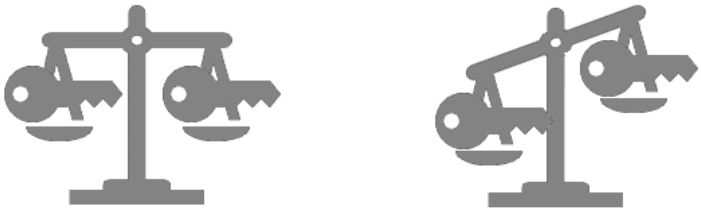
Таким образом, в полноценном симметричном шифре большая часть работы криптоаналитика заключается в попытках поиска в выходных данных алгоритма хоть каких-нибудь шаблонов, чтобы использовать их в качестве отправной точки для взлома кода.

Если в этом плане алгоритм шифрования не имеет недостатков, другим главным фактором, влияющим на его надежность, будет размер пространства ключа; т. е. общее количество всевозможных значений ключа. Наш простенький пример будет «расколот» очень быстро, потому что в нем есть только 25 возможных позиций, на которые можно сместить ключи. Можно провести атаку «грубой силой», просто перебирая по очереди каждый ключ до тех пор, пока не получили бы такое сообщение, которое имело бы смысл.

Реально существующие симметричные шифры используют числовые ключи размером, как правило, от 40 до 256 бит. Даже для самых маленьких из них атака грубой силой должна была бы перебрать в среднем 2 в 39-й степени, или почти 550.000.000.000 возможных значений ключей. Для человека взлом такого шифра методом простого перебора невозможен в принципе. Для компьютера же, если представить, например, что он способен перебирать 1000 вариантов ключей в секунду, для вскрытия такого шифра понадобится всего на всего каких-то 550.000.000 секунд, ну или 9.166.667 минут, или 152.778 часов, или 6.366 суток, или почти 17,5 лет. При этом каждый дополнительный бит в размере ключа удваивает пространство ключа.

Так в чем же заключаются различия симметричного и асимметричного шифров?

Некоторые люди испытывают затруднения при запоминании, какой тип шифрования симметричный, а какой асимметричный. Чтобы помочь, давайте дадим инструмент для запоминания. Посмотрите на рис. 55.



Симметричный шифр Асимметричный шифр

Рис. 55.

В этом нашем мнемоническом примере предположим, что ключи имеют какой-то определенный вес. Вес секретного ключа = x и вес открытого ключа = x + 1 (таким образом, у них разные веса). В случае асимметричного шифрования для зашиф-

ровки и расшифровки используются два различных ключа и, таким образом, на весах ключи не будут сбалансированы, весы будут выглядеть асимметричными. Симметричное же шифрование использует только открытый ключ, который один и тот же как для зашифровки, так и для расшифровки. Соответственно вес ключей одинаков, и на весах они будут сбалансированы, весы будут выглядеть симметричными.

Давайте рассмотрим пример алгоритма с симметричным ключом, то есть поймем, как работает симметричное шифрование. Для этого нам понадобится ввести пару персонажей, которые традиционно используются при объяснении концепций безопасности.

Конечно, можно было бы использовать A, B и C для схематического отображения потока информации между двумя точками. Однако поскольку этот поток информации вовлекает людей, лучше все-таки дать им нормальные имена. Итак, двумя нашими персонажами для примеров с этого момента будут Алиса и Боб. По мере необходимости будут вводиться новые персонажи, но в настоящий момент давайте сконцентрируем наше внимание на Бобе и Алисе.

Почему именно Алиса и Боб, а не, например, Иван да Марья? Принципиальной разницы, конечно, не существует, просто эти персонажи в течение многих лет использовались для демонстрации примеров того, как работают техники шифрования, и, как и многие другие выдуманные герои-долгожители, Боб и Алиса имеют свою собственную занимательную биографию. Эту биографию можно найти в статье под названием «Послеобеденная беседа Боба и Алисы» («The AliceandBobafter-dinnerspeech»), которую Джон Гордон (John Gordon) зачитал на семинаре в Цюрихе в апреле 1984 г.

Итак, вернемся к нашему примеру с Бобом и Алисой. Скажем, Алиса хочет послать Бобу сообщение, хочет, чтобы оно было отправлено защищенным, и хочет, чтобы Боб и только Боб мог прочитать его. Рис. 56 иллюстрирует этот пример, обмен происходит слева направо.

Рис. 56.

Давайте разберемся, что происходит в нашем примере:

1. Сообщение Алисы шифруется секретным ключом.

2. Боб получает зашифрованное сообщение Алисы; видит, что оно зашифровано, и хочет прочитать его.

3. Боб расшифровывает сообщение, используя тот же самый секретный ключ, что использовался и при шифровании.

4. Теперь после расшифровки сообщение может быть прочитано Бобом.

В этом примере предполагается, что Алиса и Боб знают друг друга достаточно хорошо. По этой причине можно считать, что Алиса получила – безопасно – копию секретного ключа, использованного для шифрования сообщения.

Существует два вида симметричных шифров: блочные и потоковые. Блочные шифры оперируют с блоками данных и используются, как правило, для шифрования документов и баз данных. Потоковые шифры работают с битовыми потоками и обычно используются для шифрования коммуникационных каналов.

Достоинства алгоритмов на симметричном ключе

Как видно, в настоящее время используется целый ряд шифров на симметричном ключе. Давайте очень поговорим о тех достоинствах, которые присущи всем этим алгоритмам на симметричном ключе.

Собственно, такое достоинство всего одно. Из-за коротких ключей, которые тем не менее обеспечивают достаточно высокую безопасность, эти алгоритмы быстры и требуют относительно небольшой загрузки системы. По этой причине о шифровании на симметричном ключе часто говорят как о массовом шифровании, так как оно эффективно для больших объемов данных.

Недостатки алгоритмов на симметричном ключе

Самый ключевой недостаток симметричного шифра состоит в том, что ему присущи трудности в управлении этими самыми симметричными ключами, используемыми при шифровании. В частности, как можно безопасно передать их в руки противоположной стороны без того, чтобы не скомпрометировать их?

В следующем учебном вопросе разберем, как эта проблема управления ключами решается при использовании алгоритмов на асимметричном ключе, но и в использовании асимметричных ключей существуют недостатки, для которых тоже требуется использование симметричных ключей и алгоритмов на симметричном ключе.

2. Алгоритмы с асимметричным ключом

Отталкиваясь от знакомых аналогий, нематематик может интуитивно понять, как работает алгоритм симметричного ключа. Однако алгоритмы асимметричного ключа непрофессионалу доступны намного хуже. Фактически иногда они выглядят скорее, как магия, нежели как технология. На самом деле это не так. Для них требуется немного больше объяснений, чем для алгоритмов на симметричном ключе, но тем не менее любой, кто внимательно отнесется к материалу лекции, легко справится с ними.

Основы алгоритмов на асимметричном ключе.

Асимметричное шифрование получило свое название из того факта, что в нем участвует два ключа. Один содержится в тайне (закрытый, или секретный, ключ пользователя), другой общедоступен (открытый, или публичный, ключ пользователя). Открытый ключ обычно помещается в общедоступные каталоги, и совершенно не имеет значения, кто будет иметь его копию.

Существует строгое математическое соответствие между закрытым и открытым ключами, которое заключается в том, что все, что зашифровано при помощи одного из двух ключей, может быть расшифровано только другим ключом пары. Длина ключей и вся математика, стоящая за ними, дают достаточную гарантию того, что не

существует никакого другого ключа, не являющегося частью пары, который мог бы дешифровать сообщение.

Давайте вернемся к Бобу и Алисе и посмотрим, что же происходит при отправке защищенного при помощи алгоритма на асимметричном ключе сообщения. На рис. 57 приведен пример, где обмен происходит слева направо.

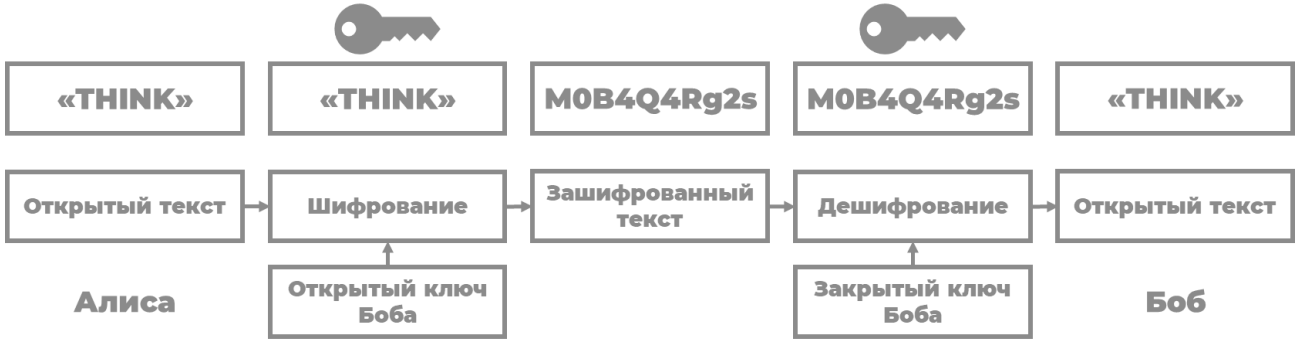


Рис. 57.

На первый взгляд, поменялось здесь не так уж и много. Но это только на первый взгляд.

Вот что происходит в нашем примере:

1. Алиса хочет послать Бобу еще одно сообщение.

2. Сообщение Алисы зашифровывается при помощи открытого ключа Боба (с тем, чтобы его можно было расшифровать только закрытым ключом, находящимся в единоличном владении Боба).

3. Боб получает Алисино зашифрованное сообщение, видит, что оно зашифровано, и хочет прочитать его.

4. С помощью своего закрытого ключа Боб дешифрует сообщение.

5. После дешифровки теперь сообщение может быть прочитано Бобом.

Отметим важный факт: в этом сценарии нет необходимости в обмене закрытыми ключами и, таким образом, весь процесс работы с ключами гораздо проще, чем в примере с симметричным шифрованием.

Достоинства алгоритмов на асимметричном ключе.

Как вы увидели, в настоящее время используется целый ряд алгоритмов на асимметричном ключе. Давайте коротко обозначим те достоинства, которые присущи всем алгоритмам на асимметричном ключе.

Алгоритмы асимметричного ключа делают более легким управление ключами благодаря тому, что не надо искать безопасный канал для передачи копии ключа конечному получателю. Закрытый ключ остается закрытым, а открытый – открытым. Другими словами, большим преимуществом этого механизма над механизмом симметричного ключа является то, что больше нет того секрета, которым требуется делиться. Фактически совершенно не имеет значения, у кого имеется открытый ключ, поскольку он бесполезен без соответствующего закрытого.

Еще одним важнейшим достоинством алгоритмов на асимметричном ключе является то, что они способны предоставить такую цифровую подпись, которую невозможно подделать.

Недостатки алгоритмов на асимметричном ключе.

Недостаток алгоритмов на асимметричном ключе состоит в том, что они очень медленные. В настоящий момент есть множество методов шифрования секретным ключом, которые значительно быстрее, чем любой из существующих методов шифрования открытым ключом. Это проистекает из того факта, что для получения сравнимого уровня безопасности требуются большие длины ключей по сравнению с меньшими симметричными ключами.

Гибридный алгоритм.

Для получения всего лучшего из обоих миров можно использовать алгоритм асимметричного ключа вместе с алгоритмом симметричного. При шифровании наилучшим решением будет объединить оба типа алгоритмов, чтобы получить и высокую безопасность алгоритмов асимметричного ключа, и высокую скорость алгоритмов симметричного.

Соответственно таким гибридным решением будет использование симметричного ключа для шифрования данных, а асимметричного для шифрования самого симметричного ключа. Такой марьяж называется числовой упаковкой.

Кроме того, симметричный ключ обычно генерируется каждый раз как новый и называется «сессионным» ключом. Он действителен только на то время, пока два человека обмениваются сообщениями друг с другом. Этот протокол используется практически во всех «шифраторах открытым ключом», таких, как Notes, SSL, S/MIME. Он обеспечивает высокую производительность и легкость реализации.

Пример гибридного алгоритма.

Посмотрим, как работает гибридное решение. Для этого продолжим рассматривать общение между Алисой и Бобом. Пример изображен на рис. 58, обмен происходит слева направо.

Рис. 58.

В нашем примере происходит следующее. Сначала на одном конце:

1. Алиса желает послать Бобу еще одно сообщение.
2. Сообщение Алисы шифруется при помощи закрытого ключа.
3. Затем Алиса открытым ключом Боба (таким, что только закрытый ключ Боба, который есть у Боба и только у него одного, может расшифровать его) зашифровывает закрытый ключ (в таком сценарии, как уже говорилось, он обычно зовется сессионным, так как всякий раз при отправлении сообщения генерируется новый, отличный от старого ключ).

4. Алиса отсылает Бобу зашифрованное сообщение и зашифрованный ключ.

На другом конце:

1. Боб получает зашифрованное сообщение Алисы и хочет его прочитать.

2. Боб своим закрытым ключом дешифрует закрытый (сессионный) ключ, затем он использует этот дешифрованный ключ (тот же самый, что и тот, которым сообщение зашифровывалось) для расшифровывания Алисиного сообщения; теперь расшифрованное сообщение может быть прочитано Бобом.

4. Цифровые подписи и сценарии их использования

Есть еще одна полезная вещь, которую дают нам алгоритмы асимметричного ключа.

Представьте в предыдущем примере, что Алиса использует свой закрытый ключ для шифрования сообщения и затем отсылает его Бобу. Посланное сообщение хотя и является все еще зашифрованным, но больше уже не имеет частного характера, поскольку любой, у кого есть открытый ключ, может расшифровать его (все равно, у кого он есть).

Итак, для чего же можно использовать такое сообщение от Алисы? Ответ следующий – авторизация. Поскольку только Алиса имеет доступ к закрытому ключу, при помощи которого было создано это сообщение, оно может прийти от нее и только от нее. В этом состоит понятие цифровой подписи.

Цифровые подписи участвуют в обеспечении целостности, аутентификации и идентификации, в определении авторства (невозможность отказа), в то время как алгоритмы и симметричного и асимметричного ключей, которые обсуждались ранее, касались только конфиденциальности.

Хеш-функции.

Для того чтобы предоставить эти дополнительные услуги, нам потребуется ввести новый вид криптографического алгоритма – хеш-функции (еще называемые свертками сообщений).

Тогда как при помощи алгоритмов и симметричного и асимметричного ключей можно как шифровать, так и дешифровать, хеш-функции только шифруют. Именно поэтому их принято относить к однонаправленным функциям. Вы никогда не сможете из хеш-функции восстановить первоначальное сообщение.

Еще, хеш-функции называются «функциями» потому, что они принимают на вход сообщение и возвращают результат. Более точно, они используются для индексирования исходного содержания или ключа сообщения или блока данных, а затем всякий раз при получении данных, относящихся к этому содержанию или ключу. У хеш-функции безопасности есть три основные характеристики:

Она принимает сообщение любого размера и генерирует из него маленький, фиксированного размера блок данных (называется сверткой сообщения). Повторное выполнение хеш-функции с теми же самыми исходными данными в результате всегда дает ту же самую свертку. Это называется отпечатком сообщения.

Это непредсказуемая операция. То есть даже небольшое изменение в исходном сообщении может оказать непредсказуемо большое влияние на конечную свертку. Или скажем по-другому, если используется хорошая хеш-функция, даже изменение 1 бита сообщения должно повлечь изменение половины битов на ее выходе.

Операция хэширования для всех намерений и целей является необратимой. Другими словами, это означает, что из полученной в результате операции хэширования свертки ни при каких обстоятельствах невозможно получить исходные данные.

Для чего же используется тогда хеш-функция безопасности? Собственно, ее основное предназначение заключается в том, чтобы отслеживать, были ли изменения в отдельных частях данных или нет. В комбинации с RSA это используется для создания цифровой подписи.

Под цифровой подписью понимается то, что при помощи хеш-функции можно численно подписать документ и обеспечить аутентификацию без необходимости шифровать все сообщение целиком.

Пример цифровой подписи.

Давайте сделаем паузу и рассмотрим, как же работают цифровые подписи. Пример показан на рис. 59. Однако в этом примере обмен происходит справа налево, а не слева направо, как было в предыдущих примерах, так как Боб отвечает на сообщения Алисы.

В нашем примере происходит следующее. Сначала на одном конце:

1. Боб хочет ответить на сообщение Алисы.
2. Боб составляет сообщение, предназначенное Алисе (чтобы было проще, пусть сообщение не требуется шифровать, и тогда можно будет сосредоточиться исключительно на функциональности цифровой подписи).
3. Боб вычисляет свертку своего сообщения.
4. Боб шифрует свертку своим закрытым ключом.
5. Боб отправляет сообщение и зашифрованную свертку.

Рис. 59.

На другом конце:

1. Алиса получает сообщение Боба и зашифрованную свертку (поскольку они приходят вместе, ей приходится отделять свертку от самого сообщения).
2. Алиса вычисляет новую свертку сообщения, полученного ею от Боба (хеш-алгоритм дает всегда одинаковые значения для одного и того же документа).
3. Алиса расшифровывает полученную свертку открытым ключом Боба (это можно сделать, так как между открытым и закрытым ключами Боба существует взаимно-однозначное соответствие).
4. Алиса сравнивает вычисленную ею свертку с полученной.

Таким образом:

– если обе свертки совпадают, значит, сообщение аутентифицированно (оно пришло от Боба) и целостно (помним, что изменение даже 1 бита изменило бы по меньшей мере половину битов свертки);

– это может быть использовано также для подтверждения авторства (невозможность отказа). Из-за взаимно-однозначного соответствия между открытым и закрытым ключами Боба, Боб не сможет утверждать, что это не он посылал сообщение;

– если свертки не совпадают, значит, либо сообщение было изменено во время пересылки (недостаток целостности), либо не Боб, а кто-то другой послал его (сообщение неаутентифицированно и не может быть использовано для целей подтверждения авторства).

Вопросы доверия цифровым подписям.

Цифровые подписи неидеальны, поскольку остается проблема доказательства того, «кто» действительно подписал, так как доверие, по сути дела, относится к компьютеру, поставившему цифровую подпись, а не к человеку.

Если компьютер скомпрометирован или если скомпрометирован закрытый ключ человека, вполне возможно выдать себя за этого человека и поставить за него цифровую подпись. Таким образом, доверие должно быть направлено на подписывающий компонент (машина, код и т. д.).

Исходя из общей безопасности подписывающего устройства (т. е. компьютера пользователя) и практики помещения ключей на депонент (где они технически доступны администраторам и менеджерам организации), цифровые подписи представляют не большую юридическую ценность для судебной практики. Следовательно, вопрос доверия цифровым подписям в настоящее время следует уравновесить пониманием того факта, что они не способны дать полной и абсолютной гарантии при определении авторства.

В предыдущем учебном вопросе рассматривался так называемый гибридный алгоритм шифрования, но не приводили примеров его реализации. Это сделано не просто так, а потому, что для полного понимания того, как это работает, нам необходимо было сначала рассмотреть вопрос цифровой подписи, тесно связанный с гибридными алгоритмами. Теперь же, когда все необходимые вопросы были рассмотрены, можно привести пример практической реализации гибридного протокола шифрования. Таким примером являются криптографические протоколы Security Sockets Layer (SSL) и Transport Layer Security (TLS), которые были разработаны для обеспечения безопасной связи в Интернете.

Давайте кратко рассмотрим протокол SSL на примере открытого программного обеспечения OpenSSL.

Итак, что такое OpenSSL и для чего используется

OpenSSL – это криптографический инструментарий, реализующий сетевые протоколы Secure Sockets Layer (SSL v2/v3) и Transport Layer Security (TLS v1) и соответствующие им стандарты криптографии.

Программа OpenSSL – это инструмент командной строки для использования различных криптографических функций криптографической библиотеки OpenSSL в консоли. Основные возможности:

– Создание и управление закрытыми ключами, открытыми ключами и параметрами;

– Криптографические операции с открытым ключом;
– Создание сертификатов X.509, CSR и CRL;
– Расчёт дайджестов сообщений;
– Шифрование и дешифрование с помощью шифров;
– Клиентские и серверные тесты SSL/TLS;
– Обработка подписанной или зашифрованной почты S/MIME;
– Запросы отметок времени, генерация и проверка.

Как работают SSL сертификаты.

Сгенерированные в OpenSSL ключи могут использоваться для шифрования различных данных, но самое популярное использование – шифрование в HTTPS протоколе, где используется ассиметричное шифрование, что означает, что для шифрования используется публичный или открытый ключ, а для расшифровки – приватный или закрытый ключ.

Как известно, публичный ключ не является секретным. Он свободно распространяется и используется для шифрования данных, которые можно расшифровать только приватным ключом. При этом публичный и приватный ключ генерируются вместе и криптографически связаны.

Ещё данная пара ключей может использоваться для подписи данных и проверки подписи. Эта подпись подтверждает то, что данные удостоверены владельцем приватного ключа и впоследствии эти данные не были изменены. Подписываются данные приватным ключом (которые имеет одно определённое лицо), а проверить подпись можно публичным ключом, который может получить каждый.

Любой может сгенерировать пару ключей, поэтому возникает проблема идентификации – как проверить, что публичный ключ выпущен определённым лицом?

Это можно было бы сделать, например, так: владелец сайт mysite.ru генерирует пару публичный-приватный ключ и просит третью сторону подписать его публичный ключ. В результате публичный ключ распространяется с цифровой подписью, которую можно проверить публичным ключом третьей стороны. На самом деле, всё именно так и происходит, а подписанный публичный ключ, вместе с дополнительной информацией (например, название домена, для которого он подписан) упаковываются в сертификат.

Сертификат, по сути, это публичный ключ, а также информация о домене и другая сопутствующая информация, подписанная электронной подписью.

В результате процедура создания сертификата выглядит так:

1. Владельцем сайта генерируется пара приватный и публичный ключ.

2. Публичный ключ вместе с другой информацией для подписи (например, название доменного имени) упаковывается в файл в специальном формате. Он называется – CertificateSigningRequest (CSR), то есть «запроса на подпись сертификата».

3. Данный запрос на подпись (CSR) отправляется в Центр Сертификации (CA), который, используя свой приватный корневой ключ, создаёт подпись для этих данных и всё это упаковывается в другой специальный файл, называемый сертификат.

В результате получается сертификат со следующими свойствами:

– Он может зашифровать данные (в нём есть публичный ключ), которые способен расшифровать только приватный ключ, составляющий пару этому сертификату;

– Сертификат может быть проверен на подлинность (у него есть цифровая подпись) с помощью сертификата Центра Сертификации (CA), который его создал.

При подключении к сайту пользователи получают свою копию сертификата этого сайта, и браузер автоматически проверяет её по доверенным корневым сертификатам, которые содержаться в операционной системе или хранятся в веб браузере.

После этого браузер шифрует с помощью сертификата сайта данные и отправляет их на сервер, эти данные может расшифровать только владелец приватного ключа, то есть сервер. Таким образом происходит согласование ключа, используемого для последующего шифрования.

Дополнительно отметим, что протоколы SSL на данный момент считаются небезопасными и ими не рекомендуют пользоваться. В свою очередь, протоколы TLS считаются безопасными и широко используются всеми современными веб-браузерами.

5. Инфраструктура общих ключей. Управление общими ключами. Системы доверия на основе инфраструктуры общих ключей

В криптографии с асимметричным ключом людям не надо знать закрытый ключ. Если Алиса хочет передать сообщение Бобу, она должна знать только открытый ключ Боба, который является открытым для всех и доступен каждому. Если Боб должен передать сообщение Алисе, он должен знать только открытый ключ Алисы, который также известен каждому. В криптографии открытого ключа каждый сохраняет секретный ключ и объявляет общедоступный или открытый ключ, при этом каждый имеет доступ к общедоступному ключу, то есть общедоступные ключи доступны обществу.

Общедоступные ключи, подобно секретным ключам в симметричном шифровании, должны быть распределены, чтобы быть полезными. Давайте кратко обсудим способы, которым могут быть распределены общедоступные ключи.

Общедоступное объявление.

Наивный подход состоит в том, чтобы объявить открытые ключи публично. Боб может поместить свой открытый ключ на своем сайте или объявить его в средствах, например, массовой информации. Когда Алиса должна передать конфиденциальное сообщение Бобу, она может получить открытый ключ Боба из его сайта или из СМИ или даже передать Бобу сообщение, чтобы попросить его об этом.

Этот подход, однако, небезопасен. Он допускает подделку. Например, Ева может сделать такое же общедоступное объявление. Прежде, чем Боб сможет среагировать, его отношениям с Алисой может быть нанесен определенный вред. Ева может послать глупой Алисе свое сообщение, которое якобы написано Бобом. Ева может также подписать документ фальшивым секретным ключом и вызвать тем самым у каждого, кто видит этот документ, предположение, что сообщение было подписано Бобом. Этот подход также уязвим, если Алиса сама запрашивает открытый ключ Боба. Ева может перехватить ответ Боба и заменить его собственным фальшивым открытый ключом.

Центр доверия.

Более безопасный подход состоит в том, чтобы иметь центр, которому доверяют и который хранит каталог общедоступных (открытых) ключей: каталог, подобно

используемому в телефонной системе, но динамически модифицируемый. Каждый пользователь может выбрать секретный и открытый ключ, сохраняя секретный ключ, и вставлять открытый ключ в каталог. Центр может предоставить пользовательский регистр и проверить опознавательный код. Каталог может публично рекламироваться центром, которому доверяют. Центр может также ответить на любой запрос об общедоступном ключе.

Управляемый центр доверия.

Более высокий уровень безопасности может быть достигнут, если добавить управление распределением открытого ключа. При объявлении открытого ключа можно включить в ответ метку времени и подпись администрации, чтобы предотвратить перехват и переделку ответа. Если Алиса хочет знать открытый ключ Боба, она может передать запрос центру, включая в запрос имя Боба и метку времени. Центр отвечает открытым ключом Боба, первоначальным запросом и меткой времени, подписанной секретным ключом центра. Алиса использует открытый ключ известного всем центра и проверяет метку времени. Если метка времени правильная, она извлекает общедоступный ключ Боба.

Центр сертификации.

Предыдущий подход может породить высокую нагрузку на центр, если число запросов будет большим. Альтернатива этому – создание сертификата (удостоверения) общедоступного ключа. Боб имеет два желания: он хочет, чтобы люди знали его открытый ключ, и он хочет, чтобы никто не сформировал фальшивый открытый ключ, такой же, как у него. Боб может обратиться в центр сертификации, который связывает открытый ключ с объектом и выдает сертификат. Центр сертификации имеет известный общедоступный ключ, который не может быть фальшивым. Центр сертификации проверяет идентификацию Боба, используя какое-либо принятое центром доказательство подлинности заявителя, затем запрашивает открытый ключ Боба и подписывает сертификат своим секретным ключом. Теперь Боб может загрузить подписанное свидетельство в каталог. Любой, кто хочет получить для своих нужд открытый ключ Боба, загружает себе подписанное свидетельство и использует общедоступный ключ центра, чтобы извлечь общедоступный ключ Боба.

Хотя использование сертификационных центров решило проблему мошенничества при распределении открытых ключей, они создали побочный эффект. Дело в том, что теоретически каждое свидетельство может иметь различный формат. Если Алиса хочет использовать программу, чтобы автоматически загрузить различные сертификаты, принадлежащие различным людям, программа не сможет сделать это. Одно свидетельство может иметь открытый ключ в различных форматах. Открытый ключ может быть на первой линейке в одном сертификате и на третьей линейке в другом. Отсюда логичный вывод о том, что было бы неплохо разработать какой-то общепринятый стандарт. Собственно, так и поступили в дальнейшем. Чтобы обеспечить универсальность, была разработана рекомендация X.509, которая была принята в Internet с некоторыми изменениями. X.509 – способ описать сертификат структурированным способом.

Сертификат имеет следующие поля:

– Номер версии. Это поле определяет версию сертификата X.509. Номер версии начинается отсчитываться с 0; текущая версия (третья версия) – 2.

– Серийный номер. Это поле определяет число, назначаемое каждому сертификату. Значение этого числа является уникальным для каждого выпускаемого свидетельства.

– Алгоритм подписи ID. Это поле идентифицирует алгоритм, используемый для подписи сертификата. В этом поле определяется любой параметр, который необходим для подписи.

– Название выдавшего сертификат. Это поле идентифицирует центра сертификации, который выдал свидетельство. Название - обычно иерархия строк, которые определяют страну, штат, организацию, отдел и так далее.

– Срок действия. Это поле определяет начальное время (не раньше) и последнее время (не позже), когда сертификат считается действительным.

– Имя пользователя. Это поле определяет объект, которому принадлежит открытый ключ. Это также иерархия строк. Часть поля определяет то, что называется общим именем, которое является фактическим именем обладателя ключа.

– Имя общедоступного ключа. Это поле определяет открытый ключ владельца. Это - центральная информация сертификата. Поле также определяет соответствующий алгоритм общедоступного ключа (например, RSA) и его параметры.

– Уникальный идентификатор выдавшего сертификат. Это дополнительное поле позволяет двум организациям, выдавшим ключ, иметь одно то и же значение поля выдавшего, если уникальные идентификаторы выдавшего различны.

– Уникальный идентификатор пользователя. Это дополнительное поле позволяет двум различным пользователям иметь одно и то же поле пользователя, если уникальные идентификаторы пользователя различны.

– Дополнительное расширение формата. Это дополнительное поле позволяет выпускающим прикладывать больше частной информации, дополняющей сертификат.

– Подпись. Это поле состоит из трех секций. Первая секция содержит все другие поля в сертификате. Вторая содержит дайджест первой секции, зашифрованный с общедоступным ключом сертификационного центра (CA). Третья – идентификатор алгоритма, использованного для создания второй секции.

Возобновление сертификата.

Каждое свидетельство имеет срок действия. Если нет никаких проблем с сертификатом, Центр сертификации выдает новый сертификат прежде, чем истекает старый. Этот процесс подобен возобновлению кредитных карточек банком – держатель кредитной карточки обычно получает возобновленную кредитку прежде, чем срок действия старой истекает.

Аннулирование сертификата.

В некоторых случаях сертификат должен быть отменен перед тем, как истечет срок его действия. Например:

1. Секретный ключ (объекта) пользователя, соответствующий открытому ключу, который перечислен в сертификате, возможно, был скомпрометирован.

2. Центр Сертификации больше не желает удостоверять пользователя. Например, свидетельство пользователя касается организации, в которой он больше не работает.

3. Секретный ключ центра сертификации, который может проверять сертификаты, возможно, был скомпрометирован.

В этом случае центр сертификации должен отменить все неистекшие сертификаты.

Аннулирование происходит путем периодического выпуска списка аннулированных сертификатов (CRL – certificaterevocation). Список содержит все отменяемые сертификаты, срок которых не истек в день выпуска CRL. Когда пользователь хочет использовать сертификат, он сначала должен проверить каталог соответствующего сертификационного Центра, просмотрев последний список аннулирования сертификатов.

Список аннулирования сертификатов имеет следующие поля:

– Алгоритм подписи ID. Это поле то же самое, как и в сертификате,

– Название выдавшего сертификат. Это поле то же самое, как и в сертификате.

– Дата модификации. Это поле определяет, когда список был выпущен.

– Дата последнего обновления. Это поле определяет следующую дату, когда будет выпущен новый список.

– Аннулированный сертификат. Это повторяемый список всех аннулированных сертификатов, у которых не истек срок. Каждый список содержит две части: пользовательский серийный номер сертификата и дату аннулирования.

Подпись. Это поле такое же, как и в списке сертификатов.

Инфраструктура открытых ключей.

Инфраструктура открытых ключей (PKI – Public Key Infrastructures) – модель для создания, распределения и аннулирования сертификатов, основанная на рекомендации X.509.

Режимы работы.

Для PKI были определены несколько режимов работы. Самые важные из них перечислены ниже:

– Выпуск, возобновление и аннулирование сертификатов. Эти режимы работы были определены в X.509. Поскольку PKIX базируется на X.509, он должен обработать все режимы работы, имеющие отношение к сертификатам.

– Хранение и модификация ключей. PKI должен быть местом хранения секретных ключей для тех участников, у которых есть необходимость держать свои секретные ключи где-нибудь в сейфе. В дополнение к этому PKI несет ответственность за обновление этих ключей по запросу участников.

– Обеспечение услуг другим протоколам. Некоторые протоколы безопасности Internet, такие как IPSec и TLS, базируются на услугах PKI.

– Обеспечение управления доступом. PKI может обеспечить различные уровни доступа к информации, сохраненной в ее базе данных. Например, организация PKI может обеспечить доступ к полной базе данных для высшего исполнительного руководства, но ограниченный доступ – для служащих.

Модель доверия.

Невозможно иметь только один центр сертификации, выпускающий все сертификаты для всех пользователей в мире. Должно быть много центров сертификации (CA), каждый – ответственный за создание, сохранение, издание и аннулирование

ограниченного числа сертификатов. Модель доверия (Trust Model) определяет правила, которые говорят, как пользователь может проверить сертификат, полученный от Центра Сертификации (CA).

Иерархическая модель.

У этой модели – структура типа дерева, корнем которого является центр сертификации (корневой центр). Корневой центр сертификации имеет сертификат, подписанный и выпущенный им самим. Другим центрам сертификации и пользователям для того, чтобы работать, необходимо доверять ему. В общем случае иерархия выглядит следующим образом:

1. Корневой центр сертификации;
2. Прочие центры сертификации;
3. Пользователи 1, 2, 3, …, N.

При этом корневой центр сертификации подписывает сертификаты для прочих центров (центр 1, центр 2 и т. д.). Центр 1 подписывает сертификаты для пользователей 1, 2, 3. Центр 2 – для пользователей 4 и 5. Центр 3 – для пользователей 6, 7, 8, 9 и т. д. То есть образуется своего рода цепочка сертификатов (см. рис. 60).

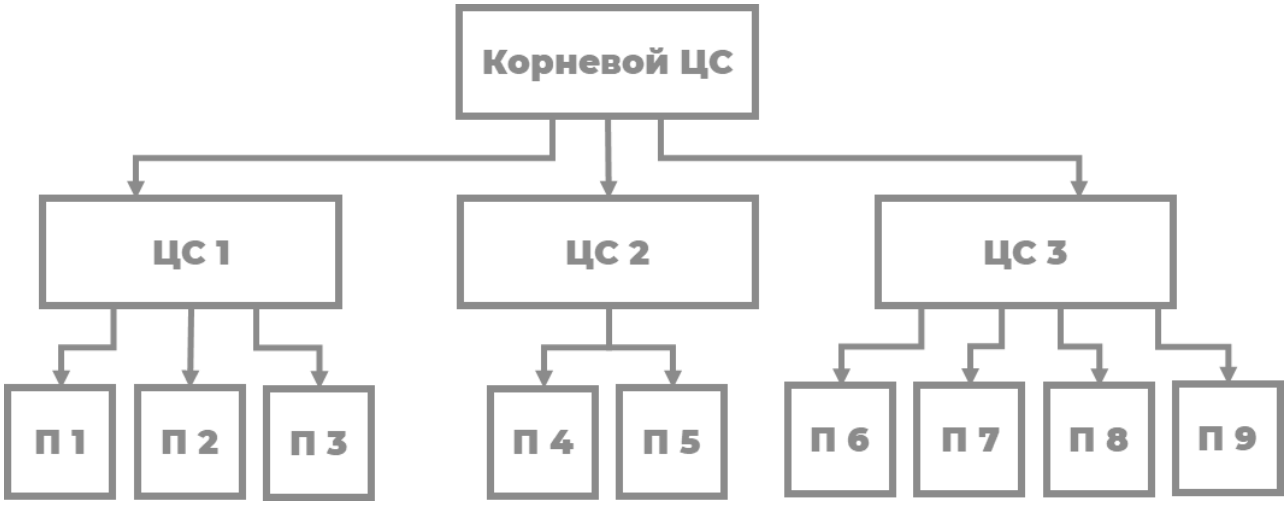


Рис. 60.

В случае, когда между собой взаимодействуют пользователи одного и того же ЦС, например, П1 и П3, проблем с проверкой подлинности сертификатов нет. П1 и П3 доверяют ЦС1 и имеют его корневой сертификат, поэтому могут проверить сертификат любого пользователя ЦС1.

При взаимодействии П1 и П4 ситуация усложняется: П1 не доверяет ЦС2, т. к. не является его пользователем и не имеет его сертификата. Аналогично, П4 не доверяет ЦС1.Решение здесь очень простое:

1. П1 обращается в свой родной ЦС и узнает, какой ЦС выпускал для него сертификат: корневой ЦС является в данном случае родителем.
2. П1 запрашивает сертификат корневого ЦС.
3. П1 узнает, какая цепочка сертификатов нужна для проверки П4. Эта информация содержится в самом сертификате П4.
4. П1 понимает, что следующим в цепочке является ЦС2, проверяет его сертификат, а затем проверяет сертификат П3.

Таким образом, можно очень легко проверить подлинность сертификатов любого пользователя такой модели.

Безусловно, уровней в иерархии может быть гораздо больше, чем 3, как в нашем примере. В такой ситуации процедуру проверки можно упростить, если при регистрации П1 ему сразу выдается вся цепочка сертификатов от его родного ЦС до корневого, то есть можно избежать последовательной проверки сертификатов от родного ЦС до корневого и перейти сразу к корневому.

Система имеет как плюсы, так и минусы. Из плюсов:

– Сравнительная простота реализации

– Удобство наложения такой модели на структуру ведомств

Самый главный минус – в случае компрометации любого ЦС, сертификаты всех стоящих ниже по иерархии ЦС и пользователей становятся недействительными.

Существуют также и другие модели доверия, например сетевая модель или мостовая, но в рамках данногокурса лекций они рассматриваться не будут.

Вопросы и задания для самоконтроля

1. Криптология, криптография, криптоанализ: определение и состав понятий, их связь между собой.
2. Дайте определение основным терминам криптографии: алфавит, текст, шифрование, дешифрование, ключ.
3. Дайте определение основным терминам криптографии: криптосистема, электронная подпись, криптостойкость.
4. Перечислите и охарактеризуйте основные требования, которые предъявляются к современным криптографическим системам защиты информации.
5. Поясните, как проверяется и обосновывается надежность современных криптографических систем защиты информации. Назовите основные виды нападений на засекречивающие системы, применяемые в современном криптоанализе.
6. Перечислите основные задачи современной криптографии.
7. Дайте определение перестановочных шифров.
8. Объясните принцип маршрутного шифрования.
9. Объясните принцип шифрования с помощью решеток.
10. Дайте определение подстановочных шифров (шифров замены).
11. Объясните принцип шифрования при помощи шифра Сцитала.
12. Назовите и поясните с точки зрения криптоанализа основной недостаток шифров простой замены.
13. Многоалфавитные шифры: определение и примеры практической реализации.
14. Алгоритмы с симметричным ключом: определение, принцип работы, достоинства и недостатки.
15. Алгоритмы с асимметричным ключом: определение, принцип работы, достоинства и недостатки.
16. Цифровые подписи: понятие, принцип работы, вопросы доверия цифровым подписям.

Лекция 6. Реагирование на инциденты кибербезопасности и их обработка[1]

Тема посвящена таким важнейшим вопросам как реагирование на киберинциденты и их обработка. Реагирование на инциденты понятие достаточно специфическое, в мире информационной безопасности так называют комплекс мероприятий по обнаружению и прекращению кибератаки или утечки данных из инфраструктуры организации и устранению последствий.

Основная цель реагирования – свести к минимуму ущерб от инцидента, а также позволить организации как можно скорее и с наименьшими затратами вернуться к нормальному режиму работы. За реагирование на инциденты может отвечать как внутренняя команда специалистов, так и внешний Центр управления событиями кибербезопасности, о чем говорилось в рамках изучения первой темы курса.

Выделяют шесть основных этапов процесса реагирования на инциденты.

Первый этап – подготовка. Она начинается с разработки плана реагирования на инциденты, который включает в себя сценарии работы сотрудников при наступлении того или иного события кибербезопасности, список необходимых ресурсов, перечень применяемых инструментов, права и обязанности команды реагирования. Также к этапу подготовки относится обучение ответственных за реагирование на инцидент сотрудников. Этот этап не привязан к конкретному инциденту.

Второй этап – идентификация. Собственно реагирование на инцидент начинается с обнаружения кибератаки или утечки данных. На этом этапе поступает оповещение об инциденте, специалисты оценивают угрозу и собирают данные о ней. Обычно процесс идентификации сводится к изучению логов.

Третий этап – сдерживание. Команда реагирования принимает меры для пресечения распространения угрозы. К ним может относиться изоляция пораженных устройств, изоляция затронутых сегментов сети, временное отключение Интернета и так далее. Одна из дополнительных целей этого этапа – не допустить уничтожения следов атаки, которые потребуются при расследовании.

Четвертый этап – ликвидация. Именно на этом этапе происходит устранение угрозы, удаление вредоносных файлов, смена паролей пострадавших учетных записей, восстановление утраченных данных и так далее.

---

[1] В данной лекции использованы следующие материалы: *Аграновский А. В., Хади Р. А*. Новый подход к защите информации – системы обнаружения компьютерных угроз // Информационный бюллетень JetInfo. 2007. № 4 (167). С. 3–22; *Пелешенко В. С.* Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учеб. пособие. Ставрополь: СКФУ, 2017; Руководство по реагированию на инциденты информационной безопасности // Управление технологических решений АО Kaspersky Lab: [сайт]. URL: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07172131/Incident_Response_Guide_rus.pdf; Что такое Cyber-KillChain и почему ее надо учитывать в стратегии защиты // Интернет-портал PCNews: [сайт]. 2017. 27 апр. URL: https://pcnews.ru/blogs/cto_takoe_cyber_kill_chain_ i_pocemu_ee_nado_ucityvat_v_strategii_zasity-765773.html#gsc.tab=0; *Шелухин О. И.* Обнаружение вторжений в компьютерные сети (сетевые аномалии): учеб. пособие для вузов. М.: Горячая Линия-Телеком, 2018.

Пятый этап – возвращение к работе, то есть ввод обратно в эксплуатацию систем, затронутых инцидентом, подключение устройств к сети, тестирование и мониторинг корректности их работы.

Завершающий, шестой этап – улучшение, представляет собой обновление плана реагирования на инциденты с учетом опыта, полученного при устранении кибератаки.

Мероприятия по реагированию на инциденты могут быть частично или полностью автоматизированы. О некоторых средствах такой автоматизации, в частности о системах управления событиями и данными безопасности (они имеют общепринятое аббревиатурное сокращение SIEM), также будет говориться в рамках изучения данной темы.

Важно понимать, в чем состоит различие между реагированием на инциденты и управлением инцидентами или как его еще называют менеджментом инцидентов. Вообще понятия «реагирование на инциденты» и «менеджмент инцидентов» довольно близки, но все-таки это не одно и то же.

Принято считать, что реагирование на инциденты включает все действия технического характера для устранения угрозы и возобновления работы. Менеджмент инцидентов – это более широкое понятие, включающее в том числе коммуникации по теме инцидента внутри компании и вне нее, координацию и планирование. Часто реагирование на инциденты считают частью менеджмента инцидентов.

1. Реагирование на уязвимости, связанные с компьютерной безопасностью

1. Инциденты кибербезопасности. В рамках данного вопроса еще раз вернемся к понятию инцидента кибербезопасности, о котором говорилось при изучении предыдущих тем курса. Различие в том, что в данном случае это будет не исключительно теоретическое рассмотрение, а анализ с точки зрения второго этапа реагирования на инциденты, который, как вы помните из вводной части лекции, называется «идентификация».

Для начала определимся с ключевыми терминами и их определениями, необходимыми для дальнейшего изучения материалов лекции.

Кибербезопасность – совокупность различных концепций, доктрин, стратегий, методов и средств защиты от атак злоумышленников (хакеров) на компьютеры, серверы, информационные системы, сети передач данных, мобильные устройства и т. д. Кибербезопасность является понятием более узким по отношению к понятию информационной безопасности, которая, в свою очередь, определяется как сфера науки и техники, охватывающая совокупность проблем, связанных с обеспечением защищенности объектов информационной сферы в условиях существования угроз. Под информационной безопасностью также понимают защищенность информации от несанкционированного ознакомления, преобразования и уничтожения, защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности.

Событие кибербезопасности – это идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики кибербезопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

Инцидент кибербезопасности – это появление одного или нескольких нежелательных, или неожиданных событий кибербезопасности, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы кибербезопасности.

Угроза кибербезопасности – потенциально возможное событие, действие (воздействие), процесс или явление, создающее опасность возникновения инцидента кибербезопасности.

Уязвимость информационной системы – недостаток в ИС, используя который внешний злоумышленник может намеренно реализовать угрозу кибербезопасности.

Эксплоит – компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на ИС.

Реагирование на инцидент кибербезопасности – структурированная совокупность действий, направленная на установление деталей инцидента, минимизацию ущерба от инцидента и предотвращение повторения инцидента кибербезопасности.

Целевая атака – атака, нацеленная на одного человека, компанию или группу. В процессе атаки может использоваться различное вредоносное программное обеспечение и методы социальной инженерии.

APT-атака (AdvancedPersistentThreat) – сложная, продолжительная, хорошо спланированная многоходовая атака, использующая сложное вредоносное ПО, методы социальной инженерии и данные об информационной инфраструктуре атакуемого.

Жизненный цикл атаки – последовательность шагов осуществления атаки.

SIEM (SecurityInformationAndEventManagement) – система, которая обеспечивает анализ событий кибербезопасности, исходящих от сетевых устройств и приложений, в реальном времени. Одной из возможностей SIEM-систем является сопоставление событий с потоками данных об угрозах.

Индикаторы компрометации – наблюдаемая в компьютерной сети или на одном из компьютеров сущность, наличие которой может свидетельствовать о компрометации ИС. Обычно под такими индикаторами понимают IP-адреса, URL-адреса, хеши файлов.

Потоки данных об угрозах – информация, содержащая индикаторы компрометации и позволяющая выявлять факт компрометации, используя SIEM-системы и другие сетевые устройства и средства защиты информации.

Разведка на основе открытых источников (OSINT) – военный термин, применительно к кибербезопасности означает поиск в открытых источниках необходимой информации, в том числе индикаторов компрометации, отчетов по конкретным угрозам и другой информации, которая может способствовать расследованию инцидента кибербезопасности.

Атака типа WateringHole – одна из разновидностей многоуровневых целенаправленных кибератак. Атака заключается в том, что злоумышленники заражают вредоносным ПО веб-сайты, часто посещаемые их потенциальными жертвами. Это могут быть сайты компаний-партнеров или подрядчиков, общественных организаций и даже правительственных учреждений.

Теперь давайте рассмотрим примеры инцидентов кибербезопасности и разберем их причины. Причем в двух вариантах, как непосредственно киберинциденты, то есть случаи, когда угроза реализуется техническими средствами и в отношении технических же средств и систем, а также как инциденты, которые могут реализовываться без участия технических средств, когда узкое понятие киберинцидента трансформируется в более широкое понятие инцидента информационной безопасности.

1. Отказ в обслуживании (DDoS).

Отказ в обслуживании является обширной категорией инцидентов кибербезопасности, имеющих одну общую черту. Подобные инциденты приводят к неспособности систем, сервисов или сетей продолжать функционирование с прежней производительностью, чаще всего при полном отказе в доступе авторизованным пользователям.

Существует два основных типа инцидентов кибербезопасности, связанных с отказом в обслуживании, создаваемых техническими средствами: уничтожение ресурсов и истощение ресурсов.

Некоторыми типичными примерами таких преднамеренных технических инцидентов кибербезопасности «отказ в обслуживании» являются:

– зондирование сетевых широковещательных адресов с целью полного заполнения полосы пропускания сети трафиком ответных сообщений;

– передача данных в непредусмотренном формате в систему, сервис или сеть в попытке разрушить или нарушить их нормальную работу;

– одновременное открытие нескольких сеансов с конкретной системой, сервисом или сетью в попытке исчерпать их ресурсы (то есть замедление их работы, блокирование или разрушение).

Одни технические инциденты кибербезопасности «отказ в обслуживании» могут возникать случайно, например в результате ошибки в конфигурации, допущенной оператором, или из-за несовместимости прикладного программного обеспечения, а другие – преднамеренными. Одни технические инциденты кибербезопасности «отказ в обслуживании» инициируются намеренно с целью разрушения системы, сервиса и снижения производительности сети, тогда как другие являются всего лишь побочными продуктами иной вредоносной деятельности. Например, некоторые наиболее распространенные методы скрытого сканирования и идентификации могут приводить к полному разрушению старых или ошибочно сконфигурированных систем или сервисов при их сканировании. Следует заметить, что многие преднамеренные технические инциденты типа «отказ в обслуживании» часто инициируются анонимно (то есть источник атаки неизвестен), поскольку злоумышленник обычно не получает информации об атакуемой сети или системе.

Инциденты «отказ в обслуживании», создаваемые не техническими средствами и приводящие к утрате информации, сервиса и (или) устройств обработки информации, могут вызываться, например, следующими факторами:

– нарушениями систем физической защиты, приводящими к хищениям, преднамеренному нанесению ущерба или разрушению оборудования;

– случайным нанесением ущерба аппаратуре и (или) ее местоположению от огня или воды/наводнения;

– экстремальными условиями окружающей среды, например высокой температурой (вследствие выхода из строя системы кондиционирования воздуха);

– неправильным функционированием или перегрузкой системы;

– неконтролируемыми изменениями в системе;

– неправильным функционированием программного или аппаратного обеспечения.

2. Сбор информации.

В общих чертах инциденты кибербезопасности «сбор информации» подразумевают действия, связанные с определением потенциальных целей атаки и получением представления о сервисах, работающих на идентифицированных целях атаки. Подобные инциденты информационной безопасности предполагают проведение разведки с целью определения:

– наличия цели, получения представления об окружающей ее сетевой топологии и о том, с кем обычно эта цель связана обменом информации;

– потенциальных уязвимостей цели или непосредственно окружающей ее сетевой среды, которые можно использовать для атаки.

Типичными примерами атак, направленных на сбор информации техническими средствами, являются:

– сбрасывание записей DNS (системы доменных имен) для целевого домена Интернета (передача зоны DNS);

– отправка тестовых запросов по случайным сетевым адресам с целью найти работающие системы;

– зондирование системы с целью идентификации (например, по контрольной сумме файлов) операционной системы хоста;

– сканирование доступных сетевых портов на протокол передачи файлов системе с целью идентификации соответствующих сервисов (например, протоколы электронной почты, протокол FTP, иные сетевые протоколы и т. д.) и версий программного обеспечения этих сервисов;

– сканирование одного или нескольких сервисов с известными уязвимостями по диапазону сетевых адресов (горизонтальное сканирование).

В некоторых случаях технический сбор информации расширяется и переходит в несанкционированный доступ, если, например, злоумышленник при поиске уязвимости пытается получить несанкционированный доступ. Обычно это осуществляется автоматизированными средствами взлома, которые не только производят поиск уязвимости, но и автоматически пытаются использовать уязвимые системы, сервисы и (или) сети.

Инциденты, направленные на сбор информации, создаваемые не техническими средствами, приводят:

– к прямому или косвенному раскрытию, или модификации информации;

– хищению интеллектуальной собственности, хранимой в электронной форме;

– неправильному использованию информационных систем (например, с нарушением закона или политики организации).

Инциденты могут вызываться, например, следующими факторами:

– нарушениями физической защиты безопасности, приводящими к несанкционированному доступу к информации и хищению устройств хранения данных, содержащих значимые данные, например ключи шифрования;

– неудачно и (или) неправильно конфигурированными операционными системами по причине неконтролируемых изменений в системе или неправильным функционированием программного или аппаратного обеспечения, приводящим к тому, что персонал организации или посторонний персонал получает доступ к информации, не имея на это разрешения.

3. Несанкционированный доступ.

Несанкционированный доступ как тип инцидента включает в себя инциденты, не вошедшие в первые два типа. Главным образом он состоит из несанкционированных попыток доступа в систему или неправильного использования системы, сервиса или сети. Примеры несанкционированного доступа с помощью технических средств включают в себя:

– попытки извлечь файлы с паролями;

– атаки переполнения буфера с целью получения привилегированного (например, на уровне системного администратора) доступа к сети;

– использование уязвимостей протокола для перехвата соединения или ложного направления легитимных сетевых соединений;

– попытки расширить привилегии доступа к ресурсам или информации по сравнению с легитимно имеющимися у пользователя или администратора.

Инциденты несанкционированного доступа, создаваемые не техническими средствами, которые приводят к прямому или косвенному раскрытию, или модификации информации, нарушениям учетности или неправильному использованию информационных систем, могут вызываться следующими факторами:

– разрушением устройств физической защиты с последующим несанкционированным доступом к информации;

неудачной и (или) неправильной конфигурацией операционной системы вследствие неконтролируемых изменений в системе или неправильного функционирования программного или аппаратного обеспечения.

2. Кибератака и ее жизненный цикл.

Для того, чтобы успешно противостоять киберинцидентам, чтобы иметь возможность своевременно реагировать на их возникновение, необходимо четко понимать, как осуществляется в общем случае любая кибертатака.

В процессе атаки злоумышленники осуществляют структурированную последовательность шагов, называемую жизненный цикл атаки или в англоязычной литературе – cyber-killchain. Первоначально термин «killchain» использовался как военный термин для описания структуры военного вторжения. Зная последовательность действий противника, обороняющаяся сторона может выработать стратегию защиты и противостоять нападению. Впоследствии термин «жизненный цикл атаки» стал использоваться для описания компьютерных угроз, но с приставкой «cyber». Эта модель определяет, что должен сделать злоумышленник для того, чтобы достичь своих целей, атакуя сеть, извлекая данные и поддерживая присутствие в организации. Благодаря этой модели ясно, что блокировка злоумышленника на любом этапе разрывает всю цепочку атаки, так как ему для достижения успеха необходимо прой-

ти через все этапы, а нам, как обороняющейся стороне, достаточно всего лишь блокировать злоумышленника на любом этапе, чтобы добиться хотя бы минимального успеха.

Кибератаки могут осуществляться самыми разными способами, но всегда есть некоторая неизбежная точка, через которую они проходят в обязательном порядке. Этой точкой, как нетрудно догадаться, является то самое оконечное оборудование, которое, как говорилось в рамках изучения третьей темы курса, является самым уязвимым элементом любой сети. Поскольку точка, через которую пройдет любая кибератака, нам известна, то именно на уровне этой точки, на уровне оконечного устройства, у нас появляется наибольший шанс остановить как конкретную атаку, так и противодействовать в принципе любой кибератаке. При этом вероятность успеха будет выше, если злоумышленник будет остановлен на ранних этапах ее реализации.

Кроме того, необходимо понимать, что каждое вторжение в систему, а также следы, которое оно неизбежно оставляет на оконечном устройстве, – это шанс лучше узнать о действиях злоумышленника, который дает возможность использовать данную информацию себе на пользу. В военном плане, чем лучше мы понимаем врага и его способы осуществления атак, тем вероятнее сможем построить более эффективную оборону. Аналогично, на основе информации об этапах компрометации ИС, сотрудники, ответственные за информационную и кибербезопасность, могут выстраивать систему защиты ИС. Структурная схема жизненного цикла кибератаки приведена на рис. 61.

Рис. 61.

От того, на каком этапе жизненного цикла была обнаружена угроза, зависит эффективность расследования и размер материального и репутационного ущерба, нанесённого атакуемой организации. Так, обнаружение на этапе достижения цели (позднее обнаружение) означает, что система информационной и кибербезопасности ИС оказалась не способна противостоять атаке и злоумышленник достиг поставленных целей. Наименьший ущерб будет нанесён в случае обнаружения на этапах Доставки или Закрепления (раннее обнаружение).

Далее коротко обозначим каждый из этапов жизненного цикла кибератаки.

1. Разведка и сбор данных.

На этом этапе 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 информационной и кибербезопасности, возможности использования социальной инженерии по отношению к сотрудникам (например, выявить их аккаунты в социальных сетях).

По сути дела, на этом этапе злоумышленник пытается получить ответы на такие вопросы: «Какие методы атаки будут работать с наибольшей степенью успеха?» или, например, «Какие из них будет легче всего осуществить с точки зрения инвестиций и ресурсов?».

Разведка может быть пассивной и активной. Пассивная разведка заключается в получении информации без непосредственного воздействия на атакуемую ИС (например, просмотр DNS и Who Is информации, связанной с ИС организации). Активная разведка, в свою очередь, включает в себя взаимодействие с атакуемой ИС: сканирование портов, поиск уязвимостей ИС и другие действия. Независимо от того, какая именно разведка – активная или пассивная – применялась злоумышленником, в любом случае вся собранная им на этом этапе информация служит источником знаний для следующего этапа.

2. Выбор способа атаки.

Используя информацию, полученную на этапе разведки и сбора данных, злоумышленник определяет способ атаки. При этом он может создать новое вредоносное ПО, позволяющее эксплуатировать обнаруженные уязвимости либо использовать уже имеющееся.

На данном этапе злоумышленник, используя известные уязвимости различного рода прикладного программного обеспечения, используемого на оконечных устройствах жертвы, внедряет специальное зловредное ПО, которое будет использоваться при атаке, в файлы MS Office (.docx, .xlsx) или иных офисных приложений, PDF-документы, электронные письма или на съёмные носители. На этом же этапе происходит выбор способа доставки созданного вредоносного ПО в атакуемую организацию: с помощью заражения публичного ресурса компании, через одного из сотрудников или через компрометацию компаний-субподрядчиков, работающих с атакуемой организацией.

3. Доставка.

Атакующий должен обеспечить попадание разработанного на прошлом шаге вредоносного ПО в ИС атакуемой организации. Передача требуемого вредоносного контента возможна либо по инициативе жертвы (обычно для этого используются вложения электронной почты, вредоносные и фишинговые ссылки, WateringHole-атаки (заражения сайтов, которые посещают сотрудники атакуемой организации) или зараженные USB-устройства), либо по инициативе самого злоумышленника (SQL-инъекция или компрометация сетевой службы).

4. Эксплуатация.

После попадания в ИС атакуемой организации вредоносное ПО распространяется по сети и закрепляется на зараженных машинах в ожидании команд, посту-

пающих от злоумышленника. Как правило, это происходит при использовании известной уязвимости, для которой ранее был выпущен патч разработчиком программного обеспечения. В большинстве случаев (в зависимости от цели) злоумышленнику не требуется нести дополнительные расходы на поиск и эксплуатацию каких-либо неизвестных уязвимостей, поскольку известных оказывается более чем достаточно для достижения стоящих перед ним целей. Команды от злоумышленника могут поступать как через Интернет (от командных центров), так и с помощью доставки другого вредоносного ПО (например, если на машине отсутствует прямое подключение к Интернету).

5. Закрепление.

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 (так называемые бэкдоры). Очень часто заражение происходит на фоне каких-то внешних сетевых соединений. Обычно вредоносная программа скрывается в этих операциях, незаметно проникая на оконечные устройства, к которым можно получить доступ. После этого злоумышленник может контролировать это приложение без ведома жертвы.

6. Исполнение команд (CommandandControl, C&C).

С помощью соединения, устанавливаемого изнутри ИС атакованной организации, вредоносное ПО реализует взаимодействие с сервером управления, подконтрольным злоумышленнику (C&C Server). Таким образом, атакующий получает управление компьютером внутри ИС атакуемой организации. В результате злоумышленник передает на контролируемые им при помощи вредоносного ПО оконечные устройства требуемые команды: что делать далее и какую информацию собирать. Для сбора необходимых атакующему данных используются самые разные методы, такие как снимки экрана, контроль нажатия клавиш, взлом паролей, мониторинг сети на учетные данные, сбор критического контента и документов. Достаточно часто злоумышленник назначает так называемый промежуточный хост, куда копируются все данные, а затем они сжимаются и шифруются для дальнейшей отправки.

7. Достижение цели.

Получив управление, злоумышленник может работать с данными на скомпрометированном компьютере, не только осуществляя несанкционированный доступ, но и изменяя или удаляя их. На этом этапе атакующий отправляет собранные данные и/или выводит из строя ИТ-активы во время своего нахождения в сети жертвы. Затем, как правило, проводятся мероприятия по выявлению других целей, расширению своего присутствия внутри организации и (что самое важное) извлечению данных.

Затем вся цепочка повторяется. Вообще, особенностью жизненного цикла атаки является то, что он круговой, а не линейный. Как только злоумышленник проник в сеть, он снова начинает эту цепочку внутри сети, осуществляя дополнительную разведку и выполняя горизонтальное продвижение внутри атакованной сети.

Жизненный цикл кибератаки – это круговой и нелинейный процесс, когда злоумышленник выполняет непрерывное горизонтальное продвижение внутри сети. Этапы, которые выполняются уже внутри атакованной сети, на самом деле ровно

такие же, как и те, что выполняются на этапе получения доступа к ней. Однако необходимо понимать, что хотя этапы жизненного цикла кибератаки вне сети и внутри ее в целом одинаковы, но при нахождении внутри сети злоумышленники будут использовать другие методы для этапов внутренней цепочки, чем в случае, когда они находятся вне сети. Фактически, после проникновения злоумышленника в сеть, он становится инсайдером (пользователем с определенными правами и присутствием в сети), а это мешает специалистам по кибербезопасности подозревать атаку и понимать, что уже идут поздние стадии расширенной модели жизненного цикла кибератаки.

Сочетание внешнего и внутреннего жизненного цикла кибератаки называется расширенной моделью cyber-killchain. Это означает появление дополнительных этапов, которые фактически представляют собой практически такой же набор этапов, только они имеют в своем названии слово «внутренний»: внутренняя разведка, внутреннее выбор способов атаки и т. д.).

Каждый этап атаки после проникновения внутрь сети жертвы может занять от нескольких минут до нескольких месяцев, включая время окончательного ожидания, когда на месте уже все подготовлено, и можно начинать атаку.

Отметим, что злоумышленник никогда не действует напролом и наобум. Он всегда будет выжидать оптимальное время для запуска атаки, чтобы получить от нее максимальную отдачу. Например, этапы разведки и выбора способа атаки (иногда его называют этапом вооружения) могут занять достаточно длительный срок, вплоть до нескольких месяцев. При этом перехватить эти этапы чрезвычайно сложно, т. к. они выполняются без соединения со злоумышленником. Именно поэтому очень важно, чтобы средства безопасности на оконечных устройствах анализировали и контролировали все системы и приложения, запущенные на них. Это может существенно затруднить работу злоумышленника, в результате чего атака может стать финансово невыгодна для него.

На этапе внутренней разведки злоумышленник имеет доступ к рабочей станции какого-то одного пользователя, где он осуществляет извлечение данные из локальных файлов, сетевых папок, истории браузера, и т. д. Цель здесь одна, но она глобальна и заключается в том, чтобы дать злоумышленнику возможность выяснить, как эта машина может помочь исследовать сеть и позволить выйти на другие более ценные активы.

Воспользовавшись тем, что в системе могут быть не установлены необходимые патчи безопасности, а также известными уязвимостями веб-приложений и протоколов передачи данных, или даже такими банальными простыми вещами, которые, однако, очень часто встречаются, как учетные данные по умолчанию, злоумышленник получает возможность перейти от рабочих станций к серверам, используя расширение прав, горизонтальное продвижение внутри сети и воздействуя на отдельные целевые машины.

Если основываться на вышеизложенном, возникает резонный вопрос: как можно качественно защититься от киберугроз?

Для того, чтобы решить эту задачу нужно понимать, что у злоумышленника есть определенные цели, и он готов потратить определенные ресурсы для их достижения. Если механизмы безопасности оконечных устройств могут повысить стои-

мость атаки (деньги, люди или время) выше ожидаемой стоимости, тогда злоумышленник реже будет добиваться успехов или может даже отказаться от атаки организации.

В целом, все организации должны быть готовы к ситуации, когда злоумышленник получил доступ к внутренней корпоративной сети, логинам и паролям, ко всей документации и всем спецификациям сетевых устройств, системам, бэкапам и приложениям, а также быть в состоянии действовать незамедлительно. В этом может помочь более совершенная стратегия безопасности оконечных устройств и активов организации. Безусловно, она не будет являться панацеей и не сможет предотвратить все атаки, но сможет становить большинство из них на более ранних этапах реализации. Таким образом, одна из важнейших задач обеспечения кибербезопасности заключается в том, чтобы иметь эффективные механизмы защиты с учетом расширенной модели жизненного цикла киберугрозы, чтобы замедлить действия злоумышленника, сделать процесс развития его атаки более дорогим и максимально затруднить ее переход на каждый последующий этап.

Совершенно очевидно, что если злоумышленник не может достичь своих целей экономически оправданным способом, то он (если атака именно этой организации не является его принципиальной задачей), скорее всего, переключится на другие цели или будет достигать аналогичных целей при атаке на другие организации.

Стратегия безопасности организации должна учитывать атаки, осуществляемые не только снаружи, но, что особенно важно, изнутри, т. к. после проникновения хакера внутрь сети, он становится инсайдером с доступом к оконечным устройствам вместе с их активами.

Традиционный подход к обеспечению безопасности должен быть расширен за счет методов, основанных на понимании жизненного цикла кибератаки, и использования технологий, которые способны предотвратить получение злоумышленником доступа к оконечным устройствам, а также остановить его на любом возможном этапе в рамках внутреннего жизненного цикла кибератаки.

Добиться достижения этой цели достаточно трудно в силу целого ряда факторов: приложения становятся все более сложными и взаимосвязанными, они уязвимы, потому что многие программы разработаны без использования строгих принципов безопасности. Немаловажным является и человеческий фактор, поскольку сотрудники также остаются основным вектором риска, а значит, здесь есть возможности для атак, основанных на социальной инженерии.

Однако трудно – не означает «невозможно». Эта цель может быть достигнута различными методами, в частности путем использования специализированных систем защиты, о которых достаточно подробно говорится во втором вопросе в рамках изучения данной темы.

3. Характеристика основных этапов процесса реагированияна инциденты кибербезопасности.

Основными целями реагирования на инциденты кибербезопасности 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.

Основные этапы процесса реагирования на инциденты кибербезопасности представлены на рис. 62.

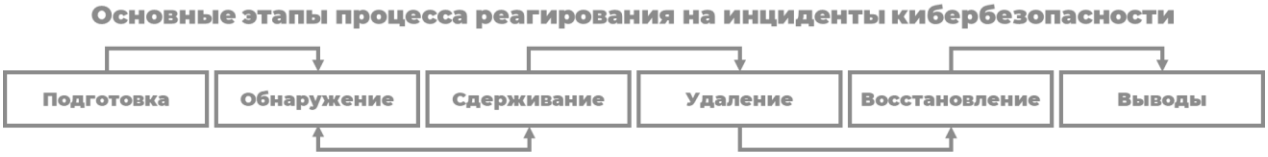


Рис. 62.

На основе информации о жизненном цикле атаки возможно формирование системы защиты. Исходя из анализа стратегии, используемой при атаке на ИС, специалистами в области кибербезопасности выработана встречная контрстратегия, целью которой является реагирование на инциденты. Основные элементы этой контрстратегии рассмотрим ниже.

1. Подготовка.

В момент, когда происходит инцидент кибербезопасности, от сотрудников, ответственных за ее обеспечение, требуются моментальные и точные действия. Поэтому для эффективного реагирования необходима предварительная подготовка. Сотрудники, ответственные за кибербезопасность, должны обеспечить защиту ИС и проинформировать пользователей, а также ИТ-персонал, о важности мер по обеспечению кибербезопасности.

Кроме того, очень важно, чтобы сотрудники, занимающиеся реагированием на инциденты кибербезопасности, в обязательном порядке прошли соответствующее обучение. При этом необходимо понимать, что появление новых видов киберугроз и новых стратегий их реализации требует от специалистов в области кибербезопасности постоянного повышения собственного уровня теоретической и практической подготовки, для чего им необходимо регулярно посещать тренинги по кибербезопасности, а также самостоятельно следить за последними тенденциями в области кибербезопасности и быть в курсе новейших программных и аппаратных решений в области кибербезопасности, а также отслеживать появляющиеся новые типы угроз и сценарии атак. Только в этом случае можно говорить о том, что специалисты в области кибербезопасности обладают необходимыми знаниями, умениями и навыками для того, чтобы оперативно и эффективно реагировать на инциденты кибербезопасности.

Для того чтобы эффективно противостоять киберугрозам, необходимо обеспечить защиту ИС на всех уровнях. Для этого на рабочих станциях рекомендуется установить специализированные, так называемые Endpoint-антивирусы, а в сети ИС

должны присутствовать системы предотвращения вторжений, файрволлы, прокси-серверы с авторизацией, анти-APT-решения, системы SIEM с интегрированными потоками данных об угрозах, системы сетевых ловушек и другие системы кибербезопасности.

Повышению безопасности ИС также способствует проведение тестов на проникновение в ИС данной компании и ознакомление специалистов, обеспечивающих кибербезопасность, с отчетами по тестированию на проникновение. Тестирование может быть проведено сторонними организациями, а информация из отчётов поможет выявить и устранить уязвимости в ИС организации.

Для отслеживания и ведения статистики инцидентов кибербезопасности необходимо выработать процедуру реагирования на такие инциденты, а также выбрать средство накопления и хранения экспертной информации и отчётов о произошедших ранее инцидентах. Такая информация позволит ускорить расследования инцидентов кибербезопасности в будущем.

2. Обнаружение.

Обнаружение события кибербезопасности может осуществляться любым работником, а также автоматически, например, при срабатывании модулей специализированных систем обнаружения вторжений.

В случае обнаружения события кибербезопасности в первую очередь необходимо:

– принять меры по локализации инцидента: прекратить (приостановить) работу, изолировать компьютер от сети передачи данных путем физического отключения сетевого кабеля от корпуса компьютера (требование применимо не всегда, о чем будет более подробно сказано ниже);

– поставить в известность о случившемся своего непосредственного руководителя (при наличии) и специалиста по кибербезопасности;

– при наличии возможности принять меры к сохранению свидетельств инцидента (скриншоты экрана, сохранение копий документов).

В дальнейшем, сотрудники, занимающиеся реагированием на инциденты, должны определить, является ли обнаруженное с помощью различных систем обеспечения кибербезопасности 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.

К источникам событий кибербезопасности относятся Anti-APT-системы, сетевые ловушки (honeypot), системы обнаружения вторжений и многие другие решения для обеспечения кибербезопасности. В рамках данной лекции область источников событий сужена до SIEM-систем (SIEM поддерживают интеграцию с различными программными и аппаратными решениями обеспечения кибербезопасности, в том числе прокси-серверами, брандмауэрами и другими) и систем централизованного

управления корпоративными Endpoint-антивирусами. Более подробно о SEIM системах поговорим в рамках третьего учебного вопроса данной темы.

Соответственно, триггерами для начала реагирования на инцидент будут следующие события:

– Событие в SIEM, возникающее в результате сопоставления событий от устройств обеспечения кибербезопасности с потоками данных об угрозах. Такое событие свидетельствует о наличии в исходном событии от устройства обеспечения кибербезопасности (например, прокси-сервера) одного из индикаторов, содержащихся в потоках данных об угрозах.

– Некоторые срабатывания антивируса на Endpoint-компьютере (информация о срабатывании отображается в центре управления антивирусами). Реагировать на это событие нужно точно таким же образом, как при получении события в SIEM, содержащего хеш вредоносного объекта.

Не всякое срабатывание антивируса должно инициировать процесс реагирования на инциденты. Требующими расследования можно считать следующие срабатывания:

– обнаружение взаимодействия с сервером управления C&C;

– безуспешное лечение зараженных объектов;

– неоднократное заражение одного и того же компьютера;

– ошибки в работе антивируса, которые приводят к снижению уровня защищённости.

Эти триггеры почти всегда свидетельствуют о наличии инцидента кибербезопасности. Однако не следует опираться только на них. О наличии инцидента могут свидетельствовать и иные события, наличие которых должно заставить сотрудника, ответственного за обеспечение кибербезопасности, более внимательно отнестись к исследованию данного события кибербезопасности, например:

– наличие неизвестного ПО в списках автозагрузки;

– появление неизвестных сервисов в списке сервисов ОС;

– запуск исполняемых файлов из папок, в которых ПО обычно не располагается (например, временные папки системы, системный кэш и другие);

– загрузка динамических библиотек из папок, в которых обычно данные библиотеки не располагаются (например, загрузка системных библиотек из папки, в которой располагается загружающий их исполняемый файл);

– непредвиденная или необычная сетевая активность;

– непредвиденное повышение привилегий пользователя и многие другие.

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 кибербезопасности.

3. Сдерживание.

Сотрудники, ответственные за обеспечение кибербезопасности, 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 организации могла продолжать работать без зараженных машин.

Цель этого этапа заключается не только в том, чтобы изолировать скомпрометированные компьютеры, но и в том, чтобы не допустить уничтожения индикаторов компрометации, которые могут помочь в расследовании инцидента. Некоторые угрозы не создают файлов на накопителях информации, а полностью размещают себя в оперативной памяти, так как там их сложнее обнаружить. Поэтому недопустимо отключать питание компьютера, так как при этом будет утрачена вся информация, содержащаяся в оперативной памяти.

Рекомендуется вывести инфицированные компьютеры в отдельную сеть. Однако в случае, если есть подозрение на APT-атаку, не следует физически отключать компьютер от локальной сети (путем извлечением провода). Дело в том, что некоторые виды угроз отслеживают наличие сетевого соединения и могут начать уничтожение следов в случае, если сеть была отключена на длительное время. Вместо этого следует перенастроить правила маршрутизации таким образом, чтобы инфицированные машины не смогли коммуницировать с другими компьютерами организации.

Для дальнейшего расследования необходимо получить дампы оперативной памяти и диска скомпрометированного компьютера. Снятие образов позволяет получить все компоненты вредоносного ПО. По результатам исследования этих компонентов можно определить, как следует бороться с заражением. Также анализ образов позволит определить вектор распространения угрозы, чтобы не допустить повторного заражения по аналогичному сценарию. При снятии образа диска записывается полный образ диска (в том числе с неиспользуемых секторов), а не только видимая пользователю часть, поэтому необходим носитель информации, превышающий общую емкость жесткого диска.

Далее необходимо осуществить перевод ИС в режим работы без изолированных машин. Это важно, поскольку проведение этапа восстановления займет некоторое время, и на это время ИС должна быть сконфигурирована таким образом, чтобы отсутствие пораженных машин минимально влияло на ее функционирование.

4. Удаление.

Цель этого этапа заключается в том, чтобы привести скомпрометированную ИС в состояние, в котором она была до заражения. Сотрудники, ответственные за обеспечение кибербезопасности, удаляют вредоносное ПО, а также все артефакты, которые оно могло оставить на зараженных компьютерах в ИС.

Существуют две стратегии проведения данного этапа – полное восстановление из образа рабочей станции или обнаружение и удаление угрозы и всех её артефактов.

В корпоративных сетях, где рабочее место пользователя, как правило, стандартизовано, может оказаться, что эффективнее вместо этапов сдерживания, удаления и восстановления полностью переустановить операционную систему и ПО на скомпрометированных пользовательских рабочих станциях (но образцы вредоносного ПО при этом необходимо сохранить для расследования). В случае заражения мо-

бильного устройства эффективнее может быть проведение процедуры аппаратного сброса.

5. Восстановление.

На этом этапе ранее скомпрометированные компьютеры вводятся обратно в сеть. При этом сотрудники, ответственные за обеспечение кибербезопасности, некоторое время продолжают наблюдать за состоянием этих машин и ИС в целом, чтобы убедиться в полном устранении угрозы.

6. Выводы.

На данном этапе сотрудники, ответственные за обеспечение кибербезопасности, анализируют произошедший инцидент, вносят необходимые изменения в конфигурацию ПО и оборудования, обеспечивающего кибербезопасность, 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.

По результатам расследования инцидента сотрудники, ответственные за обеспечение кибербезопасности, готовят отчет, содержание которого должно отвечать на вопросы:

– Когда, кем, и с помощью каких инструментов был впервые обнаружен инцидент?

– Что включал в себя инцидент?

– Как проводилось сдерживание, удаление и восстановление?

– На каких этапах реагирования сотрудники, ответственные за обеспечение кибербезопасности, были наиболее эффективны?

– Что необходимо улучшить в работе сотрудников, ответственных за обеспечение кибербезопасности?

Также на этом этапе необходимо подготовить рекомендации по повышению кибербезопасности ИС. Рекомендации основываются на информации о способах доставки и закрепления угрозы, полученной в ходе расследования. Такие рекомендации позволяют дополнить правила устройств, обеспечивающих кибербезопасность, новыми правилами и индикаторами угроз, в том числе расширить черные списки полученными индикаторами, например, URL- и IP-адресами, хеш-суммами угроз.

Выводы также могут повлечь обновление регламентов и правил пользования ИС организации. В таком случае новые правила должны быть доведены до сведения всех сотрудников организации и отражены в технологическом процессе обработки информации в ИС.

2. Мониторинг кибербезопасности

Во время своей работы практически все компании регулярно подвергаются угрозам, связанным с несанкционированным доступом к корпоративным информационным ресурсам.

Среди таких угроз наиболее часто встречающиеся – это атаки хакеров и распространение вредоносного ПО, однако риски кибербезопасности могут появляться и со стороны самих сотрудников. Низкий уровень компьютерной грамотности, устаревшее или уязвимое программное обеспечение, даже использование облачных сер-

висов или услуг сторонних IT-провайдеров могут нести угрозы, из которых самой серьезной является утечка или подмена критически важных для организации данных.

Так как подобные риски являются в настоящее время широко распространенными, и полностью исключить их нельзя, большое значение приобретает оперативное выявление подобных угроз и быстрое реагирование на них. Реализовать это возможно, используя средства мониторинга кибербезопасности. Работая в непрерывном автоматическом режиме, данные средства значительно снижают шанс для несанкционированных действий остаться незамеченными.

Мониторинг кибербезопасности представляет собой сбор, систематизирование и анализ сведений о состоянии корпоративной сети и поведении ее пользователей.

Основная цель такого анализа заключается в выявлении несанкционированных действий самих сотрудников или посторонних лиц, проникших в сеть. Современные системы мониторинга кибербезопасности позволяют обнаруживать такие действия и выдавать соответствующие уведомления, помогая тем самым своевременно пресекать риски.

С технической точки зрения это процесс автоматизированной проверки всех событий безопасности, которые система получает из ряда источников. Такими источниками являются:

– журналы операционной системы;

– антивирусные приложения;

– программное обеспечение, анализирующее защищенность инфраструктуры;

– сетевое оборудование.

На сегодняшний день существует ряд решений для обеспечения постоянного отслеживания угроз. Любая система мониторинга событий кибербезопасности может быть отнесена к одной из следующих категорий:

– SIEM (Security Information and Event Management) – системы, которые отслеживают и анализируют события в режиме реального времени;

– UBA (User Behavioral Analytics) – системы, которые собирают данные о действиях сетевых пользователей с целью последующего анализа и выявления возможных угроз;

– UEBA (User andEntityBehavioral Analytics) – системы, позволяющие обнаруживать аномалии в действиях пользователей и работе самих корпоративных сетей;

– Решения, контролирующие эффективность сотрудников и отслеживающие внутри сети все их действия, которые касаются работы с корпоративными конфиденциальными данными;

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

Рассмотрим основные компоненты систем мониторинга кибербезопасности.

Системы данного класса, как правило, включают в себя следующие основные компоненты:

– программные агенты – их задача заключается в сборе данных, поступающих из различных источников;

– сервер – выполняет централизованный анализ поступившей информации, основываясь на тех правилах и политиках, которые были заданы ИБ-специалистом;

– хранилища информации – консолидируют данные обо всех событиях безопасности, поступающих из источников. Информация в хранилище может содержаться от нескольких дней до нескольких месяцев, в зависимости от размера самого хранилища и объемов поступающих данных;

– консоль – служит для управления параметрами обработки, просмотра журналов событий и обращения к хранилищу;

– персонал, работающий с системой;

– регламенты работы по мониторингу.

Для того чтобы настроить мониторинг кибербезопасности средств и систем информатизации, необходимо определить ряд параметров:

– что должно рассматриваться в качестве инцидента кибербезопасности;

– какие виды инцидентов присущи или могут быть присущи данной компании;

– какие события могут предварять каждый тип инцидента;

– какие источники могут производить инциденты;

– к каким рискам ведет каждый вид инцидента и каков взаимный приоритет данных рисков.

В каждой компании определение этих параметров и настройка систем мониторинга индивидуальны. Выбор самой системы предполагает учет таких нюансов, как планируемое количество источников событий для обработки, возможности системы по анализу поступающих событий, функционал визуализации и детализации отчетов. Сегодня на рынке существует широкий выбор решений для мониторинга ИБ, как отечественных, так и зарубежных, среди которых – системы от Cisco, McAfee, Fortinet и др.

Для целей предотвращения угроз, выявляемых в ходе мониторинга, создаются центры управления событиями кибербезопасности, о которых подробно говорилось в рамках изучения первой темы курса. Напомним, что центр управления событиями кибербезопасности представляет собой команду специалистов по кибербезопасности, основная задача которых заключается в выявлении и предотвращении угроз корпоративным данным.

Мониторинг состояния кибербезопасности дает возможность в автоматическом режиме анализировать работу IT-ресурсов компании, сетевых приложений, оборудования и веб-сервисов. Применение специализированных решений для мониторинга позволяет эффективно управлять рисками и обеспечивать соответствие всех систем корпоративным политикам кибербезопасности.

В то же время некорректно настроенная, пусть и дорогая, система мониторинга кибербезопасности не позволит снизить потери от негативных инцидентов кибербезопасности. Поэтому рекомендуется проводить ее аудит не реже одного раза в год.

3. Системы обнаружения вторжений, принципы их построения и использования

Вопрос, связанный с системами обнаружения и предотвращения вторжений, уже рассматривался в рамках изучения третьей темы курса. Однако тогда рассмотрение было ограничено лишь перечислением видов таких систем и очень краткой их характеристикой. В рамках данного вопроса рассмотрим более детально системы

обнаружения и предотвращения вторжений и обозначим достоинства и недостатки каждого вида систем подобного рода.

Системы обнаружения сетевых вторжений и выявления признаков компьютерных атак на информационные системы уже давно применяются как один из необходимых рубежей обороны информационных систем. На российском рынке широко представлены коммерческие системы обнаружения вторжений и атак (СОВ, СОА) иностранных компаний (ISS RealSecure, NetPatrol, Snort, Cisco и т. д.) и в то же время практически не представлены комплексные решения российских разработчиков. Это вызвано тем, что многие отечественные исследователи и разработчики реализуют СОА, сохраняя аналогии архитектур и типовых решений уже известных систем, не особенно стараясь увеличить эффективность превентивного обнаружения атак и реагирования на них.

В настоящее время системы обнаружения вторжений и атак обычно представляют собой программные или аппаратно-программные решения, которые автоматизируют процесс контроля событий, протекающих в компьютерной системе или сети, а также самостоятельно анализируют эти события в поисках признаков проблем безопасности. Поскольку количество различных типов и способов организации несанкционированных проникновений в чужие компьютерные сети за последние годы значительно увеличилось, СОА стали необходимым компонентом инфраструктуры безопасности большинства организаций.

В настоящее время можно разделить все системы обнаружения вторжений на сетевые и локальные. Сетевые системы обычно устанавливаются на выделенных для этих целей компьютерах и анализируют трафик, циркулирующий в локальной вычислительной сети. Локальные (или системные) СОА размещаются на отдельных компьютерах, нуждающихся в защите, и анализируют различные события (действия пользователя или программные вызовы). Также различают методики обнаружения аномального поведения и обнаружения злоумышленного поведения пользователей. Выделяют две основные методики:

1. Системы обнаружения аномального поведения (от англ. anomalydetection) основаны на том, что СОА известны некоторые признаки, характеризующие правильное или допустимое поведение объекта наблюдения. Под «нормальным» или «правильным» поведением понимаются действия, выполняемые объектом и не противоречащие политике безопасности.

2. Системы обнаружения злоумышленного поведения (misusedetection) основаны на том, что заранее известны некоторые признаки, характеризующие поведение злоумышленника. Наиболее распространенной реализацией технологии обнаружения злоумышленного поведения являются экспертные системы. Представительным западным аналогом такой системы является бесплатно распространяемая и наиболее популярная система Snort.

Рассмотрим классификацию компьютерных атак и систем их обнаружения. Это важный вопрос, поскольку эффективная защита от потенциальных сетевых атак невозможна без их детальной классификации, облегчающей их выявление и задачу противодействия им. В настоящее время известно большое количество различных типов классификационных признаков. В качестве таких признаков может быть выбрано, например, разделение на пассивные и активные, внешние и внутренние ата-

ки, умышленные и неумышленные и т. д. К сожалению, несмотря на то, что некоторые из существующих классификаций мало применимы на практике, их активно используют при выборе СОА и их эксплуатации.

Рассмотрение существующих классификаций начнем с работы Питера Мелла «Компьютерные атаки: что это и как им противостоять». В ней все возможные сетевые атаки делятся на следующие типы:

– удаленное проникновение – это тип атак, которые позволяют реализовать удаленное управление компьютером через сеть; например, атаки с использованием программ NetBus или BackOrifice;

– локальное проникновение – это тип атак, которые приводят к получению несанкционированного доступа к узлу, на который они направлены; примером такой атаки является атака с использованием программы GetAdmin;

– удаленный отказ в обслуживании – тип атак, которые позволяют нарушить функционирование системы в рамках глобальной сети; пример такой атаки – Teardrop или trinOO;

– локальный отказ в обслуживании – тип атак, позволяющих нарушить функционирование системы в рамках локальной сети. В качестве примера такой атаки можно привести внедрение и запуск враждебной программы, которая загружает центральный процессор бесконечным циклом, что приводит к невозможности обработки запросов других приложений;

– атаки с использованием сетевых сканеров – это тип атак, основанных на использовании сетевых сканеров – программ, которые анализируют топологию сети и обнаруживают сервисы, доступные для атаки; пример: атака с использованием утилиты nmap;

– атаки с использованием сканеров уязвимостей – тип атак, основанных на использовании сканеров уязвимостей – программ, осуществляющих поиск уязвимостей на узлах сети, которые в дальнейшем могут быть применены для реализации сетевых атак; примерами сетевых сканеров могут служить системы SATAN и Shadow Security Scanner;

– атаки с использованием взломщиков паролей – это тип атак, которые основаны на использовании взломщиков паролей – программ, подбирающих пароли пользователей; например, программа LOphtCrack для ОС Windows или программа Crack для ОС Unix;

– атаки с использованием анализаторов протоколов – это тип атак, основанных на использовании анализаторов протоколов – программах, «прослушивающих» сетевой трафик. С их помощью можно автоматизировать поиск в сетевом трафике такой информации, как идентификаторы и пароли пользователей, информацию о кредитных картах и т. д. Примерами анализаторов сетевых протоколов являются программы Microsoft Network Monitor, NetXRay компании Network Associates или Lan Explorer.

Приведенная классификация является достаточно полной с практической точки зрения, так как она охватывает почти все возможные действия злоумышленника. Однако для противодействия сетевым атакам этого недостаточно, так как ее использование в данном виде не позволяет определять элементы сети, подверженные воз-

действию той или иной атаки, а также последствия, к которым может привести успешная реализация атак. В таком случае в анализ не включается самый важный компонент, а именно – модель угроз безопасности, с построения которой должны начинаться все мероприятия по обеспечению защиты информации.

Аналогичным недостатком страдает и более компактная классификация, предложенная компанией Internet Security Systems, Inc., в которой содержится всего лишь пять типов атак:

– сбор информации;

– попытки несанкционированного доступа;

– отказ в обслуживании;

– подозрительная активность;

– системные атаки.

В своих продуктах, предназначенных для защиты сетей, серверов и рабочих станций (таких как, например, Real Secure, System scanner и др.) компания Internet Security Systems использует несколько других классификационных признаков возможных сетевых атак, они более эффективны с точки зрения защиты от вторжений. Опишем их подробнее.

По степени риска: имеет большое практическое значение, так как позволяет ранжировать опасность атак по следующим классам:

– высокий – атаки, успешная реализация которых позволяет атакующему немедленно получить доступ к машине, получить права администратора или обойти межсетевые экраны (например, атака, основанная на использовании ошибки в ПО Sendmail версии 8.6.5, позволяет атакующему исполнять любую команду на сервере);

– средний – атаки, успешная реализация которых потенциально может дать атакующему доступ к машине. Например, ошибки в сервере NIS, позволяющие атакующему получить файл с гостевым паролем;

– низкий – атаки, при успешной реализации которых атакующий может получить сведения, облегчающие ему задачу взлома данной машины. Например, используя сервис finger, атакующий может определить список пользователей сервера и, используя атаку по словарю, попытаться получить доступ к машине.

По типу атаки: позволяет судить о том, может ли атака быть осуществлена удаленно, или только локально:

– осуществляемые локально;

– осуществляемые удаленно.

По подверженному данной атаке программному обеспечению. Например: Microsoft Internet Explorer 11, Opera Browser 12.18, Google Chrome 96.

Кроме того, существует классификация **по характеру действий, используемых в атаке**:

– «черные ходы» (Backdoors) – атаки, основанные на использовании недокументированных разработчиками возможностях ПО, которые могут привести к выполнению пользователем несанкционированных операций на атакуемом сервере;

– атаки типа «отказ в обслуживании» (DoS) – атаки, основанные на использовании ошибок, позволяющие атакующему сделать какой-либо сервер недоступным для легитимных пользователей;

– распределенные атаки типа «отказ в обслуживании» (DDoS) – несколько пользователей (или программ) посылают большое количество фиктивных запросов на сервер, приводя последний в нерабочее состояние;

– потенциально незащищенная операционная система;

– неавторизованныйдоступ.

К недостаткам приведенных классификационных признаков можно отнести то, что они не позволяют описать цель атаки, а также ее последствия. Например, классификационный признак «по характеру действий» содержит два класса атак типа «отказ в обслуживании», но в то же время не содержит классов, описывающих атак, направленных на перехват трафика.

Существуют и другие виды классификаций, но, как можно заметить, большинство из них страдают неполнотой, а в некоторых случаях под видом единой классификации делается попытка объединить несколько классификаций, проведенных по разным характеристическим параметрам.

Появление новых атак приводит к снижению эффективности применения существующих классификаций, поэтому их использование без внесения изменений не представляется возможным. Данная ситуация объясняется огромным количеством различных сетевых атак и постоянным появлением новых, некоторые из которых не подчиняются критериям существующих классификаций.

Из отечественных вариантов наиболее информативная и краткая классификация приведена в книге Милославской и Толстого. В ней все СОА делятся на минимальное количество классов – по поведению после обнаружения (на активные и пассивные), по расположению источника результатов аудита (регистрационные файлы хоста либо сетевые пакеты), по методу обнаружения (поведенческие либо интеллектуальные).

Данная классификация наилучшим образом подходит для построения первичных фильтров СОА, поскольку позволяет ответить на вопрос о том, как именно СОА анализируют информацию, как должны различать атаки, какие технологии для этого использовать.

Перейдем к рассмотрению технологий построения систем обнаружения вторжений.

Системы обнаружения вторжений, как и большинство современных программных продуктов, должны удовлетворять ряду требований. Это и современные технологии разработки, и ориентировка на особенности современных информационных сетей, и совместимость с другими программами. Чтобы понять, как правильно использовать СОА, нужно четко представлять, как они работают и каковы их уязвимые места.

Рассмотрим принципы, на которых основана идея обнаружения компьютерных атак. Если не учитывать различные минорные инновации в области обнаружения компьютерных атак, то можно смело утверждать, что существуют две основные технологии построения СОА. Суть их заключается в том, что СОА обладают некоторым набором знаний либо о методах вторжений, либо о «нормальном» поведении наблюдаемого объекта.

1. Системы обнаружения аномального поведения основаны на том, что СОА известны некоторые признаки, характеризующие правильное или допустимое пове-

дение объекта наблюдения. Под нормальным или правильным поведением понимаются действия, выполняемые объектом и не противоречащие политике безопасности.

2. Системы обнаружения злоумышленного поведения основаны на том, что СОА известны некоторые признаки, характеризующие поведение злоумышленника. Наиболее распространенной реализацией технологии обнаружения злоумышленного поведения являются экспертные системы (например, системы Snort, RealSecure IDS, Enterasys Advanced Dragon IDS).

Технологии обнаружения аномальной деятельности. Датчики-сенсоры аномалий идентифицируют необычное поведение, аномалии в функционировании отдельного объекта – трудности их применения на практике связаны с нестабильностью самих защищаемых объектов и взаимодействующих с ними внешних объектов. В качестве объекта наблюдения может выступать сеть в целом, отдельный компьютер, сетевая служба (например, файловый сервер FTP), пользователь и т. д. Датчики срабатывают при условии, что нападения отличаются от «обычной» (законной) деятельности. Здесь появляется еще одно слабое место, характерное в большей степени для конкретных реализаций, заключающееся в некорректности определения «дистанции» отклонения наблюдаемого поведения от штатного, принятого в системе, и определении «порога срабатывания» сенсора наблюдения.

Меры и методы, обычно используемые в обнаружении аномалии, включают в себя следующие:

– пороговые значения: наблюдения за объектом выражаются в виде числовых интервалов. Выход за пределы этих интервалов считается аномальным поведением. В качестве наблюдаемых параметров могут быть, например, такие: количество файлов, к которым обращается пользователь в данный период времени, число неудачных попыток входа в систему, загрузка центрального процессора и т. п. Пороги могут быть статическими и динамическими (т. е. изменяться, подстраиваясь под конкретную систему);

– статистические меры: решение о наличии атаки делается по большому количеству собранных данных путем их статистической предобработки;

– параметрические: для выявления атак строится специальный «профиль нормальной системы» на основе шаблонов (т. е. некоторой политики, которой обычно должен придерживаться данный объект);

– непараметрические: здесь уже профиль строится на основе наблюдения за объектом в период обучения;

– меры на основе правил (сигнатур): они очень похожи на непараметрические статистические меры. В период обучения составляется представление о нормальном поведении объекта, которое записывается в виде специальных «правил». Получаются сигнатуры «хорошего» поведения объекта;

– другие меры: нейронные сети, генетические алгоритмы, позволяющие классифицировать некоторый набор видимых сенсору-датчику признаков.

Следует заметить, что существуют две крайности при использовании данной технологии (выявление аномальной активности):

– обнаружение аномального поведения, которое не является атакой, и отнесение его к классу атак (ошибка второго рода);

– пропуск атаки, которая не подпадает под определение аномального поведения (ошибка первого рода). Этот случай гораздо более опасен, чем ложное причисление аномального поведения к классу атак.

Поэтому при инсталляции и эксплуатации систем такой категории обычные пользователи и специалисты сталкиваются с двумя довольно нетривиальными задачами:

– построение профиля объекта – это трудно формализуемая и затратная по времени задача, требующая от специалиста по кибербезопасности большой предварительной работы, высокой квалификации и опыта;

– определение граничных значений характеристик поведения субъекта для снижения вероятности появления одного из двух вышеназванных крайних случаев.

Обычно системы обнаружения аномальной активности используют журналы регистрации и текущую деятельность пользователя в качестве источника данных для анализа. Достоинства систем обнаружения атак на основе технологии выявления аномального поведения можно оценить следующим образом:

– системы обнаружения аномалий способны обнаруживать новые типы атак, сигнатуры для которых еще не разработаны;

– они не нуждаются в обновлении сигнатур и правил обнаружения атак;

– обнаружения аномалий генерируют информацию, которая может быть использована в системах обнаружения злоумышленного поведения.

Недостатками систем на основе технологии обнаружения аномального поведения являются следующие:

– системы требуют длительного и качественного обучения;

– системы генерируют много ошибок второго рода;

– системы обычно слишком медленны в работе и требуют большого количества вычислительных ресурсов.

Методы статистического анализа компьютерных атак. Применение методов статистического анализа является наиболее распространенным видом реализации технологии обнаружения аномального поведения. Статистические датчики собирают различную информацию о типичном поведении объекта и формируют ее в виде профиля. Профиль в данном случае – это набор параметров, характеризующих типичное поведение объекта. Существует период начального формирования профиля. Профиль формируется на основе статистики объекта, и для этого могут применяться стандартные методы математической статистики, например метод скользящих окон и метод взвешенных сумм.

После того как профиль сформирован, действия объекта сравниваются с соответствующими параметрами и при обнаружении существенных отклонений подается сигнал о начале атаки. Параметры, которые включаются в профиль системы, могут быть отнесены к следующим распространенным группам:

– числовые параметры (количество переданных данных по различным протоколам, загрузка центрального процессора, число файлов, к которым осуществлялся доступ и т. п.);

– категориальные параметры (имена файлов, команды пользователя, открытые порты и т. д.);

– прочие параметры, не вписывающиеся в классификацию наравне с предыдущими типами параметров.

Профили также должны иметь механизмы динамического изменения, для того чтобы более полно описывать изменяющееся поведение объекта. Системы, применяющие статистические методы, обладают целым рядом достоинств:

– не требуют постоянного обновления базы сигнатур атак. Это значительно облегчает задачу сопровождения данных систем;

– могут обнаруживать неизвестные атаки, сигнатуры для которых еще не написаны. Могут являться своеобразным сдерживающим буфером, пока не будет разработан соответствующий шаблон для экспертных систем;

– позволяют обнаруживать более сложные атаки, чем другие методы. Они могут обнаруживать атаки, распределенные во времени или по объектам нападения;

– могут адаптироваться к изменению поведения пользователя и поэтому являются более чувствительными к попыткам вторжения, чем люди.

Среди недостатков систем обнаружения вторжений можно отметить следующие:

– трудность задания порогового значения (выбор этих значений – очень нетривиальная задача, которая требует глубоких знаний контролируемой системы);

– злоумышленник может обмануть систему обнаружения атак, и она воспримет деятельность, соответствующую атаку, в качестве нормальной из-за постепенного изменения режима работы с течением времени и «приручения» системы к новому поведению;

– в статистических методах вероятность получения ложных сообщений об атаке является гораздо более высокой, чем при других методах;

– статистические методы не очень корректно обрабатывают изменения в деятельности пользователя (например, когда менеджер исполняет обязанности подчиненного в критической ситуации). Этот недостаток может представлять большую проблему в организациях, где изменения являются частыми. В результате могут появиться как ложные сообщения об опасности, так и отрицательные ложные сообщения (пропущенные атаки);

– статистические методы не способны обнаружить атаки со стороны субъектов, для которых невозможно описать шаблон типичного поведения;

– системы, построенные исключительно на статистических методах, не справляются с обнаружением атак со стороны субъектов, которые с самого начала выполняют несанкционированные действия. Таким образом, шаблон обычного поведения для них будет включать только атаки;

– статистические методы должны быть предварительно настроены (заданы пороговые значения для каждого параметра, для каждого пользователя);

– статистические методы на основе профиля нечувствительны к порядку следования событий.

Тем не менее, существуют пути решения данных проблем, и их практическая реализация является лишь вопросом времени. Очевидно, что статистический метод является чистой реализацией технологии аномального поведения. Статистический метод наследует у технологии обнаружения аномалий все так необходимые на практике достоинства.

Краткий анализ систем, использующих сигнатурные методы обнаружения кибератак.

Сигнатурные методы позволяют описать атаку набором правил или с помощью формальной модели, в качестве которой может применяться символьная строка, семантическое выражение на специальном языке и т. п. Суть данного метода заключается в использовании специализированной базы данных шаблонов (сигнатур) атак для поиска действий, подпадающих под определение «атака».

Сигнатурный метод может защитить от вирусной или хакерской атаки, когда уже известна сигнатура атаки (например, неизменный фрагмент тела вируса) и она внесена в базу данных СОА. То есть, когда сеть переживает первое нападение извне, первое заражение еще неизвестным вирусом и в базе попросту отсутствует сигнатура для его поиска, сигнатурная СОА не сможет сигнализировать об опасности, поскольку сочтет атакующую деятельность легитимной.

Таким образом, эффективность работы сигнатурной СОА определяется тремя основными факторами: оперативностью пополнения сигнатурной базы, ее полнотой с точки зрения определения сигнатур атак, а также наличием интеллектуальных алгоритмов сведения действий атакующих к некоторым базовым шагам, в рамках которых происходит сравнение с сигнатурами.

Для успешной реализации первых двух факторов необходима поддержка международных стандартов и рекомендаций обмена сигнатурами и информацией об атаках. Поскольку на данный момент не существует достаточно большого количества распределенных и объективных источников сигнатур, то СОА данного типа имеют весьма ограниченную эффективность в реальных сетях.

Краткий анализ систем, использующих методы поиска аномалий в поведении.

Системы поиска аномалий идентифицируют необычное поведение («аномалии») в функционировании контролируемого объекта. В качестве объекта наблюдения может выступать сеть в целом, отдельный компьютер, сетевая служба (например, файловый сервер FTP), пользователь и т. д. Сигнализация СОА срабатывает при условии, что действия, совершаемые при нападении, отличаются от «обычной» (законной) деятельности пользователей и компьютеров. Как уже указывалось выше меры и методы, обычно используемые в обнаружении аномалии, включают использование:

– пороговых значений (наблюдения за объектом выражаются в виде числовых интервалов);

– статистических мер (решение о наличии атаки делается по большому количеству собранных данных);

– профилей (для выявления атак на основе заданной политики безопасности строится специальный список легитимных действий «профиль нормальной системы»);

– нейронных сетей, генетических алгоритмов.

Отличительной чертой данных систем является необходимость их обучения на «стандартное» поведение контролируемого объекта (например, корпоративной интрасети). Это же является и основным недостатком всех подобных методов, поскольку время обучения составляет довольно большой промежуток времени и все это время на контролируемые объекты не должно быть произведено ни единой ата-

ки. И это большая проблема, поскольку если с целью исключения или минимизации риска атак защищаемая интрасеть на этапе обучения отключается от других сетей, то на этапе эксплуатации система защиты будет классифицировать все попытки легального взаимодействия с внешними сетями как атаки.

В случае создания СОА, использующей профильные системы следует учитывать, что далеко не все пользователи компьютерных сетей могут быть в принципе спрофилированы в силу разных причин, в том числе в силу того, что их поведение невозможно стандартизировать, особенно в современных условиях, оно имеет тенденции к очень существенному изменению в очень ограниченные сроки. Статичность существующих профильных систем позволяет говорить об этом как об одном из основных недостатков, явно мешающих эксплуатации СОА на базе контроля «профилей» пользователей.

В случае динамической подстройки и модификации профилей необходимо найти компромисс между количеством признаков профилирования (чем их меньше, тем грубее оценивается поведение контролируемого объекта) и скоростью обработки (скорость оценки аномальности поведения по профилю является экспоненциальной функцией от количества исследуемых признаков). Кроме того, большое число конфигурационных параметров в этом случае неизбежно потребуют от администратора системы защиты высокой квалификации в весьма специализированной области обнаружения атак.

Такой подход реализован в некоторых отечественных СОА. Данные разработки относятся к классу системных СОА, их экземпляры должны эксплуатироваться на каждом информационном ресурсе, нуждающемся в защите. Особенностью одной из данных систем является использование процедур нечеткого поиска. Для каждого из пользователей создается свой индивидуальный профиль, при этом поведение, характерное для одного из пользователей, может считаться необычным для другого, и наоборот. Поскольку такие профили трудно формализовать, они создаются на основе примеров нормальной работы того или иного пользователя.

В завершение рассмотрения вопроса дадим общую оценку современного подхода к обнаружению вторжений.

Большинство рассмотренных недостатков современных СОА являются недостатками, с которыми может столкнуться пользователь в реальных компьютерных сетях. Существующие подходы к решению задач обнаружения вторжений зачастую отличаются не только реализацией методов обнаружения, но и своей архитектурой, уровнем детализации и типами обнаружения вторжений. Естественно, что у каждой системы есть свои достоинства и недостатки. Несмотря на постоянное развитие применяемых при разработке СОА технологий, о легкости развертывания, эксплуатации и модификации систем обнаружения вторжений придется забыть, все существующие разработки имеют тенденцию лишь к усложнению. Это связано с тем, что технологии взлома постоянно совершенствуются, атаки становятся комбинированными и распространяются с очень большой скоростью, поэтому к современным СОА выдвигаются все более жесткие требования, а это, в свою очередь, затрудняет их практическую эксплуатацию.

4. Системы управления событиями и данными безопасности (SIEM)

В рамках данного вопроса кратко рассмотрим SEIM-системы и как они применяются для реагирования на инциденты кибербезопасности.

SIEM – это Security Information and Event Management, система управления событиями и информацией о безопасности. Как видно из названия – «сама по себе» такая система не способна что-либо предотвращать или защищать. Данная система предназначена для анализа информации, поступающей от различных других систем, таких как DLP (DataLeakPrevention, специализированное ПО, обеспечивающее защиту от утечек информации), систем обнаружения и предотвращения вторжений, антивирусов, различного оборудования (маршрутизаторов, роутеров, АРМ пользователей, серверов и т. д.) и дальнейшего выявления отклонения от норм по каким-то критериям. Как только система выявляет отклонение от нормы, она генерирует сообщение об инциденте. Таким образом в основе работы SIEM лежит почти голая математика и статистика, а сама по себе SEIM каких-либо защитных функций в себе не несет.

Перед системой SIEM ставятся следующие задачи.

– Консолидация и хранение журналов событий от различных источников – сетевых устройств, приложений, журналов ОС, средств защиты. Заглянув в любой стандарт информационной или кибербезопасности, можно увидеть в нем технические требования по сбору и анализу событий. Очевидно, что они нужны не только для того, чтобы выполнить требование стандарта. На практике достаточно часто возникают ситуации, когда инцидент выявлен поздно, а события уже давно затерты или журналы событий почему-либо недоступны, в результате чего причины инцидента выявить фактически невозможно. Кроме того, соединение с каждым источником и просмотр событий займет слишком много времени. Именно здесь на помощь приходят системы SEIM.

– Предоставление инструментов для анализа событий и разбора инцидентов. Форматы событий в различных источниках различаются. Текстовый формат при больших объемах сильно утомляет, снижает вероятность выявления инцидента. Часть продуктов класса SIEM унифицирует события и делает их более читабельными, а интерфейс визуализирует только важные информационные события, акцентирует на них внимание, позволяет отфильтровывать некритические события.

– Корреляция и обработка по правилам. По одному событию не всегда можно судить об инциденте. Простейший пример – событие «loginfailed»: один случай ничего не значит, вполне возможно, что это пользователь ошибся при вводе имени пользователя или пароля, но три и более таких события с одной учетной записью уже могут свидетельствовать о попытках подбора. К тому же, возможны ситуации, когда внешне безобидные события, полученные от различных источников, в совокупности несут в себе угрозу. Например, когда происходит отправка письма с важными для организации данными человеком, имеющим на это право, но на адрес, находящийся вне его обычного круга адресов, на которые он отправляет почту. Система предотвращения утечек информации может не отреагировать на такое событие, но SIEM, используя накопленную статистику, на основании этого уже сгенерирует инцидент. В простейшем случае в SIEM правила представлены в формате RBR (Rule

Based Reasoning, разрешения, основанные на правилах) и содержат набор условий, триггеры, счетчики, сценарий действий.

– Автоматическое оповещение и инцидент-менеджмент. Основная задача SIEM – не просто собрать события, но автоматизировать процесс обнаружения инцидентов с документированием в собственном журнале или внешней системе, а также своевременно информировать о событии.

SIEM способна выявлять:

– сетевые атаки во внутреннем и внешнем периметрах;

– вирусные эпидемии или отдельные вирусные заражения, неудаленные вирусы, бэкдоры и трояны;

– попытки несанкционированного доступа к конфиденциальной информации;

– фрод и мошенничество;

– ошибки и сбои в работе информационных систем;

– уязвимости;

– ошибки конфигураций в средствах защиты и информационных системах.

Система SIEM универсальна за счет своей логики. Но для того, чтобы возложенные на нее задачи решались – необходимы полезные источники и правила корреляции. Любое событие (например, если в определенной комнате открылась дверь) может быть подано на вход SIEM и использовано.

5. Банк данных угроз безопасности информации ГНИИИ ПТЗИ ФСТЭК России

Огромную роль для реагирования на инциденты кибербезопасности и их обработки играют банки и базы данных, содержащие сведения о различных киберугрозах, способах их реализации и методах защиты от них. Одним из примеров таких банков данных является банк данных угроз безопасности информации, сформированный в 2015 году Государственным научно-исследовательским испытательным институтом проблем технической защиты информации ФСТЭК России совместно с заинтересованными органами власти и организациями. Банк данных находится в свободном доступе и размещен на сайте https://bdu.fstec.ru/. Целью создания и ведения этого банка данных является повышение информированности заинтересованных лиц о существующих угрозах безопасности информации в информационных (автоматизированных) системах.

Банк данных угроз безопасности информации предназначен:

– для заказчиков информационных (автоматизированных) систем и их систем защиты;

– операторов информационных (автоматизированных) систем и их систем защиты;

– разработчиков информационных (автоматизированных) систем и их систем защиты;

– разработчиков и производителей средств защиты информации;

– испытательных лабораторий и органов по сертификации средств защиты информации;

– иных заинтересованных организаций и лиц.

Банк содержит сведения об основных угрозах безопасности информации и уязвимостях, в первую очередь, характерных для государственных информационных систем и автоматизированных систем управления производственными и технологическими процессами критически важных объектов.

Важно понимать, что сведения об угрозах безопасности информации и уязвимостях программного обеспечения, содержащиеся в данном банке, не являются исчерпывающими и могут дополняться по результатам анализа угроз безопасности информации и уязвимостей в конкретной информационной (автоматизированной) системе с учетом особенностей ее эксплуатации. Угрозы безопасности информации, включенные в состав банка, не являются элементами иерархической классификационной системы угроз, а представляют собой обобщенный перечень основных угроз безопасности информации, потенциально опасных для информационных систем.

По состоянию на август 2022 года банк содержит детальную информацию о 222 угрозах и 41919 уязвимостях. Банк данных активно развивается и каждый желающий может сообщить об обнаруженной им угрозе посредством специальной формы обратной связи.

В качестве фильтров для поиска угроз можно выбрать:

1. Источник угрозы – тип нарушителя и его минимально необходимый функционал:

– внутренний нарушитель с низким потенциалом;

– внутренний нарушитель со средним потенциалом;

– внутренний нарушитель с высоким потенциалом;

– внешний нарушитель с низким потенциалом;

– внешний нарушитель со средним потенциалом;

– внешний нарушитель с высоким потенциалом.

2. Последствия реализации угрозы:

– нарушение конфиденциальности;

– нарушение целостности;

– нарушение доступности.

Также доступен контекстный поиск по названию угрозы.

Описание угрозы выглядит следующим образом (рис. 63):

В паспорте каждой угрозы есть ее наименование, уникальный идентификатор, описание, источники угрозы (минимальные возможности внешнего или внутреннего нарушителя, необходимые для реализации угрозы), объекты воздействия и последствия реализации угрозы. Последствия реализации угрозы категорированы в соответствии с тремя основными свойствами информации с точки зрения информационной безопасности – конфиденциальностью, доступностью и целостностью.

Для поиска уязвимостей программного обеспечения доступны следующие фильтры:

– контекстный поиск по названию уязвимости;

– производитель ПО, в котором обнаружена уязвимость;

– аппаратная платформа, при установке на которой программное обеспечение содержит уязвимость;

– версия ПО – версия программного обеспечения, в которой обнаружена уязвимость;

– статус уязвимости – характеристика уязвимости, определяющая степень подтверждения факта существования уязвимости. Возможны следующие значения статуса:

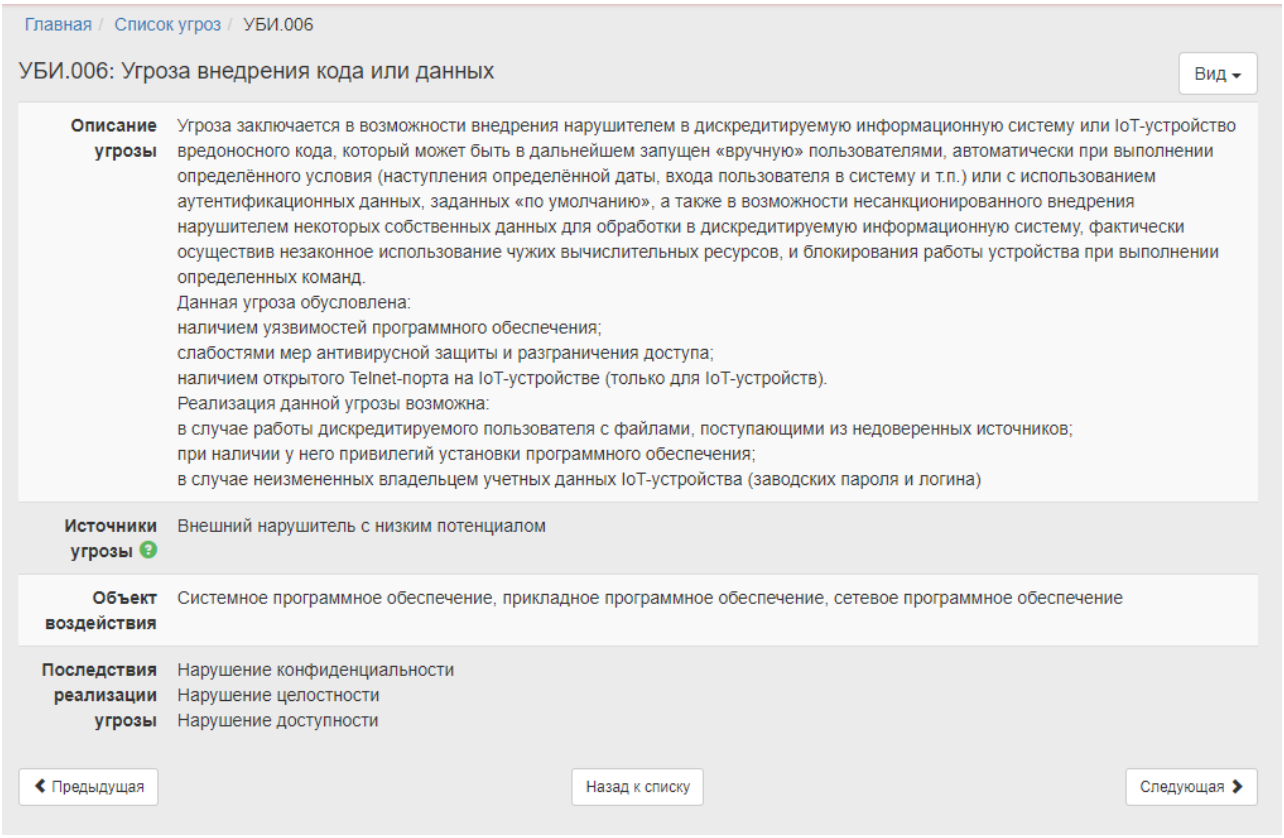


Рис. 63.

• «Подтверждена производителем» – если наличие уязвимости было подтверждено производителем (разработчиком) программного обеспечения, в котором содержится уязвимость;

• «Подтверждена в ходе исследований» – если наличие уязвимости было подтверждено исследователем (организацией), не являющимся производителем (разработчиком) программного обеспечения;

• «Потенциальная уязвимость» – во всех остальных случаях.

В качестве дополнительных параметров поиска доступны фильтры:

– Диапазон дат выявления уязвимостей;

– Уязвимости, связанные с инцидентами информационной безопасности – настройка, позволяющая выводить в списке поиска только уязвимости программного обеспечения, связанные с инцидентами информационной безопасности;

– Год добавления;

– Класс уязвимости – характеристика, уязвимости программного обеспечения, определяющая причину возникновения уязвимости. Может принимать следующие значения:

• уязвимость кода – уязвимость, появившаяся в результате разработки программного обеспечения без учета требований по безопасности информации;

• уязвимость архитектуры – уязвимость, появившаяся в результате выбора, компоновки компонентов программного обеспечения, содержащих уязвимости;

• уязвимость многофакторная – уязвимость, обусловленная наличием в программном обеспечении уязвимостей различных классов.

– Уровень опасности обнаруженной уязвимости – оценка опасности уязвимостей, определяемая на основе численного значения базовой оценки уязвимости. В банке данных в зависимости от значения базовой оценки уязвимости V используются следующие уровни опасности:

• низкий уровень, если 0,0 <= V <= 3,9;
• средний уровень, если 4,0 <= V <= 6,9;
• высокий уровень, если 7,0 <= V <= 9,9;
• критический уровень, если V = 10,0.

– Базовый вектор – текстовая формализованная запись (строка), представляющая собой комбинированные данные о базовых метриках (критериях) уязвимости, на основании которой определяется численная базовая оценка уязвимости.

– Идентификатор типа ошибки – идентификатор, установленный в соответствии с общим перечнем ошибок CWE.

– Другие системы идентификации – в этом поле можно ввести идентификатор угрозы в других системах учета уязвимостей.

– Наличие эксплойта (существует/существует в открытом доступе). Эксплойт (англ. exploit, эксплуатировать) – компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему.

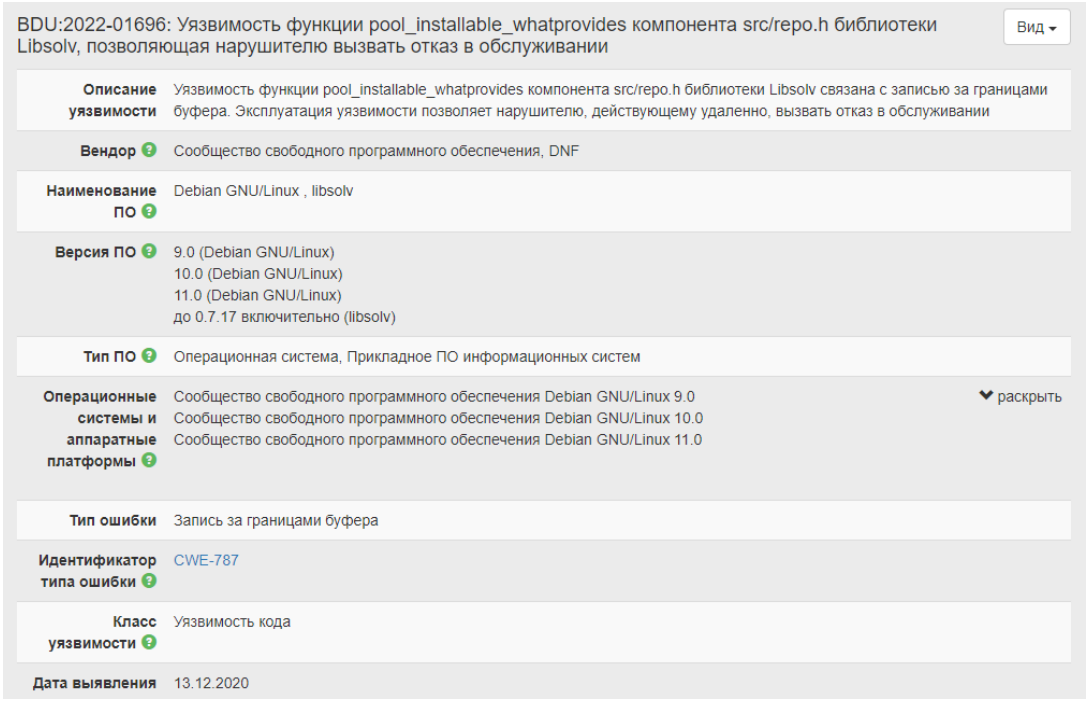
– Способ эксплуатации уязвимости, принимающий значения:

• несанкционированный сбор информации;
• исчерпание ресурсов;
• инъекция;
• анализ целевого объекта;
• подмена при взаимодействии;
• злоупотребление функционалом;
• нарушение авторизации;
• нарушение аутентификации;
• манипулирование структурами данных;
• манипулирование ресурсами;
• манипулирование сроками и состоянием;
• вероятностные методы.

– Операционная система – операционная система, под управлением которой функционирует программное обеспечение с обнаруженной уязвимостью.

Стоит отметить особую ценность банка данных угроз безопасности информации с точки зрения описания уязвимостей в отечественном программном обеспечении и средствах защиты информации. ФСТЭК взаимодействует с ведущими вендорами в области информационной безопасности, учебными заведениями и другими заинтересованными организациями (Digital Security, Институт системного программирования Российской академии наук, АО «НПО РусБИТех» и прочими) для пополнения банка угроз информационной безопасности.

Описание уязвимости выглядит следующим образом (рис. 64):


BDU:2022-01696: Уязвимость функции pool_installable_whatprovides компонента src/repo.h библиотеки Libsolv, позволяющая нарушителю вызвать отказ в обслуживании

Вид

Описание уязвимости	Уязвимость функции pool_installable_whatprovides компонента src/repo.h библиотеки Libsolv связана с записью за границами буфера. Эксплуатация уязвимости позволяет нарушителю, действующему удаленно, вызвать отказ в обслуживании
Вендор	Сообщество свободного программного обеспечения, DNF
Наименование ПО	Debian GNU/Linux , libsolv
Версия ПО	9.0 (Debian GNU/Linux) 10.0 (Debian GNU/Linux) 11.0 (Debian GNU/Linux) до 0.7.17 включительно (libsolv)
Тип ПО	Операционная система, Прикладное ПО информационных систем
Операционные системы и аппаратные платформы	Сообщество свободного программного обеспечения Debian GNU/Linux 9.0 Сообщество свободного программного обеспечения Debian GNU/Linux 10.0 Сообщество свободного программного обеспечения Debian GNU/Linux 11.0 раскрыть
Тип ошибки	Запись за границами буфера
Идентификатор типа ошибки	CWE-787
Класс уязвимости	Уязвимость кода
Дата выявления	13.12.2020

Рис. 64.

Очевидно, что вручную проанализировать 222 угрозы и 41919 уязвимости является достаточно сложной и крайне трудозатратной задачей. Для автоматизации процесса поиска угроз и уязвимостей в конкретной системе ФСТЭК разработала специальное программное обеспечение ScanOVAL, предназначенное для оперативного автоматизированного обнаружения уязвимостей программного обеспечения на рабочих станциях и серверах, функционирующих под управлением операционных систем семейства Microsoft Windows.

6. Уровневая структура описания инцидентов в международной базе данных VERIS

Безусловно, рассмотренный банк данных не является единственным решением такого рода. Существуют и другие банки и базы данных, предназначенные для описания угроз кибербезопасности. В частности, в качестве примера можно выделить международную базу данных VERIS, использующую уровневую структуру описания инцидентов.

VERIS (The Vocabulary for Event RecordingandIncidentSharing) – словарь для записи событий и обмена инцидентами в дословном переводе на русский язык, представляет собой набор метрик, предназначенных для обеспечения общего языка описания инцидентов безопасности структурированным и повторяемым образом.

База VERIS называется уровневой, поскольку для описания любого инцидента она использует два уровня перечислений. Перечисления верхнего уровня (в VERIS всего два обязательных перечисления первого уровня) дают информацию о том:

1. Было ли описываемое событие фактическим инцидентом безопасности;
2. Как этот инцидент был выявлен.

Перечисления второго уровня позволяют дать больше информации о киберинциденте. Всего в VERIS существует четыре обязательных перечисления второго

уровня, каждое из которых представляет собой некоторый набор переменных, описывающих инцидент:

1. Субъект (был ли у угрозы внешний субъект; был ли у угрозы внутренний субъект; была ли это неизвестная угроза).

2. Действия (были ли доказательства взлома; были ли доказательства вредоносного ПО; были ли доказательства социальной инженерии; были ли доказательства злоупотребления привилегиями; была ли ошибка, которая привела к инциденту и т. д.).

3. Атрибуты (возможно ли, что конфиденциальная информация была раскрыта; была ли затронута целостность какой-либо системы; была ли потеря доступности).

4. Активы (был ли сервер затронут инцидентом; было ли затронуто сетевое устройство; были ли затронуты какие-либо устройства конечных пользователей; были ли затронуты какие-либо терминальные устройства (например, банкомат, киоск и т. д.); повлиял ли инцидент на какие-либо бумажные документы или носители информации; были ли скомпрометированы какие-то люди (например, при помощи методов социальной инженерии) и т. д.)

По своей сути VERIS – это ответ на одну из самых острых и постоянных проблем в индустрии кибербезопасности – нехватку качественной информации. Именно на решение этой проблемы направлена база VERIS, помогая организациям собирать полезную информацию, связанную с инцидентами, и делиться этой информацией – анонимно и ответственно – с другими. Общая цель состоит в том, чтобы заложить основу, на которой все заинтересованные организации и лица могут конструктивно и совместно учиться на общем опыте, чтобы лучше измерять риски и управлять ими.

Вопросы и задания для самоконтроля

1. Дайте развернутое определение понятию «кибербезопасность». Определите соотношение между понятиями «кибербезопасность» и «информационная безопасность».

2. Дайте определение терминам «событие кибербезопасности» и «инцидент кибербезопасности».

3. Дайте определение терминам «угроза кибербезопасности», «уязвимость информационной системы», «эксплоит».

4. Дайте определение терминам «реагирование на инцидент кибербезопасности», «целевая атака», «APT-атака».

5. Дайте определение терминам «SEIM-система», «индикаторы компрометации», «потоки данных об угрозах».

6. Дайте определение терминам «разведка на основе открытых источников», «аката типа WateringHole».

7. Атака типа DDoS: общее понятие, типы, примеры.

8. Атака типа «Сбор информации»: суть, назначение, примеры.

9. Несанкционированный доступ как тип киберинцидента – суть, примеры.

10. Модель Cyber-KillChain – общее понятие.

11. Структура жизненного цикла кибератаки.

12. Особенность жизненного цикла кибератаки (процесс круговой, а не линейный).

13. Эффективность киберзащиты – от чего зависит и как качественно защититься от киберугроз.

14. Основные цели реагирования на инциденты кибербезопасности.

15. Основные этапы реагирования на инциденты кибербезопасности (общая информация).

16. Подготовка как один из этапов реагирования на инциденты кибербезопасности.

17. Обнаружение как один из этапов реагирования на инциденты кибербезопасности.

18. Сдерживание как один из этапов реагирования на инциденты кибербезопасности.

19. Удаление как один из этапов реагирования на инциденты кибербезопасности.

20. Восстановление и выводы как этапы реагирования на инциденты кибербезопасности.

21. Дайте развернутое определение понятию «мониторинг кибербезопасности». Укажите его цели и задачи, а также источники данных для осуществления мониторинга.

22. Охарактеризуйте основные компоненты систем мониторинга кибербезопасности.

23. Системы обнаружения вторжений: понятие, назначение, цели, виды.

24. Охарактеризуйте основные методики работы систем обнаружения вторжений.

25. Основные принципы работы систем обнаружения вторжений.

26. Раскройте суть технологий обнаружения аномальной деятельности.

27. Охарактеризуйте методы статистического анализа компьютерных атак.

28. Банк данных угроз безопасности информации ФСТЭК России.

29. Международная уровневая база данных киберинцидентов VERIS.

Заключение

В курсе лекций «Основы кибербезопасности» изложен теоретический материал, охватывающий все темы рабочих программ учебной дисциплины «Основы кибербезопасности».

Предлагаемое издание рассматривает основные понятия и принципы кибербезопасности, вопросы ее международного и внутригосударственного нормативного правового регулирования. Отдельно раскрываются важнейшие темы обеспечения кибербезопасности, связанные с каналами утечки информации, криптографической защитой информации, реагированием на инциденты кибербезопасности и их обработкой.

Курс лекций «Основы кибербезопасности» позволит организовать преподавание одноименной учебной дисциплины с целью формирования соответствующих компетенций, а обучающимся Уральского юридического института МВД России – освоить теоретические основы обеспечения кибербезопасности в органах внутренних дел Российской Федерации.

Список использованных источников

1. Конституция Российской Федерации: принята 12.12.1993 всенародным голосованием (с учетом поправок, внесенных законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ; с изм. от 01.07.2020) // Собрание законодательства Российской Федерации (далее – СЗ РФ). – 2014. – № 1. – Ст. 4398.

2. Об информации, информационных технологиях и о защите информации: федеральный закон от 27.07.2006 № 149-ФЗ // СЗ РФ. – 2006. – №31 (ч. 1). – Ст. 3448.

3. О персональных данных: федеральный закон от 27.07.2006 № 152-ФЗ. // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3451.

4. О государственной тайне: федеральный закон от 21.07.1993 № 5481–1 // СЗ РФ. – 1997. – № 41. – Ст. 8220–8235.

5. О коммерческой тайне: федеральный закон от 29.07.2004 № 98-ФЗ // СЗ РФ. – 2004. – № 32. – Ст. 3283.

6. Об электронной подписи: федеральный закон от 06.04.2011 № 63-ФЗ // СЗ РФ. – 2011. – № 15. – Ст. 2036.

7. О безопасности критической информационной инфраструктуры Российской Федерации: федеральный закон от 26.07.2017 № 187-ФЗ // СЗ РФ. – 2017. – № 31 (ч. 1). – Ст. 4736.

8. Об оперативно-розыскной деятельности: федеральный закон от 12.08.1995 № 144-ФЗ // СЗ РФ. – 1995. – №33. – Ст. 3349.

9. Об организации предоставления государственных и муниципальных услуг: федеральный закон от 27.07.2010 № 210-ФЗ // СЗ РФ. – 2010. – № 31. – Ст. 4179.

10. О полиции: федеральный закон от 07.02.2011 № 3-ФЗ // СЗ РФ. – 2011. – № 7. – Ст. 900.

11. Гражданский кодекс Российской Федерации (часть четвертая): федеральный закон от 18.12.2006 № 230-ФЗ // СЗ РФ. – 2006. – № 52 (ч. 1). – Ст. 5496.

12. Кодекс Российской Федерации об административных правонарушениях: федеральный закон от 30.12.2001 № 195-ФЗ // СЗ РФ. – 2002. – № 1 (ч. 1). – Ст. 1.

13. Уголовный кодекс Российской Федерации: федеральный закон от 13.06.1996 № 63-ФЗ // СЗ РФ. – 1996. – № 25. – Ст. 2954.

14. Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления: федеральный закон от 09.02.2009 № 8-ФЗ // СЗ РФ. – 2009. – № 7. – Ст. 776.

15. Вопросы Министерства внутренних дел Российской Федерации: указ Президента РФ от 01.03.2011 № 248 // СЗ РФ. – 2011. – № 10. – Ст. 1334.

16. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указа Президента РФ от 09.05.2017 № 203 // СЗ РФ. – 2017. – № 20. – Ст. 2901.

17. Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям: постановление Правительства РФ от 18.05.2009 № 424 // СЗ РФ. – 2009. – № 21. – Ст. 2573.

18. 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 21.03.2021 № 211 // СЗ РФ. – 2012. – № 14. – Ст. 1626.

19. О мерах по совершенствованию использования информационно-коммуникационных технологий в деятельности государственных органов: постановление Правительства РФ от 25.04.2012 № 394 // СЗ РФ. – 2012. – № 19. – Ст. 2419.

20. О мерах по совершенствованию электронного документооборота в органах государственной власти: постановление Правительства РФ от 06.09.2012 № 890 // СЗ РФ. – 2012. – № 38. – Ст. 5102.

21. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: постановление Правительства РФ от 01.11.2012 № 1119 // СЗ РФ. – 2012. – № 45. – Ст. 6257.

22. Об утверждении Правил обмена документами в электронном виде при организации информационного взаимодействия: постановление Правительства РФ от 24.07.2021 № 1264 // СЗ РФ. – 2021. – № 31. – Ст. 5927.

23. *Аграновский А. В.* Новый подход к защите информации – системы обнаружения компьютерных угроз / А. В. Аграновский, Р. А. Хади // Информационный бюллетень JetInfo. – 2007. – № 4 (167). – С. 3–22.

24. *Ахмаджонов А.* Технические каналы утечки и защиты информации от перехвата / А. Ахмаджонов // Информационное противодействие угрозам терроризма. – 2013. – № 21. – С. 42–46.

25. *Бахаров Л. Е.* Информационная безопасность и защита информации (разделы криптография и стеганография): практикум [Электронный ресурс] / Л. Е. Бахаров. – Москва: Изд. дом МИСиС, 2019. – 59 с. // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: http://www.iprbookshop.ru/98171.html.

26. *Башлы П. Н.* Информационная безопасность: учеб.-метод. пособие для студентов высших учебных заведений, обучающихся по спец. 080801 Прикладная информатика и другим междисциплинар. специальностям / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. – Москва: Изд. центр ЕАОИ, 2011. – 375 с.

27. *Белоус А. И.* Кибероружие и кибербезопасность. О сложных вещах простыми словами [Электронный ресурс] / А. И. Белоус, В. А. Солодуха. – Москва, Вологда: Инфра-Инженерия, 2020. – 692 с. // Электронно-библиотечная система IPRBOOKS: [сайт]. – URL: http://www.iprbookshop.ru/98349.html.

28. *Белоус А. И.* Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения [Электронный ресурс] / А. И. Белоус, В. А. Солодуха. – Москва: Техносфера, 2021. – 482 с. // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: http://www.iprbookshop.ru/108023.html.

29. *Фороузан Б. А.* Управление ключами шифрования и безопасность сети: курс лекций / Б. А. Фороузан. – Москва: Интуит НОУ, 2016. – 527 с.

Фороузан Б. А. Криптография и безопасность сетей [Электронный ресурс]: учеб. пособие / Б. А. Фороузан; пер. с англ.; под ред. А. Н. Берлина. – Москва: Бином. Лаборатория знаний, Интернет-университет информационных технологий. – URL: https://www.livelib.ru/publisher/4914/books-internetuniversitet-informatsionnyh-tehnologij?ysclid=lbq90x3xd8514499595

30. *Бузов Г. А.* Практическое руководство по выявлению специальных технических средств несанкционированного получения информации / Г. А. Бузов. – Москва: Горячая линия-Телеком, 2010. – 240 с.

31. Вирусы-вымогатели (шифровальщики) Ransomware [Электронный ресурс] // Интернет-портал и аналитическое агентство TAdviser : [сайт]. – 2022. – 26 авг. – URL: https://www.tadviser.ru/index.php/Статья:Вирусы-вымогатели_(шифровальщики)_Ransomware.

32. *Галкин А. П.* Защита учреждений и предприятий от несанкционированного доступа к информации в технических каналах связи: дис. ... д-ра техн. наук / А. П. Галкин. – Владимир, 2003. – 276 с.

33. *Голиков А. М.* Защита информации от утечки по техническим каналам: учеб. пособие / А. М. Голиков. – Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2015. – 256 с.

34. *Зайцев А. П.* Технические средства и методы защиты информации: учеб. пособие для вузов / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков и др.; под ред. А. П. Зайцева и А. А. Шелупанова. – 4-е изд., испр. и доп. – Москва: Горячая линия-Телеком, 2012. – 616 с.

35. *Зиновьева Е. С.* Анализ внешнеполитических инициатив РФ в области международной информационной безопасности / Е. С. Зиновьева // Вестник МГИМО-Университета. – 2014. – № 6 (39). – С. 47–52.

36. *Зиновьева Е. С.* Информационная безопасность Российской Федерации на современном этапе развития международных отношений [Электронный ресурс] / Е. С. Зиновьева // СМИ mgimo.ru (МГИМО-Университет): [сайт]. – 2014. – 23 июля. – URL: https://mgimo.ru/about/news/experts/258416/.

37. *Кемпф В. А.* Обеспечение информационной безопасности в органах внутренних дел [Электронный ресурс]: учеб. пособие / В. А. Кемпф. – Барнаул: Барнаул. юрид. ин-т МВД России, 2019. – 64 с. – URL: http://212.49.112.158:81/cgi-bin/irbis64r_plus/cgiirbis_64_ft.exe?C21COM=F&I21DBN=IBIS_FULLTEXT&P21DBN=IBIS&Z21ID=&S21CNR=5.

38. Компьютерный вирус [Электронный ресурс] // Интернет-портал и аналитическое агентство TAdviser: [сайт]. – 2010. – 29 апр. – URL: https://www.tadviser.ru/index.php/Статья:Компьютерный_вирус.

39. *Креопалов В. В.* Технические средства и методы защиты информации: учеб.-практ. пособие / В. В. Креопалов. – Москва: Евразий. открытый ин-т, 2011. – 278 с.

40. *Лобач Д. В.* Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам / Д. В. Лобач, Е. А. Смирнова // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. – 2019. – Т. 11. – № 4. – С. 23–32.

41. *Лямцев А. Н.* Некоторые проблемы российского законодательства в сфере компьютерных преступлений / А. Н. Лямцев // Вопросы современной науки и практики. Университет им. В. И. Вернадского. – 2013. – № 1 (45). – С. 232–237.

42. *Малюк А. А.* Введение в информационную безопасность: учеб. пособие для вузов / А. А. Малюк, В. С. Горбатов, В. И. Королев и др.; под ред. В. С. Горбатова. – Москва: Горячая линия-Телеком, 2011. – 288 с.

43. Обзор международных стандартов в области ИБ [Электронный ресурс] // Интернет-портал «Безопасность пользователей в сети Интернет»: [сайт]. – 2020. – 7 мая. – URL: https://safe-surf.ru/specialists/article/5259/644530/.

44. Организация защиты персональных данных в органах внутренних дел: учеб. пособие / А. В. Воробьев, А. Н. Бабкин, Д. Ю. Лиходедов [и др.]. – Москва: ДГСК МВД России, 2019. – 160 с.

45. Отказ от обслуживания [Электронный ресурс] // Интернет-портал и аналитическое агентство TAdviser: [сайт]. – 2022. – 18 марта. – URL: https://www.tadviser.ru/index.php/Статья:Distributed_Denial-of-Service,_DDoS_(отказ_от_обслуживания).

46. *Пелешенко В. С.* Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учеб. пособие / В. С. Пелешенко, С. В. Говорова, М. А. Лапина. – Ставрополь: Северо-Кавказ. федерал. ун-т, 2017. – 85 с.

47. *Рахметов Р. Г.* Анализ международных документов по управлению рисками информационной безопасности. Ч. 1 [Электронный ресурс] / Р. Г. Рахметов // Интернет-портал Habr: [сайт]. – 2020. – 2 апр. – URL: https://habr.com/ru/post/495236/.

48. Руководство по безопасности в Lotus Notes: курс: учеб. пособие. – Москва: ИНТУИТ, 2008. – 834 с.

49. Руководство по реагированию на инциденты информационной безопасности [Электронный ресурс] // Управление технологических решений АО Kaspersky-Lab: [сайт]. – URL: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07172131/Incident_Response_Guide_rus.pdf.

50. *Салий В. Н.* Криптографические методы и средства защиты информации: учеб. пособие / В. Н. Салий. – Саратов: Саратов. гос. ун-т, 2017. – 43 с.

51. *Скрипник Д. А.* Общие вопросы технической защиты информации [Электронный ресурс]: учеб. пособие / Д. А. Скрипник. – 3-е изд. – Москва, Саратов: ИНТУИТ, Ай Пи Ар Медиа, 2020. – 424 с. // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: http://www.iprbookshop.ru/89451.html.

52. *Соколов А. И.* Технические средства защиты информации: технические каналы утечки информации: учеб. пособие / А. И. Соколов, М. Ю. Монахов. – Владимир: Владимир. гос. ун-т, 2007. – 71 с.

53. *Сухов А. Н.* Реальная социальная психология: учеб.-метод. пособие / А. Н. Сухов. – Москва: Московский психолого-социальный ин-т, 2004. – 351 с.

54. *Титов А. А.* Технические средства защиты информации [Электронный ресурс]: учеб. пособие / А. А. Титов. – Томск: Томск. гос. ун-т систем управления и радиоэлектроники, 2010. – 194 с. // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: https://www.iprbookshop.ru/13989.html.

55. *Торокин А. А.* Инженерно-техническая защита информации: учеб. пособие для студентов, обучающихся по спец. в обл. информ. безопасности / А. А. Торокин. – Москва: Гелиос АРВ, 2005. – 960 с.

56. Трояны [Электронный ресурс] // Интернет-портал и аналитическое агентство TAdviser: [сайт]. – 2022. – 20 авг. – URL: https://www.tadviser.ru/index.php/Статья:Трояны.

57. Физические основы технической защиты информации [Электронный ресурс]: учеб. пособие / сост. А. В. Еськов. – Краснодар: Краснодар. ун-т МВД России, 2020. – 56 с. – URL: http://212.49.112.158:81/cgi-bin/irbis64r_plus/cgiirbis_64_ft.exe?C21COM=F&I21DBN=IBIS_FULLTEXT&P21DBN=IBIS&Z21ID=&S21CNR=5.

58. Фишинг [Электронный ресурс] // Интернет-портал и аналитическое агентство TAdviser: [сайт]. – 2022. – 14 апр. – URL: https://www.tadviser.ru/index.php/Статья:Фишинг_(phishing).

59. Что такое Cyber-KillChain и почему ее надо учитывать в стратегии защиты [Электронный ресурс] // Интернет-портал PCNews: [сайт]. – 2017. – 27 апр. – URL: https://pcnews.ru/blogs/cto_takoe_cyber_kill_chain_i_pocemu_ee_nado_ucityvat_v_strategii_zasity-765773.html#gsc.tab=0.

60. *Шарыпин Е. М.* Системы обнаружения вторжений [Электронный ресурс] // Образовательный Интернет-портал StudyLib: [сайт]. – URL: https://studylib.ru/doc/4374337/sharypin-e.m.-sistemy-obnaruzheniya-vtorzhenij.

61. *Шелухин О. И.* Обнаружение вторжений в компьютерные сети (сетевые аномалии): учеб. пособие для вузов / О. И. Шелухин, Д. Ж. Сакалема, А. С. Филинова. – Москва: Горячая Линия-Телеком, 2018. – 220 с.

62. *Шолин И. М.* Алгоритм переносной шифровальной машины Энигма / И. М. Шолин, Н. О. Чубырь // Форум молодых ученых. – 2018. – № 10 (26). – С. 1352–1356.

Содержание

ЛЕОНОВ Александр Петрович
КОПЕИНА Александра Владимировна
МАКШАНЦЕВА Анастасия Вячеславовна

Основы кибербезопасности

Курс лекций

Корректура и компьютерная верстка *И. Б. Бебих*

Подписано в печать 30.11.2022. Формат 60x84 1/16
Печать трафаретная. Бумага офисная
Усл. печ. л. 10,0. Уч.-изд. л. 11,0
Тираж 215 экз. Заказ № 75

Типография научно-исследовательского
и редакционно-издательского отдела
Уральского юридического института МВД России

620057, Екатеринбург, ул. Корепина, 66