МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского»

Дзержинский филиал ННГУ

Е.А. Поляков

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

Рекомендовано методической комиссией Дзержинского филиала ННГУ для студентов, обучающихся по направлениям: 09.03.03 Прикладная информатика, 38.03.01 Экономика, 38.03.02 Менеджмент, 38.03.04 Государственное и муниципальное управление

Н.Новгород

2021

УДК 004.056
ББК А682
П-54

П-54 Поляков Е.А.
Основы информационной безопасности: Учебное пособие. - Нижний Новгород: Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского, 2021. – 71 с.

Рецензенты:
кандидат технических наук, доцент О.Г. Савихин
кандидат педагогических наук, доцент А.А. Беспалько

Учебное пособие предназначено для справочной, дидактической поддержки разделов курса «Информационная безопасность» по направлениям подготовки 09.03.03 Прикладная информатика, 38.03.01 «Экономика», 38.03.02 Менеджмент, 38.03.04 Государственное и муниципальное управление. Рассматриваются правовые, концептуальные основы защиты информации, раскрывающие сущность, цели, структуру и стратегию защиты. Анализируются источники, способы и результаты дестабилизирующего воздействия на информацию, а также каналы и методы несанкционированного доступа к информации. Определяются методологические подходы к организации и технологическому обеспечению защиты информации на предприятии. Особое внимание уделено проблеме «человеческого фактора». Включает основы принципов обеспечения информационной безопасности, подходов к анализу угроз информационной инфраструктуры организации. Предложенный подход к защите информации обеспечит целостное видение проблемы, повышение качества, следовательно, и надежности ИБ предприятия.

Учебные вопросы по темам и позволяет осваивать профессиональные компетенции по решению задач защиты информации в информационных системах.

Пособие предназначено для студентов высших учебных заведений, обучающихся по различным направлениям, а также для преподавателей и широкого круга специалистов, проявляющих интерес к организации или решению профессиональных задач по обеспечению информационной безопасности предприятия, организации.

УДК 004.056
ББК А682

Содержание

Введение

В начале 1990-х гг. появилась новая угроза информационной безопасности отдельных лиц, предприятий и государств. Появились такие понятия, как «информационное противостояние», «информационная война», «информационное оружие». В США, Европе, а затем и в России стали проводиться НИОКР в области информационной безопасности (ИБ) и защиты информации, были разработаны нормативные и руководящие документы, приняты стандарты.

В промышленных группах США наряду с Федеральным центром защиты инфраструктуры при ФБР планируется организовать собственные центры анализа корпоративной информации. Таким образом, в США создается многоступенчатая система защиты информации.

Европейские страны приняли документ под названием «Общие критерии» (позже формализованный в форме ISO 15408: 19991-3), определяющий критерии безопасности.

В декабре 2016 г. Указом Президента РФ утверждена Доктрина информационной безопасности Российской Федерации. Этот документ дает совершенно четкую систему взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности в Российской Федерации и в субъектах Российской Федерации.

Особенно актуальна проблема использования экономической информации в сфере управления материальным производством, где рост информационного потока находится в квадратичной зависимости от промышленного потенциала страны. В свою очередь, быстрое развитие процессов автоматизации, использование компьютеров во всех сферах современной жизни, помимо несомненных преимуществ, привело к возникновению ряда специфических проблем. Один из них - необходимость обеспечения эффективной защиты информации.

Защита информации, особенно в экономической сфере, - это очень специфический и важный вид деятельности. В мире средняя сумма ущерба от кражи одного банка с использованием электронных средств, по материалам зарубежной прессы, оценивается в 9 тысяч долларов. Ежегодные убытки от компьютерных преступлений в США и Западной Европе достигают 140 миллиардов долларов.

Данное учебное пособие предназначено для справочной, дидактической поддержки разделов курса «Информационная безопасность» по направлениям подготовки 09.03.03 Прикладная информатика, 38.03.01 «Экономика», 38.03.02 Менеджмент, 38.03.04 Государственное и муниципальное управление. Включает основы правовых принципов обеспечения информационной безопасности, подходов к анализу угроз информационной инфраструктуры организации на основе рекомендаций, учебные вопросы по темам и позволяет осваивать профессиональные компетенции по решению задач защиты информации в информационных системах.

Содержание учебного пособия, как и содержание указанного курса, разработано в соответствии с требованиями ФГОС ВПО по направлениям подготовки 09.03.03 Прикладная информатика, 38.03.01 «Экономика», 38.03.02 Менеджмент, 38.03.04 Государственное и муниципальное управление в области формирования необходимых компетенций.

Настоящее учебное пособие включает теоретические сведения, которые помогут решать экзаменационные или зачетные билеты, перечень контрольных вопросов приводится к каждой главе.

Самостоятельная работа студентов должна поддерживать различные виды деятельности, чтобы полноценно дополнять аудиторную подготовку. В настоящее издание включены правовые документы, список литературы, дополнительные источники информации, которые позволят расширить кругозор в области основ информационной безопасности.

Учебное пособие предназначено для студентов высших учебных заведений, обучающихся по различным направлениям. Пособие поможет студентам сориентироваться при организации текущей аудиторной и внеаудиторной самостоятельной работы, при подготовке к тестам, практикумам и экзаменам. Учебное пособие будет полезен преподавателям дисциплины «Информационная безопасность», дисциплин, содержащих правовые основы политики информационной безопасности, построение моделей угроз нарушителей и безопасности информации, а также может заинтересовать методистов, магистрантов, аспирантов и широкого круга специалистов, проявляющих интерес к организации образовательного процесса по дисциплине «Информационная безопасность».

Глава 1. Политика государства в области информационной безопасности

1.1 Стратегия национальной безопасности

Стратегия определяет систему государственных взглядов на безопасность Российской Федерации в общем, не только информационном, но и в различных других аспектах.

Принята Указом Президента РФ от 2 июля 2021 г. N 400 и по состоянию на 2021 год является действующей.[12] Это актуальный документ, который регламентирует национальную безопасность в целом. Стратегия состоит из 5 частей они описывают общие положения, то есть государственные взгляд на национальную безопасность, положение России в современном мире, перечисляет национальные интересы и стратегические приоритеты в области безопасности, меры по обеспечению национальной безопасности, организационные основы и механизмы реализации стратегии.

В рамках курса Информационной безопасности значимо следующее: суть стратегии описана в пункте 1 части первой. Данная стратегия является базовым документом стратегического планирования, в ней определяются национальные интересы и стратегические национальные приоритеты Российской Федерации, цели задачи и меры в области внутренней и внешней политики направленные на укрепление национальной безопасности Российской Федерации и обеспечение устойчивого развития страны на долгосрочную перспективу. данная стратегия определяет, являются ли те или иные мероприятия, процессы, действия власти, граждан или чиновников согласованными с политикой государства в области безопасности или нет. Разумеется, если они являются, то это основания для признания актуальными, востребованными и достойными финансирование выделения средств из различных бюджетов.

При этом **национальная безопасность Российской Федерации** определяется как состояние защищенности национальных интересов Российской Федерации от внешних и внутренних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, достойные качество и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета Российской Федерации, ее независимости и государственной целостности, социально-экономическое развитие страны. Этим законодатель формулирует такое определение и стремится обеспечить в нём, максимально охватить все возможные аспекты понятия безопасность, которые в нём и перечислены. Таким образом национальная безопасность направлена на максимальное стабильное и плодотворное существование и развитие Российской Федерации как самостоятельного государства.

Такие понятия как государственная территориальная целостность и устойчивое социально-экономическое развитие как раз подчеркивают такую задачу. Нам важно и то, что в соответствии с данной стратегией, национальная безопасность включает в себя разные аспекты безопасности: такие как оборону

страны, все виды безопасности, предусмотренные Конституцией Российской Федерации и, в частности, среди них информационную безопасность.

Кроме того, в п.1.1 Стратегии определены приоритеты дальнейшего развития России в качестве правового социального государства, в котором высшее значение имеют соблюдение и защита прав и свобод человека и гражданина, повышение благосостояния народа, защита достоинства граждан России. Эти конституционные основы являются приоритетом в данной Стратегии:

Статья 29

1. Каждому гарантируется свобода мысли и слова.

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

5.Гарантируется свобода массовой информации. Цензура запрещается.[6]

Похожие формулировки в области распространения информации записаны в Европейской Конвенции о защите прав человека и основных свобод. Россией Конвенция и протоколы к ней ратифицированы и действуют с марта 1998 года.

Статья 10 — Свобода выражения мнения]

Статья декларирует право человека свободно выражать и придерживаться своего мнения, а также распространять информацию и идеи без какого-либо ограничения, а также оговаривает случаи, когда государства вправе устанавливать ограничения в части распространения информации посредством лицензирования либо иным способом установленном законом.[5]

Однако декларация информационных прав и свобод не означает отказ государства от защиты информационных ресурсов. Правовое обеспечение информационной безопасности формируется на основе поддержания *баланса интересов граждан, общества, государства,* что особенно важно в условиях существования различных форм собственности. Поэтому Конституцией определены и основания для ограничения информационных прав и свобод граждан. К их числу относятся: защита основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечение обороны страны и безопасности государства (ст. 17, п. 3, ст. 55, п. 3).

Таким образом, Конституция рассматривается в данном аспекте как часть национальной безопасности, что сразу демонстрирует максимальную заинтересованность законодателя, в лице исполнительной и законодательной в ее государственной поддержке, в её регулировании и соответственно в создании прозрачного правового поля, которое бы регулировалась данными законодательными актами, Федеральными законами, самой стратегией национальной безопасности.

Сформулируем, какие мероприятия государства предполагает, какие правовые статусы различных лиц предполагает, какие задачи перед ними ставят, какими правами их наделяет, какие формы правоотношения между ними

предполагает и какие обязательства на них в случаях правоотношений накладывает. В рамках пособия выясним об общем государственном планировании в области информационной безопасности, о принципах, на которых строится регулирование этой деятельности и об отдельных категориях информации, которую на основании действующего законодательства требуется защищать, при этом чаще всего обеспечивать её конфиденциальность, но в отдельных случаях и целостность и доступность.

1.2 Доктрина информационной безопасности

Основным документом, составляющим совокупность таких официальных взглядов, является **доктрина информационной безопасности**. Действующая версия доктрины информационной безопасности утверждена Указом Президента Российской Федерации в 2016 году.[13] Она во многом сохраняет преемственность с предыдущей редакцией, которая была утверждена президентом Российской Федерации в 2000 году, то есть более 15 лет до этого и, естественно, потребовала обновление и все актуальные настоящий момент взгляды в ней перечислены. Доктрина информационной безопасности Российской Федерации состоит из следующих пяти частей:

1. В первой части перечисляются общие положения, то есть система взглядов правительства на информационную безопасность.

2. Эти взгляды базируются на таком понятии, как национальные интересы в информационной сфере и как они описаны в во 2 части данного документа

3. Третья часть доктрина перечисляет основные информационные угрозы и состояние информационной безопасности. То есть в этой части формулируется то, от чего требуется защищать информацию, то на пресечении каких угроз направлены меры по обеспечению информационной безопасности.

4. Стратегические цели и основные направления обеспечения информационной безопасности составляют предмет четвертой части данного документа. Они перечисляются и определяются таким образом направления деятельности по информационной безопасности в Российской Федерации

5. Пятая часть перечисляет организационные основы обеспечения информационной безопасности.

Остановимся на некоторых выдержках с данного документа, которые позволят взглянуть на основные принципы, на основании которых строится информационная безопасность в нашей с вами стране.

Суть доктрины описана в пункте 1 части первой - настоящая доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

Это означает, что доктрина информационной безопасности также является установочным документом, на который можно ссылаться при обосновании различных проектов в различных решений, обоснование актуальности различных решений их соответствие духу, можно сказать нормативного документа, хотя данный документ не является законом, духу

доктрины, духу официальных взглядов на обеспечение информационной безопасности.

То, что эти взгляды во многом влияют на реалии различных действий по информационной безопасности мы разберем на примере конкретных законов, которые должны согласовываться с доктриной. Ну и они видимо согласовываются, поскольку законы разрабатываются и утверждаются таким образом, что проходят многочисленные согласования, обсуждения и утверждение и, таким образом, максимально законодатель стремится к их согласованности.

Одним из понятий, которые употребляются в данном документе, является понятие информационной сферы.

Под ***Информационной сферой*** понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети Интернет, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

Определение является практически всеобъемлющим, в него входят информация, все виды процессов и объектов, связанных с обработкой информации, о которых вам должно быть известно из курса Информатика, а также добавляется совокупность механизмов регулирования соответствующих общественных отношений. Иными словами, информационная сфера, это информация и все способы и методы ее обработки + однозначное установленные законодательно механизмы регулирования соответствующих общественных отношений. То есть некие правовые статусы, которые накладываются на лица в зависимости от того, кем они являются в тех или иных процессах обработки и передачи, хранения информации, в отношении их прав и обязанностей в этих правоотношениях. Таким образом информационная сфера представляет собой совокупность информации, всех возможных способов и методов ее обработки, а также добавляется совокупность механизмов регулирования соответствующих общественных отношений.

Другим определением, которые водятся в доктрине информационной безопасности, является понятие ***информационной безопасности Российской Федерации*** в рамках данного документа сокращённо ИБ. Но мы данной аббревиатурой будем обозначать понятие информационной безопасности, которая была сформулирована в первой части лекции, то есть это такое состояние информации, при котором сохраняются её целостность, доступность и конфиденциальность. Но, для понимания политики нашего законодателя в области ИБ, вводится понятие ИБРФ: как *состояние защищенности личности общества и государства от внутренних и внешних информационных угроз*, при котором *обеспечивается реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет и территориальную целостность, устойчивое социально-экономическое*

развитие Российской Федерации, оборона и безопасность. Таким образом информационной безопасности Российской Федерации, в рамках данного документа, принимается как состояние максимально благополучное для Российской Федерации с точки зрения её существования и максимально благополучная также для личности и общества с точки зрения их конституционных прав и свобод, с точки зрения развития общества, имея в виду именно отсутствие угроз в информационной сфере, как одной из частей национальной безопасности. Так мы к информационной безопасности Российской Федерации будем относиться именно как части национальной безопасности и, в рамках данного документы, будем её понимать как некую форму национальной безопасности, как отсутствие угроз именно такого рода, информационных угроз.

Еще одним объектом, которой определяется в данном документе ***информационная инфраструктура*** Российской Федерации. Это уже более конкретный объект, о защите и о безопасности которого можно говорить.

Информационная инфраструктура, это совокупность объектов информатизации и информационных систем, сайтов в сети Интернет и сетей связи расположенных на территории Российской Федерации, а также на территориях находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров. Таким образом, информационная инфраструктура Российской Федерации, это материальная составляющая информационной сферы. Здесь уже нет речи о конкретных лицах, которые участвуют в информационных процессах и нет речи о каком правовом регулировании их статуса, отношение их прав и обязанностей. Информационная инфраструктура, это именно физическая составляющая Информационной сферы.

Для того чтобы определить, что требуется делать для обеспечения информационной безопасности, вводятся также понятие ***угрозы информационной безопасности Российской Федерации***. Под угрозой такого свойства предполагается понимать совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам РФ в информационной сфере, то есть любые угрозы, которые вредны для Российской Федерации и являются угрозами в информационной сфере. Для противодействия угрозам информационной безопасности Российской Федерации существуют некие лица и некие объекты.

Следующим понятиям, с которым предлагается ознакомиться это понятие ***сил обеспечения информационной безопасности***. Это государственные органы, а также подразделения и должностные лица государственных органов и органов местного самоуправления, организаций уполномоченные, в соответствии с законодательством Российской Федерации, на решение задач по обеспечению информационной безопасности. То есть, силы обеспечения информационной безопасности, это субъекты безопасности, это те, кто борется с угрозами информационной безопасности.

Далее вводится понятие средств обеспечения информационной опасности. ***Средства обеспечения информационной безопасности,*** это правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности. То есть это инструмент, это все возможные методы и средства защиты информации, которые рассмотрим далее.

Также вводится понятие обеспечения информационной безопасности. ***Обеспечение информационной безопасности*** - это осуществление взаимосвязанных правовых, организационных, оперативно-розыскных, разведывательных и иных мир по прогнозированию, обнаружению, сдерживанию и предотвращению, отражению информационных угроз и ликвидации последствий их проявлений. Это действия сил обеспечения информационной безопасности, это то, что они делают - они обеспечивают информационную безопасность. Совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированною деятельность и используемых ими средств обеспечения информационной безопасности, объясняется в понятии обеспечение информационной безопасности.

Таки образом, ***система обеспечения информационной безопасности,*** это совокупность мер, целенаправленно действующих в целях обеспечения информационной безопасности и используемых ими средств обеспечения информационной безопасности, инструментов.

Также доктрина информационной безопасности вводят понятие ***Национальных интересов Российской Федерации в информационной сфере*** - это объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационных систем.

Из этого следует то, что национальные интересы опять раскладываются на три категории интересов. Это потребности личности, общества и государства, это некая общая основа государственной политики в области безопасности, безопасность этих трех субъектов государства, общества и личности. У каждого из них есть свои сферы интересов и на обеспечение интересов всех этих трёх субъектов направлена государственная политика в области информационной безопасности.

Национальными интересами в информационной сфере являются следующие:

- обеспечение и защита конституционных прав и свобод человека в части, касающейся получения и использования информации, то есть обеспечении конституционных прав свобод личности;
- обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры
- развитие в РФ отрасли информационных технологий и электронной промышленности

- доведение до российской и международной общественности достоверной информации о государственной политике РФ и ее официальной позиции по социально значимым событиям в стране и мире.

Это тоже интересы касающиеся всех трёх перечисленных субъектов и, наконец, такой интерес:

- содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на защиту суверенитета Российской Федерации в информационном пространстве.

Но это скорее интерес государства

1.3 Законодательство в области защиты информации

Рассмотрев о системе взглядов законодателя и правительства на информационную безопасность, разберем положения конкретных законах в области информационной безопасности, конкретно регламентирующих правовой статус различных участников информационных процессов, об их обязанностях и правах. Основным законом в данной сфере является Федеральный Закон «Об информации, информационных технологиях и о защите информации». Данный закон регламентирует, помимо прочего, вопросы защиты информации, определяет основные взгляды на защиту информации, основные принципы на которых защиты информации должна строиться. Данные закон состоит из 18 статей.[14]

Статья 1 указывает, какие взаимоотношения между субъектами регулируют данный закон. Он регулирует отношения возникающие при осуществлении права на поиск, получение и передачу, производство и распространение информации, предусмотренные Конституцией Российской Федерации,

Настоящий Федеральный закон регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации.

Статья 3 включает в себя принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

- свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
- установление ограничений доступа к информации только федеральными законами;
- открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

Статья включает в себя правовое регулирование отношений в сфере информации информационных технологий и защиты информации. Эти принципы таковы:

Во-первых: все законодательные документы в данной сфере не должны ограничивать свободу получения, передачи, производства и распространения информации любым законным способом. Соответственно и меры по защите информации также не должны эту свободу ограничивать.

Во-вторых: установление ограничений доступа к информации возможно только на основании Федеральных законов. Этот важный принцип, который декларирован в данном документе, который им устанавливается, то есть только законодатель имеет право ограничивать доступ к информации. Ну, за исключением отдельных категорий информации, о которых мы поговорим далее, на который имеет право устанавливать ограничения на доступ её обладатель.

В-третьих: вводится принцип открытости информации о деятельности государственных органов и органов самоуправление, свободный доступ к такой информации, кроме случаев, установленных Федеральными законами. Законодатель вводит принцип, определяющий, что информация, касающаяся государственных органов и органов местного самоуправления, за исключением небольшого ряда особых случаев, всегда является открытым и общедоступным.

Следующий принцип – это *равноправие языков народов Российской Федерации* при создании информационных систем и их эксплуатации. Этот принцип устанавливает такое положение, что информационная система, даже в интересах информационной безопасности, не может регулироваться таким образом, чтобы содержание, контент, информация на каких языках дискриминировалась в пользу других языков, более общего употребительных или более распространенных в данной конкретной информационной системе.

Обеспечения безопасности Российской федерации при создании информационных систем их эксплуатации и защите содержащейся в них информации следующий принцип, постулируемый в данном документе: *обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации*.

Далее данным законом формулируется принцип: *достоверность информации и своевременность ее предоставления*. Эти параметры информации, достоверность и своевременность предоставления, не должны страдать от тех или иных мероприятий. И к обеспечению достоверности и своевременности предоставления информации должны стремиться все мероприятия, связанные с обработкой, хранением и защитой информации.

Следующий принцип: неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия. Данный принцип накладывает некоторые ограничения на кажущееся очевидными меры информационной безопасности, заключающееся в некоем контроле за

субъектами, либо над сотрудниками организации, либо над гражданами. К счастью, неприкосновенность частной жизни постулируется законом и такие меры противозаконны. Порой начальство некоторых организаций желала бы максимально контролировать в том числе и частную жизнь своих сотрудников следить за их лояльностью, следить за тем как они высказываются о руководстве, довольны ли они своей работой, заработной платой и т.д. Эти действия законодатель прямо запрещает.

Следующий принцип: недопустимости установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими. Если только обязательность применения определенных информационных технологий, для создания и эксплуатации государственных информационных систем, не установлено Федеральными законами. это некий антимонопольный принцип, запрещающий в рамках отдельных информационных систем, устанавливать, например, требования использовать только сетевое оборудование конкретного производителя или программное обеспечение конкретной страны.

Статья четвёртая данного закона включает в себя информацию о законодательстве Российской Федерации об информации информационных технологиях и о защите информации. Основной принцип здесь таков: законодательство Федерации об информации информационных технологиях и о защите информации в обязательном порядке основывается на Конституции Российской Федерации, международных договорах Российской Федерации и состоит из Федерального закона и других регулирующих отношений и регулирующих отношения по использованию информации федеральных законов.

Кроме того, правовое регулирование отношений, связанных с организацией и деятельностью средств массовой информации, осуществляется в соответствии с законодательством Российской Федерации о средствах массовой информации. Это отдельный принцип, указывающий на то, что средства массовой информации в ряде случаев имеют исключительное права. Например, право присутствовать на некоторых мероприятиях, право освещать эти мероприятия, право публиковать записи интервью, видео-, фото- материалы с различных мероприятий в соответствии с законодательством Российской Федерации о СМИ.[16]

Шестая статья данного закона включает в себя сведения об обладателе информации. Здесь вводится важный правовой статус, который во многом будет определять то, кто принимает решение по защите того или иного объекта информации. Обладатель информации - это лицо на законных основаниях получивший её и право распоряжаться доступом к ней получает на основании данного закона следующие права: разрешать или ограничивать доступ к информации, определяет порядок и условия такого доступа, использовать информацию, в том числе распространять ее по своему усмотрению, а также передавать информацию другим лицам по договору или на ином установленном законом оснований. То есть обладатель информации осуществляет всю полноту

прав по распоряжению информации, которая ему принадлежит, которой он обладает. Также в его правах - защищать установленными законом способами своё право, в случае незаконного получения информации или её незаконного использования иными лицами, а также осуществлять иные действия с информацией или разрешать осуществление таких действий. То есть, понятие обладатель информации является важным для понимания того, кому принадлежит информация, кто принимает решение по ней. Обладатель информации, при осуществлении своих прав, помимо самих прав, имеет также ряд обязанностей.

Статья 6 данного закона вменяет ему в обязанность следующие действия: соблюдать права и законные интересы иных лиц, принимать меры по защите информации. Это не просто право, это обязанность обладателя информации. при осуществлении своих прав. Например, автор какого это произведения, публикуя своё произведение и стремясь и защитить его от незаконного использования, от плагиата, обязан принимать меры по защите информации, а также ограничивать доступ к информации, если такая обязанность установлена Федеральными законами. То есть любой обладатель информации, сталкиваясь с теми категориями, информация о которых есть в специальных федеральных законах, имеет обязанность ограничивать доступ к ней, если законодатель такое ограничение предусмотрел.

Девятая статья данного закона говорит об ограничении доступа к информации. Здесь действуют следующие принципы: ограничения доступа к информации устанавливается Федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Кроме того, обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен Федеральными законами. Данный принцип подчеркивает, что ограничение доступа к информации устанавливается не в интересах отдельных лиц, не в интересах отдельных субъектов, не по чьему-то желанию, а именно в соответствии с предыдущими рассмотренными документами, в целях защиты интересов личности, общества и государства. В других случаях, для защиты каких других интересов ограничение доступа к информации, по крайней мере в рамках данного закона, не предусматривается.

Порядок хранения и использования включенной в состав архивных фондов документированной информации в соответствии со статьей 4 данного документа устанавливается законодательством об архивном деле в Российской Федерации.[15]

К примеру, ст. 64 Семейного кодекса РФ раскрывает обязанность родителей по защите прав и интересов детей и, чтобы ограничить для них нежелательную информацию, родители вправе установить родительский контроль на компьютер, смартфон.[17] Но поисковая система, любая информационная система не вправе этого делать для всех граждан, так как будут нарушены международные договора, Конституция России, федеральные законы.

Статья 10 149-ФЗ говорит *о распространении информации или предоставлении информации*.[14] Это процесс, который является одним из наиболее частых, при возникновении тех или иных отношений между субъектами различных информационных процессов. Кто-то информацию предоставляет и либо распространяет, а кто-то является получателем информации. В Российской Федерации распространение информации осуществляется свободно, при соблюдении требований законодательства Российской Федерации, то есть постулируется свобода распространения информации. Нет ограничений, нет какого-то регулирования, жёсткого в рамках распространения информации. А 4 пункт той же статьи гласит, что предоставление информации осуществляется в порядке, который устанавливается соглашением лиц участвующих в обмене информации. То есть распространять, предоставлять неограниченному кругу лиц любой обладатель информации может, если это не противоречит законам. А вопросы предоставления информации, то есть доступа к ней конкретному лицу, осуществляется в порядке соглашения тех лиц, кто предоставляет и кто этот доступ получает.

11 статья касается документирования информации и гласит, что право собственности и иные вещные права на материальные носители, содержащие документированную информацию, устанавливаются гражданским законодательством. Иными словами, кто-то может быть обладателем не самой информации, но носителем информации и, в ряде случаев, на это стоит обращать внимание, решая задачи по защите информации.

Таким образом, данный документ постулирует основные взгляды законодателя на регламентирование информации, информационных технологий и защиты информации.

Учебные вопросы:

1. Что определяет Стратегия национальной безопасности РФ?
2. В чем состоит суть Стратегии национальной безопасности РФ?
3. Что такое национальная безопасность Российской Федерации?
4. Приведите формулировку Конституции России в части информационной безопасности:
5. Что такое свобода выражения мнения с точки зрения информационной безопасности России?
6. Какой документ выражает систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере?
7. Что такое Информационная сфера?
8. Что понимается под Информационной безопасностью России в Доктрине ИБ?
9. Что такое угроза информационной безопасности России?
10. Что такое Национальные интересы России в информационной сфере?

11. Информационная безопасность, согласно Стратегии национальной безопасности Российской Федерации….

12. Укажите все компоненты, согласно Доктрине информационной безопасности Российской Федерации, входящие в понятие «Информационная инфраструктура РФ»:

13. Перечислите территории, на которых, согласно Доктрине информационной безопасности Российской Федерации, могут размещаться объекты информационной инфраструктуры РФ:

14. Укажите все предусмотренные статьей 3 Федерального закона «Об информации, информационных технологиях и о защите информации» основания для ограничения доступа к информации:

15. Укажите все действия, которые, согласно ФЗ «О персональных данных» предусмотрены для оператора (персональных данных):

16. Перечислите все лица, которые, согласно ФЗ «О персональных данных», могут выступать в качестве субъекта персональных данных:

Глава 2. Угрозы и нарушители безопасности информации

2.1 Понятие угрозы безопасности информации

Что такое угрозы и нарушители безопасности информации? Это те, кто является непосредственными противниками, с которыми приходится сталкиваться в процессе обеспечения информационной безопасности.

Прежде всего, определим ряд понятий и для этого обратимся к государственному стандарту Российской Федерации — «Защита информации. Основные термины и определения», ГОСТ Р 50922-2006.[2]

Под угрозой безопасности информации в нем понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. Иными словами, это комплексное сочетание различных факторов и обстоятельств, приводящее к тому, что реализация нарушения безопасности информации становится актуальной, настоящей, действительной, т.е. ее можно рассматривать как действительно существующий фактор, как не какую-то фантастику. Для того чтобы подробно определить понятие угрозы, то есть разложить ее на составляющие, дадим еще ряд определений.

Источником угрозы безопасности информации будем называть любого субъекта, физическое лицо либо материальный объект, физическое явление, возможно, являющееся непосредственной причиной возникновения угрозы безопасности информации. То есть это некое лицо или сила, от которой исходит угроза, это источник угрозы безопасности информации.

Следующее понятие — это *уязвимость информационной системы*. Это такое свойство информационной системы, которое обуславливает возможность реализации угроз безопасности, обрабатываемой в ней информации. Иными словами, это какой-то недостаток, какой-то изъян, возможно, либо неизбежное и неустранимое свойство информационной системы, которое делает возможным реализацию угрозы.

Можно привести такой пример с человеком: человек должен дышать, следовательно, если в каком-то помещении не хватает кислорода, он будет себя чувствовать плохо и может задохнуться — это уязвимость. Это не означает, что по какой-то причине он не совершенен, не слишком хорош, а просто это его свойство. Поэтому стоит понимать, что практически любая информационная система, насколько бы хорошая она ни была, обязательно обладает какими-то уязвимостями. В силу того, что она так спроектирована и решает такие-то конкретные задачи, она обрабатывает информацию в том или ином виде, уязвимости так или иначе возникают, отсюда возникают и угрозы безопасности информации, поэтому следует информационную безопасность обеспечивать.

Следующее понятие, которое нам понадобится, это понятие *фактора, воздействующего на защищаемую информацию*. Это явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации либо блокирование доступа к ней. Это, в свою

очередь, непосредственно явление или процесс, заключающийся в нарушении безопасности информации, в воздействии на защищаемую информацию. То есть это уже действие.

Для того чтобы определить еще одно понятие — такое понятие, как несанкционированный доступ к информации, обратимся к руководящему документу Федеральной службы по техническому и экспортному контролю. Сокращенно ФСТЭК России, — одна из служб, входящих в органы исполнительной власти Российской Федерации, являющаяся регулятором в области защиты информации.

Согласно определяющим документам, которые устанавливают род деятельности данной организации, она имеет право, наделена полномочиями издавать руководящие документы, касающиеся защиты информации не криптографическими методами. О том, что такое криптографический метод защиты информации, мы поговорим в курсе далее. Пока просто остановимся на том, что вот эта самая ФСТЭК, является одним из регуляторов, одной из организаций, которые наделены правами такие документы издавать.

Обратимся к руководящему документу «Защита от несанкционированного доступа к информации. Термины и определения» и воспользуемся определением из этого самого документа.[9]

Несанкционированный доступ к информации, или сокращенно НСД (эта аббревиатура нам неоднократно понадобится в рамках нашего курса), это доступ к информации, нарушающей правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Под штатными средствами здесь предлагается понимать совокупность программного, микропрограммного и технического обеспечения, средств вычислительной техники или автоматизированных систем. Иными словами, несанкционированный доступ к информации — это явление, заключающееся в том, что лицо, не являющееся легальным пользователем, получает доступ к информации. В большинстве случаев это первый шаг к совершению чего-то нежелательного с информацией. Существуют исключения, когда, например, злоумышленник не стремится сам получить доступ к информации, а скажем, стремится нарушить ее доступность и не дать другим легальным пользователям получить доступ к ней. Но во всех остальных случаях, по крайней мере в большинстве из них, одной из первых целей нарушителей, необязательно единственной, является именно несанкционированный доступ к информации. Но, по крайней мере, если он случился, уже можно говорить о том, что безопасность информации нарушена.

Опираясь на эти четыре определения, можно представить понятие угрозы безопасности информации в виде следующей логической схемы:

- Угроза безопасности информации имеет свой источник.
- Источник угрозы информации, который является лицом или каким-то явлением, реализует некую угрозу, действие.

- И реализует он ее, эксплуатируя или используя некую уязвимость, то есть изъян информационной системы или автоматизированной системы, или объекта информатизации, если угроза реализуется через, например, поддерживающую инфраструктуру, через систему электроснабжения, через различные информационные линии, через персонал.
- И результатом угрозы в большинстве случаев является несанкционированный доступ.

Далее из этого несанкционированного доступа могут следовать другие виды нежелательного воздействия на информацию, но, по крайней мере, несанкционированный доступ может свидетельствовать о том, что безопасность информации нарушена, что реализована угроза.

Разобравшись таким образом с понятием угрозы безопасности информации, далее разберемся конкретно о том, какие бывают угрозы по своему проявлению, что нежелательного может произойти с информацией, кроме уже ранее известных нам формальных определений нарушения целостности, доступности, конфиденциальности, что конкретно нежелательного может сделать нарушитель с информацией.

2.2 Виды угроз безопасности информации

Прежде всего, попробуем перечислить основные виды угроз безопасности, то есть те нежелательные явления, которые могут воздействовать на информацию, что плохого с ней может случиться, что мы можем только вообразить, и, соответственно, от чего в дальнейшем придется защищаться.

Самое очевидное — это хищение или копирование информации, то есть, несанкционированный доступ к ней. Тот факт, что нарушитель у нас ознакомился с информацией, которую он не должен получать в доступ, уже, является хищением. И то, что он потом ее зафиксирует на каком-то ином носителе может быть отложено во времени. Он может ознакомиться, а далее изложить то, что он прочел, то, что он увидел, на каком-то другом носителе и кому-то передать. Кроме того, он может информацию уничтожить, либо ознакамливаясь с ней, либо без этого. То есть в этом случае будет нарушена доступность информации, в этом случае уже легальный пользователь не сможет получить к ней доступ. Поэтому такое явление также является нежелательным.[20, 23]

Кроме того, нарушитель может информацию модифицировать, то есть исказить. В этом случае будет нарушена ее целостность, опять же легальный пользователь вместо достоверной информации, например, получит информацию искаженную или лишенную логической структуры, не читаемую, бессмысленный набор символов. Поэтому от модификации либо искажения информации мы также будем ее защищать, то есть соблюдать ее целостность, поддерживать ее целостность.[21]

Следующая угроза — это угроза нарушения доступности либо блокирования информации. Это такой вид угрозы, который однозначно не предполагает, что нарушитель будет стремиться получить к информации, но в данном случае опять же пострадают интересы легальных пользователей. В этом случае пользователи, как и в случае с уничтожением, не смогут получить доступ к информации. Разница заключается в том, что сама информация при этом не уничтожается и доступность может быть восстановлена тем или иным способом. Такая временная угроза, тем не менее она не является какой-то менее опасной, менее реальной, поскольку, особенно в случае с различными организациями, с коммерческими структурами, может быть чревато финансовыми потерями.

Еще две угрозы связаны с целостностью информации, с авторством различных сообщений и часто имеют актуальные проявления в банковской сфере, в экономической сфере — там, где речь идет о каких-то финансовых потоках, о каких-то поручениях сделать денежные переводы. Это, во-первых, *угроза отрицания подлинности информации* и *угроза навязывания ложной информации*.

Угроза отрицания подлинности информации заключается в том, что нарушитель в ситуации, когда мы не имеем возможности проверить целостность пришедшей от него информации, отказывается от ее авторства, отрицает подлинность. Простой пример мошенничества с такой угрозой информации заключается в том, что лицо, совершившее покупку по банковской карте, отказывается от того, что оно данную покупку совершало или какую-то оплату через онлайн-банк, через интернет-магазин. Т.е. отрицает, что соответствующие информационные пакеты, то есть ключевая информация, касающаяся карточки, была отправлена именно им. Поэтому в рамках обеспечения информационной безопасности желательно разработать и эксплуатировать какие-то механизмы, которые бы не позволяли злоумышленнику так действовать.

И последняя угроза — навязывание ложной информации. Это всевозможные мошенничества, связанные с информацией, подделка различных информационных сообщений. Например, вы посылаете запрос в интернет-магазин о том, чтобы с вашей карты была списана некая сумма за покупку. Злоумышленник, действуя, например, через вредоносную программу на вашем компьютере перехватывает отправленную информацию и увеличивает сумму на большую. Например, с банковской карты списывается большая сумма, если все происходит автоматизированно и без участия человека, который проверит корректность, а соответственно, интернет-магазин в данном случае в некоторых условиях может действовать добропорядочно и не являться виновным в этом. И пользователь вроде правильную сумму ввел, а на самом деле, соответственно, злоумышленник в каких-то интересах получил выгоду, например, являясь сам сотрудником этого интернет-магазина. Дальше могут быть продемонстрированы соответствующие информационные ресурсы — логи, свидетельствующие о том, что пришел запрос на списание именно этой суммы.

Далее покупателю могут быть навязаны покупки, которые он не совершал, а доказать, что этого не делалось, будет достаточно проблематично. Поэтому от навязывания ложной информации также желательно защищаться в рамках обеспечения безопасности информации.

Все угрозы информационной безопасности, к какому бы из перечисленных выше проявлений они не относились, можно классифицировать по ряду признаков. Это удобно для того, чтобы собирать их в некие кластеры и типовыми методами от них защищаться. Можно предложить четыре основания таких классификаций.

Первое основание классификации — по *аспекту информационной безопасности*, на которую направлена угроза.

Следующее основание — *по компонентам объекта информатизации*.

Следующее основание — *по способу осуществления угрозы*.

Также можно предложить классификацию *по расположению источника угроз*.

Такая классификация позволяет собирать угрозы в группы. Это делается для того, чтобы одинаковыми средствами от них защищаться.

По аспекту информационной безопасности, соответственно, существуют три класса угроз: угрозы нарушения доступности, угрозы нарушения целостности и угрозы нарушения конфиденциальности. Здесь следует сразу оговориться, что большинство реальных угроз не укладываются однозначно в какой-то из этих классов. Можно выделять тот аспект информационной безопасности, на который угрозы направлены в первую очередь, то есть наносят наибольший ущерб: либо доступности, либо целостности, либо конфиденциальности, либо разделять крупные угрозы на ряд маленьких этапов — на ряд отдельных действий нарушителя, которые нарушают либо доступность, либо целостность, либо конфиденциальность.

Соответственно, угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. То есть увеличивается несанкционированный ограниченный круг лиц, которому информация должна быть доступна — нарушается конфиденциальность прямо в соответствии с определением понятия конфиденциальности.

Угроза нарушения целостности включает в себя любое умышленное изменение информации, хранящееся в вычислительной системе или передаваемое из одной системы в другую. То есть это угроза, заключающаяся в том, что пользователь информации получает к ней доступ, не может быть уверен в том, что получает ее без каких-либо несанкционированных изменений.

Угроза нарушения доступа к информации или угроза доступности, возникает всякий раз, когда в результате несакционированных или непреднамеренных воздействий блокируется доступ к некоторому информационному ресурсу автоматизированной системы. То есть возникает ситуация, когда легальный пользователь уже не может беспрепятственно

получить доступ к информации, даже выполняя условия владельца этой информации.

По компонентам объекта информатизации, на который угрозы нацелены, можно разделить угрозы на следующие классы: угрозы, реализуемые через воздействия на данные, то есть на информацию, обрабатываемую в информационной системе объекта информатизации, угрозы, реализуемые через воздействие на программы — это всевозможные вирусы, модифицирующие программы, программные закладки, вывод программ из строя.

Далее класс угроз, реализуемый через воздействие на аппаратуру, вывод аппаратуры из строя, добавление в нее каких-то аппаратных закладок, добавление несанкционированный аппаратуры, например модемов для выхода в глобальную сеть Интернет в нарушение действующей политики безопасности и разграничения доступа.

Рассмотрим класс угроз, реализуемых через воздействие на поддерживающую инфраструктуру, например угроза обесточивания объекта информатизации. На первый взгляд может показаться, что эта угроза никак не относится к информационной безопасности, но, в данном случае вполне нарушается доступность информации, если данные информационной системы, находящиеся на объекте информатизации, например, предлагает некий интернет-сервис, к которому пользователи получают доступ. В этом случае, если объект информатизации остается без энергоснабжения, нарушается доступность информации. Некоторые data-центры, например, могут от такого страдать, поэтому они вкладывают серьезные средства в предотвращение подобных угроз, в их недопущение.

По способу осуществления угрозы безопасности информации можно разделить на следующие классы. Здесь как бы нарастает уровень преднамеренности воздействия нарушителя и отдельно выделяются классы, никак не связанные с человеком.

Первый класс — это случайные действия.

Это такие угрозы, которые реализуются по невнимательности, по халатности пользователи либо совершенно случайно.

Следующий класс — это преднамеренные действия, это действия человека, совершенные с явным злым умыслом.

Далее класс угроз природного характера — всевозможные стихийные бедствия, пожары, наводнения.

И угрозы техногенного характера, связанные с аппаратным обеспечением, с оборудованием, с поддерживающей инфраструктурой.

По расположению источника угроз выделяется всего два класса: либо угрозы, источник которых находится *внутри* рассматриваемой автоматизированной системы, либо угрозы, источник которых находится *вне рассматриваемой автоматизированной системы*. Данная классификация, основанная на расположении источника угроз, подводит нас к следующему вопросу: какие же бывают источники угроз безопасности информации?

2.3 Источники угроз безопасности информации

Прежде всего, разделим их на ряд классов.

Все источники угроз в соответствии с той классификацией, которую мы ранее предложили, могут быть разделены на три больших класса: *антропогенные*, *техногенные и стихийные*. Это следует из определения источника угроз безопасности информации, это может быть как субъект, то есть физическое лицо, и тогда источник угроз антропогенный, либо какое-то явление, либо объект, то есть техногенные и стихийные источники, таким образом, мы подразумеваем.

Антропогенные и техногенные источники в свою очередь могут быть разделены на внешние и внутренние. Стихийные источники, как правило, на внешние и внутренние не делятся, здесь подразумеваются различные стихийные явления, которые почти всегда являются внешними по отношению к рассматриваемому объекту информатизации.

Поговорим подробнее про каждый из этих классов и рассмотрим примеры.

Внутренние. Антропогенными источниками угроз, как правило, являются лица, так или иначе связанные с деятельность информационной системы объекта информатизации либо самого объекта информатизации. Это, разумеется, основной персонал, то есть пользователи информационной системы, это представители служб защиты информации как более привилегированные пользователи и как лица, обладающие более серьёзным знанием по отношению к информационной системе, это вспомогательный персонал, уборщики, охрана и другие лица подобного рода. Они важны тем, что они являются лицами, которые имеют правомерный доступ в различные помещения объекта информатизации и, соответственно, на основании своих должностных обязанностей могут иметь доступ к различной информации, к различным носителям информации. Например, могут так или иначе, действуя злоумышленно, похищать различные носители информации, там флешки, диски, могут осуществлять подглядывание, послушивание, установку различных технических средств несанкционированного доступа к информации, о которых мы поговорим далее. Так или иначе, они могут являться источниками угроз безопасности. И, соответственно, таким же аналогичным источником угроз безопасности является технический персонал, то есть лица, ответственные за жизнеобеспечение и эксплуатацию помещения.

Они отличаются от вспомогательного персонала часто тем, что являются представителями других юридических лиц, то есть, например, электрической компании, телефонной компании, провайдера услуг сети Интернет, и поэтому они даже могут не подчиняться действующим на территории объекта информатизации правилам, регламентам, порядкам, различным распоряжениям. У них может быть свой порядок действий, который не всегда может соответствовать ожиданиям специалистов по защите информации, может нарушать безопасность информации.

Внешними антропогенными источниками угроз являются следующие лица. Это криминальные структуры, наиболее часто приходящий в голову источник угроз безопасности, различные преступники, которые могут действовать и из хулиганских побуждений, и из корыстного интереса, либо по другим каким-то мотивам, просто некие преступники. Такой наиболее обобщённый вид источника угроз безопасности. Потенциальные нарушители, хакеры — это лица, действующие, как правило, в одиночку либо, наоборот, организованной группой, деятельность которых напрямую связана именно с угрозами информационной безопасности, с атаками на различные информационные системы чаще всего посредством глобальной сети Интернет.

Недобросовестные партнёры могут являться источниками угроз безопасности информации. Действуя из корыстного интереса, действуя для получения тех или иных конкурентных преимуществ, они могут реализовывать различные угрозы извне информационной системы, извне объекта информатизации.

Технический персонал провайдеров услуг может являться источником угроз, реализуемых не столько злоумышленно, сколько на основе халатности, например, допуская какие-то ошибки в своей работе, которые могут приводить к нарушениям доступности информации.

Представители надзорных организаций и аварийных служб и представители силовых ведомств также выделяются в качестве источников угроз безопасности, поскольку могут также действовать непреднамеренно, но, тем не менее, допускать различные угрозы безопасности информации, например, действуя на основе своих приказов, постановлений, указов, которые нарушают безопасность информации в той или иной информационной системе.

Здесь речь идёт о том, что в рамках тех или иных необходимых и нужных действий могут допускаться какие-то действия типовые, которые, возможно, не отвечают особенностям той или иной информационной системы. Например, превентивное отключение от глобальной сети Интернет, блокирование каких-то сайтов, блокирование корпоративного сайта организации по чьему-либо, соответственно, заявлению. В этом случае нельзя сказать, что кто-то действует злоумышленно, но при этом доступность информации страдает, и, возможно, страдает и её целостность. То есть, если нет резервного копирования, если не обеспечена система восстановления доступности, то какая-то информация на сайте может быть полностью потеряна, например, заявки клиентов, например, какая-то пользовательская информация, авторизационная пользовательская информация. Таким образом, следует предпринимать меры для того, чтобы таких ситуаций не допускать.

К *техногенным внутренним* угрозам отнесём следующие факторы.

Это различные некачественные программные и аппаратные средства обработки информации, различные вспомогательные средства (средства охраны, сигнализации, телефонии) сами могут являться источниками угроз безопасности информации. Например, если средство пожарной сигнализации сработает не санкционировано и поднимет ложную тревогу, будет предпринята

последовательность действий, необходимая для пожаротушения, возможно, что часть аппаратных средств обработки информации выйдет из строя.

Можно привести реальный пример из зарубежной, так сказать, практики, связанной с коллегами из британского университета, когда в рамках уборки была спровоцирована сигнализация системы пожаротушения и некий дорогостоящий сервер был выведен из строя просто потоком воды, которая была вылита для тушения предполагаемого пожара, которого в действительности не существовало. Поэтому вот эти вспомогательные средства (средства охраны, средства сигнализации, средства телефонии) могут являться источниками угрозы безопасности информации.[22]

Об этом следует помнить и предпринимать соответствующие меры. И другие технические средства так или иначе тоже могут стать источниками угроз безопасности информации, выходя из строя либо приводя к каким-то последствиям, которые могут негативно сказаться на информации. Например, отключение каких-то других устройств, блокирование каких-то других устройств, прекращение электропитания аппаратного обеспечения информационной системы.

К *внешним техногенным источникам угроз* относятся средства связи, инженерные коммуникации, транспорт, то есть, все те внешние источники техногенные, от которых зависит функционирование объекта информатизации, которые могут в неподходящий момент выйти из строя и таким образом нарушить, например, доступность информации в рамках данной информационной системы.

К *стихийным источникам*, очевидно, относятся пожары, землетрясения, наводнения, ураганы, другие форс-мажорные обстоятельства. Эта так называемые обстоятельства непреодолимой силы, как правило, полностью их исключить нельзя и даже затруднительно от них серьёзно защититься, но, тем не менее, следует предпринимать те или иные меры, минимизирующие ущерб от их воздействия и позволяющие максимально быстро восстановить, например, доступность информации, сократить потери, не допустить нарушения целостности информации, а тем более её доступность, то есть не допустить её полного уничтожения. Речь о несанкционированном доступе и нарушении конфиденциальности в этих случаях, конечно же, не идёт.

Одной из важнейшей части источников угроз безопасности являются люди, то есть это какие-то конкретные лица.

2.4 Нарушители безопасности информации

Лица, которые являются источниками антропогенных угроз, антропогенными источниками угроз безопасности информации, и попробуем разобраться с тем, что это за лица, в каких интересах они действуют, какие они бывают, с тем чтобы в дальнейшем определить, как от них защищаться, от различных их видов.

Здесь снова обратимся к одному из стандартов Российской Федерации, в данном случае — к ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения».[9]

Из этого государственного стандарта возьмем следующие определения.

Нарушитель информационной безопасности организации — это физическое лицо или логический объект, то есть в данном случае имеется в виду процесс в информационной системе, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации, то есть в самом общем виде нарушение целостности, конфиденциальности или доступности информации.

Для того чтобы определить, какие бывают виды и типы нарушителей, обратимся к методике определения угроз безопасности информации в информационных системах, разработанной уже известной нам Федеральной службой по техническому и экспортному контролю.[7]

Данная методика определения угроз безопасности информации в информационных системах разработана в 2015 году, по состоянию на сегодня имеет статус утвержденного и является актуальным. По крайней мере, это наиболее свежий документ, дающий классификацию типов и видов нарушителей безопасности информации.

Тип нарушителя в соответствии с данной методикой бывает одним из двух — это либо внешние нарушители, либо внутренние.

Внешние нарушители — это нарушители, которые находятся за пределами информационной системы, за пределами объекта информатизации и действуют оттуда, то есть в самом общем понимании не обладают правами на доступ к различным компонентам информационной или автоматизированной системы, то есть лица, у которых нет учетной записи в информационной системе, лица, которые не относятся к персоналу организации, клиенты той или иной организации, надзорные органы, просто прохожие за окном и за контролируемой зоной.

Соответственно, *внутренние нарушители* — это нарушители, относящиеся к персоналу организации того или иного уровня.

Как мы видели в классификации угроз информационной безопасности, нарушители бывают разных уровней осведомленности и полномочий по отношению к информационной системе и к автоматизированной системе. Тип нарушителя определяется в соответствии с данной методикой на основе прав доступа субъекта к следующим компонентам информационной и автоматизированной систем в соответствии с данной методикой. То есть для каждого из этих компонент нам требуется определить, есть ли у потенциального нарушителя, то есть у того лица, которое мы исследуем в качестве нарушителя, права доступа к тому или иному объекту. И эти объекты, которые в соответствии с методикой предлагается исследовать как минимальный список, — это следующие объекты: устройства ввода / вывода информации, то есть терминалы, клавиатуры, мыши, может ли злоумышленник что-то вводить сам в

информационную систему и с ней взаимодействовать; беспроводным устройствам, например, точкам доступам беспроводного выхода в сеть Интернет; программным, программно-техническим и техническим средствам обработки информации, то есть может ли он подключать что-то новое, что-то отключать, перенастраивать, менять конфигурацию; съемным машинным носителям информации — это следующий объект, о котором следует сложить свое представление — может ли лицо, которое мы рассматриваем в качестве потенциального нарушителя, подключить свою флешку, утащить чужую, подключить модем для выхода в сеть Интернет, подключить свой внешний жесткий диск и так далее; активному и пассивному оборудованию каналов связи.

Следующий объект, о котором следует сложить свое понимание того, может ли исследуемое лицо получить к ним доступ; и каналам связи, выходящим за пределы контролируемой зоны, имеется в виду та их часть, которая находится на контролируемой территории — на территории объекта информатизации.

Если лицо, которое мы исследуем в качестве нарушителя, имеет права доступа, например, потому, что это сотрудник, который обеспечивает монтаж каналов связи, настройку сетевого оборудования, профилактический контроль различных устройств, входящих в состав системы обработки информации, в состав объекта информатизации, то такой нарушитель является внутренним.

Если нарушитель не обладает правами доступа ни к какому из этих объектов, то такой нарушитель признается внешним.

Внешние нарушители составляют первый тип нарушителей. Формально это лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы.

Кто бывает такими нарушителями? Клиенты — это самый часто встречающийся тип внешнего нарушителя безопасности информации. Приглашенные посетители, то есть, например, потенциальные партнеры по каким-то бизнес-договорам, по каким-то партнерским отношения, по закупкам, по поставкам и так далее. Представители конкурирующих организаций, которые могут как минимум стремиться собирать информацию с целью получения конкурентных преимуществ. Различные наблюдатели за пределами охраняемой территории, не вдаваясь в вопросы того, для каких целей, из каких побуждений они действуют, любые лица, которые наблюдают за объектом информатизации из-за пределов охраняемой территории.

Соответственно, в противовес внешним нарушителям определяются внутренние нарушители, или нарушители типа 2. Это лица, имеющие право постоянного или разового доступа к информационной системе либо отдельным ее компонентам. Это, очевидно, либо сотрудники организации, представители ее персонала, либо лица, по той или иной причине получающие санкционированный разовый допуск к информационной системе. Это любые представители организации, которые поддерживают ту или иную

инфраструктуру, — водопроводчик, электрик, представитель интернет-провайдера, специалист по пожарной безопасности, который производит оценку безопасности помещений, сотрудник службы, который монтирует вентиляцию помещений, просто уборщик, возможно, не входящий в персонал, а приглашенный по договору аутсорса.

Соответственно, эти лица получают право на доступ в помещение, даже иногда в самые засекреченные, в самые оборудованные для обработки конфиденциальной информации. И они легально в эти помещения попадают и могут действовать злоумышленно в ряде случаев. [4. с.78, 18]

Рассмотрим несколько примеров, часть из которых уже были названы. Это операторы информационной системы, это администраторы вычислительных сетей, прикладные и системные программисты, технический персонал по обслуживанию зданий. В этом списке перечислены лица, которые на постоянной основе имеют право доступа на территорию информационной системы и объекта информатизации.

В том числе в качестве внутренних нарушителей безопасности информации могут рассматриваться и лица, являющиеся однократно санкционированными посетителями контролируемой территории, то есть не нарушающие формально пропускной режим, не нарушающие формально разграничение доступа, но не имеющие постоянного доступа на контролируемую территорию.[19]

Определив таким образом тип нарушителя как внутренний или внешний, далее поговорим о видах нарушителя, то есть о том, какие конкретно категории лиц выделяются в качестве нарушителя в соответствии с названной выше методикой.

2.5 Виды и цели нарушителей

Мы уже определили понятия типа нарушителя, определили, что бывают внешние и внутренние нарушители, теперь определимся с тем, к каким категориям лиц могут относиться как внешние, так и внутренние нарушители.

В соответствии с названной методикой определения актуальных угроз Федеральной службы по техническому и экспортному контролю, рассматриваются следующие виды нарушителей.

Это специальные службы иностранных государств, то есть подготовленные профессионалы по сбору информации из различных информационных систем, обладающие всей полнотой оборудования, различных технических средств для перехвата информации и так далее.

Террористические, экстремистские группировки, представители организованного преступного мира, действующие максимально целенаправленно, максимально эффективно, обладающие достаточным финансированием.

Преступные группы — такой типичный средний, обычный преступный мир, который, возможно, по сравнению с вторым видом нарушителей менее

неограниченный в своем финансировании, менее подготовленный и, может быть, действует менее целенаправленно. В смысле с меньшей мотивацией — они с большей вероятностью готовы отступить, встретив адекватный отпор.

Внешние субъекты — это наиболее типичный нарушитель типа внешних нарушителей, внешний субъект, не обладающий, никакими специальными чертами. Любой внешний нарушитель, если у него нет каких-то особых качеств, может считаться просто внешним субъектом. Это вид наиболее универсальный.

Конкурирующие организации — это вид нарушителей, действующих в целях получения, как правило, конкурентных преимуществ. Это представители бизнеса, они имеют нормальное финансирование, в смысле, что они могут себе позволить достаточно дорогостоящие технологии нарушения информационной безопасности, и они имеют достаточно высокую мотивацию.

Следующий вид нарушителей — это разработчики, производители, поставщики программно-технических средств. Под ними подразумеваются программисты либо производители различных технических и программно-технических средств, имея в виду, что они могут, с одной стороны, допускать брак в разработке своих продуктов, с другой стороны, могут действовать злоумышленно и вносить в них различные дополнительные узлы либо различные программные фрагменты, которые реализуют тот функционал, который потенциальному потребителю не требуется. Например, собирают и накапливают информацию, с тем чтобы впоследствии разработчик мог получить к ней доступ.

Следующий вид нарушителей — лица, привлекаемые для установки, наладки, монтажа, пуско-наладочных и иных видов работ. Это нарушители, которые однократно или периодически, но не постоянно, получают легальный доступ на территорию, контролируемую в рамках объекта информатизации, то есть получают доступ к информационной системе.

Следующий вид нарушителей — это лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора. Они подобны предыдущему виду нарушителей, но имеют постоянный доступ в некий ограниченный круг помещений, связанных с их функциями.

Далее, как отдельный вид выделяются пользователи информационной системы. Это наиболее обобщенный тип для внутренних нарушителей. Если у этих пользователей нет никаких специальных полномочий в информационной системе, то они просто пользователи.

Отдельно выделяются администраторы информационной системы и администраторы безопасности как пользователи со специальными привилегиями, как пользователи с одним из наиболее широких полей их возможностей, которые они могут реализовать в рамках информационной системы.

И отдельный вид — бывшие работники. Не секрет, что такой вид нарушителей достаточно типичен для реализации угроз информационной безопасности, часто они действуют из мести, пытаясь так или иначе навредить

своему бывшему работодателю. Они характеризуются тем, что у них в отличие от просто внешних субъектов, — в данном случае они, разумеется, рассматриваются как внешние нарушители, — они могут обладать более высоким уровнем знаний об информационной системе, поскольку прежде они были пользователями и могли вполне легально информацию о системе собирать. Плюс они знают о работе информационной системы в рамках своих бывших полномочий.

Данные виды нарушителей характеризуются своими целями. Каждый из этих видов нарушителей может преследовать одну или несколько целей из предлагаемого далее в рамках данной методики списка.

Цели предлагаются к рассмотрению следующие: нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Это мотив, которым характеризуются различные террористические группы, различные преступные группы и спецслужбы иностранных государств или групп государств.

Следующая цель нарушителей — реализация угроз безопасности информации по идеологическим или политическим мотивам. Это наиболее характерный мотив для различных экстремистских и террористических групп, взаимооднозначное соответствие.

Организация террористического акта — отдельный вид цели, тоже прямо коррелирующий с таким видом нарушителя, как террористическая группа. Его можно охарактеризовать, этот пункт, эту цель нарушителя как стремление нанести наибольший физический ущерб, в смысле говоря о безопасности информации, нарушить именно доступность в первую очередь информации, то есть полностью уничтожить или повредить оборудование объекта информатизации.

Следующая возможная цель нарушителя — причинение имущественного ущерба путем мошенничества или иным преступным путем. Это один из наиболее универсальных вариантов целей нарушителей, многие из перечисленных выше видов нарушителей могут преследовать данную цель.

Дискредитация или дестабилизация деятельности органов государственной власти, организаций — тоже один из видов целей нарушителя, достаточно универсальный для большинства видов нарушителей, за исключением, может быть, тех, у кого цель однозначно заключается в другом, например, в организации терактов.

Получение конкурентных преимуществ — типичная цель для конкурентов, для организаций, занимающихся получением конкурентных преимуществ на рынке, то есть для тех, кто пытается нарушить в данном случае конфиденциальность информации именно с целью похищения каких-то коммерческих секретов, с целью нарушения режима коммерческой тайны, с целью улучшения своих позиций на том или ином рынке.

Следующая цель — внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки.

Это цель, которую могут преследовать разработчики программных и программно-аппаратных средств на этапе разработке, действуя злоумышленно. Например, разработчики вирусов попадают как раз именно в эту категорию нарушителей, в этот вид нарушителей и преследуют именно такую цель.

Любопытство или желание самореализации — это типичная цель для сотрудников организации, для пользователей информационной системы, действующих не слишком злоумышленно. Они не стремятся нанести серьезный ущерб информационной системе или объекту информатизации, но стремятся самоутвердиться или самореализоваться, и стремясь достичь этой цели, могут наносить ущерб безопасности информации, могут нарушать безопасность информации, наносить ущерб информации, хранящейся в информационной системе.

Выявление уязвимости с целью их дальнейшей продажи и получения финансовой выгоды — цель, которая также может преследоваться нарушителями, как минимум всеми внутренними нарушителями, включая, казалось бы такая экзотика, на первый взгляд, сотрудниками, обеспечивающими просто функционирование объекта, такими как сотрудники службы обеспечения чистоты, то есть клининговыми службами, охраной, любыми электриками, водопроводчиками, монтажниками вентиляционного оборудования. Но тем не менее случаи, когда именно под видом таких сотрудников действуют нарушители информационной безопасности, они известны. Поэтому такие лица рассматриваются как потенциальные нарушители.

Реализация угроз безопасности информации из мести — типичная цель нарушителей, относящихся бывшим сотрудникам. Они, как правило, действуют из мести.

Реализации угроз безопасности информации непреднамеренно из-за неосторожности или неквалифицированных действий — также типичная цель, которая характерная для нарушителей, относящихся к видам, соответствующим различным сотрудникам организации, которые находятся на легальной основе на территории объекта информатизации. Все они, действуя неосторожно или по неквалифицированности своих действий, могут нанести ущерб информации, то есть так или иначе нарушить информационную безопасность.

Далее рассмотрим сопоставление конкретных видов и типов нарушителей возможным целям и мотивам реализации угроз безопасности информации, которые они преследуют, так, как это представлено в названной методике.

Первым рассмотрим такой вид нарушителей, как специальные службы иностранных государств.

Этот вид нарушителей может быть как внешним, так и внутренним, и он преследует самые серьезные цели — нанесение ущерба государству, дестабилизация деятельности органов государственной власти.

Большинство нарушителей, о которых мы будем говорить далее, преследуют более жизненные, такие типичные повседневные цели.

Следующий вид нарушителя — террористические экстремистские группировки. Данный тип нарушителя рассматривается всегда как внешний. Он также преследует цель нанесения ущерба государству, дестабилизация деятельности органов государственной власти. Однако, ему присущи и другие цели, такие как совершение террористических актов, идеологические и политические мотивы. Можно сказать, что данный вид нарушителя более направлен на удовлетворение собственных интересов.

Первый вид нарушителя, то есть спецслужбы иностранных государств, действуют только на уровне самых глобальных интересов.

Следующий вид нарушителя — преступные группы, криминальные структуры. Это также внешний тип нарушителя. Их основная цель — причинение имущественного ущерба тем или иным путём. В качестве одного из видов путей, который они могут для этого избирать, называется выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Иными словами, их основная цель — это собственное обогащение.

Следующий вид нарушителя — внешние субъекты, физические лица. Это самый обобщённый вид для типа нарушителя внешний, и поэтому круг возможных целей и мотивов реализации угроз для них достаточно широк: идеологические или политические мотивы, причинение имущественного ущерба, выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды, желания самореализации. Иными словами, внешние субъекты могут действовать по совершенно разным мотивам: по личным убеждениям, с целью обогащения, с целью самореализации либо из мести, из каких-то других мотивов, это попадает в понятие идеологических или политических мотивов. Также здесь тоже называется такой вид возможной цели реализации угрозы — выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. То есть любой внешний субъект по идее может выступать как разведчик, который сам хоть и не применяет знания об уязвимостях информационной системы, но может их кому-то продать.

Следующий вид нарушителя — это конкурирующая организация, также относится к типу внешний нарушитель информационной безопасности, и возможными целями или мотивами реализации угроз для него является получение конкурентных преимуществ, причинение имущественного ущерба.

Как и было ранее сказано, здесь практически однозначное соответствие конкурирующей организации: цель — получение конкурентных преимуществ.

Следующий вид нарушителя — разработчики, производители, поставщики программных, технических и программно-технических средств. Данный тип нарушителя рассматривается как внешний, и возможные цели реализации угроз безопасности информации для данного нарушителя — это причинение имущественного ущерба.

Как один из способов такого причинения имущественного ущерба — внедрение дополнительных возможностей в программное обеспечение, непреднамеренные, неосторожные или неквалифицированные действия. То

есть данный нарушитель у нас может действовать и злоумышленно, и халатно, то есть не умышленно.

Следующий вид нарушителя — лица, привлекаемые для установки, наладки, монтажа и других видов работ. Он рассматривается уже как внутренний по причине того, что имеет, хоть и иногда, и периодически, легальный доступ на территорию, контролируемую в рамках объекта информатизации. И его мотив, и его цели — это причинение имущественного ущерба, непреднамеренные, неосторожные или неквалифицированные действия. Данный нарушитель у нас тоже может быть и злоумышленным, и, назовём это, условно халатным.

Следующий вид нарушителя — лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру операторы: охранники, уборщики, и так далее. Это также внутренний тип нарушителя. От предыдущего вида отличается тем, что имеет постоянный доступ на контролируемую территорию. Его возможные цели и мотивы совпадают с предыдущим видом нарушителя. Это снова причинение имущественного ущерба, непреднамеренные, неосторожные или неквалифицированные действия. Снова ответ нарушителя может быть и злонамеренным, и халатным.

Следующий вид нарушителя — пользователи информационной системы, такой самый обобщённый, можно сказать, вид нарушителя, соответствующего пользователя информационной системы. Если нет каких-то специальных привилегий, то это просто пользователь — любой сотрудник, который имеет учётную запись в информационной системе, скажем так. Это, разумеется, и внутренний нарушитель, и его возможные цели — причинение имущественного ущерба, также непреднамеренные, неосторожные или неквалифицированные действия, как и в предыдущих видах нарушителей, но добавляются ещё желание самореализации, месть за ранее совершённые действия, любопытство. То есть данный нарушитель у нас может быть и злонамеренным, и халатным, и ещё и любопытным.

Следующий вид нарушителя — администрация информационной системы и администраторы безопасности. Это внутренний тип нарушителя, более привилегированный по сравнению с пользователем. Его мотивы совпадают с предыдущим видом нарушителей, но он обладает более широкими возможностями.

И последний вид нарушителя — бывшие работники (пользователи). Рассматривается данный тип нарушителя как внешний, он больше не имеет права доступа на территорию объекта информатизации, не имеет доступа к информационной системе, и его возможные цели — причинение имущественного ущерба, месть за ранее совершённые действия.

2.6 Потенциал и возможности нарушителей

Снова мы обращаемся к методике Федеральной службы по техническому и экспортному контролю и рассматриваем те уровни потенциала нарушителей, которые в данной методике предлагаются.[7]

Выделяются три уровня потенциала нарушителей — нарушители с базовым, или низким, потенциалом нападения; нарушители с базовым повышенным, или средним, потенциалом нападения; и нарушители с высоким потенциалом нападения.

Как правило, можно понимать это так, что нарушители с базовым, или низким, потенциалом нападения — это нарушители, обладающие умеренной мотивацией, то есть стремлением достичь своей цели, финансированием и навыками.

Нарушители с базовым повышенным, или средним, потенциалом нападения — это нарушители, которые обладают двумя из трех этих параметров на высоком уровне — финансированием, мотивацией и навыками.

И нарушители с высоким потенциалом нападения — это нарушители, которые имеют все эти три параметра на высоком уровне.

Нарушители с базовым, низким, потенциалом нападения — это внешние субъекты, физические лица, то есть любые внешние лица, которые не имеют доступа на территорию и никакими специальными навыками и никакими специальными возможностями не обладают. Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора, то есть просто сотрудники, обеспечивающие функционирование системы на территории объекта информатизации, никакой дополнительной квалификацией они не обладают, никакой особой мотивации тоже у них нет.

Пользователи информационной системы, включая самых простых операторов информационной системы, клерков, бывшие работники — это уволенные сотрудники, здесь не рассматриваются бывшие работники, являющиеся, например, сотрудниками каких-то спецслужб или являющиеся участниками каких-то криминальных группировок, это просто обычные обыватели, являющиеся бывшими работниками. А также лица, привлекаемые для установки, наладки, монтажа и других видов работ, они также не обладают ни особой квалификацией, ни особой мотивацией для совершения тех или иных нарушений безопасности информации. Не обладают мотивацией — имеется в виду, что, встречая некое препятствие, они, скорее всего, оставят попытки достичь своей цели. Они не замотивированы прилагать серьезные усилия. Если нарушить информационную безопасность легко, они с какой-то вероятностью это совершат, если сложно, скорее всего, откажутся от своих намерений.

Нарушители с базовым повышенным, или средним, потенциалом — это более серьезные наши противники. Это террористические либо экстремистские группировки. Они серьезно замотивированы и могут обладать достаточно серьезным финансированием. Преступные группы, криминальные структуры также, как правило, не имеют проблем с финансированием, а кроме того, могут

включать и достаточно серьезных специалистов. Конкурирующие организации сходны с ними в этих двух параметрах, кроме того, они могут обладать серьезной мотивацией.

Разработчики, производители, поставщики программных и технических средств — это чаще всего специалисты в области соответствующего программного или аппаратного обеспечения. Кроме того, они могут обладать достаточно серьезной мотивацией к нарушению безопасности информации.

Администраторы информационной системы и администраторы безопасности, как правило, имеют и подготовку, и мотивацию для реализации угроз безопасности информации.

И, наконец, в класс нарушителей с высоким потенциалом нападения выделяется один-единственный вид нарушителей — это специальные службы иностранных государств либо блоков государств. Считается, что они обладают и высоким уровнем финансирования, и высоким уровнем мотивации на достижение поставленной цели, и могут включать в свои ряды достаточно серьезных специалистов в области безопасности информации, сетевых технологий, программирования, разработки аппаратных средств.

Нарушители с базовым либо низким потенциалом нападения могут реализовывать следующие возможности — они могут получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках, они могут получить подобную информацию самостоятельно, то есть почитать какую-то литературу, сами разработать вредоносную программу и ее применить.

Нарушители с базовым повышенным, средним, потенциалом нападения обладают следующими возможностями — во-первых, всеми возможностями нарушителей с более низким потенциалом. Кроме того, они осведомлены о мерах защиты информации в системе данного типа, то есть уже какую-то информацию собрали. Они могут получить информацию об уязвимостях отдельных компонент информационной системы, то есть целенаправленно подготовиться к своим действиям. И, кроме того, у них есть доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы, то есть они лучше осведомлены, чем нарушители с более низким потенциалом нападения.

Наконец, нарушители с высоким потенциалом нападения, включая все возможности нарушителей с более низким потенциалом, имеют возможность осуществлять несанкционированный доступ к информации, обрабатываемой в информационной системе, могут они также получить доступ к программному обеспечению чипсетов, системному и прикладному обеспечению. Это означает, что они могут влиять на работу информационной системы активным образом. Кроме того, они имеют возможность получить информацию об уязвимостях и создать методы и средства реализации угроз безопасности информации, то есть они могут хорошо подготовиться и провести целенаправленную атаку на данную конкретную систему обработки информации, информационную систему либо объект информатизации.

2.7 Способы реализации угроз нарушителем

Как минимум угрозы безопасности информации могут быть реализованы нарушителями за счет несанкционированного доступа или воздействия на объекты на различных уровнях: на аппаратном уровне, то есть путем модификации различных компонент аппаратных информационной системы и автоматизированной системы; на общесистемном уровне, то есть путем подключения / отключения каких-то дополнительных узлов, каких-то дополнительных компьютеров, средств связи, сетевых устройств или их аналогов, то есть воздействуя на объекты на данном уровне, нарушитель может либо их перенастраивать, либо подключать свои, либо выводить из строя уже существующие, например, полностью отключив систему от связи с глобальной сетью Интернет, отключив сетевое оборудование соответствующее; на прикладном уровне, то есть на уровне программ — нарушитель может запускать свои программы, вмешиваться в работу программ, которые уже есть в информационной системе, либо вносить в них, как мы увидели в целях и мотивациях некоторых из нарушителей, различные несанкционированные возможности, в дальнейшем расширяющие возможности нарушителя, то есть дающие ему способ получить, например, несанкционированный доступ к информации; либо на сетевом уровне, то есть при помощи сетей, например, глобальной сети Интернет.

На этом уровне нарушитель может воздействовать на объекты в информационной системе, может получать доступ к информации либо выводить из строя какие-то компоненты информационной системы. Кроме того, нарушитель может реализовывать свои угрозы за счет несанкционированного физического доступа или воздействия на линии и каналы связи, технические средства, машинные носители информации, то есть просто выводить их из строя.

Такой нарушитель-вандал получается, который может разрушать различные сегменты информационной системы и автоматизированной системы.

В качестве примера можно привести ситуацию, которая иногда встречалась лет десять назад, когда провайдеры домашнего Интернета предоставляли доступ всем желающим к глобальной сети Интернет, и их сетевое оборудование размещалось в общедоступных помещениях, таких как чердаки, подвалы. И иногда некоторые нарушители реализовывали угрозы нарушения доступности информации путем воздействия на линии связи, технические средства и таким образом отключали пользователей от глобальной сети Интернет, похищая или уничтожая сетевое оборудование, принадлежащее таким провайдерами.

И еще одна возможность есть у нарушителей — это возможность воздействия на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал, то есть так называемая социальная инженерия. Этот вид воздействия включает в

себя вхождение в доверие, различные методики получения от персонала конфиденциальной информации путем, возможно, навязывания ложной информации, путем, возможно, отказа от авторства какой-то информации, путем моделирования каких-то ситуаций, вызывающих сочувствие, понимание к нарушителю. Но все это объединяет стремление к получению доступа к информации, нарушению информационной безопасности.

Угрозы безопасности информации могут реализовываться нарушителем за счет следующих действий: доступа к компонентам информационной системы, то есть напрямую; создания условий и средств, обеспечивающих такой доступ — на один шажок больше; доступа или воздействия на обслуживающую инфраструктуру, за которую оператор не отвечает — еще подальше.

Если нарушитель не имеет доступа к компонентам информационной системы, то его первая цель, как правило, заключается в получении доступа к информационной системе и в получении максимально возможных прав и привилегий при таком доступе, то есть внешний нарушитель в первую очередь будет стремиться получить доступ к информационной системе, в лучшем случае — стать нарушителем внутренним, то есть получить учетную запись и права доступа кого-то из пользователей информационной системы. Нарушители могут совершать действия, следствием которых является нарушение безопасности информации, как преднамеренно, так и случайно.

На основе этого выделяются две категории угроз безопасности информации — преднамеренной и непреднамеренной. Кроме того, угрозы безопасности информации преднамеренные могут быть направлены как на интересующую нарушителя информационную систему с заранее известными ему структурно-функциональными характеристиками, и тогда такая угроза называется целенаправленной.

Целенаправленная угроза безопасности информации адаптирована к структурно-функциональным характеристикам информационной системы, то есть специально создана таким образом, чтобы нарушитель мог достичь цели, то есть в ней учтены все особенности информационной системы — какие аппаратные средства в ней используются, какие программные средства в ней используются, какая информация обрабатывается, какой режим ее обработки и все прочие особенности, которые нарушителю удалось установить.

При подготовке и реализации целенаправленных угроз безопасности информации нарушитель может использовать методы социальной инженерии, которые позволяют ему изучить поведение пользователей и их реакцию на поступающие к ним внешние данные. Это следует учитывать, оценивая возможности нарушителя, оценивая то, каким образом нарушитель может достигать своих целей.

Другой альтернативой целенаправленной угрозе является так называемая нецеленаправленная, или веерная, угроза безопасности информации, не ориентированная на конкретную информационную систему. Это, например, рассылка вирусов.

Нарушитель в этом случае не стремится нарушить безопасность информации какой-то конкретной информационной системы — где повезет, там, соответственно, его угроза и реализуется. [11 , с.39]

Цель такой угрозы — это, как правило, несанкционированный доступ к информации, например, похищение персональных данных пользователей или их конфиденциальной информации, популярна кража кредитных карт, пин-кодов, логинов и паролей, записанных в пользовательских файлах, либо перехват управления или воздействия на как можно большее количество информационных систем. Данная цель весьма типична и касается, по сути говоря, всех. Бытует мнение, что якобы угрозы безопасности информации направлены только на тех, у кого есть какая-то информация, которую требуется защищать, например, конфиденциальная информация на сотрудников банков, на информационные системы банков, на информационные системы крупных корпораций, мелких компаний, может быть, медийных персон, известных лиц просто, первых лиц государства и так далее, а обычным пользователям, обычным гражданам якобы нечего бояться за безопасность собственной информации.

Так вот, правда заключается в том, что они также являются целями такой нецеленаправленной, веерной угрозы безопасности информации. В этом случае, если на компьютере или другом коммуникационном устройстве пользователя нет никакой конфиденциальной информации, вступает в действие вторая цель нарушителя — перехват управления или воздействие на как можно большее количество информационных систем, то есть его целью будет — контроль над вашим компьютером, мобильным телефоном, смартфоном, планшетом, ноутбуком.

Зачем? Существует ряд целей, для чего можно в дальнейшем использовать такие взятые под контроль информационные системы.

Во-первых, их можно использовать для распределенных вычислений, например, для взлома паролей, для взлома ключей шифрования различных действительно серьезных целей, к которым стремится злоумышленник, то есть банковских систем, правительственных сайтов и каких-то банков и баз данных. То есть ваши устройства могут поучаствовать в переборе всех возможных паролей.

И вторая возможность — реализация компьютерных атак с использованием большого количества зараженных компьютеров, то есть компьютер любого пользователя может стать пешкой в такой игре нарушителя, может участвовать, сам того не подозревая, в смысле, его владелец не будет об этом подозревать, его устройство будет участвовать в реализации компьютерной атаки.[4, с.80]

Но хотелось бы заострить ваше внимание на том, что информационная безопасность касается каждого, у кого есть устройство, в котором обрабатывается информация. Преднамеренные угрозы безопасности информации, как правило, включают в себя следующие действия: сбор информации об информационной системе, ее структурно-функциональных

характеристиках, условиях функционирования; затем выбор методов и средств, используемых для реализации таких угроз; далее, нарушитель, как правило, непосредственно реализует угрозу безопасности информации в информационной системе, проникает в нее, закрепляется, достигает своей цели путем реализации неправомерных действий и в заключительном этапе устраняет признаки и следы неправомерных действий в информационной системе.

Рассмотрев, таким образом, возможные виды угроз и нарушителей информационной безопасности, мы очертили круг тех противников, с которыми приходится сталкиваться специалистам по безопасности информации.

В следующей лекции разберем то, как отделять актуальных нарушителей и угрозы от неактуальных, то есть выделять их из всего возможного многообразия угроз.

Учебные вопросы:

Угрозы и нарушители безопасности информации

1. Уязвимость информационной системы, согласно ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», –

2. Укажите все угрозы доступности информации:

3. Укажите все угрозы конфиденциальности информации:

4. Укажите все внешние антропогенные источники угроз:

5. Укажите все виды нарушителей, относящихся, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК В 2015 г., к внутреннему типу:

6. Обязательным признаком нарушителя информационной безопасности организации, согласно ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения», является то, что….

7. Укажите все виды нарушителей, среди возможных целей (мотивов) которых, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК В 2015 г., есть выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды:

8. Возможность осуществлять несанкционированный доступ к информации в АС, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК В 2015 г., имеют нарушители с потенциалом …

9. Базовым (низким) потенциалом нападения, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК В 2015 г., обладает нарушитель вида:

10. Угроза безопасности информации, направленная на интересующую нарушителя ИС, с заранее известными ему характеристиками, называется, …. согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК в 2015 г.

11. Укажите типы угроз, относящихся к классу аспекта информационной безопасности:

12. Что такое несанкционированный доступ к информации?

13. Расставьте логику осуществления угрозы безопасности информации:

14. Укажите виды угроз безопасности информации:

15. Какие угрозы существуют в классе аспекта ИБ?

16. Какие угрозы существуют в классе по *компонентам объекта информатизации*?

17. Сопоставьте классификацию способов осуществления угрозы безопасности информации и их определения:

18. Уязвимость информационной системы, согласно ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», –

19. Укажите все угрозы доступности информации:

20. Укажите все угрозы конфиденциальности информации:

21. Укажите все внешние антропогенные источники угроз:

22. Укажите все виды нарушителей, относящихся, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК В 2015 г, к внутреннему типу:

23. Обязательным признаком нарушителя информационной безопасности организации, согласно ГОСТ Р 53114-2008 «Защита информации Обеспечение информационной безопасности в организации Основные термины и определения», является то, что

24. Укажите все виды нарушителей, среди возможных целей (мотивов) которых, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК В 2015 г, есть выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды:

25. Возможность осуществлять несанкционированный доступ к информации в АС, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК В 2015 г, имеют нарушители с потенциалом

26. Базовым (низким) потенциалом нападения, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК В 2015 г, обладает нарушитель вида:

27. Угроза безопасности информации, направленная на интересующую нарушителя ИС, с заранее известными ему характеристиками, называется, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК В 2015 г,

28. Укажите субъектов, от которых могут исходить внутренние антропогенные угрозы:

Глава 3. Модель угроз безопасности информации

3.1 Назначение модели угроз безопасности информации

Ранее уже были перечислили угрозы безопасности информации и возможные нарушители безопасности информации, то есть очертили круг тех противников и тех угроз, с которыми предстоит столкнуться специалисту по безопасности информации в какой-либо информационной системе.

Часть из этих угроз и нарушителей для конкретной информационной системы не являются актуальными, поскольку может быть не связана с той спецификой, которая присуща конкретному объекту информатизации, конкретной информационной системе. Вряд ли информационная система небольшой коммерческой компании станет целью террористической группы или, тем более, спецслужб иностранных государств или групп государств.

В этой главе разберем построение модели угроз безопасности информации, то есть, постараемся выделить из всего перечисленного круга угроз безопасности информации те, которые являются актуальными для конкретного объекта информатизации, для конкретной информационной системы.

Рассмотрение угроз информационной безопасности будем проводиться на основе методики определения угроз безопасности информации в информационных системах, разработанной Федеральной службой по техническому экспортному контролю.[7]

Модель угроз информационной безопасности строится для того, чтобы установить, существует ли возможность нарушения безопасности информации, содержащейся в конкретной информационной системе, а также приведет ли нарушение информационной безопасности к нанесению ущерба для, как минимум, трех заинтересованных лиц: обладателя информации, оператора информации или персональных данных и субъектов персональных данных. То есть для того лица, которое обладает всей полнотой прав на информацию, тех лиц, которые с его разрешения либо сами, являясь обладателями информации, с информацией так или иначе оперируют; и для обычных граждан, чьи персональные данные могут быть так или иначе использованы в данной информационной системе. Иными словами, глядя на эти два пункта, можно сказать, что нам с вами нужно оценить каждую угрозу с двух точек зрения: насколько она реальна и насколько она опасна.

Могут быть реальные, но не опасные угрозы. Например, рядовой сотрудник случайно удалит файл в корзину. Очевидно, что он легко сможет его восстановить. Такая угроза хотя и существует, но она кратковременна, быстро устраняется и не приводит к каким-либо серьезным последствиям, и насколько угроза реалистична. Для большинства районов Земного шара существует угроза, например, землетрясения, которое полностью уничтожит объект, но для большинства регионов эта угроза маловероятна, если и вовсе невозможна. Вот именно с этих двух точек зрения каждую угрозу и постараемся рассмотреть.

При построении модели угроз информационной безопасности следует придерживаться следующих принципов, которые предлагаются указанной методикой.

Во-первых, моделирование угроз должно носить систематический характер и осуществляться как на этапе проектирования информационной системы, то есть до ее запуска в эксплуатацию, и периодически в ходе эксплуатации.

Во-вторых, оценка угроз безопасности информации, согласно данной методике, проводится экспертным методом. То есть эксперты, люди квалифицированные в вопросах безопасности информации, угроз различного свойства, на основе специальных таблиц, на основе специальных примерных признаков оценивают уровень вероятности угрозы, уровень ее опасности и по соответствующим таблицам, оценивают настоящую, подлинную актуальность той или иной угрозы относительно конкретной информационной системы.

В модель угроз информационной безопасности, согласно методике, предлагается вставлять следующие разделы:

Первый раздел «Общие положения» указывает, зачем строится данная модель угроз безопасности информации. Указывает, в каких условиях она была построена. Возможно, содержит список привлеченных экспертов. Далее дается описание информационной системы и особенностей ее функционирования. А именно - цель и задачи, которые решает информационная система. Например, многофункциональный центр, который выдает справки, различные документы по запросам посетителей, описание структурно-функциональных характеристик информационной системы, то есть описание оборудования и программных средств, которые в ней применяются; а также описание технологии обработки информации. То есть, описание, какой путь проходит информация с момента обращения клиента, потребителя до получения им некоего результата, из каких баз данных берутся требуемые сведения, как они сопоставляются между собой, обрабатываются, копируются, передаются далее, какие из них готовятся итоговые отчеты, ну и кто ответственен за все эти процедуры.

Далее в структуру модели угроз информационной безопасности включаются возможности нарушителей, то есть, строится модель нарушителя, включающая в себя: типы и виды нарушителей (из той же классификации), возможные цели и потенциал этих нарушителей (тоже из этой методики), возможные способы реализации угроз безопасности информации.

Иными словами, на этом этапе определяется, кто противник и чего от него стоит ожидать. Это делается для того чтобы не предпринимать излишних мер по защите информации, не тратить излишний бюджет на ненужные и невостребованные действия и, наоборот, полностью парировать все ожидаемые угрозы конкретного нарушителя, с тем чтобы обеспечить некий уровень безопасности от его возможных действий.

Далее перечисляются актуальные угрозы безопасности информации, то есть те угрозы, которые в соответствии с методикой прошли оценку на уровень

актуальности, для которых актуальность подтверждена. И, при необходимости, даются различные приложения, в которые, например, могут включаться протоколы работы экспертной комиссии, для того чтобы дальнейшие эксперты могли оценить, насколько обоснованно были приняты те или иные решения.

Первым этапом построения модели угроз информационной безопасности является определение области действия данной модели. Еще до начала моделирования угроз определяются физические и логические границы информационной системы, то есть территориальные границы, в которых находятся компоненты информационной системы, а также зоны ответственности различных подразделений. Т.е - наш отдел / не наш отдел.

Это предполагает, что в одном здании могут помещаться несколько организаций, значит определяются логические границы системы, границы тех сегментов, за которые отвечает то или иное подразделение в тех пределах, в которых оно может менять конфигурацию этих компонент, программных либо аппаратных. А также включаются объекты защиты и сегменты информационной системы, которые могут стать объектом воздействий нарушителя, объектом угроз.

Модель угроз безопасности информации должна охватывать все объекты защиты и сегменты как в логических, так и в физических границах информационной системы, в которых оператором принимаются и контролируются меры защиты информации. Короче говоря, она должна распространяться на всю зону, на которую может влиять тот орган, то подразделение, которое занимается обеспечением вопросов безопасности информации в данной информационной системе.

В модель угроз безопасности информации включаются:

Область применения процесса определения угроз безопасности информации, то есть для каких конкретно процессов, для каких конкретно компонент информационной системы было проведено определение таких угроз.

Область действия модели угроз безопасности информации, то есть в каких границах действует данная модель угроз, что осталось за пределами рассмотрения, возможно; структурно-функциональные характеристики информационной системы и особенности ее функционирования, для того чтобы подтвердить действительно обоснованность тех или иных решений.

3.2 Идентификация угроз безопасности информации и их источников

Чтобы начать построение модели угроз безопасности информации, разберем идентификацию таких угроз и их источников.

Напомним, что рассматривается как угроза информационной безопасности.

В таком качестве рассматривается совокупность 4 объектов: это источник угрозы безопасности информации, это факторы, обуславливающие возможность ее реализации, то есть некие уязвимости информационной

системы, методы реализации угроз безопасности информации и последствия от ее реализации.

В рамках данной методики в первую очередь предполагается рассматривать угрозы, источник которых, во-первых, антропогенный, то есть человек, во-вторых, действующий злоумышленно. Хотя для тех информационных систем, основным назначением которых является предоставление пространства для хранения информации, то есть тех, которые предоставляют услуги распределенных хранилищ, хостинга для Интернет-сайтов, просто каких-то хранилищ, необязательно распределенных и по облачным технологиям, является рассмотрение угроз нарушения целостности и доступности. При этом источником таких угроз зачастую являются некие техногенные факторы или стихийные явления. Такие угрозы ни в коем случае нельзя сбрасывать со счетов, их тоже следует рассматривать и оценивать на актуальность, но это предлагается делать в первую очередь по иным методикам, какими-то экспертными методами.

Данные методики в первую очередь направлены на идентификацию угроз, источник которых антропогенный.

Итак, логическая цепочка угроз и их проявлений.

1. У нас есть источник.

Этот источник главным образом — некий человек, действующий злоумышленно, эксплуатирует некую уязвимость, то есть свойство информационной системы, в результате этой эксплуатации он реализует некое действие, которое, собственно, и является угрозой. Действие приводит к некоему последствию, главным образом, к несанкционированному доступу к информации, содержащейся и обрабатываемой в информационной системе.

Источники - это субъекты либо явления, мы в первую очередь говорим о субъектах, а типы таких источников — антропогенные, то есть люди. Техногенные, это некие сущности, некие программы, то есть не люди, это некие объекты. Стихийные источники угроз, то есть это некие стихийные бедствия, такие как пожары, наводнения, перебои с электропитанием, вызванные не столько неисправностью этого оборудования, сколько, например, падением дерева на линию электропередач. Это стихийный источник угроз, тем не менее, нарушающий доступность информации и поэтому рассматриваемый нами как источник конкретной угрозы.

Антропогенными источниками угроз являются лица, очевидным образом осуществляющие преднамеренные действия с целью либо доступа к информации, то есть нарушения ее конфиденциальности, либо воздействия на информацию, то есть с целью нарушения ее возможной целостности, либо с целью нарушения функционирования информационной системы или обслуживающей ее инфраструктуры, то есть с целью нарушения доступности информации. Кроме того, лица, имеющие доступ к информационной системе, непреднамеренные действие которых могут привести к нарушению безопасности информации, то есть персонал, действующий просто халатно или

не слишком квалифицированно. Он действует не злоумышленно, не является преступником, но может своей низкой квалификацией также нанести ущерб.

Техногенные угрозы, как правило, связаны с отказами или сбоями в работе различного оборудования, аппаратного либо программного обеспечения. Такие угрозы возникают чаще всего по таким причинам, как низкое качество либо низкая надежность технических, программных или программно-технических средств, низкое качество либо низкая надежность сетей связи или услуг связи либо по причине отсутствия или низкой эффективности систем резервирования или дублирование программно-технических и технических средств. По причине отсутствия механизма, который бы позволял заменять вышедшие из строя или некорректно работающие компоненты информационной системы.

Другими причинами являются низкое качество систем кондиционирования, электроснабжения, охранных систем и так далее различных инженерных систем. Просто информационные системы или отдельные ее компоненты могут выйти из строя, если, например, система кондиционирования перестанет работать, если прекратится ее электроснабжение.

Ну а в случае, если охранные системы будут работать некорректно, то, с одной стороны, это может привести к проникновению нарушителя на территорию объекта информатизации и физическому повреждению различных компонентов информационной системы, либо, охранные системы, например, система пожаротушения, могут сами спровоцировать нанесение ущерба различным отдельным компонентам информационной системы.[4, с. 96. 18]

Низкое качество обслуживания со стороны обслуживающих организацию лиц также может рассматриваться как причина техногенной угрозы. Действуя неквалифицированно, те или иные лица могут нанести ущерб надежности и качеству работы различных систем, обеспечивающих функционирование информационной системы.

В свою очередь, для того чтобы определить угрозы в информационной системе, определяются следующие параметры:

1. Возможности, то есть тип, вид и потенциал различных нарушителей, необходимый им, то есть нарушителям, для реализации угроз безопасности информации, а также уязвимости, которые могут использоваться при реализации угроз безопасности информации, включая специально внедренные программные закладки. То есть, здесь есть ответ на вопрос - кто и при помощи каких уязвимостей мог бы реализовать те или иные угрозы?. Таким образом можно прогнозировать угрозы.

2. Определяются наряду с другими параметрами способы реализации угроз

безопасности информации. Это позволяет выбрать конкретный адекватный метод противодействия, объекты информационной системы, на которые направлены угрозы безопасности информации, то есть объекты воздействия, так же выделяются и определяются на этом этапе.

3. Результаты последствия от реализации угроз безопасности информации в дальнейшем позволяют определить, насколько та или иная угроза является актуальной. Иными словами, здесь происходит некий сбор первоначальной информации, на основе которой в дальнейшем будет проводиться оценка актуальности угроз.

Каждая угроза безопасности информации описывается в результате следующим образом, неким вектором, содержащим следующие компоненты:

1. Нарушитель, или источник угрозы, то есть тип, если мы говорим об антропогенном нарушителе, и вид этого нарушителя.

2. Уязвимости, которые тот или иной нарушитель по нашему прогнозу будет эксплуатировать, способы реализации угрозы, далее объекты воздействия, на которые его действия будут направлены, и последствия от реализации этой угрозы.

Таким образом, каждая угроза записывается в виде УБИ (Угроза безопасности информации, с неким индексом j), то есть порядковым номером: угроза безопасности информации первая, вторая, и так далее, сколько их напрогнозируют эксперты на данном этапе.

3.3 Модель нарушителя

Для определения первого компонента в векторе требуется детальное изучение нарушителя, который, возможно, будет источником той или иной угрозы, то есть, по сути, построение так называемой модели нарушителя.

Целью оценки возможности нарушителя по реализации угроз безопасности информации является формирование предположения о следующих его параметрах: типах нарушителя согласно классификации, его видах, его потенциале, его целях и его возможных способах реализации угроз безопасности информации. Несмотря на то, что в вектор, описывающий ту или иную угрозу, вносится информация, только о виде нарушителя и, возможно, о типе, если есть два разных нарушителя, различающиеся по типу, но одинаковые по виду.

Полная модель нарушителей включается в модель угроз безопасности информации как составная часть. То есть, для построения модели, все пять параметров требуется определить. Несмотря на то, что используются в описании угроз первые два, целиком вся эта модель включается, и она в дальнейшем позволяет выбрать наиболее адекватные методы и средства противодействия конкретным нарушителям, действующим по конкретному, условно говоря, сценарию, воздействующим на конкретные цели и конкретными способами с конкретными целями.

Нарушители бывают внешние и внутренние.

Внешние нарушители — лица, не имеющие права доступа к информационной системе, то есть это лица, находящиеся за границами информационной системы. По сути — все, кто не обладают какими-то правами на территории объекта информатизации и не являются ее сотрудниками.

Внутренние нарушители, или нарушители второго типа — это лица, имеющие право постоянного или разового доступа к информационной системе либо ее отдельным компонентам. Еще раз обратим внимание на фразу «или разового доступа» — то есть различные специалисты, приглашенные единожды для установки, пуска, наладки тех или иных компонент информационной системы, рассматриваются как нарушители именно внутренние, такого типа.

Внешние нарушители - это спецслужбы либо разведки иностранных государств, различные преступные группировки. Отдельно выделяются террористические и экстремистские группировки как наиболее замотивированные, наиболее действующие агрессивно, наиболее финансово, технологически вооруженные в различных областях. Они выделяются из числа просто преступных групп, основным целями которых — именно преступных групп — является чаще всего личное обогащение тем или иным путем.

Далее: внешние субъекты как просто любые лица, находящиеся за пределами системы конкурирующей организации, как целенаправленно действующий нарушитель, стремящийся к получению конкурентных преимуществ: разработчики, производители, поставщики программно-технических средств, которые могут действовать как целенаправленно, то есть злонамеренно, так и просто халатно.

Внутренние нарушители - лица, привлекаемый для установки, наладки, монтажа, пусконаладочных и иных видов работ, которые также могут быть и злоумышленными и просто низкоквалифицированными. Лица, обеспечивающие функционирование информационных систем или обслуживающую инфраструктуру оператора — это постоянно находящийся на территории объекта информатизации персонал, который тоже может действовать как злоумышленно, так и халатно. Пользователи информационной системы — это самый обобщенный вид внутреннего нарушителя. Администраторы информационной системы и администраторы безопасности — наиболее привилегированные пользователи, обладающие наибольшим потенциалом из именно всех пользователей информационной системы. А также бывшие работники, которые могут сводить счеты с бывшим работодателем.

В зависимости от потенциала, которым обладают нарушители, они распределяются по трем уровням: это нарушители, обладающие базовым, либо низким, потенциалом, нарушители, обладающие базовым повышенным, другими словами, средним потенциалом нападения, и нарушители, обладающие высоким потенциалом нападения.[4, с.99]

Целями, или мотивациями, реализации ими угроз безопасности информации в информационной системе, как вы, возможно, помните, могут быть: нанесение ущерба государству либо отдельным его сферам деятельности или секторам экономики, реализация угроз безопасности по идеологическим или политическим мотивами, организация теракта, причинение имущественного ущерба путем мошенничества или иным преступным путем, дискредитация или дестабилизация деятельности органов государственной власти либо организации, получение конкурентных преимуществ, внедрение

дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки, любопытство или желание самореализации, выявление уязвимостей с целью их дальнейшей продажи и получение финансовой выгоды. А также реализация угроз безопасности информации из мести, реализация угроз безопасности информации непреднамеренно, из-за неосторожности или неквалифицированных действий.

Еще раз просто их перечислим, поскольку нам потребуется выбирать из этого перечня, какой же конкретной целью или мотивацией руководствуется наш конкретный нарушитель, которого мы моделируем.

Кроме того, нарушитель, которого мы пытаемся смоделировать, реализует свои угрозы безопасности информации за счет тех или иных действий, которые тоже нам требуется определить. Здесь не обязательно выбрать одно конкретное возможное действие, которое может использовать нарушитель — он может использовать несколько различных сценариев действий. Наша задача — определить круг предполагаемых действий нарушителя, т.е. всего, чего от него можно ожидать. Значит, это может быть несанкционированный доступ или воздействие на объекты на различных уровнях: на аппаратном, на общесистемном, на прикладном, на сетевом.

Это, как правило, зависит от того, является ли нарушитель внутренним либо внешним, какие у него есть полномочия в информационной системе, что ему позволено делать и как он делает: маскируется ли он от других пользователей либо действует в рамках своих штатных полномочий. Кроме того, нарушитель может использовать несанкционированный физический доступ или воздействие на различные компоненты автоматизированной системы, либо он может воздействовать на пользователей, администраторов безопасности информации данной системы, то есть применять так называемую социальную инженерию.

Наша задача здесь — определить, чего мы от него ждем, является ли он социальным инженером, является ли он вандалом, как он воздействует на ту или иную систему, может ли он подключать к ней новые устройства, запускать программы, штатные или разработанные им самим. Это требуется для того, чтобы в дальнейшем понимать, что достаточно, для того чтобы парировать его усилия, либо что достаточно для того, чтобы заставить его отказаться от своих намерений, с какими он должен столкнуться препятствиями.

В дальнейшем мы более подробно рассмотрим категории методов и средств обеспечения безопасности информации, поговорим о том, как выбирать их адекватный состав для противодействия конкретным смоделированным и признанным актуальными угрозами, реализуемыми с моделированными же нарушителями.

Рассмотрим два примера смоделированных нарушителей.

Нарушитель первый — это разработчик вредоносного программного обеспечения — тот, кто написал вирусы или вредоносную программу, например

типа «троянский конь», которая похищает некоторую пользовательскую информацию с его рабочей станции.

А второй нарушитель — это действующий халатно пользователь, который по своей низкой квалификации данное вредоносное программное обеспечение скачал.

Тип первого нарушителя — внешний, а тип второго — внутренний.

Далее определяем вид.

Вид нарушителя первого кратко сформулирован как разработчика программного обеспечения, а второго нарушителя — пользователь информационной системы.

Далее определим потенциал наших нарушителей.

Потенциал первого нарушителя — базовый повышенный, то есть средний. Данный нарушитель является специалистом в области разработки программного обеспечения, он обладает одним из признаков базового повышенного потенциала.

А нарушитель второй у нас имеет базовый низкий потенциал — это просто пользователь с минимальными полномочиями в системе. Но тем не менее он может запускать какие-то сторонние программные средства кроме штатных.

Далее рассмотрим цели и мотивацию данных нарушителей.

Нарушитель первый направлен на такие цели, как внедрение дополнительных функциональных возможностей в программное обеспечение или в программно-технические средства на этапе разработки. То есть он делает программу вредоносной. Возможно, эта программа распространяется бесплатно, у нее есть некий полезный функционал, например она позволяет пользователю решать какие-то задачи альтернативным способом по отношению к платному программному обеспечению, то есть, допустим, распространяется бесплатный аналог какого-то популярного программного средства, например для записи информации на оптические диски.

И другая его цель — причинение имущественного ущерба путем мошенничества или иным преступным путем. Несанкционированная, недокументированная часть этой программы, которая имеет и полезную часть, должна тем или иным образом по замыслу ее разработчика наносить имущественный ущерб, например похищать данные кредитных карт пользователя, который по своей халатности эту программу скачал и запустил. Второй нарушитель у нас имеет такие цели, как реализация угроз безопасности информации непреднамеренно из-за неосторожности или неквалифицированных действий — он попросту не смог отличить опасную программу от программы доверенной, поэтому угроза безопасности и реализовалась.

Какие возможные способы реализации угроз информационной безопасности у нас эксплуатируют эти два нарушителя?

Первый реализует несанкционированный доступ или воздействие на объекты на прикладном уровне. На самом деле, оба нарушителя действуют на

этом уровне, потому что речь идет о запуске несанкционированного программного обеспечения, то есть того, которое не является штатным. Только первый нарушитель является его разработчиком и через свою программу он получает доступ к информации. Второй нарушитель это программное обеспечение запускает и таким образом реализует воздействие на объекты на прикладном уровне. В данном случае сам он не получает несанкционированного доступа, он воздействует на объект и таким образом, давая возможность первому нарушителю, получить этот самый несанкционированный доступ.

Построив таким образом модели нарушителей, мы можем включить их в описание угроз безопасности информации и таким образом полностью сформировать вектор вот этих отобранных первоначальных угроз безопасности информации, которые, возможно, не совсем фантастичны для данной информационной системы. И далее нам с вами потребуется из них отобрать действительно актуальные.

3.4 Принцип оценки актуальности угроз

Определив, таким образом, перечень возможных угроз, которые мы рассматриваем как возможно актуальные для конкретной информационной системы, и, смоделировав нарушителя, который, возможно, будет источником таких угроз, поговорим теперь о том, как оценить актуальность угрозы, той или иной.

Сначала рассмотрим принцип оценки такой актуальности. Угроза безопасности информации подлежит нейтрализации, то есть блокированию, если она признается актуальной. А актуальность угрозы, как говорилось ранее, означает, что соблюдаются два условия: с одной стороны, в информационной системе существует возможность ее реализации тем или иным нарушителем, а с другой стороны ее реализация приведет к нанесению ущерба, который мы признаем существенным, не можем его игнорировать. То есть угроза должна быть и реальной, и опасной. Поэтому, для того чтобы оценить актуальность каждой конкретной угрозы, угрозы безопасности информации с неким номером j, если она актуальна, следует определить два ее параметра.

$$\text{УБИ}_j{}^{\text{А}} = [(P_j); (X_j)], \qquad (3.1)$$

P_j – вероятность реализации угрозы

X_j – степень ущерба

Во-первых, вероятность реализации угрозы P с тем же номером j, и степень ущерба X с тем же номером j. То есть получается такой двухкомпонентный вектор — угроза безопасности информации, пусть первая, допустим, или некое j с пометкой А — актуальное, она описывается двумя этими параметрами — ее вероятностью и ее степенью ущерба.

$$\text{УБИ}_j{}^{\text{A}} = [(Y_j);(X_j)]\,, \qquad (3.2)$$

Y_j – возможность реализации угрозы,

X_j – степень ущерба.

Соответственно, для того чтобы принять решение о том, является ли та или иная угроза актуальной, требуется как минимум оценить или вычислить эти два ее параметра. А в некоторых случаях оценить вероятность угрозы не представляется возможным, поскольку угроза может быть новой, ранее не описанной, либо в той ситуации, когда информационная система только запускается и нет сведений о том, насколько часто в ней такие угрозы будут реализовываться.

Поэтому в качестве альтернативного первого параметра, наряду со степенью ущерба, который наносит та или иная угроза в случае ее реализации, может рассматриваться возможность ее реализации. Соответственно, для того чтобы принять решение о том, актуальна ли угроза, следует оценить либо возможность ее реализации, либо ее вероятность реализации и, в качестве второго компонента, степень ущерба, ей наносимого.

Рассмотрим оценку вероятности реализации угрозы - это вероятность характеризует то, насколько вероятна реализация данной угрозы в рассматриваемой информационной системе.

Вводится три словесных градации: вероятность низкая, вероятность средняя и вероятность реализации угрозы высокая. Данная градация определяется экспертным образом на основе следующих приблизительных параметров.

Угроза признается низковероятной, или вероятность ее реализации признается низкой, если ситуация с ней описывается в основном следующими утверждениями.

Во-первых, нет объективных предпосылок реализации данной угрозы либо нет требуемой статистики по фактам реализации данной угрозы, либо отсутствует мотивация для ее реализации, либо, если есть достаточная статистика, возможная частота реализации данной угрозы — реже, чем один раз в пять лет.

Вероятность реализации угрозы признается средней, если ее вероятность описывается следующими, подобными предыдущим, им соответствующим, следующими утверждениями.

Существуют предпосылки к реализации данной угрозы, случаи реализации данной угрозы зафиксированы, есть признаки наличия у нарушителя мотивации для реализации данной угрозы, то есть мы можем представить, зачем это нарушителю надо, это не бессмысленное действие, которое просто в принципе возможно, и возможная частота реализации угрозы, если такая статистика есть, реже одного раза в год, но при этом чаще, чем раз в пять лет.

Например, возможные стихийные бедствия, очевидно, по этому параметру будут характеризоваться низкой вероятностью, такие как землетрясения, наводнения, какие-то взрывы, террористические атаки.

А некоторые другие угрозы, возможно, случаются раз в несколько лет, например, пожары. Такую угрозу можно признать угрозой со средней вероятностью реализации.

И, наконец, вероятность реализации угрозы признается высокой, если данная вероятность может быть описана следующими утверждениями.

Существуют объективные предпосылки к реализации данной угрозы, то есть все возможности, есть соответствующие уязвимости, о которых мы знаем, которые могли бы привести к реализации данной угрозы, есть достоверная статистика реализации данной угрозы, у нарушителя есть мотивы для ее реализации, и возможная частота реализации угрозы — чаще одного раза в год.

Соответственно, на основе этих утверждений эксперты выражают свое мнение, согласованно или коллегиально, или различным образом обрабатываемое, на основе которого экспертная комиссия принимает решение о том, какая вероятность угрозы приписывается соответствующей угрозе.

В ситуации, когда оценить вероятность угрозы по той или иной причине не представляется возможным, оценивается вместо вероятности возможность реализации угрозы Y с номером j. Соответственно, данный показатель рассматривается тоже как двухкомпонентный вектор.

Здесь два фактора имеют влияние. Это уровень защищенности информационной системы и потенциал нарушителя. По сути, происходит как бы сравнение брони и снаряда, что сильнее — толщина брони или мощность снаряда, который должен ее пробить.

Если считается, что нарушитель способен преодолеть такой уровень защищенности информационной системы, то угроза признается актуальной.

Не актуальной, а соответствующий уровень ее возможности реализации устанавливается экспертным способом. Рассмотрим это подробнее.

Если у нас информационная система только лишь вводится в эксплуатацию, очевидно, оценить ее уровень в процессе эксплуатации, то есть в процессе ее существования, ее функционирования также не представляется возможным.

Вместо нее рассматривается такой параметр, как уровень проектной защищенности.

$$Y_j = [(Y_{1П}); (Y_2)], \quad (3.3)$$

$Y_{1П}$ – уровень проектной защищенности,

Y_2 – потенциал нарушителя.

Уровень проектной защищенности также сравнивается с потенциалом нарушителя для того, чтобы определить, в состоянии ли конкретный нарушитель его преодолеть. На основе вычисленных данных параметров,

каждый из которых вычисляется по определенной методике, о которой мы поговорим далее, принимается окончательное решение о том, является ли та или иная угроза актуальной. И, наряду с ранее смоделированными нарушителями, включается в итоговый документ, носящий название модель безопасности информации конкретной информационной системы.

3.5 Оценка возможности реализации угрозы

Для того чтобы отследить в дальнейшем актуальность той или иной угрозы, рассмотрим методику определения возможностей реализации той или иной угрозы. Для этого сначала определим проектную защищенность информационной системы.

В случае если у нас информационная системе только готовится к запуску в эксплуатации в качестве первого параметра, мы рассматриваем проектную защищенность. Проектная защищенность оценивается на основе основных характеристик информационной системы, то есть требуется провести анализ информационной системы, определить, какие технологии применены при ее разработке, какие технологии она включает.

И на основе этой таблицы, которую мы сейчас рассмотрим, определить уровень проектной защищенности. По сути говоря, эта оценка может производиться по проекту, поэтому она и оценка проектной защищенности. Оценивается она следующим образом: в методике приводится таблица, имеющая следующую структуру.

В ней рассматриваются различные структурно-функциональные характеристики информационной системы и условия ее эксплуатации. А далее наличие либо отсутствие каждого из этих пунктов вносит некий плюс в один из трех уровней проектной защищенности: высокий, средний либо низкий.

Например, первый блок таблицы посвящен структуре информационной системы - автономное автоматизированное рабочее место, то есть рабочее место пользователя, не имеющее подключение к глобальной сети Интернет и к любым информационным сетям, в том числе к локальной информационной системе. То есть просто отдельно взятой рабочее место — это плюс в высокий уровень в проектной защищенности.

Если рабочие места пользователей подключены к локальной информационной системе, это плюс в средний уровень. И распределенные информационные системы — это плюс в уровень низкий проектной защищенности. Аналогичным образом рассматриваются используемые информационные технологии.

Здесь работает принцип, что чем больше различных технологий предполагаются в рамках в проекте данной информационной системы, тем ниже ее уровень проектной защищенности. Такие системы как: системы на основе виртуализации, системы, реализующие облачные вычисления, системы с мобильными устройствами понижают уровень проектной защищенности.

Здесь действует принцип: чем сложнее, тем больше различных уязвимостей порождается. И, наоборот: чем проще система, тем она более надежда — в ней меньше различных ходов, которые может использовать злоумышленник для реализации своих угроз. Далее рассматриваются используемые информационные технологии: системы с беспроводным доступом, грид-системы — вносят свои вклады в низкий уровень проектной защищенности, а суперкомпьютерные системы — в средний.[1, с. 28]

По архитектуре информационной системы: системы на основе тонкого клиента вносят вклад в высокий уровень проектной защищенности, системы на основе одноранговой сети — в средний, а файл-серверные системы и центры обработки данных снижают уровень проектной защищенности, так сказать, внося свою лепту в низкий уровень проектной защищенности.

По архитектуре информационной системы предпочтительнее использование разных типов операционных систем гетерогенной среды — это вклад в средний уровень проектной защищенности по сравнению с системами с удаленным доступом пользователей. Это низкий уровень проектной защищенности. А отсутствие и той, и другой специальных архитектур информационной системы, соответственно, не снижает уровня защищенности информационной системы.

Использование прикладных программ, независимых от операционных систем, либо выделенных каналов связи вносит вклад в средний уровень проектной защищенности. По наличию и отсутствию взаимосвязей с иными информационными системами рассматривается взаимодействие либо невзаимодействие системы с другими информационными системами. И на основе этого делают соответствующие вклады в различные уровни проектной защищенности.

По наличию либо отсутствию взаимосвязей к сетям связи общего пользования также рассматриваются три различных варианта, каждый из которых соответствует тому или иному уровню проектной защищенности.

Далее рассматривается размещение технических средств, предполагается три различных варианта их размещения, каждый из которых соответствует высокому, среднему либо низкому уровню проектной защищенности. Здесь, как правило, прослеживается такая тенденция, что чем удобнее для пользователя, чем более гибкая, чем более многообразная получается система, тем ниже ее уровень проектной защищенности.

И, наоборот: система максимально контролируемая, максимально однообразная, максимально изолированная от других систем обладает более высоким уровнем проектной защищенности. По режимам обработки информации в информационной системе однопользовательский режим является более предпочтительным и соответствует высокому уровню защищенности, а многопользовательский — наоборот, низкому.[1. с. 41]

По режиму разграничения прав доступа разграничение прав доступа, разумеется, более желательно, чем отсутствие такого разграничения, но в

любом случае даже с разграничением это плюс в средний уровень проектной защищенности.

И, наконец, по режимам разделения функции по управлению информационной системы действует точно такой же принцип: выделение рабочих мест для администрирования повышает уровень проектной защищенности с низкого до среднего. По режимам разделения функции по управлению информационной системой использование различных сетевых адресов и использование выделенных каналов для администрирования считаются средним уровнем проектной защищенности и вносят свой вклад. По подходам к сегментированию информационной системы вариант с сегментированием более предпочтителен — повышает уровень с низкого до среднего.

После того как все эти вычисления проведены, после того как подсчитаны количество плюсов в каждой из таблиц, подсчитывается общее количество набранный плюсов по данной таблице.

На основе того, как они распределились и сколько их всего, экспертно принимается решение о том, какой уровень проектной защищенности имеет та или иная информационная система.

Высокий уровень соответствует тому, что не менее 80 % набранных плюсов, набранных отметок соответствует уровню «высокий», а остальные — уровню «средний».

Если данные требования не выполнены, но при этом не менее 90 % характеристик соответствуют уровню ниже, чем средний, система признается имеющей средний уровень проектной защищенности. И в другом случае, во всех других случаях данная система признается имеющей низкий уровень проектной защищенности. В ситуации, когда система уже функционирует, вместо уровня проектной защищенности оценивается, собственно, уровень защищенности информационной системы.

Если по сравнению с уровнем проектной защищенности с моментом запуска информационной системы в эксплуатацию, новых угроз не появляется или их можно нейтрализовать буквально за минуты, считается, что система имеет высокий уровень защищенности. Если новые угрозы появляются, а их можно нейтрализовать оперативно — за часы, — такая система считается имеющей средний уровень защищенности.

И, наконец, низкий уровень защищенности соответствует тому, что новые угрозы появились и нельзя нейтрализовать в пределах часов — на это требуется больше времени.

После того как определены уровни проекта или просто эксплуатационной защищенности информационной системы, их можно сопоставить с уровнем потенциала нарушителя, который, соответственно, берется из ранее построенной модели нарушителя.

После этого по приведенной таблице следует найти пересечение потенциала нарушителя и уровня защищенности, либо проектной защищенности, и определить по этой таблице уровень возможности реализации

той или иной угрозы. Здесь угроза признается низко возможной либо, условно говоря, невозможной, если нарушитель с базовым или низким потенциалом пытается преодолеть высокий уровень проектной или эксплуатационной защищенности.

Если нарушитель с базовым повышенным либо средним потенциалом противостоит системе с высоким потенциалом, либо нарушитель с низким потенциалом противостоит системе со средним уровнем защищенности, то есть если уровень защищенности на одну ступеньку выше уровня нарушителя, то возможность реализации угроз средняя.

Нарушителю придется серьезно постараться, для того чтобы эту защиту преодолеть. Во всех остальных случаях, то есть когда уровень нарушителя, классифицированный как тоже низкий, средний и высокий, сопоставим либо превышает уровень защищенности — высокий, средний или низкий, — то такая угроза считается угрозой с возможностью реализации высокой.

Получив данный показатель, мы можем далее переходить к сопоставлению данного параметра со степенью ущерба, наносимого угрозой. То есть на данном этапе мы определили, какова возможность реализации угрозы: высокая, средняя либо низкая. А далее определяем ущерб наносимой угрозы, с тем чтобы далее сделать вывод о ее актуальности.

3.6. Оценка степени ущерба

Оценив уровень вероятности угрозы либо уровень возможности реализации угрозы, перейдём к оценке степени ущерба, наносимого той или иной угрозой безопасности информации.

Для того чтобы оценить степень ущерба, мы определим воздействие на каждое из свойств безопасности информации (целостность, доступность или конфиденциальность) тоже на основе таблицы, приводимой в соответствующей методике. Для каждого из свойства (конфиденциальность, целостность и доступность) прежде всего следует определить, оказывает ли та или иная угроза воздействие на соответствующий аспект безопасности информации.

Здесь надо отдельно обратить внимание, что согласно данной методике, если в информационной системе рассматривается несколько категорий информации, которую требуется защищать, например, персональные данные и коммерческая тайна, то для каждой из таких категорий информации воздействие той или иной угрозы должно рассматриваться отдельно.

Отдельно стоит упомянуть, что данная методика не предполагает, что она будет применяться для систем, в которых обрабатывается информация, составляющая государственную тайну.

Итак, для свойства конфиденциальности угроза считается не оказывающей воздействие, если в результате её реализации отсутствует возможность несанкционированного доступа, копирования, предоставления или распространения такой информации. И считается, что угроза оказывает воздействие на конфиденциальность, если подобная возможность существует,

если в результате воздействия угрозы возможен несанкционированный доступ, копирование, предоставление или распространение информации. Для такого свойства как целостность тоже следует произвести оценку для каждого вида информации, который обрабатывается в информационной системе.

Если в результате реализации угрозы возможность уничтожения или модифицирования информации не предоставляется возможной, то считается, что данная угроза не оказывает воздействия. Но, в противном случае, считается, что эта угроза воздействие на информацию оказывает. Наконец, для свойства доступности угроза считается не оказывающей воздействие на доступность информации, если в результате её реализации, то есть угрозы, возможность уничтожения или модификации информации отсутствует. В противном случае считается, что угроза воздействие на доступность информации оказывает.

Определив, таким образом, для каждого из свойств безопасности информации, оказывает либо не оказывает воздействие данная угроза на эти свойства, мы оценим степень ущерба. Для тех угроз, которые оказывают воздействие на какое-либо из этих свойств, оценка степени ущерба определяется экспертным методом по следующей таблице. Здесь требуется также определить степень ущерба для каждого из отдельных видов информации, которая обрабатывается в системе.

Угроза признаётся наносящей высокий ущерб, если в результате нарушения какого-либо из свойств безопасности информации могут наступить существенные негативные последствия либо если информационная система не сможет выполнять свои функции полностью.

То есть одно из двух: либо существенные негативные последствия, которые могут иметь разный характер, оцениваются экспертно, часть из приведена в названной методике, методики оценки актуальных угроз безопасности информации. С ними можно ознакомиться. Либо могут быть добавлены какие-то новые последствия экспертным способом, то есть, по мнению экспертов, возможно, исходя из специфики информационной системы. Главное, что угроза считается наносящей высокий ущерб, либо если наступает существенные негативные последствия, либо если система полностью выводится из строя, то есть не может свои функции выполнять.

Степень ущерба, наносимого угрозой, признаётся средней, если в результате реализации угрозы возможны умеренные негативные последствия либо информационная система не может выполнять хотя бы одну из её основных функций. То есть в целом она функционирует, но какую-то, хотя бы одну из функций, полностью не может выполнять. Например, невозможно получать доступ к базам данных, невозможно формировать отчёты, которые требуют доступ к этой базе данных. Все остальные можно, можно локально какие-то отчёты делать, а вот какой-то один вид отчётов получать не удаётся, потому что узел с базой данных, компьютер, на котором она запущена, выведен из строя. Это средняя степень ущерба.

И, наконец, степень ущерба признаётся низкой, если возможные негативные последствия признаются незначительными либо если

информационная система по-прежнему может выполнять свои функции, либо с недостаточной эффективностью, либо с привлечением дополнительных сил и сред. Если совсем не требуется никакие силы привлекать либо если сложность функции не увеличивается, считается, что ущерб вовсе не наносится. А низкая степень соответствует тому, что продолжать выполнять свои функции информационная система может, хотя и с затруднениями.

После того, как оценена степень ущерба данной конкретной угрозы для всех видов информации, обрабатываемой в информационной системе и для всех свойств безопасности информации (конфиденциальности, целостности и доступности).

Для того чтобы получить итоговое значение данного ущерба, следует взять максимум по всем видам информации и по всем аспектам информационной безопасности (конфиденциальности, целостности и доступности). Это-то максимальное значение и будет использоваться в дальнейшем для оценки актуальности угрозы.

Теперь, когда мы с вами вычислили и уровень возможности реализации угрозы либо уровень вероятности реализации угрозы, с одной стороны, и с другой стороны, степень ущерба, которую наносит та или иная угроза, всё готово для того, чтобы сделать окончательный вывод о том, является ли та или иная угроза актуальной, и мы это сделаем в следующей части лекции.

3.7 Оценка актуальности угрозы

Вычислив все необходимые параметры, характеризующие ту или иную угрозу безопасности информации, мы можем уже переходить к окончательной оценке ее актуальности.

Актуальные угрозы безопасности информации далее будут включены в модель угроз безопасности информации и именно о них мы в дальнейшем будем говорить, выбирая те или иные методы и средства защиты информации, методы и средства противодействия конкретным угрозам.

Используя вычисленные значения возможностей реализации угрозы Yj и степени наносимого ей ущерба Xj, можно по данной таблице определить уровень актуальности угрозы.

Уровень актуальности угрозы имеет две градации — либо угроза может признаваться неактуальной, либо актуальной.

Угрозы, которые имеют низкий уровень либо актуальности, либо наносимого ущерба, признаются неактуальными. Угрозы, для которых оба данных параметра средние, считаются актуальными. И угрозы, для которых хотя бы один из параметров считается высоким, признаются актуальными. В ситуации, когда один из параметров имеет значение низкой степени, а другой — средней степени, такая угроза считается неактуальной. Иными словами, угроза признается актуальной, если хотя бы один из ее параметров имеет значение высокой степени, либо если оба параметра имеют значение средней степени. Все прочие угрозы признаются неактуальными.

Актуальные угрозы безопасности информации, как было сказано, включаются в модель угроз безопасности информации, а кроме того, определение угроз безопасности информации и оценка их адекватности и актуальности производится регулярно и систематически. Согласно указанной методике, переоценку угроз безопасности информации рекомендуется производить не реже, чем ежегодно, а также в следующих особых случаях. Как правило, эти случаи связаны с тем, что кардинальным образом меняется ситуация, касающаяся информационной системы.

Она может кардинально меняться по таким причинам, как, например, изменение законодательства в области информационной безопасности, то есть появились новые, например:

- категории информации, которые требуется защищать, а значит, появились новые виды угроз;
- изменилась конфигурация информационной системы, то есть появились новые угрозы ее безопасности; выявлены новые уязвимости, то есть снова могут появиться новые угрозы, которые ранее не были рассмотрены или ранее считались неактуальными;
- также появились сведения о новых возможностях нарушителей.

То есть, возможно, круг смоделированных нарушителей расширится, либо, повысится уровень их потенциала. Регулярный пересмотр и переоценка актуальности угроз приводит к тому, что информационная система постоянно поддерживается на адекватном уровне защищенности, достигается ее эффективная работа и эффективное противодействие угрозам безопасности информации.

Таким образом, основная задача модели угроз безопасности информации, заключается в том, чтобы максимально сфокусировать усилия служб, обеспечивающих безопасность информации, только лишь на актуальных угрозах и на конкретных нарушителях, не распыляясь на весь возможный круг угроз и нарушителей.

Учебные вопросы:

1. Укажите цель построения угроз информационной безопасности ИС:
2. Сопоставьте принципы построения модели угроз информационной безопасности на основе методики ФСТЭК:
3. Что содержит модель нарушителя?
4. Что включает в себя первый этап построения угроз информационной безопасности?
5. Укажите все вопросы, установление ответов на которые относится к целям определения угроз, согласно «Методике определения угроз безопасности информации в информационных системах», разработанной ФСТЭК в 2015 г.:
6. Угроза безопасности информации, заключающаяся в удалении информации в базе данных ИС с помощью вредоносной программы с целью причинения ущерба, корректно описывается следующим образом:

7. Укажите все обстоятельства, согласно «Методике определения угроз безопасности информации в информационных системах», разработанной ФСТЭК в 2015 г., способные являться причиной техногенных угроз:

8. Уволенный из организации за халатность системный администратор, желающий в отместку навредить бывшему работодателю и предпринимающий попытку хакерской атаки на информационную систему, согласно «Методике определения угроз безопасности информации в информационных системах», разработанной ФСТЭК В 2015 г., описывается следующей моделью нарушителя (тип; вид; потенциал; цель (мотивация); возможные способы реализации угроз безопасности информации):

9. Посетитель офиса кредитной организации, проявляющий недовольство условиями ранее взятого кредита и стремящийся повредить оставленное без присмотра оборудование информационной системы организации, согласно «Методике определения угроз безопасности информации в информационных системах», разработанной ФСТЭК В 2015 г., описывается следующей моделью нарушителя (тип; вид; потенциал; цель (мотивация); возможные способы реализации угроз безопасности информации):

10. Среди угроз безопасности информации некоторой информационной системы среднюю вероятность реализации, согласно «Методике определения угроз безопасности информации в информационных системах», разработанной ФСТЭК в 2015 г., имеет угроза…

11. Актуальность угрозы, согласно «Методике определения угроз безопасности информации в информационных системах», разработанной ФСТЭК в 2015 г., означает, что…

12. Выберите утверждение, описывающее высокий уровень вероятности угрозы, согласно «Методике определения угроз безопасности информации в информационных системах», разработанной ФСТЭК в 2015 г.:

13. Угроза безопасности информации, согласно «Методике определения угроз безопасности информации в информационных системах», разработанной ФСТЭК в 2015 г., имеет средний уровень ущерба, если в результате ее реализации…

14. Угроза безопасности информации признается неактуальной, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК в 2015 г., в случае, если…

Список литературы

1. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие/Глинская Е.В., Чичварин Н.В. - Москва : НИЦ ИНФРА-М, 2016. - 118 с. (Высшее образование: Бакалавриат) ISBN 978-5-16-010961-9. - Текст : электронный. - URL: https://znanium.com/read?id=211506 (дата обращения: 23.04.2021). – Режим доступа: по подписке.

2. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения (Protection of information. Basic terms and definitions) [Электронный ресурс] URL: https://docs.cntd.ru/document/1200058320 (дата обращения: 27.10.2021).

3. ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» [Электронный ресурс] URL: https://docs.cntd.ru/document/1200075565 (дата обращения: 27.10.2021).

4. Гришина, Н. В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд., доп. - Москва : Форум: НИЦ ИНФРА-М, 2015. - 240 с.: ил.; . - (Высшее образование: Бакалавриат). ISBN 978-5-00091-007-8. - Текст : электронный. - URL: https://znanium.com/read?id=277236 (дата обращения: 23.04.2021). – Режим доступа: по подписке]

5. Конвенция о защите прав человека и основных свобод [Электронный ресурс] URL: https://ru.wikipedia.org/wiki/Конвенция_о_защите_прав_человека_и_основных_свобод#Статья_10_—_Свобода_выражения_мнения (дата обращения: 27.10.2021).

6. Конституция Российской Федерации ст.29 свобод [Электронный ресурс] URL: http://base.garant.ru/10103000/7a69fb6632f5876efd3160114758a106/ (дата обращения: 27.10.2021).

7. Методический документ. Методика оценки угроз безопасности информации. ФСТЭК России, 5.02.2021 года. [Электронный ресурс] URL: https://docs.cntd.ru/document/607699443 (дата обращения: 27.10.2021).

8. Настрой все / Что такое родительский контроль, его установка или отключение [Электронный ресурс] URL: https://nastroyvse.ru/opersys/android/roditelskij-kontrol-android.html (дата обращения: 27.10.2021).

9. РД Защита от несанкционированного доступа к информации. Термины и определения. [Электронный ресурс] URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3 (дата обращения: 27.10.2021).

10. Тумбинская, М. В. Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184 (дата обращения: 23.04.2020). — Режим доступа: для авториз. пользователей.

11. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2019. — 344 с. — ISBN 978-5-8114-3940-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/reader/book/125739/#1 (дата обращения: 23.04.2021). — Режим доступа: для авториз. пользователей.

12. Указ Президента РФ от 2 июля 2021 г. N 400 "О Стратегии национальной безопасности Российской Федерации" [Электронный ресурс] URL: http://base.garant.ru/401425792/ (дата обращения: 27.10.2021).

13. Указ Президента РФ от 5 декабря 2016 г. N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" [Электронный ресурс] URL:https://base.garant.ru/71556224/ (дата обращения: 27.10.2021).

14. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ [Электронный ресурс] URL: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 27.10.2021).

15. Федеральный закон от 22 октября 2004 г. N 125-ФЗ "Об архивном деле в Российской Федерации" [Электронный ресурс] URL: http://base.garant.ru/12137300/ (дата обращения: 27.10.2021).

16. Федеральный закон от 27.12.1991 N 2124-1 (ред. от 01.07.2021) "О средствах массовой информации" (с изм. и доп., вступ. в силу с 01.08.2021) [Электронный ресурс] URL: http://www.consultant.ru/document/cons_doc_LAW_1511/605ce8e8e7f256b2c7764fb44b68f0403be9631c/ (дата обращения: 27.10.2021).

17. Федеральный закон Семейный кодекс Российской Федерации от 29.12.1995 N 223-ФЗ (ред. от 02.07.2021) [Электронный ресурс] URL: http://www.consultant.ru/document/cons_doc_LAW_8982/2236d37faf59dafdc4b2bc53c6b05841fe616ee9/ (дата обращения: 27.10.2021).

18. «Медвежатник». Фрэнк Оз, 2001, Эпизод фильма [Электронный ресурс] URL: https://www.kinopoisk.ru/film/819/ (дата обращения: 27.10.2021).

19. «Хакеры», Иэн Софтли, 1995, Эпизод из фильма [Электронный ресурс] URL: https://www.kinopoisk.ru/film/4134/ (дата обращения: 27.10.2021).

20. Данные 60 млн кредитных карт Сбербанка утекли в интернет / Русская редакция Deutsche Welle [Электронный ресурс] URL: https://www.dw.com/ru/данные-60-млн-кредитных-карт-сбербанка-утекли-в-интернет/a-50687151 (дата обращения: 27.10.2021).

21. Красноярские школьники вставили в порно фото пожилой учительницы и выложили в Сеть / Вести-RU, 04 октября 2019 [Электронный ресурс] URL: https://www.vesti.ru/doc.html?id=3196081 (дата обращения: 27.10.2021).

22. Пожар в библиотеке ИНИОН РАН / RG.RU 02.02.2015 [Электронный ресурс] URL: https://rg.ru/sujet/5376/ (дата обращения: 27.10.2021).

23. Роскомнадзор затребовал у Сбербанка информацию по утечке данных 60 млн клиентов/ Интерфакс, 3 октября 2019. [Электронный ресурс] URL: https://www.interfax.ru/russia/678973 (дата обращения: 27.10.2021).

Список сокращений

АЗ — акустическая закладка
АК — акустический канал
АЛ — абонентская линия
АМ — амплитудная модуляция
АНБ — Агентство национальной безопасности
АР — акустическая разведка
АРМ — автоматизированное рабочее место
АРУ — автоматическая регулировка усиления
АС — автоматизированная система
АСУ — автоматизированная система управления
АТС — автоматическая телефонная станция
АФУ — антенно-фидерное устройство
АФХ — амплитудно-фазовая характеристика
АЧХ — амплитудно-частотная характеристика
АЭП — акустоэлектрическое преобразование
АЭС — атомная электростанция
БЗ — ближняя зона
ВАК — виброакустический канал
ВИП — вторичный источник питания
ВП — выделенное помещение
ВС — вычислительная система
ВТ — вычислительная техника
ВТСС — вспомогательные технические средства и системы ВЧ — высокая частота (высокочастотный)
ГИП — графический интерфейс пользователя
ГК — Гражданский кодекс
ГОС — государственный образовательный стандарт
ДВ — длинные волны (длинноволновый)
ДФ — деструктивная функция
ЗИ — защита информации
ЗП — защищаемое помещение
ИАО — информационно-аналитический отдел
ИАП — информационно-аналитическое подразделение ИАС — информационно-аналитическая служба
ИБ — информационная безопасность
ИВС — информационно-вычислительная система
ИВЭП — источник вторичного электропитания
ИК — инженерные конструкции
ИЛ — испытательная лаборатория
ИЛС — информационные линии связи
ИСПДн — информационная система персональных данных ИП — источник помех
ИР — информационные ресурсы

ИТ — информационные технологии
ИТР — иностранная техническая разведка
КВ — короткие волны (коротковолновый)
КЗ — контролируемая зона
КоАП — Кодекс административных правонарушений
КПП — контрольно-пропускной пункт
КСЗИ — комплексная система защиты информации КУ — канал утечки
МНИ — машинный носитель информации
НМД — нормативно-методическая документация НПВ — непреднамеренное воздействие
НСВ — несанкционированное воздействие
НСД — несанкционированный доступ
НТД — нормативно-техническая документация
НЧ — низкая частота (низкочастотный)
ОЗИ — организация защиты информации
ОИ — объект информатизации
ПДн — персональные данные
ПДТК — постоянно действующая техническая комиссия ПК — персональный компьютер
ПО — программное обеспечение
ПОС — положительная обратная связь
ППП — преднамеренные программные помехи
ППрП — преднамеренное программное подавление ПЧ — промежуточная частота
РД — руководящий документ
САПР — система автоматизированного проектирования
СБ — система безопасности
СВТ — средства вычислительной техники
СД — секретный документ
СЗИ — система защиты информации
СЗСИ — система защиты секретной информации
СКЗИ — средства криптографической защиты информации
СлР — служебное расследование
СМПП — самовоспроизводящиеся программные помехи
СО — средства охраны
СОЗИ — системы организационной защиты информации
СОИ — система отображения информации
СП — структурное подразделение
ТБИ — требования безопасности информации
ТЗ — техническое задание
ТК — Трудовой кодекс
ТКУ — технический канал утечки
ТКУИ — технический канал утечки информации
ТСОИ — технические средства обработки информации

ТСПИ — технические средства передачи информации

ТСР — технические средства разведки

ТСС — технические средства и система

ТТЗ — тактико-техническое задание

ТУ — технические условия

УЗ — устройство защиты

УК — Уголовный кодекс

УМС — Управление международного сотрудничества

ФАПСИ — Федеральное агентство правительственной связи и информации ФМР — фотометрическая разведка

ФР — фотографическая разведка

ФСБ — Федеральная служба безопасности

ФСТЭК — Федеральная служба по техническому и экспортному контролю ХР — химическая разведка

ЭВМ — электронно-вычислительная машина

ЭВТ — электронно-вычислительная техника

ЭК — экспертная комиссия

ЭМС — электромагнитная совместимость

Заключение

Защита информации - неотъемлемая часть общей проблемы информационной безопасности, роль и значение которой во всех сферах жизни и деятельности общества и государства на современном этапе неуклонно возрастает. Любые фундаментальные технические или технологические инновации, дающие возможности для решения одних социальных проблем и открывающие широкие перспективы для их развития, всегда усугубляют другие или порождают новые, ранее неизвестные проблемы, становятся источником новых потенциальных опасностей и опасных технологий для общества. К таким технологиям, помимо транспорта и энергетики, относится информатизация общества.

Незаконное искажение или фальсификация, уничтожение или разглашение определенной части информации, а также дезорганизация процессов ее обработки и передачи в системах управления информацией наносят серьезный материальный и моральный ущерб многим субъектам (государству, юридическим и физическим лицам). участие в процессах автоматизированного информационного взаимодействия.

Острота проблемы обеспечения безопасности субъектов информационных отношений, защиты их законных интересов при использовании информационных и управляющих систем, хранящейся и обрабатываемой в них информации все более возрастает. Этому есть целый ряд объективных причин.

Прежде всего, это расширение области применения компьютерных технологий и повышение уровня доверия к автоматизированным системам управления и обработки информации. На компьютерные системы возлагается самая ответственная работа, от качества которой зависит жизнь и благополучие многих людей. Компьютеры контролируют технологические процессы на предприятиях и атомных станциях, движение самолетов и поездов, проводят финансовые операции, обрабатывают государственную и конфиденциальную информацию.

Изменился и подход к самому понятию «информация». Этот термин все чаще используется для обозначения специального продукта, стоимость которого часто превышает стоимость информационных и телекоммуникационных систем, в которых он существует. В сфере создания и оказания информационных услуг происходит переход к рыночным отношениям, которым присуща конкуренция и промышленный шпионаж.

Проблема защиты компьютерных систем становится еще более серьезной в связи с развитием и распространением компьютерных сетей, географически распределенных систем и систем с удаленным доступом к общим ресурсам.

Доступность компьютерных технологий, и в первую очередь компьютеров и смартфонов, привела к распространению компьютерной грамотности среди населения, доступности многих специализированных инструментов и программных возможностей, что закономерно привело к увеличению количества попыток незаконного вмешательства в работу

государственных и коммерческих автоматизированных систем. Многие из этих попыток оказываются успешными и наносят значительный ущерб всем заинтересованным субъектам информационных отношений.

Отставание в области создания стройной и непротиворечивой системы законодательно-правового регулирования отношений в сфере накопления и использования информации создает условия для возникновения и распространения «компьютерной преступности».

Еще одним весомым аргументом в пользу усиления внимания к вопросам защиты информации является бурное развитие и распространение специализированных программных продуктов. В сочетании с наличием технических устройств, ОС и ПО они способны скрытно существовать в информационно-телекоммуникационных системах и совершать потенциально любые несанкционированные действия.

Особую опасность для таких систем представляют злоумышленники, специалисты-профессионалы в области вычислительной техники и программирования, досконально знающие все достоинства и слабые места вычислительных систем и располагающие подробнейшей документацией и самыми совершенными инструментальными и технологическими средствами для анализа и взлома механизмов защиты.

При выработке подходов к решению проблемы компьютерной, информационной безопасности всегда следует исходить из того, что защита информации и вычислительной системы не является самоцелью. Конечной целью создания системы компьютерной безопасности является защита всех категорий субъектов, прямо или косвенно участвующих в процессах информационного взаимодействия, от нанесения им ощутимого материального, морального или иного ущерба в результате случайных или преднамеренных воздействий на информацию и системы ее обработки и передачи.

Евгений Артурович **Поляков**

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие

Федеральное государственное автономное образовательное учреждение
высшего образования «Нижегородский государственный университет
им. Н.И. Лобачевского»
603950, Нижний Новгород, пр. Гагарина, 23.

Подписано в печать Формат 60x84 1/16.
Бумага офсетная. Печать офсетная. Гарнитура Таймс.
Усл. печ. л.. Уч.-изд. л..
Заказ № __Тираж экз.__

Отпечатано в типографии Нижегородского госуниверситета
им. Н.И. Лобачевского
603600, г. Нижний Новгород, ул. Большая Покровская, 37
Лицензия ПД № 18-0099 от 14.05.01