ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Московский институт новых информационных технологий

М. М. Тараскин, А. В. Царегородцев

ЗАЩИТА ИНФОРМАЦИИ В ОРГАНИЗАЦИЯХ: МЕТОДИКА ИССЛЕДОВАНИЯ УГРОЗ, УЯЗВИМОСТЕЙ И РИСКОВ

Москва
2012

Федеральная служба безопасности Российской Федерации
Московский институт новых информационных технологий

М. М. Тараскин, А. В. Царегородцев

ЗАЩИТА ИНФОРМАЦИИ В ОРГАНИЗАЦИЯХ: МЕТОДИКА ИССЛЕДОВАНИЯ УГРОЗ, УЯЗВИМОСТЕЙ И РИСКОВ

МОНОГРАФИЯ

МОСКВА – 2012

УДК
621.396.6.019.3

Тараскин М. М., Царегородцев А. В.

Защита информации в организациях: методика исследования угроз, уязвимостей и рисков: Монография. – М.: МИНИТ, 2012. –114 с.

Монография посвящена разработке методике исследования угроз, уязвимостей и рисков при защите информации в организациях.

Обоснован математический аппарат научных исследований: аксиоматика алгебры логики, которая как наиболее адекватно описывает процессы мыследеятельности экспертов при построении модели системы защиты информации в организации, так и исключает различного рода эвристики, характерные для языков искусственного интеллекта.

Методика содержит описательную (вербальную) и математическую (формализованную) составляющие.

Разработанная методика формализованного описания угроз, уязвимостей и рисков системы защиты информации и синтеза соотношений между ними позволяет полностью проанализировать и документально оформить требования, связанные с обеспечением безопасности информации в организации, избежать расходов на избыточные меры безопасности, возможные при субъективной оценке рисков, оказать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем, обеспечить проведение работ в сжатые сроки, представить обоснование для выбора мер противодействия, оценить эффективность контрмер, сравнить их различные варианты.

В монографии приведены примеры использования методики для фактических расчетов, обеспечивающих корректную обоснованность решений экспертов при защите информации в организациях.

Для руководителей и специалистов подразделений по защите информации.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ ОСНОВНЫХ СОКРАЩЕНИЙ

БИ	–	безопасность информации
ЗИ	–	защита информации
ИБ	–	информационная безопасность
ИР	–	информационный ресурс
ИС	–	информационная сфера
ТР	–	техническая разведка
НИР	–	научно-исследовательская работа
ОКР	–	опытно-конструкторская работа
СЗИ	–	система защиты информации
РФ	–	Российская Федерация

ПРЕДИСЛОВИЕ

Ни одна сфера жизни цивилизованного государства в настоящее время не может эффективно функционировать без развитой информационной инфраструктуры. Безопасность информации выдвигается на первый план и становится элементом национальной безопасности. Защита информации, несомненно, должна рассматриваться как одна из приоритетных государственных задач.

Происходящие в России преобразования оказывают непосредственное влияние на ее информационную безопасность. Возникают новые факторы, которые нужно учитывать при оценке состояния информационной безопасности и определении ключевых проблем в этой области.

Оценка состояния информационной безопасности и определение ключевых проблем в этой области должны базироваться на анализе источников угроз.

При этом необходимо понимать, что эти угрозы в настоящее время носят не умозрительный характер, а каждой из них соответствуют целенаправленные действия конкретных носителей враждебных намерений (начиная с иностранных разведывательных служб и кончая криминальными группировками). В результате этих действий может быть нанесен серьезный ущерб жизненно важным интересам Российской Федерации в политической, экономической, оборонной и других сферах деятельности государства либо причинен существенный социально-экономический ущерб обществу в целом, различным организациям и отдельным гражданам.

В монографии на основе открытых публикаций приводятся классификация и описание различных угроз, уязвимостей и рисков, традиционно характерных при защите информации в организациях. Особое внимание уделено методике, позволяющей математически как описывать различные угрозы, уязвимости и риски для информации организаций, так и синтезировать соотношения между ними.

Для руководителей и специалистов подразделений по защите информации.

ВВЕДЕНИЕ

Отличительной особенностью современного периода времени в мире является переход от индустриального общества к информационному: информация становится наряду с материальными, энергическими и т.п. жизненно-важным ресурсом.

При этом объектом информационных правоотношений является сама информация в ее многочисленных и многообразных формах, таких, например, как документированная информация: документ, информационные ресурсы, средства обеспечения автоматизированных информационных систем, различные виды конфиденциальной информации.

В информационных правоотношениях основными объектами являются разнообразные информационные ресурсы: печатные издания, газеты, журналы, книги, аудио- и аудиовизуальные материалы, рекламная продукция, компьютерные программы, базы и банки данных, информационные сети и системы, средства связи и т.п. Именно они наиболее часто попадают в поле зрения информационных споров, сделок, договоров.

Под термином «информационные ресурсы» следует понимать отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах) [1].

При этом отдельные документы, отдельные массивы документов, документы и массивы документов в информационных системах могут быть выполнены в бумажном или электронном исполнении.

Информационные ресурсы являются собственностью, находятся в ведении соответствующих организаций, подлежат учету и защите, так как информацию можно использовать не только для услуг, но и превратить ее в наличность, продав кому-нибудь, или уничтожить.

В настоящее время именно через информационные ресурсы реализуется значительная часть угроз национальной безопасности Российской Федерации.

Доктриной информационной безопасности Российской Федерации к внешним источникам угроз информационной безопасности Российской Федерации относятся разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам информационной безопасности Российской Федерации относятся [2]:

- критическое состояние отечественных отраслей промышленности;
- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;
- недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;
- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
- недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;

- недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

В последние годы реализованы некоторые практические меры по укреплению информационной безопасности в Российской Федерации. Начато формирование нормативно-правового обеспечения информационной безопасности – приняты законы “О безопасности” и “О государственной тайне”, развернуты работы по созданию механизмов их реализации, завершена подготовка законопроектов, регламентирующих деятельность в информационной сфере.

Осуществлен ряд мероприятий по совершенствованию информационной безопасности в органах государственной власти и управления, в государственных организациях и на предприятиях. Успешному решению ряда вопросов информационной безопасности способствует создание Государственной системы защиты информации в Российской Федерации от технических разведок и от ее утечки по техническим каналам, а также систем лицензирования деятельности предприятий в области защиты информации и сертификации средств защиты информации.

В последнее время утверждена госпрограмма "Информационное общество (2011-2020 годы)" [3].

Проанализировано состояние отрасли информационных и телекоммуникационных технологий.

Среди основных проблем - низкий уровень компьютерной грамотности населения. Не во всех органах используется система электронного документооборота. Отсутствует необходимая нормативно-правовая база. Кроме того, доля нашей страны на мировом рынке электроники составляет лишь 0,5%. Недостаточно развита базовая инфраструктура информационного общества.

Анализ состояния информационной безопасности в Российской Федерации показывает – в настоящее время ее уровень не отвечает жизненно важным потребностям личности, общества и государства. Сегодняшние условия политического и социально-экономического развития государства и общества вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения определенных ограничений на ее распространение со стороны государства. Отсутствие действенных механизмов регулирования информационных отношений в обществе и государстве приводит ко многим негативным последствиям. Слабое обеспечение органов государственной власти и управления достоверной, своевременной и полной информацией затрудняет принятие обоснованных решений. Недостаточная защищенность государственного информационного ресурса приводит к потере важной политической, экономической и научно-технической информации (в том числе о высокоэффективных технологиях военного и двойного назначения).

Неразвитость информационных отношений в сфере предпринимательства тормозит становление цивилизованного рынка, а отсутствие механизма включения национального информационного ресурса в хозяйственный оборот приводит к серьезным экономическим потерям.

Целями защиты информации в организациях должны являться: предотвращение разглашения, утечки и несанкционированного доступа к охра-

няемым сведениям; предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы [4]; обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации в соответствие с законодательством; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения.

Из перечисленных целей защиты информации можно сделать вывод о том, что достижение требуемого уровня информационной безопасности в организации должно, прежде всего, базироваться на исследовании источников угроз для информации, уязвимостей в ее защите, и, проистекающих из их соотношений, рисков.

В книге основной акцент сделан как на классификации угроз для информации в организации, уязвимостей в защите информации и, как следствие, возникающих при этом рисков, так и на методике, позволяющей в формализованном виде их описывать и синтезировать соотношения между ними на основе применения аксиоматики алгебры логики.

Глава 1. НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ РОССИИ

Безопасность есть одна из характеристик и условий функционирования и развития социальных, экономических, технических, экологических и биологических систем. Это – одна из фундаментальных потребностей социума. На уровне общественного сознания понятие «безопасность» трактуется как отсутствие опасности, сохранность, надежность, и употребляется применительно к самым различным процессам, как природным, так и социальным. В широком, философском смысле безопасность имеет значение надежности существования и устойчивости развития любых объектов социальной природы, является атрибутивной характеристикой, выделяемой, наблюдаемой и оцениваемой социальными субъектами. Состояние безопасности во многом определяют зрелость общества, степень осознания им угроз, реальных источников опасности. Само понятие чрезвычайно ёмкое, поэтому при анализе проблематики обычно выделяют ряд сфер безопасности: государственную безопасность, социальную, экономическую, общественную, военную, криминогенную и др. [5].

Общим, характерным для всех областей жизнедеятельности человека и общества является то, что безопасность как цель, условие и стратегия защиты от опасности нацелена, в конечном счете, на выживание социальной системы, личности, общества и государства. Однако система обеспечения безопасности не сводится только к пассивной безопасности, например, защите. Безопасность должна предполагать активность, учет состояния объекта воздействия со стороны угрозы, упреждающую реакцию. Поддерживающим и стабилизирующим фактором спонтанных защитных реакций социальных субъектов является государственное управление. Исключительную важность для обеспечения социальной безопасности имеет нормальное функционирование государственно-правовых институтов [5].

Законодательством Российской Федерации определено, что Основными принципами обеспечения безопасности являются [6]:

1) соблюдение и защита прав и свобод человека и гражданина;

2) законность;

3) системность и комплексность применения федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, другими государственными органами, органами местного самоуправления политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности;

4) приоритет предупредительных мер в целях обеспечения безопасности;

5) взаимодействие федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов с общественными объединениями, международными организациями и гражданами в целях обеспечения безопасности.

Невиданный рост количества и качественное разнообразие возможных разрушающих воздействий, масштабов реальных и потенциальных опасностей в прошедшем XX в. и в новом столетии, угрожающих человеку, человеческим сообществам и всей человеческой цивилизации в целом, обусловили потребность в совершенно новом осмыслении, осознании и выработке новых подходов к решению проблемы обеспечения безопасности людей во всех сферах их жизнедеятельности. В последнее время в зарубежной и отечественной литературе все большее место занимают вопросы глобального философского осмысления проблем международной и национальной безопасности из-за усиления нетрадиционных угроз выживанию человечества и отсутствия гармонизированной с природой модели общественного устройства. Кризисное состояние современной цивилизации было констатировано на известной международной конференции в Рио-де-Жанейро в 1992 г., продекларировавшей «Концепцию выживания и устойчивого развития цивилизации». Понятие «устойчивость» при этом приобрело принципиально иную методологическую на-

грузку, выражая имманентность развития цивилизации, т.е. адекватность законам ее саморазвития и самоорганизации.

Одной из разновидностей безопасности выступает национальная безопасность. «Национальная безопасность – многоплановое явление, охватывающее все сферы и уровни общественной жизни. Так, можно говорить о политической, экономической, духовно-идеологической безопасности. Национальная безопасность предполагает не только безопасность государства, но и общества, социальных и национальных общностей, личности» [7]. Первоначально, как известно, понятие национальной безопасности возникло одновременно с институтом национального государства и проблемой его суверенитета среди других государств-конкурентов. В отечественной социально-философской литературе и в официальных документах сам термин «национальная безопасность» стал употребляться лишь в последнее десятилетие XX в. и им пытались определить границы сфер национальных интересов того или иного государства [7].

В настоящее время в нашей стране утверждена Стратегия национальной безопасности Российской Федерации до 2020 г. [8].

К национальным интересам РФ на долгосрочную перспективу отнесены развитие демократии и гражданского общества, повышение конкурентоспособности национальной экономики; незыблемость конституционного строя, территориальной целостности и суверенитета РФ; превращение России в мировую державу.

Основными приоритетами национальной безопасности РФ являются национальная оборона, государственная и общественная безопасность. В число стратегических целей национальной обороны включены предотвращение глобальных и региональных войн и конфликтов, стратегическое сдерживание в интересах обеспечения военной безопасности страны.

Как угроза военной безопасности РФ расценена политика ряда ведущих зарубежных стран, направленная на достижение преобладающего превосходства в военной сфере. В связи с этим предусмотрен переход к качест-

венно новому облику Вооруженных Сил РФ с сохранением потенциала стратегических ядерных сил, наращиванием количества частей постоянной готовности, совершенствованием оперативной и боевой подготовки войск.

Основную угрозу государственной и общественной безопасности представляют терроризм, экстремизм, разведывательная деятельность иностранных спецслужб, организованная преступность. В связи с этим необходимо повысить эффективность деятельности правоохранительных органов и спецслужб, создать единую систему профилактики правонарушений, снизить уровень коррумпированности и криминализации общества. Особое внимание должно быть уделено охране госграницы РФ.

Одной из стратегических целей национальной безопасности является повышение качества жизни россиян. Основные задачи в данной сфере - обеспечение личной безопасности, доступности комфортного жилья, высококачественных и безопасных товаров и услуг, достойной оплаты труда.

Большое значение придается экономическому росту (Россия планирует войти в среднесрочной перспективе в 5 стран-лидеров по объему ВВП), развитию науки, технологий, здравоохранения и образования, сохранению культурного потенциала.

Ранее утвержденные концепции национальной безопасности РФ признаны утратившими силу.

Под национальной безопасностью Российской Федерации в Стратегии понимается состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства;

Стратегия национальной безопасности Российской Федерации до 2020 года - официально признанная система стратегических приоритетов, целей и мер в области внутренней и внешней политики, определяющих состоя-

ние национальной безопасности и уровень устойчивого развития государства на долгосрочную перспективу.

Концептуальные положения в области обеспечения национальной безопасности базируются на фундаментальной взаимосвязи и взаимозависимости Стратегии национальной безопасности Российской Федерации до 2020 года и Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года [9].

На протяжении десятилетий задача безопасности нашей страны понималась как узковоенная и внешнеполитическая. В конституционных актах советского государства эти вопросы практически не затрагивались. Проблеме безопасности придавался, как правило, политический смысл, она сводилась к обороне страны от внешних врагов, безопасности государства, борьбе с внутренним врагом. Соответственно нормативные акты, регулировавшие вопросы безопасности, имели не законодательный, а подзаконный характер и предназначались для служебного пользования. Культивировалась практика преимущественно силового обеспечения внешней безопасности государства и репрессивного решения проблем внутренней безопасности.

Объективные потребности принятия новой модели общественного устройства в России повлекли качественное изменение социально-политической и социально-экономической ситуации в стране, необходимость преодоления конфронтационной политической философии и основанных на этой ориентации концепций «силового баланса» в международных отношениях с постепенной переориентацией на идеи партнерства концепции «баланса интересов». Вслед за этим на смену идеологическому пониманию стало приходить общепринятое в мировой теории и практике понимание безопасности. Вошли в употребление понятия «безопасность личности», «безопасность общества» и «национальная безопасность» наряду с существовавшим всеобъемлющим понятием «государственная безопасность».

В настоящее время в России действует Федеральный закон от 28 декабря 2010 г. № 390-ФЗ "О безопасности".

Новый Закон о безопасности заменяет тот, который был введен в действие в 1992 г.

Уточняются принципы и содержание деятельности по обеспечению безопасности. Закрепляются основные цели международного сотрудничества в данной области.

Расширяются функции Президента Российской Федерации в соответствующей сфере. В частности, он определяет основные направления государственной политики в указанной области. При этом Правительство Российской Федерации только участвует в этом. Именно Президент Российской Федерации утверждает стратегию национальной безопасности. Он не только возглавляет, но и формирует Совет Безопасности Российской Федерации. Глава страны принимает меры, чтобы защитить граждан от противоправных посягательств, противодействовать терроризму и экстремизму, решает в соответствии с законодательством Российской Федерации вопросы, связанные с обеспечением защиты информации и государственной тайны.

Совет Безопасности Российской Федерации готовит решения Президента Российской Федерации в определенной сфере. К ней отнесены не только обеспечение безопасности, но и ряд других вопросов. Среди них - оборона, военное строительство, техническое сотрудничество с другими государствами и т. д.

Пересмотрены задачи и основные функции указанного органа. Президент Российской Федерации вправе расширять их перечень.

1.1. Информационная безопасность Российской Федерации

Составной частью национальной безопасности Российской Федерации является информационная безопасность (рисунок 1).

Цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации сформулированы в Доктрине информационной безопасности Российской Федерации, которая представляет собой совокупность официальных взглядов для:

- формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
- подготовки предложений по совершенствованию правового, ме- тодического, научно-технического и организационного обеспечения инфор- мационной безопасности Российской Федерации;
- разработки целевых программ обеспечения информационной безопасности Российской Федерации.

Под *информационной безопасностью* Российской Федерации будем понимать состояние защищенности национальных интересов Российской Федерации в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства [2].

Рисунок 1 – Структура национальной безопасности Российской Федерации

Информационная безопасность Российской Федерации является одной из составляющих национальной безопасности Российской Федерации и оказывает влияние на защищенность национальных интересов Российской Федерации в различных сферах жизнедеятельности общества и государства. Угрозы информационной безопасности Российской Федерации и методы ее обеспечения являются общими для этих сфер.

На основе национальных интересов для личности, общества и государства в информационной сфере на территории Российской Федерации формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

При этом интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Дальнейшее изучение излагаемого материала книги предварим введением основных терминов и определений из области информационной безопасности.

1.1.1. Основные термины и определения в области информационной безопасности

Материалы данного пункта включают ряд основополагающих положений, без которых сложно рассчитывать на успех в решении проблем информационной безопасности. Это, прежде всего, терминологический аппарат данной предметной области, основные принципы и требования к системе информационной безопасности организации, последовательность и содержание действий на каждом из этапов построения системы информационной безопасности, а также некоторые современные взгляды на разрешение сложных проблем информационной безопасности.

Для того чтобы освоить методологические основы обеспечения информационной безопасности, прежде всего, необходимо владеть понятийным аппаратом данной предметной области. Раскрытие некоторых ключевых терминов не самоцель, а попытка на этой основе сформировать начальные представления о целях и задачах защиты информации.

Методологической базой данного подраздела явились законодательство Российской Федерации (законы, указы, постановления), а также действующие международные и национальные стандарты.

Прежде определимся с термином «информация».

1.1.2. Информация как объект защиты

Основные свойства информации

Под информацией понимаются сведения (сообщения, данные) независимо от формы их представления [4].

Информация имеет ряд особенностей:

– информация нематериальна; нельзя измерить ее параметры (массу,

размеры, энергию и т. д.) известными физическими методами и приборами;

– информация, записанная на материальном носителе, может храниться, обрабатываться, передаваться по различным каналам связи;

– любой материальный объект содержит информацию о самом себе или о другом объекте.

На сегодняшний день новейшие информационные технологии, СМИ, многократно усилили возможности информационного воздействия на человека, население государства в целом. В результате информация превратилась в важнейший ресурс государства наряду с его другими основными ресурсами (природными, экономическими, трудовыми, материальными и т.д.).

Некоторые психологи утверждают, что человек разумный постепенно превращается в человека информационного. Наряду с традиционными методами управления обществом (административно-организационными, экономическими, социально-психологическими, правовыми) и отдельными личностями все большее распространение получает специальный метод централизованного воздействия на широкие слои населения - метод информационного управления.

В конце 50-х годов один из основоположников кибернетики, Н. Виннер определил информацию как: "обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему и приспособления к нему наших чувств. Процесс получения и использования информации является процессом нашего приспособления к случайностям внешней среды и нашей жизнедеятельности в этой среде" [10]. В данном определении ученый впервые затрагивает проблему неполноты получаемой индивидом информации, с одной стороны, а с другой, необходимость защиты сведений от "случайностей внешней среды".

Развитие информационных технологий заставляет интенсивно совершенствовать законодательную базу, вводит в юридическую сферу понятия, ранее применявшиеся в кибернетике и информатике.

В настоящее время с точки зрения защиты информация обладает рядом свойств:

1. Информация доступна человеку, если она содержится на материальном носителе. Так как с помощью материальных средств можно защищать только материальный объект, то объектами защиты являются материальные носители информации.

2. Ценность информации определяется ее полезностью для пользователя.

Полезность информации всегда конкретна. Нет ценной информации вообще. Информация полезна или вредна для конкретного ее пользователя. Чрезвычайно ценная информация для одних пользователей может не представлять ценности для других.

Ценность информации определяется степенью важности охраняемых сведений – сведений, составляющих государственную или иную охраняемую законом тайну.

Под *государственной тайной* понимаются защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Служебная тайна содержит сведения, не являющиеся государственной тайной.

Служебная тайна в настоящее время представляет собой защищаемую по закону конфиденциальную информацию, ставшую известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебную информацию о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости [11].

Коммерческая тайна содержит сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с законодательством Российской Федерации.

В настоящее время коммерческая тайна – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду [12].

При этом термин «информация, составляющая коммерческую тайну (секрет производства)» означает сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны;

3. Информацию можно рассматривать как товар, т.к. для получателя она может быть полезной или вредной, она покупается и продается. Цена информации и ее ценность понятия разные (затрачены огромные ресурсы, а результат может быть отрицательным).

Для принятия любого решения нужна информация, причем, чем выше риск и цена решения, тем большего объема должна быть информация.

4. Ценность информации изменяется во времени. Ценность большинства видов информации со временем уменьшается (информация стареет).

5. Невозможно оценить количество информации без учета полезности ее для потребителя (владельца, собственника). Количество информации, содержащейся, например, в книге, для разных читателей разное. Даже один и тот же человек в разные периоды своей жизни находит в книге каждый раз что-то новое для себя.

6. При копировании, не изменяющем информационные параметры носителя, количество информации не меняется, а цена снижается.

После снятия копии с документа на ксероксе или другим способом количество информации в нем не меняется.

При каждом копировании документа увеличивается число ее законных и незаконных пользователей, что снижает цену информации.

Источники и носители информации

С точки зрения защиты информации, ее источниками являются субъекты и объекты, от которых информация может поступить к несанкционированному получателю (злоумышленнику).

Основными источниками информации являются: люди; документы; продукция; измерительные датчики; интеллектуальные средства обработки информации; черновики и отходы производства; материалы и технологическое оборудование.

В [4] под документированной информацией понимается зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

При этом под понятием электронный документ понимается документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Документы являются наиболее информативным источникам, так как они содержат, как правило, достоверную информацию в отработанном и сжатом виде, в особенности, если документы подписаны или утверждены.

Технические средства и системы обработки информации, за исключением датчиков измерительных устройств, не являются источниками инфор-

мации, т.к. служат лишь инструментом для преобразования информации.

При производстве возможен брак и технологические газообразные, жидкие или твердые отходы. Отходы производства в случае небрежного отношения с ними (сбрасывания на свалку без предварительной селекции, сжигания или резки бумаги и т.д.) могут привести к утечке ценной информации.

Информативными могут быть не только продукция и отходы ее производства, но и исходные материал и сырье, а также используемое оборудование.

Между источником и получателем существует посредник – носитель информации, который позволяет органу разведки или злоумышленнику получать информацию дистанционно, в более безопасных условиях. Информация источника также содержится на носителе.

Носитель информации это физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Носителями информации являются: люди, материальные тела, поля, элементарные частицы (микрочастицы).

Человек как носитель информации ее запоминает и пересказывает получателю в письменном виде или устно, он может быть носителем других носителей информации – документов, продукции и т.д.

Материальные тела являются носителями различных видов информации и, прежде всего, материальные тела содержат информацию о своем составе. В настоящее время самым распространенным носителем семантической информации является бумага.

Носителями информации могут быть различные поля: акустические, электрические, магнитные и электромагнитные (в диапазоне видимого и инфракрасного света, в радио диапазоне). Информация содержится в значениях параметров полей. Если поля представляют собой волны, то информация содержится в амплитуде, частоте и фазе.

Из многочисленных элементарных частиц в качестве носителей информации используются электроны, образующие статические заряды и электрический ток, а также частицы (электроны и ядра гелия) радиоактивных излучений.

Информация, в зависимости от ее содержания, может быть текущей, срочной и чрезвычайной.

К текущей информации относятся постоянно или периодически поступающие, запланированные к получению сведения и данные, сроки представления которых не устанавливаются. Обычно такая информация докладывается по требованию или по мере накопления.

К срочной информации относится информация, содержащая такие сведения и данные, сроки и очередность доведения которых заранее установлена. Обычно она представляется в соответствии с табелем срочных донесений или по отдельным распоряжениям.

К чрезвычайной относится информация, содержание которой требует незамедлительного принятия решений. Она доводится до соответствующих лиц и органов управления немедленно.

Под информацией, как отмечалось выше, понимаются сведения (сообщения, данные) независимо от формы их представления.

По степени достоверности сведения об обстановке подразделяются на сведения достоверные, вероятные, сомнительные, ложные.

Достоверными считаются сведения, полученные от нескольких источников, заслуживающих полного доверия, и не противоречащие общей обстановке и действиям данной информационной структуры.

При этом, на основании законодательства Российской Федерации достоверность данных, представляет собой свойство данных не иметь скрытых ошибок [13].

К *вероятным* сведениям относятся сведения, которые в основном соответствуют обстановке, ранее полученным данным и характеру действий данного органа управления, но получены из одного источника. *Сомнитель-*

ными называют сведения, которые противоречат ранее имевшимся сведениям или получены от источника, не заслуживающего доверия. *Ложными* являются сведения, которые не соответствуют сложившейся обстановке, противоречат сведениям, полученным от надежных источников, или ложность которых неоспоримо доказана.

По степени важности сведения (данные) об обстановке подразделяются на особо важные, важные, обычные. Особо важные и важные сведения (данные) подлежат немедленному докладу старшему начальнику.

1.1.3. Используемые термины и определения

Стандартами Российской Федерации определено, что безопасность информации [данных] – это состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность [14].

При этом безопасность информации [данных] определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые при применении информационной технологии [15].

Законодательством Российской Федерации определено, что защита информации означает деятельность, направленную на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [14].

Также законодательством Российской Федерации установлено, что конфиденциальность информации – это обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [4].

Кроме того, уточняя технические аспекты конфиденциальности информации нормативными правовыми документами Российской Федерации установлено, что конфиденциальность информации это состояние информа-

ции, при котором доступ к ней осуществляют только субъекты, имеющие на него право [16].

При этом конфиденциальность информации [ресурсов автоматизированной информационной системы] понимается состояние информации [ресурсов автоматизированной информационной системы], при котором доступ к ней [к ним] осуществляют только субъекты, имеющие на него право [15].

Основным стандартом Российской Федерации в сфере защиты информации установлено, что целостность это такое состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право [14].

Доступность информации [ресурсов автоматизированной информационной системы] – такое состояние информации [ресурсов автоматизированной информационной системы], при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно [15].

При этом к правам доступа относятся: право на чтение, изменение, копирование, уничтожение информации, а также права на изменение, использование, уничтожение ресурсов.

Объект – пассивный компонент системы, хранящий, принимающий или передающий информацию [17].

Объект защиты информации – информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации [14].

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров [18].

Организация (от греч. – ργανον – *инструмент*) – это целевое объединение ресурсов. Организация – это группа людей, работающих совместно, во главе с руководителем и выполняющих определенные планы [19].

Угроза (безопасности информации) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации, связанную с утечкой информации, и/или несанкционированными и/или непреднамеренными воздействиями на нее [14, 23].

Вариант классификации угроз безопасности информации приведен в приложении № 1.

Источник угрозы безопасности информации – субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации [14].

Модель угроз безопасности информации – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации [14].

При этом видом описательного представления свойств или характеристик угроз безопасности информации может быть специальный нормативный документ.

Уязвимость (информационной системы); *брешь* — свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации [14].

Примечания:

1. Условием реализации угрозы безопасности обрабатываемой в системе информации может быть недостаток или слабое место в информационной системе.

2. Если уязвимость соответствует угрозе, то существует риск.

Вариант классификации уязвимостей безопасности информации приведен в приложении № 2.

Риск – вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муни-

ципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учетом тяжести этого вреда [24].

В интересах обеспечения информационной безопасности организации используется другое, более уточненное определение «риск – влияние неопределенностей на процесс достижения поставленных целей» [25].

Примечания:

1. Цели могут иметь различные аспекты: финансовые, аспекты, связанные со здоровьем, безопасностью и внешней средой, и могут устанавливаться на разных уровнях: на стратегическом уровне, в масштабах организации, на уровне проекта, продукта и процесса.

2. Риск часто характеризуется ссылкой на потенциальные события, последствия или их комбинацию, а также на то, как они могут влиять на достижение целей.

3. Риск часто выражается в терминах комбинации последствий события или изменения обстоятельств и их вероятности.

Риск нарушения безопасности сети электросвязи – вероятность причинения ущерба сети электросвязи или ее компонентам вследствие того, что определенная угроза реализуется в результате наличия определенной уязвимости в сети электросвязи [26].

Таким образом, риск безопасности информации – совокупность условий и факторов, при которых потенциально или реально реализуется угроза. Условием реализации угрозы безопасности обрабатываемой в системе информации может быть недостаток или слабое место в информационной системе [20, 21, 22].

Если уязвимость соответствует угрозе, то существует риск.

Риск – реализованная через уязвимость угроза.

Анализ информационного риска – систематическое использование информации для выявления *угроз* безопасности информации, *уязвимостей* информационной системы и количественной оценки вероятностей реализации угроз с использованием уязвимостей и последствий реализации угроз

для информации и информационной системы, предназначенной для обработки этой информации [14].

Кроме того, важно определить анализ процедур защиты, как независимый просмотр и анализ системных записей и активностей с целью проверки их адекватности системным управляющим функциям для обеспечения соответствия с принятой стратегией защиты и операционными процедурами, обнаружения пробелов в защите и выдачи рекомендаций по любым указанным изменениям в управлении, стратегии и процедурах [27].

Цель безопасности – изложенное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации и предположениям [28].

Цель защиты информации – заранее намеченный результат защиты информации [14].

Примечание: результатом защиты информации может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

Цель информационной безопасности (организации); цель ИБ (организации) – заранее намеченный результат обеспечения информационной безопасности организации в соответствии с установленными требованиями в политике ИБ (организации) [25].

Примечание: результатом обеспечения ИБ может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

Таким образом, целью защиты информации является сведение к минимуму потерь в управлении, вызванных нарушением целостности данных, их конфиденциальности или недоступности информации для потребителей.

Основными задачами системы информационной безопасности являются:

– своевременное выявление и устранение угроз безопасности и ресурсам, причин и условий, способствующих нанесению финансового, материального и морального ущерба его интересам;

– создание механизма и условий оперативного реагирования на угрозы безопасности и проявлению негативных тенденций в функционировании предприятия;

– эффективное пресечение посягательств на ресурсы и угроз персоналу на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности;

– создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения безопасности на достижение целей организации.

Основными задачами обеспечения безопасности сетей электросвязи являются [26]:

– своевременное выявление, оценка и прогнозирование источников угроз безопасности, причин и условий, способствующих нанесению ущерба, нарушению нормального функционирования и развития сетей электросвязи на всех уровнях иерархии единой сети электросвязи России (международном, междугороднем, зоновом, местном, на уровне пользования услугами связи и т. д.);

– выявление и устранение уязвимостей в средствах связи и сетях электросвязи;

– предотвращение, обнаружение угроз безопасности, пресечение их реализации и своевременная ликвидация последствий возможных ВН, в том числе и террористических действий;

– организация системы пропуска приоритетного трафика по сети электросвязи в случае чрезвычайных ситуаций, организация бесперебойной работы международной аварийной службы;

– совершенствование и стандартизация применяемых мер обеспече-

ния безопасности сетей электросвязи.

Примечание: операторами связи могут быть определены дополнительные цели и задачи обеспечения безопасности сетей электросвязи в зависимости от выполняемых организацией связи функций и ее бизнес-целей, но формулировка целей и задач должна быть независима от способов их реализации.

Мероприятия по защите информации должны исключать:

– выход излучений электромагнитного и акустического полей, а также наводок в сетях питания, кабельных линиях, заземлении, радио- и телефонных сетях за пределы контролируемой зоны;

– доступ в помещение, где осуществляется обработка информации, а также визуально-оптические возможности съема информации;

– работу специальных устройств ведения разведки, которые могут находиться в строительных конструкциях помещений и предметах их интерьера, а также внутри самого помещения или непосредственно в средствах обработки и передачи информации;

– перехват информации из каналов передачи данных;

– несанкционированный доступ к информационным ресурсам;

– воздействие излучений, приводящих к разрушению информации.

При этом различают организационные меры обеспечения ИБ и организационно-технические мероприятия по обеспечению защиты информации.

К организационным мерам обеспечения информационной безопасности относятся меры обеспечения информационной безопасности, предусматривающие установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации [25].

Организационно-технические мероприятия по обеспечению защиты информации представляют собой совокупность действий, направленных на применение организационных мер и программно-технических способов защиты информации на объекте информатизации [16].

Примечание:

1. Организационно-технические мероприятия по обеспечению защиты информации должны осуществляться на всех этапах жизненного цикла объекта информатизации.

2. Организационные меры предусматривают установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации.

Приведенная совокупность определений достаточна для формирования общего, пока еще абстрактного взгляда на построение системы информационной безопасности. Для уменьшения степени абстракции и формирования более детального замысла необходимо знание, в частности, методики формализованного представления угроз безопасности информации, уязвимостей информационной системы (в том числе и ее защиты) и возникающих рисков, а также синтеза соотношений между ними.

1.1.4. Современное состояние информационной безопасности в России

Происходящие в России преобразования самым существенным образом влияют на ее информационную безопасность; возникают новые факторы, которые требуют обязательного учета в проблемной области, связанной с защитой информации, как на государственном уровне, так и на уровне организаций и отдельных граждан.

Всю совокупность факторов можно разделить на политические, экономические и организационно-технические.

К политическим факторам следует отнести:

– становление новой российской государственности на основе принципов демократии, законности, информационной открытости;

– изменение геополитической обстановки вследствие фундаментальных перемен в различных регионах мира, сведения к минимуму вероятности мировой ядерной и обычной войн;

– информационная экспансия США и других развитых стран, осуществляющих глобальный мониторинг мировых политических, экономических, военных, экологических и других процессов, распространяющих информацию в целях получения односторонних преимуществ;

– разрушение ранее существовавшей командно-административной системы государственного управления, а также сложившейся системы обеспечения безопасности страны;

– нарушение информационных связей вследствие образования независимых государств на территории бывшего СССР;

– стремление России к более тесному сотрудничеству с зарубежными странами в процессе проведения реформ на основе максимальной открытости сторон;

– низкая общая правовая и информационная культура в российском обществе.

Среди экономических факторов наиболее существенными являются:

– переход России на рыночные отношения в экономике, появление множества отечественных и зарубежных коммерческих структур – производителей и потребителей информации, средств информатизации и защиты информации, включение информационной продукции в систему товарных отношений;

– критическое состояние отраслей промышленности, производящих средства информатизации и защиты информации;

– расширяющаяся кооперация с зарубежными странами в развитии информационной инфраструктуры России.

Из организационно-технических факторов определяющими являются:

– недостаточная нормативно-правовая база информационных отношений, в том числе в области обеспечения информационной безопасности;

– слабое регулирование государством процессов функционирования и развития рынка средств информатизации, информационных продуктов и услуг в России;

– широкое использование в сфере государственного управления и кредитно-финансовой сфере незащищенных от утечки информации импортных технических и программных средств для хранения, обработки и передачи информации;

– рост объемов информации, передаваемой по открытым каналам связи, в том числе по сетям передачи данных и межмашинного обмена;

– обострение криминогенной обстановки, рост числа компьютерных преступлений, особенно в кредитно-финансовой сфере.

Оценка состояния информационной безопасности и определение ключевых проблем в этой области обычно основываются на исследовании источников угроз.

Доктриной информационной безопасности Российской Федерации установлены источники угроз информационной безопасности Российской Федерации. При этом источники угроз информационной безопасности России подразделяются на внешние и внутренние.

К внешним источникам относятся:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;
- стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
- обострение международной конкуренции за обладание информационными технологиями и ресурсами;
- деятельность международных террористических организаций;
- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;

- деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам информационной безопасности России относятся:

- критическое состояние отечественных отраслей промышленности;
- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;
- недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;
- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;
- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
- недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;

- недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан [2].

Положение дел с обеспечением информационной безопасности в Российской Федерации таково, что не позволяет ей на равноправной основе включиться в мировую информационную систему и требует безотлагательного решения ключевых проблем, которые сформулированы в государственной программе Российской Федерации «Информационное общество (2011 – 2020 годы)» [3].

Государственной программой Российской Федерации "Информационное общество (2011 – 2020 годы)" определены также приоритеты и цели государственной политики в сфере развития информационного общества в Российской Федерации.

В соответствии со Стратегией развития информационного общества в Российской Федерации (далее - Стратегия), целями формирования и развития информационного общества в Российской Федерации являются повышение качества жизни граждан, обеспечение конкурентоспособности России, развитие экономической, социально-политической, культурной и духовной сфер жизни общества, совершенствование системы государственного управления

на основе использования информационных и телекоммуникационных технологий [20].

Таким образом, создание информационного общества рассматривается как платформа для решения задач более высокого уровня – модернизации экономики и общественных отношений, обеспечения конституционных прав граждан и высвобождения ресурсов для личностного развития.

Цели государственной политики определяют необходимость решения задач не только в сфере информационных технологий, но и в других отраслях экономики, науке и технике, социальной сфере и государственном управлении.

Текущее состояние готовности России к информационному обществу определяет в соответствии со Стратегией необходимость не только развития отрасли информационных технологий, но и определения приоритетов ее развития, создания на ее основе сервисов и обеспечения готовности граждан и организаций к использованию технических возможностей. Таким образом, на первый план выходят задачи координации действий различных субъектов правовых отношений инфраструктуры страны, согласования их интересов и ресурсов.

Международные обязательства Российской Федерации, с одной стороны, предполагают соблюдение положений соответствующих документов в области формирования информационного общества, а с другой – обеспечивают участие в разработке международных норм права и механизмов, регулирующих отношения в области использования глобальной информационной инфраструктуры, международных исследовательских проектах по приоритетным направлениям развития науки, технологий и техники, а также создают возможность использовать лучший опыт. Необходимо создание атмосферы заинтересованности в инновациях, готовности к нововведениям, открытости и непрерывности обучения как основы информационного общества.

Стратегией также установлено, что информационное общество характеризуется высоким уровнем развития информационных технологий и их ин-

тенсивным использованием гражданами, бизнесом и органами государственной власти, то есть для создания информационного общества высокий уровень развития информационных технологий является необходимым, но не достаточным условием. Необходимо обеспечить возможность внедрения технологий и создать привычку их использования в повседневной жизни. Поскольку информационное общество по своей природе не может быть локальным, то для всех граждан Российской Федерации независимо от места их проживания и социального статуса должны соблюдаться единые минимальные федеральные стандарты доступности информационных технологий.

В соответствии с целями и задачами формирования и развития информационного общества в Российской Федерации, предусмотренными Стратегией, а также с учетом текущего состояния сферы создания и использования информационных технологий в Российской Федерации целью Программы является получение гражданами и организациями преимуществ от применения информационных технологий за счет обеспечения равного доступа к информационным ресурсам, развития цифрового контента, применения инновационных технологий и радикального повышения эффективности государственного управления при обеспечении безопасности в информационном обществе.

При этом повышение качества жизни граждан и улучшение условий развития бизнеса в информационном обществе предусматривает:

- развитие сервисов для упрощения процедур взаимодействия общества и государства с использованием информационных технологий;
- перевод государственных и муниципальных услуг в электронный вид;
- развитие инфраструктуры доступа к сервисам электронного государства;
- повышение открытости деятельности органов государственной власти;
- создание и развитие электронных сервисов в области здравоохра-

нения, а также в областях жилищно-коммунального хозяйства, образования и науки, культуры и спорта.

Построение электронного правительства и повышение эффективности государственного управления предусматривает:

- формирование единого пространства электронного взаимодействия;
- создание и развитие государственных межведомственных информационных систем, предназначенных для принятия решений в реальном времени;
- создание справочников и классификаторов, используемых в государственных и муниципальных информационных системах;
- повышение эффективности внедрения информационных технологий на уровне субъектов Российской Федерации и муниципальных образований;
- создание инфраструктуры пространственных данных Российской Федерации;
- развитие системы учета результатов научно-исследовательских и опытно-конструкторских работ, выполненных в рамках государственного заказа;
- обеспечение перевода в электронный вид государственной учетной деятельности;
- создание и развитие специальных информационных и информационно-технологических систем обеспечения деятельности органов государственной власти, в том числе защищенного сегмента сети Интернет и системы межведомственного электронного документооборота.

Развитие российского рынка информационных технологий, обеспечение перехода к экономике, осуществляемой с помощью информационных технологий, предусматривает:

- стимулирование отечественных разработок в сфере информационных технологий;
- подготовку квалифицированных кадров в сфере информационных технологий;
- развитие экономики и финансовой сферы на основе использования информационных технологий;
- формирование социально-экономической статистики развития информационного общества;
- развитие технопарков в сфере высоких технологий.

Преодоление высокого уровня различия в использовании информационных технологий регионами, различными слоями общества и создание базовой инфраструктуры информационного общества предусматривает:

- развитие телерадиовещания;
- развитие базовой инфраструктуры информационного общества;
- популяризацию возможностей и преимуществ информационного общества;
- повышение готовности населения и бизнеса к возможностям информационного общества, в том числе обучение использованию современных информационных технологий.

Обеспечение безопасности в информационном обществе предусматривает:

- противодействие использованию потенциала информационных технологий в целях угрозы национальным интересам Российской Федерации;
- обеспечение технологической независимости Российской Федерации в отрасли информационных технологий;
- развитие технологий защиты информации, обеспечивающих неприкосновенность частной жизни, личной и семейной тайны, а также безопасность информации ограниченного доступа;

- обеспечение развития законодательства Российской Федерации и совершенствование правоприменительной практики в сфере информационных технологий.

Развитие цифрового контента и сохранение культурного наследия предусматривает:

- оцифровку объектов культурного наследия, включая архивные фонды;
- развитие средств обработки и предоставления удаленного доступа к цифровому контенту.

В государственной программе Российской Федерации «Информационное общество (2011 – 2020 годы)» прогноз развития сферы информационных технологий основан на прогнозе социально-экономического развития Российской Федерации на период до 2020 года и выполнен в двух вариантах – инерционном и инновационном. В инерционном варианте развития объем услуг связи к 2020 году по сравнению с 2007 годом вырастет в сопоставимых ценах почти в 6 раз, объем рынка информационных технологий – возрастет в 2,7 раза. В инновационном варианте прогнозируется рост объема услуг связи в 2020 году по сравнению с 2007 годом в сопоставимых ценах почти в 10 раз, объем рынка информационных технологий возрастет по сравнению с 2007 годом в 5,9 раза.

Решение вышеперечисленных ключевых проблем информационной безопасности должно осуществляться на основе соответствующей государственной политики.

Государственная политика в области обеспечения безопасности в нашей стране закреплена на высшем законодательном уровне [6].

В соответствии с Федеральным законом государственная политика в области обеспечения безопасности является частью внутренней и внешней политики Российской Федерации и представляет собой совокупность скоординированных и объединенных единым замыслом политических, организа-

ционных, социально-экономических, военных, правовых, информационных, специальных и иных мер.

Основные направления государственной политики в области обеспечения безопасности определяет Президент Российской Федерации.

Реализуется государственная политика в области обеспечения безопасности усилиями федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления на основе Стратегии национальной безопасности Российской Федерации [8], иных концептуальных и доктринальных документов, разрабатываемых Советом Безопасности Российской Федерации и утверждаемых Президентом Российской Федерации.

Граждане и общественные объединения участвуют в реализации государственной политики в области обеспечения безопасности.

Правовую основу обеспечения безопасности составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, настоящий Федеральный закон, другие федеральные законы и иные нормативные правовые акты Российской Федерации, законы и иные нормативные правовые акты субъектов Российской Федерации, органов местного самоуправления, принятые в пределах их компетенции в области безопасности.

Координацию деятельности по обеспечению безопасности осуществляют Президент Российской Федерации и формируемый и возглавляемый им Совет Безопасности, а также в пределах своей компетенции Правительство Российской Федерации, федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления.

Международное сотрудничество Российской Федерации в области обеспечения безопасности осуществляется на основе общепризнанных прин-

ципов и норм международного права и международных договоров Российской Федерации.

При этом, основными целями международного сотрудничества в области обеспечения безопасности являются:

1) защита суверенитета и территориальной целостности Российской Федерации;

2) защита прав и законных интересов российских граждан за рубежом;

3) укрепление отношений со стратегическими партнерами Российской Федерации;

4) участие в деятельности международных организаций, занимающихся проблемами обеспечения безопасности;

5) развитие двусторонних и многосторонних отношений в целях выполнения задач обеспечения безопасности;

6) содействие урегулированию конфликтов, включая участие в миротворческой деятельности.

Элементы государственной системы защиты информации и их основные функции приведены в приложении № 3.

На основе принципов и положений государственной политики обеспечения информационной безопасности должны проводиться все мероприятия по защите информации в политической, экономической, оборонной и других сферах деятельности государства. В этой связи следует иметь в виду, что в каждой из этих сфер имеются свои особенности, что в первую очередь связано с характером решения поставленных задач, наличием свойственных каждой области информационной безопасности слабых элементов и уязвимых звеньев.

В каждой сфере деятельности государства требуется специальная организация работ, а также использование форм и способов обеспечения информационной безопасности.

В политической сфере наиболее серьезной опасности подвергаются:

1. Общественное сознание и политическая ориентация различных групп населения страны (регионов), непрерывно формируемые под воздействием отечественных и зарубежных средств массовой информации (печать, радио, телевидение).

2. Система принятия политических решений, существенно зависящая от качества и своевременности ее информационного обеспечения.

3. Право политических организаций, партий, объединений и движений на свободное выражение своих программ, социально-политических и экономических ориентацией через средства массовой информации.

4. Система регулярного информирования населения органами государственной власти и управления о политической и социально-экономической жизни через средства массовой информации, пресс-центры, центры общественных связей и т.п.

5. Система формирования общественного мнения, включающая специальные институты, центры и службы выявления, изучения и анализа общественного мнения.

В сфере экономики наиболее подвержены воздействию угроз информационной безопасности система государственной статистики, источники, порождающие информацию о коммерческой деятельности хозяйственных субъектов всех форм собственности, о потребительских свойствах товаров и услуг, системы сбора и обработки финансовой, биржевой, налоговой, таможенной информации, информации о внешнеэкономической деятельности государства и коммерческих структур.

Уязвимости в оборонной сфере будут рассмотрены ниже.

Таким образом, проблема обеспечения информационной безопасности России принадлежит к числу проблем, без решения которых невозможен полномасштабный и эффективный переход к рыночной экономике, открытому информационному обществу.

1.2. Информационная безопасность оборонной сферы

Под *информационной безопасностью оборонной сферы* будем понимать состояние защищенности ее интересов в информационной сфере.

При этом будем руководствоваться, что информационная сфера – совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений [2].

Совокупность хранимой, обрабатываемой и передаваемой информации, используемой для обеспечения процессов управления оборонной сферы, будем называть *информационным ресурсом.*

К информационным ресурсам относятся:

– информационные ресурсы аппарата Министерства обороны, Генерального штаба, Главных штабов видов Вооруженных сил, штабов родов войск, других силовых ведомств, научно-исследовательских учреждений, содержащие ведения о стратегических и оперативных планах подготовки и ведения боевых действий, о дислокации и составе войск, о мобилизационной готовности, тактико-технические характеристики вооружения и военной техники;

– информационные ресурсы предприятий оборонного комплекса, содержащие сведения об основных направлениях развития оружия, о научно-техническом и производственном потенциале, об объемах поставок и запасах стратегических видов сырья и материалов;

– информационное обеспечение системы связи и управления оружием;

– информация о проводимых в интересах обороны фундаментальных и прикладных научно-исследовательских работ и др.

Информационная инфраструктура – совокупность объектов информатизации, обеспечивающая доступ потребителей к информационным ресурсам [25].

Таким образом, можно сформулировать, что *информационная инфраструктура* – это совокупность информационных подсистем, центров управления, аппаратно-программных средств и технологий обеспечения сбора, хранения, обработки и передаче информации.

Информационная инфрастуктура оборонной сферы состоит из:

– информационной инфраструктуры центральных органов военного управления и органов военного управления видов Вооруженных сил Российской Федерации и родов войск, объединений, соединений, воинских частей и организаций, входящих в Вооруженные силы Российской Федерации, научно-исследовательских учреждений Вооруженных сил Российской Федерации;

– информационной инфраструктуры предприятий оборонного комплекса и научно-исследовательских учреждений, выполняющих государственные оборонные заказы либо занимающихся оборонной проблематикой;

– программно-технических средств автоматизированных и автоматических систем управления войсками и оружием, вооружения и военной техники, оснащенных средствами информатизации;

– информационной инфраструктуры системы связи и других войск, воинских формирований и органов;

– узлов и линий радио- и проводной связи, развертываемых или арендуемых Министерством обороны.

Угрозы информационной безопасности Российской Федерации в оборонной сфере подразделяются на внешние и внутренние.

Внешними угрозами, представляющими наибольшую опасность для объектов обеспечения, являются [30]:

– все виды разведывательной деятельности зарубежных государств;

– информационно-технические воздействия (в том числе радиоэлектронная борьба, проникновение в компьютерные сети) со стороны вероятных противников;

– диверсионно-подрывная деятельность специальных служб ино-

странных государств, осуществляемая методами информационно-психологического воздействия;

– деятельность иностранных политических, экономических и военных структур, направленная против интересов Российской Федерации в сфере обороны.

К *внутренним угрозам*, которые будут представлять особую опасность в условиях обострения военно-политической обстановки относятся:

– нарушение установленного регламента сбора, обработки, хранения и передачи информации, находящейся в штабах и учреждениях Вооруженных силах Российской Федерации, на предприятиях оборонного комплекса;

– преднамеренные действия, а также ошибки персонала информационных и телекоммуникационных систем специального назначения;

– ненадежное функционирование информационных и телекоммуникационных систем специального назначения;

– возможная информационно-пропагандистская деятельность, подрывающая престиж Вооруженных Сил Российской Федерации и их боеготовность;

– нерешенность вопросов защиты интеллектуальной собственности предприятий оборонного комплекса, приводящая к утечке за рубеж ценнейших государственных информационных ресурсов;

– нерешенность вопросов социальной защиты военнослужащих и членов их семей.

На основании Доктрины информационной безопасности Российской Федерации [2], к угрозам безопасности уже развернутых и создаваемых информационных и телекоммуникационных средств и систем оборонной сферы относятся:

– противоправные сбор и использование информации;

– нарушения технологии обработки информации;

– внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

– разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

– уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;

– воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;

– компрометация ключей и средств криптографической защиты информации;

– утечка информации по техническим каналам;

– внедрение электронных устройств, предназначенных для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;

– уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

– перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;

– использование не сертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;

– несанкционированный доступ к информации, находящейся в банках и базах данных;

– нарушение законных ограничений на распространение информации.

К объектам обеспечения информационной безопасности Российской Федерации в сфере обороны относятся [2]:

- информационная инфраструктура центральных органов военного управления и органов военного управления видов Вооруженных Сил Россий-

ской Федерации и родов войск, объединений, соединений, воинских частей и организаций, входящих в Вооруженные Силы Российской Федерации, научно-исследовательских учреждений Министерства обороны Российской Федерации;

- информационные ресурсы предприятий оборонного комплекса и научно-исследовательских учреждений, выполняющих государственные оборонные заказы либо занимающихся оборонной проблематикой;
- программно-технические средства автоматизированных и автоматических систем управления войсками и оружием, вооружения и военной техники, оснащенных средствами информатизации;
- информационные ресурсы, системы связи и информационная инфраструктура других войск, воинских формирований и органов.

При этом в оборонной сфере к наиболее уязвимым звеньям относятся:

– информационные ресурсы аппарата Министерства обороны, Генерального штаба, Главных штабов видов Вооруженных сил и родов войск, других силовых ведомств, научно-исследовательских учреждений, содержащие сведения и данные об оперативных и стратегических планах подготовки и ведения боевых действий, о составе и дислокации войск, о мобилизационной готовности, тактико-технических характеристиках вооружения и военной техники;

– информационные ресурсы предприятий оборонного комплекса, содержащие сведения о научно-техническом и производственном потенциале, об объемах поставок и запасах стратегических видов сырья и материалов, об основных направлениях развития вооружения;

– военной техники, их боевых возможностях и проводимых в интересах обороны фундаментальных и прикладных научно-исследовательских работ (НИР);

– системы связи и управления войсками и оружием, их информационное обеспечение;

– политико-моральное состояние войск в части, зависящей от информационно-пропагандистского воздействия;

– информационная инфраструктура, в том числе центры обработки и анализа информации Генерального штаба и информационные подразделения штабов видов Вооруженных Сил, штабов объединений и соединений видов Вооруженных Сил и родов войск, пункты управления, узлы и линии радиосвязи, радиорелейной, тропосферной и спутниковой, а также линии проводной связи, развертываемые и арендуемые Министерством обороны и другими силовыми структурами.

Основными направлениями совершенствования системы обеспечения информационной безопасности Российской Федерации в оборонной сфере являются:

- систематическое выявление угроз и их источников, структуризация целей обеспечения информационной безопасности в сфере обороны и определение соответствующих практических задач;
- регулярное проведение мероприятий по выявлению уязвимостей в системе защиты информации объектов оборонного назначения;
- проведение сертификации общего и специального программного обеспечения, пакетов прикладных программ и средств защиты информации в существующих и создаваемых автоматизированных системах управления военного назначения и системах связи, имеющих в своем составе элементы вычислительной техники;
- постоянное совершенствование средств защиты информации от несанкционированного доступа, развитие защищенных систем связи и управления войсками и оружием, повышение надежности специального программного обеспечения;
- совершенствование структуры функциональных органов системы, координация их взаимодействия;
- совершенствование приемов и способов стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы, методов и средств

активного противодействия информационно-пропагандистским и психологическим операциям вероятного противника;

- подготовка специалистов в области обеспечения информационной безопасности в сфере обороны.

Оценка состояния информационной безопасности должна базироваться на исследовании источников угроз (потенциальной возможности нарушения защиты), уязвимостей в системе защиты информации и возникающих при этом потенциальных (реальных) рисков.

Глава 2. ЗАЩИТА ИНФОРМАЦИИ В ОРГАНИЗАЦИЯХ

В соответствии с законами Российской Федерации "О государственной тайне", "Об информации, информационных технологиях и о защите информации" и других законодательных актов Российской Федерации сведения, составляющие государственную и служебную тайну, подлежат обязательной защите. Мероприятия по защите информации и противодействию техническим разведкам (ТР) являются составной частью управленческой, научной и производственной деятельности и осуществляются во взаимосвязи с другими мерами по обеспечению установленного режима секретности проводимых организацией работ.

Проведение мероприятий по защите информации в организациях возлагаются на их руководителей, а методическое руководство и контроль за обеспечением защиты информации – на руководителей подразделений по защите информации.

Создаваемые на предприятиях системы защиты информации (СЗИ) призваны обеспечить защиту секретных (служебных) данных от утечки по техническим каналам и противодействие средствам ТР.

Система защиты информации, в общем виде, включает в себя комплекс организационных, технических и программных мероприятий, направленных на предотвращение утечки секретной (служебной) информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе ее обработки, передачи и хранения, противодействие иностранным техническим разведкам.

Разработка СЗИ должна производится подразделением по технической защите информации предприятия или ответственным за это направление во взаимодействии с разработчиками и ответственными за эксплуатацию объектов информатизации. Для проведения работ по созданию СЗИ могут

привлекаться на договорной основе специализированные предприятия, имеющие соответствующие лицензии на данный вид деятельности.

2.1. Направления защиты информации

Объектом защиты является информация или носитель информации, или информационный процесс, которые нужно защищать [25].

Первое направление – защита информации от утечки. Под утечкой информации будем понимать неконтролируемый выход секретной информации за пределы войсковой части (организации) или круга лиц, которым она была доверена.

Защита информации от разглашения направлена на предотвращение несанкционированного доведения ее до потребителя, не имеющего права доступа к этой информации.

Защита информации организуется по трем направлениям (рисунок 2).

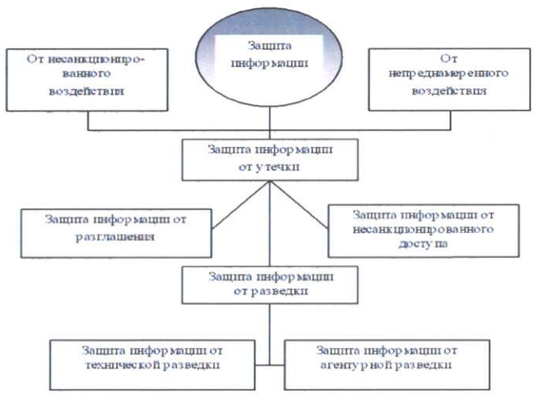

Рисунок 2 – Защита информации в организации

Защита информации от несанкционированного доступа направлена на предотвращение получения информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

Информацию, содержащую государственную или конфиденциальную, тайну необходимо защищать от агентурной и технической разведок иностранных государств.

Защита информации от технической разведки направлена на предотвращение получения информации разведкой с помощью технических средств.

Второе направление – защита от несанкционированного воздействия. Информация защищается от нарушения установленных прав и/или правил; от изменений, приводящих к ее уничтожению, искажению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Третье направление – защита информации от непреднамеренного воздействия:

– ошибок ее пользователя;

– сбоя технических и программных средств информационных систем;

– природных явлений;

– мероприятий, не имеющих целью изменение информации, но приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от несанкционированного доступа направлена на исключение доступа к информации с нарушением установленных прав и правил доступа к защищаемой информации.

Для предотвращения перехвата информации разведкой организуется защита информации от технической разведки (разведка с помощью технических средств) и агентурно-технической разведки.

Организовать защиту информации – значит создать систему защиты информации и разработать мероприятия по защите и контролю эффективности защиты информации (рисунок 3).

2.2. Система защиты информации

Для защиты информации создается *система защиты информации,* состоящая из совокупности органов и (или) исполнителей, используемой ими техники защиты, организованная и функционирующая по правилам, установленным правовыми, распорядительными и нормативными документами в области защиты информации.

Национальными стандартами Российской Федерации установлено, что система защиты информации – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации [14].

Применительно к автоматизированной системе система защиты информации автоматизированной системы представляет собой совокупность технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации [31].

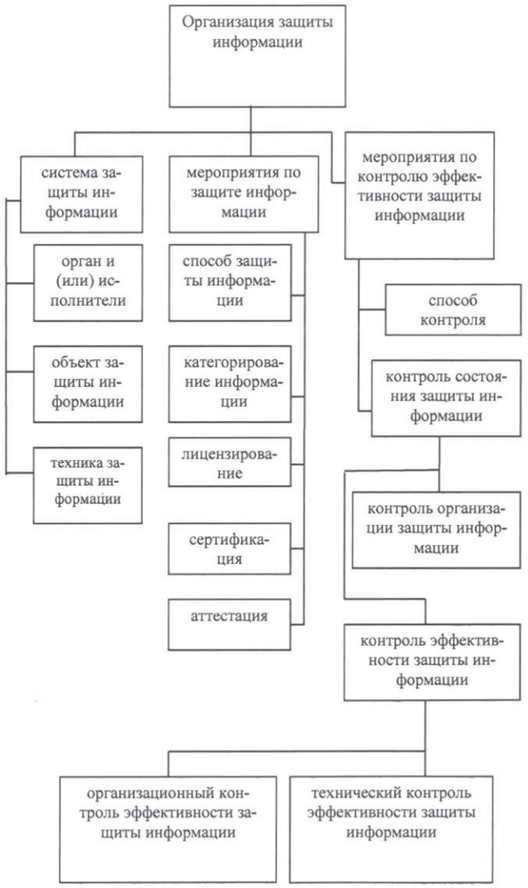

Рисунок 3 – Организация защиты информации

Система защиты информации должна удовлетворять следующим важнейшим требованиям [32]:

– обеспечивать безопасность информации, средств информатизации, защиту интересов участников информационных отношений;

– быть, по возможности, прозрачной для участников информационного обмена, не создавать им излишних неудобств, связанных с дополнительными процедурами проверки, надзора, контроля за доступом и т.д.;

– реализовывать различные методы управления: жесткие (административно-директивные) и мягкие (рекомендательного характера).

Основными целями защиты информации в организациях являются предотвращение проявления и нейтрализация преднамеренных и непреднамеренных источников угроз безопасности информации. В соответствии с этими целями процесс защиты информации должен обеспечить поддержание ее целостности и конфиденциальности. При этом под целостностью информации следует понимать ее неизменность (физическую целостность) и непротиворечивость (логическую целостность) в процессе хранения и обработки.

Целостность – состояние информации, при котором отсутствует любое ее изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право [25].

Конфиденциальность информации предполагает ее доступность только для тех лиц, которые имеют на это соответствующие полномочия.

В правовом смысле конфиденциальность информации представляет обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [4].

Целостность информации тесно связана с понятием надежности как технических, так и программных средств, реализующих процессы накопления, хранения и обработки информации.

Из выше изложенного следует, что достичь максимального (требуемого) уровня защищенности можно только за счет комплексного использования существующих методов и средств защиты. Комплексность является одним из принципов, которые должны быть положены в основу разработки, как концепции защиты информации, так и конкретных систем защиты.

Цели защиты информации в организациях могут быть достигнуты при проведении работ по следующим направлениям:

– определению охраняемых сведений об объектах защиты;

– выявлению и устранению (ослаблению) демаскирующих признаков, раскрывающих охраняемые сведения;

– оценке возможностей и степени опасности технических средств разведки;

– выявлению возможных технических каналов утечки информации;

– анализу возможностей и опасности несанкционированного доступа к информационным объектам;

– анализу опасности уничтожения или искажения информации с помощью программно-технических воздействий на объекты защиты;

– разработке и реализации организационных, технических, программных и других средств и методов защиты информации от всех возможных угроз;

– созданию комплексной системы защиты;

– организации и проведению контроля состояния и эффективности системы защиты информации;

– обеспечению устойчивого управления процессом функционирования системы защиты информации.

При этом цели защиты информации в автоматизированных системах в защищенном исполнении должны включать [23]:

• содержательную формулировку цели защиты;

• показатель эффективности достижения цели и требуемое его значение;

• время актуальности каждой цели защиты информации (этапы жизненного цикла, в течение которых цель должна достигаться).

В организациях комплексная защита информации должна осуществляться непрерывно на всех этапах их жизненного цикла.

При этом жизненный цикл автоматизированной системы представляет собой совокупность взаимосвязанных процессов создания и последовательного изменения состояния АС от формирования исходных требований к ней до окончания эксплуатации и утилизации комплекса средств автоматизации АС [33].

Реализация непрерывного процесса защиты информации возможна только на основе системно-концептуального подхода и промышленного производства средств защиты, а создание механизмов защиты и обеспечение их надежного функционирования и высокой эффективности может быть осуществлено только специалистами высокой квалификации в области защиты информации.

Необходимые для создания и поддержания эффективного функционирования системы защиты информации виды обеспечения включают законодательно-правовое, организационно-техническое и страховое обеспечение.

Законодательно-правовое обеспечение включает систему законодательно-правовых актов, устанавливающих правовой статус субъектов правоотношений, субъектов и объектов защиты, формы и способы защиты. Система законодательно-правовых актов и разработанных на их базе нормативных и организационно-распорядительных документов должна обеспечить организацию эффективного надзора за их исполнением со стороны правоохранительных органов и реализацию мер судебной защиты.

Организационно-техническое обеспечение представляет собой комплекс взаимно координируемых организационных мероприятий, технических, программных и других мер, реализующих все практические механизмы защиты.

Страховое обеспечение предназначено для защиты собственника информации или средств информатизации как от традиционных угроз (краж, стихийных бедствий и т.п.), так и от угроз, возникающих в ходе информатизации общества (утечка, уничтожение, блокирование и т.п.). Важным является вопрос защиты от промышленного шпионажа, а также страхование риска. Особенностью страховых методов обеспечения защиты является их эффективное действие в независимом секторе экономики, где административные методы управления и особенно контроля мало приемлемы.

В целом, обеспечение информационной безопасности организации представляет собой деятельность, направленная на устранение (нейтрализацию, парирование) внутренних и внешних угроз информационной безопасности организации или на минимизацию ущерба от возможной реализации таких угроз [25].

При разработке и создании системы комплексной защиты информации в организации основное внимание должно быть уделено ее оптимальности. Оптимальность системы защиты заключается в следующем: система должна обеспечить требуемый уровень защиты информации при минимальном расходовании ресурсов (финансовых, технических, информационных и др.) на ее создание, организацию и обеспечение функционирования или при заданном объеме ресурсов обеспечить максимально возможный уровень защищенности информации.

При оптимизации системы защиты ключевым исходным моментом является формирование полного множества функций защиты, так как надлежащим распределением ресурсов в осуществление каждой из функций можно оказывать воздействие на уровень защищенности информации, создавая, таким образом, объективные предпосылки для разработки оптимальной системы защиты. Общеизвестно, что полное множество составляют семь функций защиты следующего содержания:

– создание таких условий, при которых угрозы безопасности информации не могли бы проявляться;

– предупреждение появления угроз, даже если для этого есть объективные предпосылки;

– обнаружение появления угроз;

– предупреждение воздействия появившихся угроз на защищаемую информацию;

– обнаружение воздействия угроз на защищаемую информацию;

– локализация воздействия угроз на информацию;

– ликвидация последствий воздействия угроз.

На основе вышесказанного и с учетом состояния аналитической базы решения задачи оптимизации систем защиты может быть реализован следующий подход к построению оптимальной системы комплексной защиты информации:

– проводится анализ структурного построения и принципов функционирования организации, и выделяются на основе анализа уязвимые элементы, которые влияют на безопасность объекта;

– определяются и анализируются возможные угрозы выделенным элементам и формируется перечень требований к системе защиты;

– на основе опыта создания систем защиты информации определяются наиболее подходящие варианты набора средств и мер защиты, использованием которых может быть реализована каждая из функций защиты, и для этих вариантов методами экспертных оценок определяются показатели эффективности составленных вариантов;

– на основе технико-экономических оценок средств и мер защиты определяются размеры ресурсов, необходимых для практического использования различных средств и мер;

– решается задача синтеза оптимальной системы защиты информации математическими методами, в частности, на основе аксиоматики алгебры логики.

Необходимым условием разработки системы защиты информации является соблюдение следующих принципов: учет требований защиты инфор-

мации при построении организации и разработке технологии автоматизированной обработки информации; комплексность использования средств и методов защиты; обеспечение непрерывности процесса защиты; обеспечение периодического контроля правильности функционирования всех подсистем защиты. Разработка системы комплексной защиты информации может выполняться как без использования каких-либо ранее созданных средств защиты, так и с их использованием в качестве элементов системы.

Таким образом, одними из важнейших этапов построения системы защиты информации в организации являются этапы всестороннего исследования угроз, уязвимостей и, как следствие, рисков.

Следовательно, конечным элементом исследования является риск, как влияние неопределенностей на процесс достижения поставленных целей [25].

Национальный стандарт Российской Федерации ГОСТ Р 53114-2008 констатирует, что цели могут иметь различные аспекты: финансовые, аспекты, связанные со здоровьем, безопасностью и внешней средой, и могут устанавливаться на разных уровнях: на стратегическом уровне, в масштабах организации, на уровне проекта, продукта и процесса.

Также риск часто характеризуется ссылкой на потенциальные события, последствия или их комбинацию, а также на то, как они могут влиять на достижение целей.

Риск часто выражается в терминах комбинации последствий события или изменения обстоятельств и их вероятности.

Глава 3. МЕТОДИКА ИССЛЕДОВАНИЯ УГРОЗ, УЯЗВИМОСТЕЙ И РИСКОВ

Национальным стандартом Российской Федерации ГОСТ Р 50922-2006 установлено, что цель защиты информации – заранее намеченный результат защиты информации [14].

Результатом защиты информации при этом может быть предотвращение ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

Главная цель любой системы защиты информации заключается в обеспечении устойчивого функционирования объекта: предотвращении угроз его безопасности, защите законных интересов владельца информации от противоправных посягательств, в том числе уголовно наказуемых деяний в рассматриваемой сфере отношений, предусмотренных Уголовным кодексом Российской Федерации [34], обеспечении нормальной производственной деятельности всех подразделений объекта.

Другая задача сводится к повышению качества предоставляемых услуг и гарантий безопасности имущественных прав и интересов клиентов [35].

Для этого необходимо:

– отнести информацию к категории ограниченного доступа (служебной тайне) [36];

– прогнозировать и своевременно выявлять угрозы безопасности информационным ресурсам, причины и условия, способствующие нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития [37, 38];

– создать условия функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба [37, 38];

– создать механизм и условия оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций в функционировании, эффективное пресечение посягательств на ресурсы на основе правовых, организационных и технических мер и средств обеспечения безопасности [37];

– создать условия для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц, и тем самым ослабить возможное негативное влияние последствий нарушения информационной безопасности.

Учет вышеперечисленных особенностей при создании системы защиты информации в организации обычно осуществляется посредством разработки модели.

При этом модель угроз (безопасности информации) представляет собой физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации [14, 25].

Видом описательного представления свойств или характеристик угроз безопасности информации может быть специальный нормативный документ.

3.1. Модель системы защиты информации

При построении системы защиты информации в организации может быть использован следующий вариант модели (рисунок 4), учитывающей слагаемые, являющиеся существенными при обеспечении безопасности информации: угрозы (внутреннего и внешнего характера); уязвимости, имеющиеся как в информационной системе, так и в системе защиты информации; риски (потенциальные и реальные потери); конкретно очерчен контур участников процесса – владельца информации (например, организации), нарушителя и ресурса (информационные массивы, процессы и т.п.); а также потенциально возможные связи между всеми выше перечисленными элементами.

Рисунок 4 – Вариант модели системы защиты информации в организации

Представленный вариант модели защиты информации можно интерпретировать как совокупность объективных внешних и внутренних факторов и их влияние на состояние безопасности информации в организации. При разработке модели учитывались рекомендации представленные в [40, 42, 43].

Ниже будут рассматриваться следующие объективные факторы:

– угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации;

– уязвимости информационной системы или системы контрмер (системы информационной безопасности), влияющие на вероятность реализации угрозы;

– риск – фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования (риск в конечном итоге отражает вероятные финансовые потери – прямые или косвенные).

Для построения сбалансированной системы защиты информации в организации первоначально необходимо проводить исследование рисков в области информационной безопасности. Второе – определить оптимальный уровень риска для организации на основе заданного критерия. Систему защиты информации (контрмеры) необходимо строить таким образом, чтобы достичь заданного уровня риска.

При разработке модели системы защиты информации в организации должны быть установлены границы исследования. Для этого необходимо выделить ресурсы информационной системы, для которых в дальнейшем будут получены оценки рисков. При этом предстоит разделить рассматриваемые ресурсы и внешние элементы, с которыми осуществляется взаимодействие. Ресурсами могут быть средства вычислительной техники, программное обеспечение, данные, а также в соответствии с Национальным стандартом Российской Федерации ГОСТ Р 51275-2006 [18] – информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах). Примерами внешних элементов могут являться сети связи (абз. 4 ст. 2 Федерального закона «О связи»), внешние сервисы и т.п.

При разработке модели должны учитываться взаимосвязи между ресурсами. Например, выход из строя какого-либо оборудования может привести к потере данных или выходу из строя другого критически важного элемента системы. Подобные взаимосвязи определяют основу построения модели организации с точки зрения безопасности информации.

При разработке модели должна выполняться следующая этапность: для выделенных ресурсов определяется их ценность, как с точки зрения ас-

социированных с ними возможных финансовых потерь, так и с точки зрения ущерба репутации организации, дезорганизации ее деятельности, нематериального ущерба от разглашения конфиденциальной информации и т.д. Затем описываются взаимосвязи ресурсов, определяются угрозы безопасности и оцениваются вероятности их реализации.

На основе разработанной модели представляется возможным обоснованно выбрать систему контрмер, снижающих риски до допустимых уровней и обладающих наибольшей ценовой эффективностью. Частью системы контрмер будут рекомендации по проведению регулярных проверок эффективности системы защиты информации.

Обеспечение повышенных требований к безопасности информации предполагает соответствующие мероприятия на всех этапах жизненного цикла информационных технологий. Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия текущего режима безопасности информации политике безопасности, сертификация информационной системы (технологии) на соответствие требованиям определенного стандарта безопасности.

По завершении работ, можно будет определить меру гарантии безопасности информационной среды, основанную на оценке, с которой можно доверять информационной среде объекта. Данный подход предполагает, что большая гарантия следует из применения больших усилий при проведении оценки безопасности. Адекватность оценки основана на вовлечении в процесс оценки большего числа элементов информационной среды объекта, глубине, достигаемой за счет использования при проектировании системы обеспечения безопасности большего числа проектов и описаний деталей выполнения, строгости, которая заключается в применении большего числа инструментов поиска и методов, направленных на обнаружение менее очевидных уязвимостей или на уменьшение вероятности их наличия.

Выше было указано, что наиболее существенным фактором с точки зрения обеспечения требуемой эффективности системы защиты информации в организации является полный и достоверный учет в исследованиях угроз (см. рисунок 4), уязвимостей и рисков для информационных технологий. Представляется целесообразным подробно рассмотреть возможность формализованного описания как собственно вышеперечисленных элементов модели системы защиты информации в организации, так и синтеза соотношений между ними.

3.2. Методика формализованного описания угроз, уязвимостей и рисков системы защиты информации и синтеза соотношений между ними

Цель исследований – повысить эффективность построения системы защиты информации в организации.

Научная цель исследований – разработать методику формализованного описания угроз, уязвимостей и рисков системы защиты информации и синтеза соотношений между ними (далее именуется методика).

Научная гипотеза – разработка методики должна повысить эффективность построения системы защиты информации в организации за счет использования математических методов, исключающих субъективные ошибки и повышающих обоснованность принимаемых решений.

Вводимые ограничения научных исследований – в модели (см. рисунок 4) рассматриваются только элементы системы защиты информации, связанные с угрозами, уязвимостями и рисками, а также их соотношения.

Обоснование математического аппарата научных исследований – аксиоматика алгебры логики, которая как наиболее адекватно описывает процессы мыследеятельности экспертов [38] при построении модели системы защиты информации в организации, так и исключает различного рода эвристики, характерные для языков искусственного интеллекта.

Методика содержит описательную (вербальную) и математическую (формализованную) составляющие.

3.2.1. Описательная (вербальная) составляющая методики

На *первом этапе* обычно определяются цели защиты информации в организации.

Необходимо попытаться – при помощи руководства и работников организации – понять, что же на самом деле нужно защищать и от кого. С этого момента начинается специфическая работа на стыке информационных технологий и основной деятельностью организации, которая состоит в определении таких мероприятий и (если возможно) целевого состояния обеспечения безопасности информации, которое будет сформулировано одновременно и в терминах основной деятельности, и в терминах безопасности информации. Исследование рисков – это и есть инструмент, с помощью которого можно определить цели защиты информации, оценить основные критичные факторы, негативно влияющие на ключевые аспекты основной деятельности организации, и выработать эффективные решения для их контроля или минимизации.

Ниже будет представлено, какие задачи решаются в рамках исследования рисков безопасности информации.

На *втором этапе* осуществляется идентификация и оценка информационных активов организации.

Цель обеспечения безопасности информации состоит в сохранении ее конфиденциальности, целостности и доступности. Вопрос только в том, какую именно информацию необходимо охранять и какие усилия прилагать для обеспечения ее сохранности.

Обеспечение безопасности информации основано на осознании конкретной ситуации, в которой оно реализуется. В терминах исследования рисков осознание ситуации выражается в инвентаризации и оценке активов организации. С точки зрения исследования рисков безопасности информации к основным активам относятся непосредственно информация, инфраструктура, персонал, имидж и репутация компании. Без инвентаризации активов на уровне основной деятельности организации невозможно ответить на вопрос,

что именно нужно защищать. Очень важно понять, какая информация обрабатывается в организации, где и как выполняется ее обработка.

В условиях крупной современной организации количество информационных активов может быть очень велико. Если деятельность организации автоматизирована при помощи тех или иных сервисных приложений, то можно говорить, что практически любому материальному объекту, использующемуся в этой деятельности, соответствует какой-либо информационный объект. Поэтому первоочередной задачей исследования рисков становится определение наиболее значимых активов.

Решить эту задачу невозможно без привлечения менеджеров основного направления деятельности организации, как среднего, так и высшего звена. Оптимальна ситуация, когда высший менеджмент организации лично задает наиболее критичные направления деятельности, для которых крайне важно обеспечить безопасность информации. Мнение высшего руководства по поводу приоритетов в обеспечении безопасности информации очень важно и ценно в процессе анализа рисков, но в любом случае оно должно уточняться путем сбора сведений о критичности активов на среднем уровне управления компанией. При этом дальнейший анализ целесообразно проводить именно по обозначенным высшим менеджментом направлениям основной деятельности организации. Полученная информация обрабатывается, агрегируется и передается высшему менеджменту для комплексной оценки ситуации.

Идентифицировать и локализовать информацию можно на основании описания основной деятельности организации, в рамках которой информация рассматривается как один из типов ресурсов. Задача несколько упрощается, если в организации принят подход регламентации основной деятельности организации (например, в целях повышения качества и оптимизации процессов). Формализованные описания процессов основной деятельности организации обычно служат стартовой точкой для инвентаризации активов. Если описаний нет, можно идентифицировать активы на основании сведений, по-

лученных от сотрудников организации. После того как активы идентифицированы, необходимо определить их ценность.

Работа по определению ценности информационных активов в разрезе всей организации одновременно наиболее значима и сложна. Именно оценка информационных активов позволяет начальнику отдела информационной безопасности выбирать основные направления деятельности по обеспечению безопасности информации.

Ценность актива выражается величиной потерь, которые понесет организация в случае нарушения безопасности актива. Определение ценности проблематично, потому что в большинстве случаев менеджеры организации не могут сразу же дать ответ на вопрос, что произойдет, если, к примеру, информация о закупочных ценах, хранящаяся на файловом сервере, уйдет к конкуренту. Вернее сказать, в большинстве случаев менеджеры организации не задумываются о таких ситуациях.

Но экономическая эффективность процесса обеспечения безопасности информации во многом зависит именно от осознания того, что нужно защищать и какие усилия для этого потребуются, так как в большинстве случаев объем прилагаемых усилий прямо пропорционален объему затрачиваемых финансовых средств и операционных расходов. Управление рисками позволяет ответить на вопрос, где можно рисковать, а где нельзя. В данном случае термин «рисковать» означает, что в определенной области можно не прилагать значительных усилий для защиты информационных активов и при этом в случае нарушения безопасности организация не понесет значимых потерь. Здесь можно провести аналогию с классами защиты автоматизированных систем: чем значительнее риски, тем более жесткими должны быть требования к защите.

Чтобы определить последствия нарушения безопасности, нужно либо иметь сведения о зафиксированных инцидентах аналогичного характера, либо провести сценарный анализ (моделирование). В рамках сценарного анализа изучаются причинно-следственные связи между событиями нарушения

безопасности активов и последствиями этих событий для основной деятельности организации. Последствия сценариев должны оцениваться несколькими людьми (экспертами), итерационным или совещательным методом. Следует отметить, что разработка и оценка таких сценариев не может быть полностью оторвана от реальности. Всегда нужно помнить, что сценарий должен быть вероятным. Критерии и шкалы определения ценности индивидуальны для каждой организации. По результатам сценарного анализа можно получить информацию о ценности активов.

Если активы идентифицированы и определена их ценность, можно говорить о том, что цели обеспечения безопасности информации частично установлены: определены объекты защиты и значимость поддержания их в состоянии информационной безопасности для организации. Пожалуй, осталось только определить, от кого необходимо защищаться.

На *третьем этапе* исследуются источники проблем для безопасности информации в организации.

После определения целей обеспечения безопасности информации следует проанализировать проблемы, которые мешают приблизиться к требуемому целевому состоянию. На этом уровне исследование рисков спускается до информационной инфраструктуры и традиционных понятий информационной безопасности – нарушителей, угроз и уязвимостей (рисунок 5).

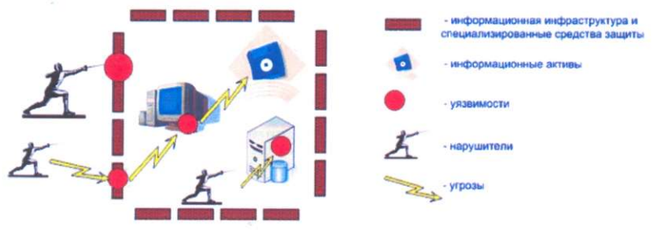

Рисунок 5 – Составляющие рисков безопасности информации

Модель нарушителя

Для оценки рисков недостаточно ввести стандартную модель нарушителя, разделяющую всех нарушителей по типу доступа к активу и знаниям о структуре активов. Такое разделение помогает определить, какие угрозы могут быть направлены на актив, но не дает ответа на вопрос, могут ли эти угрозы быть в принципе реализованы.

В процессе анализа рисков необходимо оценить мотивированность нарушителей при реализации угроз. При этом под нарушителем подразумевается не абстрактный внешний хакер или инсайдер, а сторона, заинтересованная в получении выгоды путем нарушения безопасности актива.

Первоначальную информацию о модели нарушителя, как и в случае с выбором изначальных направлений деятельности по обеспечению безопасности информации, целесообразно получить у высшего менеджмента, представляющего себе положение организации на рынке, имеющего сведения о конкурентах и о том, каких методов воздействия можно от них ожидать. Сведения, необходимые для разработки модели нарушителя, можно получить и из специализированных исследований по нарушениям в области компьютерной безопасности в той сфере деятельности, для которой проводится анализ рисков. Правильно проработанная модель нарушителя дополняет цели обеспечения безопасности информации, определенные при оценке активов организации. Вариант модели нарушителя (кибернарушителя) представлен в приложении № 4.

Модель угроз

Разработка модели угроз и идентификация уязвимостей неразрывно связаны с инвентаризацией окружения информационных активов организации. Сама собой информация не хранится и не обрабатывается. Доступ к ней обеспечивается при помощи информационной инфраструктуры, автоматизирующей процессы основной деятельности организации. Важно понять, как информационная инфраструктура и информационные активы организации связаны между собой. С позиции безопасности информации значимость информационной инфраструктуры может быть установлена только после определения связи между информационными активами и инфраструктурой. В том случае, если процессы поддержания и эксплуатации информационной инфраструктуры в организации регламентированы и прозрачны, сбор информации, необходимый для идентификации угроз и оценки уязвимостей, значительно упрощается.

Разработка модели угроз – работа для профессионалов в области безопасности информации, которые хорошо представляют себе, каким образом нарушитель может получить неавторизованный доступ к информации, нарушая периметр защиты или действуя методами социальной инженерии. При разработке модели угроз можно также говорить о сценариях как о последовательных шагах, в соответствии с которыми могут быть реализованы угрозы. Очень редко случается, что угрозы реализуются в один шаг путем эксплуатации единственного уязвимого места системы.

В модель угроз следует включить все угрозы, выявленные по результатам исследования смежных процессов основной деятельности организации. Угрозы необходимо ранжировать друг относительно друга по уровню вероятности их реализации. Для этого при разработке модели угроз для каждой угрозы необходимо указать наиболее значимые факторы, существование которых оказывает влияние на ее реализацию.

Идентификация уязвимостей

После разработки модели угроз необходимо идентифицировать уязвимости в окружении активов. Идентификация и оценка уязвимостей может выполняться в рамках аудита. Для проведения аудита безопасности информации необходимо разработать критерии проверки. А критерии проверки могут быть разработаны как раз на основании модели угроз и модели нарушителя.

По результатам разработки модели угроз, модели нарушителя и идентификации уязвимостей можно говорить о том, что определены причины,

влияющие на достижение целевого состояния безопасности информации организации.

На *четвертом этапе* исследуются риски для безопасности информации в организации.

Идентифицировать и оценить активы, разработать модель нарушителя и модель угроз, идентифицировать уязвимости – все это стандартные шаги, описание которых должно присутствовать в любой методике исследования рисков. Все перечисленные шаги могут выполняться с различным уровнем качества и детализации. Очень важно понять, что и как можно сделать с большим количеством накопленной информации и формализованными моделями. На наш взгляд, этот вопрос наиболее важен, и ответ на него должна давать используемая методика исследования рисков.

Полученные результаты необходимо оценить, агрегировать, классифицировать и отобразить. Так как ущерб определяется на этапе идентификации и оценки активов, необходимо оценить вероятность событий риска. Как и в случае с оценкой активов, оценку вероятности можно получить на основании статистики по инцидентам, причины которых совпадают с рассматриваемыми угрозами безопасности информации, либо методом прогнозирования – на основании взвешивания факторов, соответствующих разработанной модели угроз.

Хорошей практикой для оценки вероятности станет классификация уязвимостей по выделенному набору факторов, характеризующих простоту эксплуатации уязвимостей. Прогнозирование вероятности угроз проводится уже на основании свойств уязвимости и групп нарушителей, от которых исходят угрозы.

В качестве примера системы классификации уязвимостей можно привести стандарт CVSS – common vulnerability scoring system. Следует отметить, что в процессе идентификации и оценки уязвимостей очень важен экспертный опыт специалистов по защите информации, выполняющих оценку рис-

ков, и используемые статистические материалы и отчеты по уязвимостям и угрозам в области информационной безопасности.

Величину (уровень) риска следует определить для всех идентифицированных и соответствующих друг другу наборов «актив – угроза». При этом величина ущерба и вероятности не обязательно должны быть выражены в абсолютных денежных показателях и процентах; более того, как правило, представить результаты в такой форме не удается. Причина этого – используемые методы анализа и оценки рисков безопасности информации: сценарный анализ и прогнозирование.

На *пятом этапе* принимается решение по обеспечению безопасности информации в организации.

Что же можно сделать с полученным результатом оценки рисков?

В первую очередь следует разработать простой и наглядный отчет об анализе рисков, основной целью которого будет презентация собранной информации о значимости и структуре рисков безопасности информации в организации. Отчет следует представить высшему руководству организации. Распространенная ошибка состоит в том, что вместо выводов высшему руководству представляют промежуточные результаты. Несомненно, все выводы должны быть подтверждены аргументами – к отчету необходимо приложить все промежуточные выкладки.

Для наглядности отчета риски необходимо классифицировать в привычных для организации терминах, сходные риски – агрегировать. В целом классификация рисков может быть многогранной. С одной стороны, речь идет о рисках безопасности информации, с другой – о рисках ущерба для репутации или потери клиента. Классифицированные риски необходимо ранжировать по вероятности их возникновения и по значимости для организации.

Отчет об анализе рисков должен отражать следующие сведения:

– наиболее проблемные области обеспечения безопасности информации в организации;

– влияние угроз безопасности информации на общую структуру рисков организации;

– первоочередные направления деятельности отдела информационной безопасности по повышению эффективности обеспечения безопасности информации.

На основании отчета об анализе рисков руководитель отдела информационной безопасности может разработать план работы отдела на среднесрочный период и заложить бюджет исходя из характера мероприятий, необходимых для снижения рисков. Отметим, что правильно составленный отчет об анализе рисков позволяет начальнику отдела информационной безопасности найти общий язык с высшим менеджментом организации и решить актуальные проблемы, связанные с защитой информации в организации.

Таким образом, описательная (вербальная) составляющая методики формализованного описания угроз, уязвимостей и рисков системы защиты информации и синтеза соотношений между ними позволяет систематизировать порядок этапов ее проведения, определить их содержание, выработать те или иные рекомендации по обеспечению безопасности информации в организации для конкретной ситуации. Однако, описательная (вербальная) составляющая методики не позволяет получать количественные значения, в частности рисков (ущерба), что предполагает необходимость разработки математической (формализованной) составляющей методики.

3.2.2. Математическая (формализованная) составляющая методики

Существующие в настоящее время подходы к количественной оценке рисков (ущерба) от нарушения безопасности информации в организации чаще всего основываются либо на вероятностных вычислениях, либо на экспертных оценках.

Использование вероятностных вычислений представляется адекватным только для случаев, где существует устойчивая выборка событий, что для исследуемого случая (оценка рисков) характерно крайне редко. Экспертные заключения требуют определенной квалификации специалистов и специфических знаний у них конкретной оперативной обстановки, а также всегда содержат в себе элемент субъективизма.

В связи с выше указанным для формализованного описания угроз, уязвимостей и рисков системы защиты информации и синтеза соотношений между ними предлагается применить математический аппарат алгебры логики, исключающий отмеченные недостатки и позволяющий корректно описывать исследуемую область.

Первый шаг методики.

Определяются потенциальные угрозы безопасности информации в организации. В дальнейшем в качестве угроз для защищаемой информации будем рассматривать средства технической разведки.

Техническую разведку по функциональному предназначению можно классифицировать следующим образом:

– *радиоэлектронная,* включающая в себя: радио; радиотехническую; радиолокационную; радиотепловую; разведку побочных электромагнитных излучений и наводок (ПЭМИН);

– *оптико-электронная,* включающая в себя телевизионную; инфракрасную (тепловизионную и теплопеленгационную); визуальную оптико-электронную; разведку лазерных излучений;

– *компьютерная;*

– *фотографическая;*

– *визуальная оптическая;*

– *акустическая,* подразделяющаяся на акустическую речевую и сигнальную;

– *гидроакустическая,* включающую в себя разведку гидроакустических шумовых полей; гидролокационную; разведку гидроакустических сигналов; разведку звукоподводной связи;

– *магнитометрическая;*

– *химическая;*

– *радиационная;*

– *сейсмическая.*

Из перечисленного перечня угроз выбираются конкретные, характерные для складывающейся оперативной обстановки в сфере безопасности информации в организации.

Второй шаг методики.

Предположим, что угрозу для безопасности информации в организации представляет радиомониторинг (радиоразведка), которая ведется конкурентами.

Исследуются в организации уязвимости, которые могут привести к утечке защищаемой информации.

Допустим, что в организации информация может передаваться по телефону ($Q_{тлф}$), факсу ($Q_{факс}$) и видео ($Q_{видео}$).

Введем обозначения: ($Q_{тлф}$) – передача информации по телефону в организации; $Q_{тлф} = 1$ – передача информации в организации по телефону осуществляется, $Q_{тлф} = 0$ – передача информации в организации по телефону не осуществляется. Аналогично для ($Q_{факс}$) и ($Q_{видео}$).

В организации информация может быть использована либо для внутренних целей ($Q_{пер.} = 0$), либо передана по каналам радиосвязи другим потребителям ($Q_{пер.} = 1$).

С учетом введенных обозначений для получения вида логической функции, описывающей процедуру передачи информации в организации, составим таблицу истинности (таблица № 1) [41].

Таблица № 1

Таблица истинности,
описывающая процедуру передачи информации в организации

Входы				Выход
$Q_{тлф}$	$Q_{факс}$	$Q_{видео}$	$Q_{пер.}$	$Q_{пер.вых.}$
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	1
0	1	0	0	0
0	1	0	1	1
0	1	1	0	0
0	1	1	1	1
1	0	0	0	0
1	0	0	1	1
1	0	1	0	0
1	0	1	1	1
1	1	0	0	0
1	1	0	1	1
1	1	1	0	0
1	1	1	1	1

Поскольку определяющей для передачи информации по каналам радиосвязи другим потребителям является переменная $Q_{пер.}$, то выходную переменную (логическую функцию) обозначим $Q_{пер.вых.}$

По данным таблицы истинности (см. таблицу № 1) синтезируем логическое выражение для функции $Q_{пер.вых.}$

1) $Q_{\text{тлф}} \wedge Q_{\text{факс}} \wedge Q_{\text{видео}} \wedge Q_{\text{пер.}} \vee Q_{\text{тлф}} \wedge Q_{\text{факс}} \wedge \overline{Q}_{\text{видео}} \wedge Q_{\text{пер.}} = Q_{\text{тлф}} \wedge Q_{\text{факс}} \wedge Q_{\text{пер.}}$;

2) $Q_{\text{тлф}} \wedge \overline{Q}_{\text{факс}} \wedge Q_{\text{видео}} \wedge Q_{\text{пер.}} \vee Q_{\text{тлф}} \wedge \overline{Q}_{\text{факс}} \wedge \overline{Q}_{\text{видео}} \wedge Q_{\text{пер.}} = Q_{\text{тлф}} \wedge \overline{Q}_{\text{факс}} \wedge Q_{\text{пер.}}$;

3) $\overline{Q}_{\text{тлф}} \wedge Q_{\text{факс}} \wedge Q_{\text{видео}} \wedge Q_{\text{пер.}} \vee \overline{Q}_{\text{тлф}} \wedge Q_{\text{факс}} \wedge \overline{Q}_{\text{видео}} \wedge Q_{\text{пер.}} = \overline{Q}_{\text{тлф}} \wedge Q_{\text{факс}} \wedge Q_{\text{пер.}}$;

4) $Q_{\text{тлф}} \wedge Q_{\text{факс}} \wedge Q_{\text{пер.}} \vee Q_{\text{тлф}} \wedge \overline{Q}_{\text{факс}} \wedge Q_{\text{пер.}} = Q_{\text{тлф}} \wedge Q_{\text{пер.}}$;

5) $Q_{\text{тлф}} \wedge Q_{\text{пер.}} \vee \overline{Q}_{\text{тлф}} \wedge Q_{\text{факс}} \wedge Q_{\text{пер.}} = Q_{\text{пер.}}(Q_{\text{тлф}} \vee \overline{Q}_{\text{тлф}} \wedge Q_{\text{факс}}) =$
$= Q_{\text{пер.}}(Q_{\text{тлф}} \vee Q_{\text{факс}})$ (по теореме отражения);

6) $Q_{\text{пер.}}(Q_{\text{тлф}} \vee Q_{\text{факс}}) \vee \overline{Q}_{\text{тлф}} \wedge \overline{Q}_{\text{факс}} \wedge Q_{\text{видео}} \wedge Q_{\text{пер.}} = Q_{\text{пер.}}(Q_{\text{тлф}} \vee Q_{\text{факс}} \vee \overline{Q}_{\text{тлф}} \wedge \overline{Q}_{\text{факс}} \wedge Q_{\text{видео}}) = Q_{\text{пер.}}(Q_{\text{тлф}} \vee Q_{\text{факс}} \vee Q_{\text{видео}})$ (по теореме отражения).

Таким образом,

$$Q_{\text{пер. вых.}} = Q_{\text{пер.}}(Q_{\text{тлф}} \vee Q_{\text{факс}} \vee Q_{\text{видео}}). \quad (1)$$

Следовательно, уязвимости, которые могут привести к утечке защищаемой информации в организации, при условии ее передачи по каналам радиосвязи другим потребителям в условиях ведения конкурентами радиоразведки, включают: передачу информации из организации другим потребителям по каналам радиосвязи по телефону, факсу и видео (см. 1).

Третий шаг методики.

Более подробно рассмотрим угрозу для защищаемой информации в организации с учетом введенных ограничений.

Синтезируем логическое выражение для функции $Q_{\text{рр}}$ (условие выполнения радиоразведкой возложенных на нее функций).

Введем обозначения: ($Q_{\text{поиск}}$) – поиск информации в каналах радиосвязи; $Q_{\text{поиск}} = 1$ – поиск информации в каналах радиосвязи осуществляется, $Q_{\text{поиск}} = 0$ – поиск информации в каналах радиосвязи не осуществляется. Аналогично для ($Q_{\text{обн.}}$) и ($Q_{\text{расп.}}$), где ($Q_{\text{обн.}}$) – обнаружение информации в каналах радиосвязи; ($Q_{\text{расп.}}$) – распознавание информации, полученной из каналов радиосвязи.

Условие выполнения радиоразведкой возложенных на нее функций (риски для безопасности информации в организации) может быть записано

$$Q_{\text{поиск вых.}} \wedge Q_{\text{обн. вых.}} \wedge Q_{\text{расп. вых.}} = Q_{\text{рр}}. \quad (2)$$

Детализируем выражение (2).

По аналогии с вышерассмотренным материалом составим таблицу истинности, описывающую процедуру поиска информации в каналах радиосвязи радиоразведкой. По данным таблицы истинности синтезируем логическое выражение для функции поиска

$$Q_{\text{поиск вых.}} = Q_{\text{пер. вых.}} \wedge Q_{\text{поиск}}(Q_{\text{тлф}} \vee Q_{\text{факс}} \vee Q_{\text{видео}}). \quad (3)$$

Выражение (3) предполагает, что процесс поиска информации может осуществляться для случаев передачи ее по телефону, факсу и видео.

Перепишем выражение (3) с учетом выражения (1).

$$Q_{\text{поиск вых.}} = Q_{\text{пер.}} \wedge Q_{\text{поиск}}(Q_{\text{тлф}} \vee Q_{\text{факс}} \vee Q_{\text{видео}}). \quad (4)$$

Для $Q_{\text{обн. вых.}}$ также запишем логическое выражение с предположением того, что радиоразведка может обнаруживать информацию, передаваемую только по телефону и факсу.

$$Q_{\text{обн. вых.}} = Q_{\text{пер.}} \wedge Q_{\text{поиск}} \wedge Q_{\text{обн.}}(Q_{\text{тлф}} \vee Q_{\text{факс}} \vee Q_{\text{видео}}) \wedge (Q_{\text{тлф}} \vee Q_{\text{факс}}) = Q_{\text{пер.}} \wedge Q_{\text{поиск}} \wedge Q_{\text{обн.}}(Q_{\text{тлф}} \vee Q_{\text{факс}})$$ (по теоремам идемпотентности и характеристической). (5)

Для $Q_{\text{расп.вых.}}$ запишем логическое выражение (с учетом, что может быть распознана информация, передаваемая только по телефону и факсу).

$$Q_{\text{расп.вых.}} = Q_{\text{пер.}} \wedge Q_{\text{поиск}} \wedge Q_{\text{общ.}} (Q_{\text{тлф.}} \vee Q_{\text{факс}}) \wedge Q_{\text{расп.}} (Q_{\text{тлф}} \vee Q_{\text{факс}}) = Q_{\text{пер.}} \wedge Q_{\text{поиск}} \wedge Q_{\text{общ.}} \wedge Q_{\text{расп.}} (Q_{\text{тлф}} \vee Q_{\text{факс}}). \quad (6)$$

Следовательно, угрозы, которые могут привести к утечке защищаемой информации в организации, при условии ее передачи по каналам радиосвязи другим потребителям в условиях ведения конкурентами радиоразведки, включают: передачу информации из организации другим потребителям по телефону и факсу.

Четвертый шаг методики.

Проведенные выше расчеты создают условия для получения логического выражения, характеризующего риск для безопасности информации в организации.

С учетом полученных выражений (4, 5, 6) перепишем выражение (2)

$$Q_{\text{гр}} = \{Q_{\text{пер.}} \wedge Q_{\text{поиск}} (Q_{\text{тлф.}} \vee Q_{\text{факс}} \vee Q_{\text{видео}})\} \wedge \{Q_{\text{пер.}} \wedge Q_{\text{поиск}} \wedge Q_{\text{общ.}} (Q_{\text{тлф.}} \vee Q_{\text{факс}})\} \wedge \{Q_{\text{пер.}} \wedge Q_{\text{поиск}} \wedge Q_{\text{общ.}} \wedge Q_{\text{расп.}} (Q_{\text{тлф}} \vee Q_{\text{факс}})\}$$ (по теоремам характеристическим, идемпотентности, поглощения и отражения)$= Q_{\text{пер.}} \wedge Q_{\text{поиск}} \wedge Q_{\text{общ.}} \wedge Q_{\text{расп.}} (Q_{\text{тлф}} \vee Q_{\text{факс}})$. (7)

Следовательно, риски, которые могут привести к утечке защищаемой информации в организации, при условии ее передачи по каналам радиосвязи другим потребителям в условиях ведения конкурентами радиоразведки (при условии реализации поиска, обнаружения и распознавания), включают: передачу информации из организации другим потребителям по телефону и факсу.

Анализ и оценка ущерба при реализации угроз через уязвимости (риски) от утечки информации в организации обычно осуществляются с учетом конкретной оперативной обстановки и существенных для нее свойств (параметров и характеристик) в данный период времени.

Рассмотренный выше подход с использованием методики формализованного описания угроз, уязвимостей и рисков системы защиты информации и синтеза соотношений между ними является достаточно упрощенным, так как в основном направлен на обучение с точки зрения формализации физических процессов, связанных с циркуляцией защищаемой информации, как в организации, так и за ее пределами, а также их радиоразведки со стороны конкурентов.

На первый взгляд кажется, что предлагаемая методика несколько искусственно применена для анализа и оценки ущерба (рисков) от утечки защищаемой информации в организации, так как ряд полученных выводов в рассмотренном выше материале в той или иной степени априорно очевиден. Однако, если количество реальных угроз и уязвимостей возрастает хотя бы в разы, их совместное исследование в силу конкретной оперативной обстановки требует перехода на более «тонкий» уровень (например, для рассмотренного выше случая необходимо учитывать скорость передачи сигнала, вид модуляции сигнала, протоколы кодирования информации, особенности ведения радиообмена между потребителями информации и т.п.), то вряд ли представляется возможным априорно выработать необходимые рекомендации либо по демпфированию рисков, либо по минимизации ущерба от них.

Таким образом, использование предложенной методики формализованного описания угроз, уязвимостей и рисков системы защиты информации и синтеза соотношений между ними для реальной оперативной обстановки с любым количеством угроз и уязвимостей, а также глубиной их исследования, позволит получать обоснованные выводы о наличии рисков и тем самым обуславливать выработку эффективных решений по их демпфированию или минимизации ущерба от них.

ЗАКЛЮЧЕНИЕ

Защита информации в организации представляет собой комплекс целенаправленных мероприятий ее собственников по предотвращению утечки, искажения, уничтожения и модификации защищаемых сведений.

Под системой защиты информации в целом обычно понимают государственную систему защиты информации и систему защиты информации на конкретных объектах (в организациях).

Цели защиты информации от технических средств разведки на конкретных объектах (в организациях) определяются конкретным перечнем потенциальных угроз. В общем случае цели защиты информации в организациях можно сформулировать как:

– предотвращение утечки, хищения, утраты, искажения, подделки информации;

– предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

– предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;

– защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

– сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

– обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Эффективность защиты информации определяется ее своевременностью, активностью, непрерывностью и комплексностью. Очень важно проводить защитные мероприятия комплексно, то есть обеспечивать нейтрализацию всех опасных каналов утечки информации. Необходимо помнить, что даже один-единственный не закрытый канал утечки может свести на нет эффективность системы защиты.

Одним из важнейших направлений по обеспечению безопасности информации является анализ и оценка реальных (потенциальных) угроз и уязвимостей, приводящих к реальным (потенциальным) рискам, характеризующим степень ущерба от утечки защищаемой информации в организации.

Исследование рисков – достаточно трудоемкая процедура. При исследовании рисков должны применяться методические материалы и инструментальные средства. Однако для успешного внедрения повторяемого процесса этого недостаточно; еще одна важная его составляющая – регламент управления рисками. Он может быть самодостаточным и затрагивать только риски безопасности информации, а может быть интегрирован с общим процессом управления рисками в организации.

Существующие в настоящее время подходы к исследованию управления рисками в организации, как правило, основываются либо на вероятностных вычислениях, либо на экспертных оценках.

Использование вероятностных вычислений представляется адекватным только для случаев, где существует устойчивая выборка событий, что для исследуемого случая (оценка рисков) характерно крайне редко. Экспертные заключения требуют определенной квалификации специалистов и специфических знаний у них конкретной оперативной обстановки, а также всегда содержат в себе элемент субъективизма.

Для устранения отмеченных недостатков в исследовании рисков (ущерба) для безопасности информации в организации в материалах данной работы была предложена методика анализа и оценки угроз, уязвимостей и рисков, состоящая из описательной и математической составляющих.

Для формализованного описания угроз, уязвимостей и рисков системы защиты информации и синтеза соотношений между ними был применен

математический аппарат алгебры логики, позволяющий корректно описывать исследуемую область.

Разработанная методика формализованного описания угроз, уязвимостей и рисков системы защиты информации и синтеза соотношений между ними позволяет полностью проанализировать и документально оформить требования, связанные с обеспечением безопасности информации в организации, избежать расходов на избыточные меры безопасности, возможные при субъективной оценке рисков, оказать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем, обеспечить проведение работ в сжатые сроки, представить обоснование для выбора мер противодействия, оценить эффективность контрмер, сравнить их различные варианты.

Таким образом, разработанная методика исследования угроз, уязвимостей и рисков защиты информации в организации расширяет (развивает) теоретические результаты, полученные в научных работах, посвященных данной проблемной области, а также может использоваться для практических расчетов при выработке обоснованных рекомендаций по обеспечению безопасности информации.

ИСПОЛЬЗУЕМАЯ ЛИТЕРАТУРА

1. Национальный стандарт Российской Федерации ГОСТ Р 43.0.2-2006. Информационное обеспечение техники и операторской деятельности. Термины и определения.

2. Доктрина информационной безопасности Российской Федерации (утв. Президентом Российской Федерации от 9 сентября 2000 г. № Пр-1895).

3. Распоряжение Правительства Российской Федерации от 20 октября 2010 г. № 1815-р "О государственной программе Российской Федерации «Информационное общество (2011 – 2020 годы)».

4. Федеральный закон Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями от 27 июля 2010 г.).

5. Мирошниченко В.М. Организация управления и обеспечение национальной безопасности Российской Федерации. – М., 2002.

6. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности».

7. Прохожев А.А. Национальная безопасность: основы теории, сущность, проблемы: Учеб. пособие. – М., 1995.

8. Указ Президента Российской Федерации от 12 мая 2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года».

9. Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года (утв. распоряжением Правительства Российской Федерации от 17 ноября 2008 г. № 1662-р).

10. Виннер Н. Кибернетика и общество. М., 1958 г., с. 31.

11. ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.

12. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» (с изменениями от 2 февраля, 18 декабря 2006 г., 24 июля 2007 г.).

13. Государственный стандарт Российской Федерации. ГОСТ Р 51170-98. Качество служебной информации. Термины и определения.

14. Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» (утв. Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г .№ 373-ст).

15. Р 50.1.053-2005. Рекомендации по стандартизации. Информационные технологии. Основные термины и определения в области технической защиты информации.

16. Р 50.1.056-2005. Рекомендации по стандартизации. Техническая защита информации. Основные термины и определения.

17. Национальный стандарт Российской Федерации ГОСТ Р 53113.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения.

18. Национальный стандарт Российской Федерации ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

19. Государственный стандарт Российской Федерации ГОСТ Р 40.002-2000 «Система сертификации ГОСТ Р. Регистр систем качества. Основные положения».

20. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК ТО 13335-4-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 4 «Выбор защитных мер».

21. Государственный стандарт Российской Федерации. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

22. Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены заместителем директора ФСТЭК России 15 февраля 2008 года.

23. Всемирная декларация по интеллектуальной собственности от 26 июня 2000 года.

23. Государственный стандарт Российской Федерации ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие положения.

24. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» (с изменениями от 9 мая 2005 г., 1 мая, 1 декабря 2007 г., 23 июля 2008 г., 18 июля, 23 ноября, 30 декабря 2009 г., 28 сентября 2010 г.).

25. Национальный стандарт Российской Федерации ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

26. Национальный стандарт Российской Федерации ГОСТ Р 52448-2005. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения.

27. Государственный стандарт Российской Федерации ГОСТ Р ИСО 7498-2-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации».

28. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

29. Стратегия развития информационного общества в Российской Федерации (утв. Президентом Российской Федерации 7 февраля 2008 г. № Пр-212).

30. Васильев А.Н., Степашин С.В., Сальников В.П. Национальная безопасность России: конституционное обеспечение. – СПб., 1999.

31. Государственный стандарт Российской Федерации ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.

32. Боридько С.И., Забелинский А.А., Тараскин М.М. Методы и средства защиты информации. Учебное пособие. – М.: МИНИТ, 2010.

33. Межгосударственный стандарт ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

34. УК РФ, 1996 г., ст. ст. 183, 272÷274.

35. Румянцев О.Г., Додонов В.Н. Юридический энциклопедический словарь. – М.: ИНФРА-М, 1997.

36. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера». Постановление Правительства Российской Федерации от 5 декабря 1991 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну».

37. Конституция Российской Федерации (с поправками от 30 декабря 2008 г.).

38. Гражданский кодекс Российской Федерации часть первая от 30 ноября 1994 г. № 51-ФЗ, часть вторая от 26 января 1996 г. № 14-ФЗ, часть третья от 26 ноября 2001 г. № 146-ФЗ и часть четвертая от 18 декабря 2006 г. № 230-ФЗ (с изменениями от 26 января, 20 февраля, 12 августа 1996 г., 24 октября 1997 г., 8 июля, 17 декабря 1999 г., 16 апреля, 15 мая, 26 ноября 2001 г., 21 марта, 14, 26 ноября 2002 г., 10 января, 26 марта, 11 ноября, 23 декабря 2003 г., 29 июня, 29 июля, 2, 29, 30 декабря 2004 г., 21 марта, 9 мая, 2, 18, 21 июля 2005 г., 3, 10 января, 2 февраля, 3, 30 июня, 27 июля, 3 ноября, 4, 18, 29, 30 декабря 2006 г., 26 января, 5 февраля, 20 апреля, 26 июня, 19, 24 июля, 2, 25 октября, 4, 29 ноября, 1, 6 декабря 2007 г., 24, 29 апреля, 13 мая, 30 июня, 14, 22, 23 июля, 8 ноября, 25, 30 декабря 2008 г., 9 февраля, 9 апреля, 29 июня, 17 июля, 27 декабря 2009 г., 21, 24 февраля, 8 мая, 27 июля, 4 октября 2010 г.).

39. Лихтарников Л.М., Сукачева Т.Г. Курс лекций по математической логике (учебное пособие). – Новгород: Новгородский государственный педагогический институт, 1993.

40. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий».

41. Асфаль Р. Роботы и автоматизация производства./Пер. с англ. М.Ю. Евстегнеева и др. – М.: Машиностроение, 1989.

42. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждено Федеральной службой по техническому и экспортному контролю 15 февраля 2008 года.

43. Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования. Приказ ФСБ РФ и Федеральной службы по техническому и экспортному контролю от 31 августа 2010 г. № 416/489.

ПРИЛОЖЕНИЕ № 1

Вариант классификации угроз безопасности информации

Угроза чаще всего является следствием наличия уязвимых мест в защите информационных сфер (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении). Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется окном опасности, ассоциированным с данным уязвимым местом. Пока существует окно опасности, возможны успешные атаки на информационную сферу (ИС). Если речь идет об ошибках в программном обеспечении (ПО), то окно опасности «открывается» с появлением средств использования ошибки и ликвидируется при наложении заплат, ее исправляющих.

Для большинства уязвимых мест интервал опасности существует сравнительно долго (несколько дней, иногда – недель), поскольку за это время должны произойти следующие события:

– должно стать известно о средствах использования пробела в защите;

– должны быть выпущены соответствующие заплаты;

– заплаты должны быть установлены в защищаемой ИС.

Новые уязвимые места и средства их использования появляются постоянно. Это значит, во-первых, что почти всегда существуют окна опасности и, во-вторых, что отслеживание таких окон должно производиться постоянно, а выпуск и наложение заплат – как можно более оперативно.

Отметим, что некоторые угрозы нельзя считать следствием каких-то ошибок или просчетов; они существуют в силу самой природы современных ИС. Например, угроза отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения ИС от качественного электропитания.

Рассмотрим наиболее распространенные угрозы, которым подвержены современные информационные системы. Иметь представление о возможных угрозах, а также об уязвимых местах, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности. Незнание в данном случае ведет к перерасходу средств и, что еще хуже, к концентрации ресурсов там, где они не особенно нужны, за счет ослабления действительно уязвимых направлений.

Подчеркнем, что само понятие «угроза» в разных ситуациях зачастую трактуется по-разному. Например, для открытой организации угроз конфиденциальности может просто не существовать – вся информация считается общедоступной; однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, угрозы, как и все в информационной безопасности (ИБ), зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым).

Угрозы можно классифицировать по нескольким критериям:

– по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;

– по компонентам информационных инфраструктур, на которые угрозы нацелены (данные, программы, аппаратура и т.п.);

– по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);

– по расположению источника угроз (внутри/вне рассматриваемой ИС).

Виды и источники угроз доступности

Наиболее распространенными и самыми опасными (с точки зрения размера ущерба) угрозами доступности являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные инфраструктуры. Иногда такие

ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). По некоторым данным, до 65% потерь – следствие непреднамеренных ошибок. Пожары и наводнения не приносят столько бед, сколько безграмотность и небрежность в работе. Очевидно, что самый радикальный способ борьбы с непреднамеренными ошибками – максимальная автоматизация и строгий контроль.

Другие угрозы доступности можно классифицировать по компонентам ИС, на которые нацелены угрозы:

– отказ пользователей;

– внутренний отказ системы;

– отказ поддерживающей инфраструктуры.

Обычно применительно к пользователям рассматриваются следующие угрозы:

– нежелание работать с информационной инфраструктурой (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);

– невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);

– невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

Основными источниками внутренних отказов являются:

– отступление (случайное или умышленное) от установленных правил эксплуатации;

– выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персона-

ла (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);

– ошибки при конфигурировании системы;

– отказы программного и аппаратного обеспечения;

– разрушение данных;

– разрушение или повреждение аппаратуры.

По отношению к вспомогательной (поддерживающей) инфраструктуре рекомендуется рассматривать следующие угрозы:

– нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;

– разрушение или повреждение помещений;

– невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

Весьма опасны так называемые «обиженные» сотрудники – нынешние и бывшие. Как правило, они стремятся нанести вред организации-«обидчику», например:

– испортить оборудование;

– встроить логическую бомбу, которая со временем разрушит программы и/или данные;

– удалить данные.

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

Опасны, разумеется, стихийные бедствия и события, воспринимаемые как стихийные бедствия, – пожары, наводнения, землетрясения, ураганы. По статистике, на долю огня, воды и тому подобных «злоумышленников» (среди которых самый опасный – перебой электропитания) приходится 13% потерь, нанесенных информационным системам.

Некоторые примеры угроз доступности.

Угрозы доступности могут выглядеть грубо – как повреждение или даже разрушение оборудования (в том числе носителей данных). Такое повреждение может вызываться естественными причинами (чаще всего – грозами). К сожалению, находящиеся в массовом использовании источники бесперебойного питания не защищают от мощных кратковременных импульсов, и случаи выгорания оборудования – не редкость.

Общеизвестно, что периодически необходимо производить резервное копирование данных. Однако, даже если это предложение выполняется, резервные носители зачастую хранят небрежно (к этому мы еще вернемся при обсуждении угроз конфиденциальности), не обеспечивая их защиту от вредного воздействия окружающей среды. И когда требуется восстановить данные, оказывается, что эти самые носители никак не желают читаться.

Другой тип угрозы доступности связан с программными атаками на доступность. В качестве средства вывода системы из штатного режима эксплуатации может использоваться агрессивное потребление ресурсов (обычно – полосы пропускания сетей, вычислительных возможностей процессоров или оперативной памяти). В зависимости от расположения источника угрозы такое потребление подразделяется на локальное и удаленное. При просчетах в конфигурации системы локальная программа способна практически монополизировать процессор и/или физическую память, сведя скорость выполнения других программ к нулю.

Простейший пример удаленного потребления ресурсов – атака, получившая наименование «SYN-наводнение». Она представляет собой попытку переполнить таблицу «полуоткрытых» TCP-соединений сервера (установление соединений начинается, но не заканчивается). Такая атака, по меньшей мере, затрудняет установление новых соединений со стороны легальных пользователей, то есть сервер выглядит как недоступный.

По отношению к атаке «Papa Smurf» уязвимы сети, воспринимающие ping-пакеты с широковещательными адресами. Ответы на такие пакеты «съедают» полосу пропускания.

Удаленное потребление ресурсов в последнее время проявляется в особенно опасной форме – как скоординированные распределенные атаки, когда на сервер с множества разных адресов с максимальной скоростью направляются вполне легальные запросы на соединение и/или обслуживание. Временем начала «моды» на подобные атаки можно считать февраль 2000 года, когда жертвами оказались несколько крупнейших систем электронной коммерции (точнее – владельцы и пользователи систем). Отметим, что если имеет место архитектурный просчет в виде разбалансированности между пропускной способностью сети и производительностью сервера, то защититься от распределенных атак на доступность крайне трудно.

Одним из опаснейших способов проведения атак является внедрение в атакуемые системы вредоносного программного обеспечения. Обычно выделяют следующие аспекты (составные части) вредоносного ПО:

– вредоносная функция;

– способ распространения;

– внешнее представление.

Часть, осуществляющую разрушительную функцию, будем называть собственно вредоносной функцией. Вообще говоря, спектр вредоносных воздействий такого ПО неограничен. Основными из них являются:

– внедрение другого вредоносного ПО;

– получение контроля над атакуемой системой;

– агрессивное потребление ресурсов;

– изменение или разрушение программ и/или данных.

В зависимости от способа распространения различают следующие типы вредоносного ПО:

– вирусы – код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;

– «черви» – код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации вируса требуется запуск зараженной программы).

Вирусы обычно распространяются локально, в пределах узла сети; для передачи по сети им требуется внешняя помощь, такая как пересылка зараженного файла. «Черви», напротив, ориентированы в первую очередь на путешествия по сети.

Иногда само распространение вредоносного ПО вызывает агрессивное потребление ресурсов и, следовательно, является вредоносной функцией. Например, «черви» «съедают» полосу пропускания сети и ресурсы почтовых систем. По этой причине для атак на доступность они не нуждаются во встраивании специальных «бомб».

В ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» содержится следующее определение:

«Программный вирус – это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах».

Окно опасности для вредоносного ПО появляется с выпуском новой разновидности «бомб», вирусов и/или «червей» и перестает существовать с обновлением базы данных антивирусных программ и наложением других необходимых заплат.

Основные угрозы целостности

На втором месте по размерам ущерба (после непреднамеренных ошибок и упущений) стоят кражи и подлоги. В большинстве случаев виновниками являются штатные сотрудники организаций, отлично знакомые с режи-

мом работы и мерами защиты. Это еще раз подтверждает опасность внутренних угроз.

Отметим, что между статической и динамической целостностью существует определенное различие. С целью нарушения статической целостности злоумышленник (как правило, штатный сотрудник) может:

– ввести неверные данные;

– изменить данные.

Угрозой целостности является не только фальсификация или изменение данных, но и отказ от совершенных действий. Если нет средств обеспечить «неотказуемость», невозможно построить систему электронного документооборота. Потенциально уязвимы с точки зрения нарушения целостности не только данные, но и программы. Внедрение рассмотренного выше вредоносного ПО – пример подобного нарушения.

Угрозами динамической целостности являются нарушение атомарности транзакций, переупорядочение, кража, дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т.п.).

Соответствующие действия в сетевой среде называются активным прослушиванием.

Анализ угроз конфиденциальности

Конфиденциальную информацию можно разделить на предметную и служебную. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, в информационной инфраструктуре она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной.

Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы ее конфиденциальности могут носить некомпьютерный и вообще нетехнический характер.

Многим людям приходится выступать в качестве пользователей не одной, а целого ряда систем (информационных сервисов). Если для доступа к таким системам используются многоразовые пароли или иная конфиденциальная информация, то наверняка эти данные будут храниться не только в голове, но и в записной книжке или на листках бумаги, которые пользователь часто оставляет на рабочем столе, а той попросту теряет. И дело здесь не в неорганизованности людей, а в изначальной непригодности парольной схемы. Невозможно помнить много разных паролей; рекомендации по их регулярной (по возможности – частой) смене только усугубляют положение, заставляя применять несложные схемы чередования или вообще стараться свести дело к двум-трем легко запоминаемым (и столь же легко угадываемым) паролям.

Описанный класс уязвимых мест можно назвать размещением конфиденциальных данных в среде, где им не обеспечена необходимая защита. Помимо паролей, хранящихся в записных книжках пользователей, в этот класс попадает передача конфиденциальных данных в открытом виде (в разговоре, в письме, по сети), которая делает возможным перехват данных. Для атаки могут использоваться разные технические средства (подслушивание или прослушивание разговоров, пассивное прослушивание сети и т.п.), но идея одна – осуществить доступ к данным в тот момент, когда они наименее защищены.

Угрозу перехвата данных следует принимать во внимание не только при начальном конфигурировании ИС, но и при внесении изменений или восстановлении системы с резервных копий. Для защиты данных на основных носителях применяются развитые системы управления доступом; копии же нередко просто лежат в шкафах и получить доступ к ним могут многие.

Перехват данных – очень серьезная угроза, и если конфиденциальность действительно является критичной, а данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата хорошо проработаны, доступны, просты в экс-

плуатации, а установить их, например, на кабельную сеть, может кто угодно, так что эту угрозу нужно принимать во внимание по отношению не только к внешним, но и к внутренним коммуникациям.

Опасной нетехнической угрозой конфиденциальности являются методы морально-психологического воздействия, такие как маскарад – выполнение действий под видом лица, обладающего полномочиями для доступа к данным.

К серьезным угрозам, от которых трудно защищаться, можно отнести злоупотребление полномочиями. На многих типах систем привилегированный пользователь (например, системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т.д. Другой пример – нанесение ущерба при сервисном обслуживании. Обычно сервисный инженер получает неограниченный доступ к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

ПРИЛОЖЕНИЕ № 2

Вариант классификации уязвимостей безопасности информации

Любая оценка угроз безопасности информации должна начинаться с их классификации и оценки существующих уязвимостей, так как угрозы могут быть реализованы только через известные или предполагаемые уязвимости организационно-технического обеспечения организации. Исходя из этого классификацию угроз безопасности информации возможно проводить через классификацию уязвимостей. Приведенный ниже вариант классификации уязвимостей может использоваться при оценке угроз безопасности организации.

Уязвимости безопасности информации можно разделить на организационные и технические.

Организационные уязвимости можно классифицировать как:

– связанные с действиями персонала (умышленные или неумышленные);

– связанные с воздействием на персонал (физическое или психологическое).

Технические уязвимости можно классифицировать как:

– связанные с использованием аппаратного обеспечение (форс-мажорные обстоятельства; низкая надежность функционирования; ошибки при создании аппаратных средств (умышленные и неумышленные); побочные электромагнитные излучения и т.п.);

– связанные с использованием программного обеспечения (форс-мажорные обстоятельства; сбой (отказ) функционирования программ; ошибки при создании программ (умышленные и неумышленные); вредоносные закладки и т.п.).

Существование организационных и (или) технических уязвимостей может привести к возникновению следующих рисков:

– получение несанкционированного доступа к информации;

– получение несанкционированного доступа к используемому аппаратному и программному обеспечению;

– нарушение процесса жизнедеятельности организации;

– навязывание или распространение ошибочной или (и) ложной информации и т.п.

Исследование уязвимостей – обязательный этап обеспечения эффективной защиты информации в организации. По его результатам разрабатываются проектные варианты организации защиты информации.

Исследование уязвимости безопасности информации должно основываться на системном подходе и включать в себя разработку модели нарушителя, выделение и категорирование особо важных зон организации, обоснование показателей оценки частных уязвимостей, определение наиболее «слабых» мест в системе безопасности информации.

ПРИЛОЖЕНИЕ № 3

Элементы государственной системы защиты информации и их функции:

– Федеральная служба по техническому и экспортному контролю (ФСТЭК России) и ее центральный аппарат;

– ФСБ, МВД, МО, СВР, их структурные подразделения по защите информации;

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

– специальные центры ФСТЭК России;

– головная НИО в Российской Федерации по защите информации;

– организации по защите информации органов государственной власти;

– головные и ведущие научно-исследовательские, научно-технические, проектные и конструкторские;

– предприятия оборонных отраслей промышленности, их подразделения по защите информации;

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

– ВВУЗы, институты по подготовке специалистов в области защиты информации.

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

– обеспечения безопасности информации в ключевых системах информационной инфраструктуры;

– противодействия иностранным техническим разведкам;

– обеспечение защиты информации, содержащей государственную тайну, некриптографическими способами;

– предотвращение ее течки по техническим каналам, несанкционированного доступа к ней;

– предотвращения специальных воздействий на информацию (ее носители) с целью ее добывания, уничтожения, искажения и блокирования доступа к ней.

Руководство деятельностью ФСТЭК России осуществляет Президент РФ.

ФСТЭК России подведомственна Министерству обороны.

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

В органе государственной власти могут создаваться технические комиссии, межотраслевые советы.

Специальные центры подчиняются ФСТЭК России и в пределах своих зон ответственности выполняют следующие функции:

– проверяют и оценивают состояние защиты информации;

– осуществляют противодействие техническим средствам разведки (ТСР);

– участвуют в аттестации объектов по выполнению требований по защите информации;

– ведут радиоконтроль.

Головная научно-исследовательская организация (НИО) в Российской Федерации по защите информации, головные и ведущие НИО органов государственной власти разрабатывают научные основы и концепции, проекты нормативно-технических и методических документов по защите информации. На них возлагается разработка и корректировка моделей технической разведки.

Предприятия, занимающиеся деятельностью в области защиты информации, должны получить лицензию на этот вид деятельности. Лицензии выдаются, ФСТЭК России, ФСБ, СВР в соответствии с их компетенцией и по представлению органа государственной власти.

Вузы по подготовке и переподготовке кадров в области защиты информации и осуществляют:

– первичную подготовку специалистов по комплексной защите информации;

– переподготовку специалистов по защите информации;

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

ПРИЛОЖЕНИЕ № 4

Вариант модели нарушителя (кибернарушителя)

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

Злоумышленником будем называть нарушителя, намеренно идущего на нарушение из корыстных побуждений.

Вариант модели нарушителя отражает его практические и теоретические возможности, априорные знания, время и место действия и т.п. Для достижения своих целей нарушитель должен при ложить некоторые усилия, затратить определенные ресурсы. Исследовав причины нарушений, можно либо повлиять на эти причины (конечно, если это возможно), либо точнее определить требования к системе зашиты от данного вида нарушений или преступлений.

В каждом конкретном случае, исходя из конкретной технологии обработки информации, может быть определена модель нарушителя, которая должна быть адекватна реальному нарушителю для данной организации.

При разработке модели нарушителя определяются:

– предположения о категориях лиц, к которым может принадлежать нарушитель;

– предположения о мотивах действий нарушителя (преследуемых нарушителем целях);

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

– ограничения и предположения о характере возможных действий нарушителей.

По отношению к организации нарушители могут быть внутренними (из числа персонала) или внешними (посторонними лицами). Внутренним нарушителем может быть лицо из следующих категорий персонала (в смысле автоматизированной обработки информации):

– пользователи (операторы);

– персонал, обслуживающий технические средства (инженеры, техники);

– сотрудники отделов разработки и сопровождения программного обеспечения (прикладные и системные программисты);

– технический персонал, обслуживающий помещения (уборщики, электрики, сантехники и другие сотрудники, имеющие доступ в помещения, где расположены компоненты автоматизированной обработки информации);

– сотрудники службы безопасности организации;

– руководители различных уровней должностной иерархии.

Посторонние лица, которые могут быть нарушителями:

– клиенты (представители организаций, граждане);

– посетители (приглашенные по какому-либо поводу);

– представители учреждений, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, тепло-снабжения и т.п.);

– представители конкурирующих организаций (иностранных спецслужб) или лица, действующие по их заданию;

– лица, случайно или умышленно нарушившие пропускной режим (без цели нарушить безопасность организации);

– любые лица за пределами контролируемой территории.

Можно выделить три основных мотива нарушений: безответственность, самоутверждение и корыстный интерес.

При нарушениях, вызванных безответственностью, пользователь целенаправленно или случайно производит какие-либо разрушающие действия, не связанные тем не менее со злым умыслом. В большинстве

случаев это следствие некомпетентности или небрежности.

Некоторые пользователи считают получение доступа к системным наборам данных крупным успехом, затевая своего рода игру «пользователь – против системы» ради самоутверждения либо в собственных глазах, либо в глазах коллег.

Нарушение безопасности организации может быть вызвано и корыстным интересом нарушителя. В этом случае он будет целенаправленно пытаться преодолеть систему защиты для доступа к хранимой, передаваемой и обрабатываемой информации. Даже если организация имеет средства, делающие такое проникновение чрезвычайно сложным, полностью защитить ее от проникновения практически невозможно.

Всех нарушителей можно классифицировать следующим образом.

По уровню знаний об автоматизированной системе (АС):

– знает функциональные особенности АС, основные закономерности формирования в ней массивов данных и потоков запросов к ним, умеет пользоваться штатными средствами;

– обладает высоким уровнем знаний и опытом работы с техническими средствами системы и их обслуживания;

– обладает высоким уровнем знаний в области программирования и вычислительной техники. проектирования и эксплуатации автоматизированных информационных систем;

– знает структуру, функции и механизм действия средств защиты, их сильные и слабые стороны.

По уровню возможностей (используемым методам и средствам):

– применяющий чисто агентурные методы получения сведении;

– применяющий пассивные средства (технические средства перехвата без модификации компонентов системы);

– использующий только штатные средства и недостатки систем защиты для ее преодоления (несанкционированные действия с использованием разрешенных средств), а также компактные магнитные

носители информации, которые могут быть скрытно пронесены через посты охраны;

– применяющий методы и средства активного воздействия (модификация и подключение дополнительных технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ).

По времени действия:

– в процессе функционирования АС (во время работы компонентов системы);

– в период неактивности компонентов системы (в нерабочее время, во время плановых перерывов в ее работе, перерывов для обслуживания и ремонта и т.п.);

– как в процессе функционирования АС, так и в период неактивности компонентов системы.

По месту действия:

– без доступа на контролируемую территорию организации;

– с контролируемой территории без доступа в здания и сооружения;

– внутри помещений, но без доступа к техническим средствам;

– с рабочих мест конечных пользователей (операторов) АС;

– с доступом в зону данных (баз данных, архивов и т.п.);

– с доступом в зону управления средствами обеспечения безопасности АС.

Могут учитываться следующие ограничения и предположения о характере действий возможных нарушителей:

– работа по подбору кадров и специальные мероприятия затрудняют возможность создания коалиции нарушителей, т.е. объединения (сговора) и целенаправленных действий по преодолению подсистемы защиты двух и более нарушителей;

– нарушитель, планируя попытки НСД, скрывает свои

несанкционированные действия от других сотрудников;

– НСД может быть следствием ошибок пользователей, администраторов, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки информации и т.д.

Определение конкретных значений характеристик возможных нарушителей в значительной степени субъективно. Модель нарушителя, построенная с учетом особенностей конкретной предметной области и технологии обработки информации, может быть пред ставлена перечислением нескольких вариантов его облика. Каждый вид нарушителя должен быть охарактеризован значениями характеристик, приведенных выше.

Тараскин Михаил Михайлович – доктор технических наук, профессор, профессор МИНИТ ФСБ России, Почетный работник высшего профессионального образования Российской Федерации, автор более 150 научных работ в области информационной безопасности, в том числе 6 монографий.

Царегородцев Анатолий Валерьевич – доктор технических наук, профессор, профессор НИУ "Высшая школа экономики", действительный член Академии инженерных наук им. А.М. Прохорова, автор более 150 научных работ в области информационной безопасности и информационного противоборства, в том числе 14 монографий.

Тараскин М.М., Царегородцев А.В.

Защита информации в организациях:
методика исследования угроз, уязвимостей и рисков

Монография

Подписано в печать 08.10.2012. Формат 60x84/16.
Печать на ризографе. 7.25 П.Л. Тираж 500 экз. Заказ №85.

Отпечатано в типографии МИНИТ ФСБ России.
121552, г. Москва, ул. Ярцевская, д. 30. Тел.: (499)141-20-96