Федеральное государственное казенное образовательное учреждение
высшего профессионального образования
«Орловский юридический институт
Министерства внутренних дел Российской Федерации им. В.В. Лукьянова»

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРОТИВОДЕЙСТВИЯ НЕПРАВОМЕРНОМУ ДОСТУПУ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Монография

Орел
ОрЮИ МВД России им. В.В. Лукьянова
2013

УДК 004+34С66
ББК 32.97+67.99(2) 94
Т33

Рецензенты:

Ильяшенко А.Н., доктор юридических наук, профессор
(Краснодарский университет МВД России);
Козин А.М.
(ИЦ УМВД России по Орловской области)
Еременко В.Т., доктор технических наук, профессор
(Орловский государственный университет учебно-научный производственный комплекс);
Родионова Е.М., доктор экономических наук, профессор
(Орловский государственный университет учебно-научный производственный комплекс)

Авторский коллектив:

Калиниченко И.А. (введение, гл.1 §3, гл.2 §1, гл.3 §1, заключение);
Коробов А.А. (гл.3 §2, §3);
Костин С.В. (гл.1 § 2, гл.2 §1, §3);
Мишин Д.С. (гл.1 § 1, гл.2 §2, §4, гл.3 §1, §4)

Т33 **Теоретические основы противодействия неправомерному доступу в сфере информационных технологий** : монография / под общей редакцией канд. пед. наук И.А. Калиниченко. – Орёл : ОрЮИ МВД России им. В.В. Лукьянова, 2013. – 179 с.
ISBN 978-5-88872-074-5

УДК 004+34С66
ББК 32.97+67.99(2) 94

ISBN 978-5-88872-074-5

Оглавление

Введение

Начавшаяся во второй половине XX века научно-техническая революция привела к существенным изменениям в общественной жизни. «Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений»[2].

С началом XXI века человечество вступило в эру новых информационных технологий, использование которых кроме позитивных тенденций обладает и рядом негативных. На современном этапе развития мирового сообщества информация и информационные процессы играют ключевую роль не только в функционировании общественных и государственных институтов, но и в жизни каждого человека в отдельности. Все более возрастающие требования к оперативности протекания информационных процессов в различных областях деятельности мирового сообщества, а также постоянное совершенствование технического и программного обеспечения, стали побудительным мотивом создания современных информационных систем и методов распределенной обработки данных, реализации доступа к вычислительным сетям посредством информационно-телекоммуникационных сетей. В Федеральном законодательстве дается следующее определение:

информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники [5].

Создание подобных сетей, в свою очередь, привело к интегрированию систем обработки и обмена информацией. Вместе с тем интенсификация информационных процессов порождает ряд попутных и достаточно серьезных проблем, без решения которых вообще нельзя будет говорить об эффективности информатизации. Одной из наиболее острых проблем указанного процесса выступает проблема надежной защиты информации, т.е. предупреждения ее искажения или уничтожения, несанкционированной модификации, получения и использования. Особую остроту проблема защиты приобретает в связи с повсеместной и массовой компьютеризацией информационных процессов, широким внедрением информационно-вычислительных сетей с доступом к их ресурсам массы пользователей.

Причины постоянного совершенствования процедур неправомерного доступа кроются в высокой латентности подобных инцидентов. На этом фоне особую актуальность приобретают проблемы связанные с обеспечением безопасности в информационном пространстве, а также возможности

и перспективы применения средств защиты информации. Вышесказанное указывает на то, что проблемы совершенствования систем информационного обеспечения входят в число наиболее актуальных и неотложных задач общества, и в интересах их решения, особенно в последние годы, проводятся весьма интенсивные и крупномасштабные исследования и разработки.

Доктрина информационной безопасности Российской Федерации принятая 9 сентября 2000 года определяет совокупность взглядов на «цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации» и служит основой для «подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации». В пункте «Основные функции системы обеспечения информационной безопасности Российской Федерации» определено, что «основными функциями системы обеспечения информационной безопасности Российской Федерации являются:

- разработка нормативной правовой базы в области обеспечения информационной безопасности Российской Федерации и др.» [2].

Кроме того, «Сложившееся положение дел в области обеспечения информационной безопасности Российской Федерации требует безотлагательного решения таких задач, как:

разработка современных методов и средств защиты информации, обеспечения безопасности информационных технологий, и прежде всего используемых в системах управления войсками и оружием, экологически опасными и экономически важными производствами» [2].

Анализируя результаты проведенных научных исследований и разработок в области обеспечения информационной безопасности, следует отметить, что важным достижением теоретического характера на предшествующем этапе явились научные разработки новых средств защиты (технических, программно-аппаратных, криптографических и правовых) и способов построения на их основе комплексных механизмов и систем защиты. Результаты этих разработок достаточно представительно опубликованы в различных изданиях (и прежде всего на страницах журнала «Безопасность информационных технологий», «Вестник компьютерных и информационных технологий», «Компьютерра»). В последние годы стали появляться публикации монографического характера.

В настоящее время на базе анализа множества предпосылок доказана объективная необходимость перехода от экстенсивных к интенсивным способам обеспечения информационной безопасности. В частности, дальнейшее совершенствование теории защиты связано с учетом новых обстоятельств, характерных для современного периода развития информатизации общества [94]. Все большую актуальность приобретает не только защита информации, но и защита людей и технических (главным образом,

электронных) систем от разрушающего воздействия информации, формируется задача обеспечения информационной безопасности как органической совокупности задач защиты информации и защиты от информации.

Регулярное использование автоматизированных технологий обработки информации повысило значимость обеспечения требуемого качества информации. Причем с течением времени актуальность данной задачи возрастает, а сама задача усложняется.

Одним из серьезных достижений современной информатики следует признать разработку профессором В.А. Герасименко концепции информационного кадастра как высокоорганизованной совокупности данных, необходимых для эффективной деятельности соответствующего объекта. Концепция информационного кадастра является ядром более общей концепции информационного обеспечения деятельности объектов. При этом, естественно, должны быть учтены и все задачи защиты информации, защиты от информации и обеспечения качества информации, которые необходимо решать как при формировании информационного кадастра, так и при его поддержке и использовании. Возникает обобщенное понятие управления информацией, объединяющее все упоминавшиеся выше понятия.

Углубленное изучение проблемы совершенствования научно-методологического базиса теории обеспечения информационной безопасности привело к выводу, что уже в настоящее время (а тем более в перспективе) решение проблем защиты вне органической связи с решением более общих проблем может привести к неадекватным результатам и должно вестись с использованием иных (по сравнению с прежними) более интенсивных подходов. Все это говорит о необходимости обобщения накопленного опыта теоретических исследований и практического решения задач защиты информации в целях формирования на этой основе научно-методологического базиса защиты как краеугольного камня интенсификации процессов обеспечения информационной безопасности.

Сегодня можно выделить следующие наиболее острые проблемы развития теории и практики обеспечения информационной безопасности [105]:

- создание теоретических основ и формирование научно-методологического базиса, позволяющих адекватно описывать процессы в условиях значительной неопределенности и непредсказуемости проявления дестабилизирующих факторов (информационных угроз);
- разработка научно обоснованных нормативно-методических документов по обеспечению информационной безопасности на базе исследования и классификации угроз информации и выработки стандартов требований к защите;
- стандартизация подходов к созданию систем обеспечения информационной безопасности и рационализация схем и структур управления

защитой на объектовом, региональном и государственном уровнях с учетом правовых и психологических аспектов данной проблематики.

- методика расчета экономической целесообразности с учетом не только количественных, но и качественных показателей;
- анализ целесообразности использования систем обеспечения информационной безопасности с учетом связки «затраты – экономический эффект»;
- общие принципы взаимозависимости экономической целесообразности построения систем обеспечения информационной безопасности с учетом синергетической составляющей.

Решение спектра перечисленных задач имеет важное значение для реализации положений Доктрины информационной безопасности и Концепции национальной безопасности Российской Федерации.

В настоящее время с полной уверенностью можно говорить о том, что общественные отношения в сфере использования информационных технологий в России затрагивают многие стороны жизни современного общества. Информационные технологии широко используются в промышленности, торговле, в научно-исследовательской и во многих других сферах деятельности. Вместе с тем, слабая защищенность, недостаточная эффективность существующих методов и способов защиты компьютерной информации при эксплуатации информационно-телекоммуникационных сетей вызывает повышенный интерес у криминальных элементов, в целях противоправного завладения информацией для совершения различных видов неправомерных действий.

Глава 1. Информация как объект преступных посягательств в сетях передачи данных

Современный период развития общества характеризуется периодом перехода от индустриального общества к обществу информационному. Повсеместное внедрение информационных технологий создало новые возможности для активного и эффективного развития экономики, государства, общества и гражданина. Информация, а равно и процессы, связанные с ее сбором, обработкой и хранением, являются неизменным атрибутом социальной деятельности.

Информационная система может быть представлена как организованная совокупность сведений реализующихся в виде целостного, организационного и технически обеспеченного комплекса информационных процессов. Информационная система предназначена для сбора, передачи, обработки хранения и выдачи информации по запросам. Исходя из этого, необходимо вести разговор не только об информации, циркулирующей в информационно-телекоммуникационных сетях, но и проводить анализ сетевой коммуникации, посредством которой происходит обмен данными.

1.1. Информация и ее составляющие в телекоммуникационных системах

Важность точного представления о свойствах и содержании информации как феномене, над которым осуществляются разнообразные действия в информационной сфере, трудно переоценить, так как она является основным объектом правоотношений в информационной сфере.

Информация (от лат. Informatio), первоначально — сведения, передаваемые одними людьми другим людям устным, письменным или каким-либо другим способом (например, с помощью условных сигналов, с использованием технических средств и т. д.), а также сам процесс передачи или получения этих сведений [64].

В связи с тем, что информация всегда играла в жизни человечества очень важную роль, возникла потребность в научном подходе для выявления её наиболее характерных свойств, вследствие чего возникли два принципиальных изменения в трактовке понятия «информация». Во-первых, оно было расширено и включило обмен сведениями не только между человеком и человеком, но также между человеком и автоматом, автоматом и автоматом; обмен сигналами в животном и растительном мире. Передачу признаков от клетки к клетке и от организма к организму также стали рассматривать как передачу информации. Во-вторых, была предложена количественная мера информации, что привело к созданию теории информации.

С философской точки зрения понятие «информация» определил Н. Винер: «Это не энергия и не материя» [25]. Кроме того, он предложил «информационное видение» кибернетики, как науки об управлении в живых организмах и технических системах. Под информацией стали понимать уже не просто сведения, а те сведения, которые являются новыми и полезными для принятия решения, обеспечивающего достижение цели управления. Остальные сведения не считались информацией.

В.В. Крылов считает, что термин «информация» может интерпретироваться и как совокупность формализованных сведений (знаний), предназначенных для передачи в качестве сообщения [44]. Понимая под «сообщением» активные волевые действия лица по передаче информации вовне, под «знанием» упорядоченное мысленное представление о конкретном объекте, факте (или их совокупности), о способах его (их) взаимодействия и взаимосвязи с другими объектами, фактами, поддающееся описанию, приему и передаче формальным (вербальным или символьным) образом, превращаясь в «сообщение».

Анализируя информацию нельзя говорить о ней вообще, неконкретно. Предметом рассмотрения должна быть в первую очередь информация, которая находится в гражданском, административном или ином общест-

венном обороте и по поводу которой или в связи с которой возникают общественные отношения подлежащие регулированию правом.

Информация – специфический атрибут объективного мира, создающий условия, необходимые для обеспечения устойчивости и развития систем различной природы [59]. Виды информации обеспечивающей достижение целей системы зависят от сложности самой системы и используемых предметных областей. Содержания понятия информации для различных предметных областей можно увидеть в представленной таблице 1.1 [59].

Таблица 1.1

Предметные аспекты содержания информации				
Философский	Управленческий	Технический	Экономический	Информационный
1. Информация как одна из реальностей объективного мира. 2. Происхождение и сущность информации 3. Информация как мера сущностей объективного мира.	1. Информация как непременный атрибут всякого управления. 2. Информационные процессы как основное содержание управления	1. Информация как совокупность символов зафиксированных на носителях. 2. Проблемы сбора, хранения, передачи, переработки информации	1. Информация как совокупность сведений о социально-экономических процессах. 2. Информационные процессы как основное содержание управления коллективами людей в производственной и непроизводственной сферах. 3. Сопровождает процессы производства, распределения, обмена и потребления материальных благ и услуг.	1. Информация как важнейший атрибут жизнедеятельности личности, общества, государства. 2. Проблемы определения информационных потребностей. 3. Проблемы рационализации информационных процессов. 4. Проблемы информационного обеспечения деятельности личности, общества, государства.

Законодатель в Федеральном законе «Об информации, информационных технологиях и защите информации», в котором регулируются отношения по формированию и использованию большей части информационных ресурсов, так определил данное понятие: «информация - сведения (сообщения, данные) независимо от формы их представления» [5].

Кроме того, необходимо определить понятие компьютерная информация, которое удачно сформулировано В.В. Крыловым. Он пишет: «Компьютерная информация есть сведения, знания или набор команд (программ), предназначенных для использования в ЭВМ или управления ею, находящиеся в ЭВМ или на машинных носителях, — идентифицируемый элемент информационной системы, имеющей собственника, установившего правила ее использования» [44].

С учетом социального аспекта к рассматриваемому объекту целесообразно добавить информацию, участвующую в обороте, в виде понятном для восприятия пользователем. В этом случае появляется возможность не включать программы для электронных вычислительных машин (ЭВМ, компьютеров), являющиеся средствами обеспечения ЭВМ, в понятие информация.

Информационные процессы, связанные с созданием, преобразованием и потреблением, особенно и использованием современных средств телекоммуникации и средств связи, порождают проблемы информационной безопасности (а точнее, безопасности в информационной сфере). Использование средств защиты позволяет не только предотвратить случаи неправомерного доступа, оказывающие негативное влияние на информационные права и свободы граждан, но и защитить общество и государство от воздействия «недоброкачественной» информации.

Во все времена стоял вопрос об эффективности протекания информационных процессов, адекватной передаче и хранении накопленных человечеством знаний, которые несут в себе определенный объем информации. По мере развития общества объем информации постоянно увеличивался.

Развитие человечества сопровождалось ростом объема накопленных знаний и сведений, как о самом человеке, так и об окружающем его мире. Начиная с начала XX в. темпы роста информации резко возросли. Так, если в XIX в. общая сумма человеческих знаний удваивалась через каждые 50 лет, то к 1950 г. — через 10 лет, а к 1970 г. — через каждые 5 лет [28].

Информация ценна, но довольно часто это носит субъективный характер, так как она важна для человека, который хочет ее сохранить. Ценность состоит в том, что значительная доля каждой сферы деятельности посвящена сбору, управлению, сортировке и хранению информации, при этом необходимо обеспечить ее истинность и объективность.

В начале XX века Р. Хартли в своей работе «Transmission of Information» определил меру количества информации для равновероятных событий [76], а уже середине XX столетия К. Шенноном и У. Уивером были предложены вероятностные методы для определения количества передаваемой информации. Однако такие вероятностные методы описывают лишь знаковую структуру информации и не затрагивают смысла, заложенного в ней [64]. В тоже время уже много лет развивается семантическая теория информации, которая изучает смысл, содержащийся в сведениях, полезность и ценность этих сведений для потребителя. Существенным становится субъективный подход, основанный и на априорной подготовленности субъекта к восприятию таких сведений или сообщений, и с их новизной для субъекта, а также полезностью (или ценностью) для принятия им решений, направленных на достижение поставленных целей.

Изобретение микропроцессорной техники привело к революционным изменениям информационной технологии. Помимо того, что ЭВМ является главным средством автоматизации физического и умственного труда, совершенствования управления в социальной и экономической сферах, компьютер посредством безбумажного способа ведения делопроизводства, возникновения электронной почты, создания и развития компьютерных сетей, машинной графики, использования оптических дисков и изобретения нетрадиционного безнаборного способа печати, объединяет существовавшие ранее отдельно друг от друга составляющие информационных ресурсов, придавая им невиданную гибкость и взаимозаменяемость.

Не смотря на то, что информация подразделяется на предметные области и сферы, это разделение условно, поскольку они не взаимосвязаны между собой. Исходная информация создается, базируясь на данных из информационных ресурсов, производной информации и, естественно, под воздействием окружающей среды. Информационные ресурсы являются базой ретроспективной информации и формируются на основе исходной и производной информации. В свою очередь, производная информация основывается на исходной информации и сведениях из информационных ресурсов. В результате процесса обработки создаются новая исходная документированная информация и допрлняются информационные ресурсы. Таким образом, можно отобразить процессы циркуляции информации в информационной сфере. С учетом современного уровня развития общества можно говорить о такой важной составляющей рассматриваемого процесса циркуляции, как информационное обеспечение.

Информационное обеспечение – совокупность единой системы классификации и кодирования информации, унифицированных систем документации, схем информационных потоков, циркулирующих в организации, а также методология построения баз данных [62].

Технологию информационного обеспечения можно рассматривать не только как совокупность методов и технических средств сбора и обработки информации, но и как организацию доступа к интегрированным информационным банкам и базам данных. В них накапливается информация, используемая при планировании и проведении различных мероприятий. Отсюда можно сделать вывод о важности своевременного получения информации, что привело к появлению такого свойства как оперативность.

Кроме того, в современном обществе остро стоит вопрос о документировании тех или иных данных. Законодатель в Федеральном законе «Об информации, информационных технологиях и защите информации» вводит термин «документированная информация» и определяет его как «зафиксированную на материальном носителе путем документирования информацию с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель» [5].

Следовательно, говоря о «документированной информации» необходимо учитывать ее базирование на двуединстве непосредственно сведений (данных) и материального носителя, где она может отображаться символами, буквами или другими способами. То есть, происходит материализация сведений, которые фиксируются на материальном носителе, прикрепляются к нему и обособляются от автора.

Отсюда можно сделать вывод, что информация в виде электронного документа будет подходить под понятие документированная информация, если ее закрепить на компьютерном носителе и снабдить реквизитами, позволяющими ее идентифицировать. С внедрением новых информационных технологий вместо бумаги в качестве материальных носителей стали использоваться машиночитаемые носители – магнитные и оптические диски, память ЭВМ. Информация в компьютере может находиться в трех местах: в оперативной памяти (ОЗУ), постоянной памяти (ПЗУ, чаще это устройство называют «жесткий диск») и на внешних носителях машинной информации (компакт-диски, оптические диски, FLASH-носители и т.д.). ОЗУ не подходит для фиксирования информации потому, что после выключения компьютера она полностью стирается. На жестком диске или внешнем носителе информация может храниться долго, но ее, в отличие от зафиксированной на бумажном носителе, легко удалить, модифицировать или скопировать в результате неправомерного доступа постороннего лица.

К компьютерной информации не имеет смысла применять глагол «зафиксировать», скорее ее можно «сохранить на компьютерном носителе информации», но эта сторона не принципиальная, важнее определить, с помощью каких реквизитов, возможно, ее идентифицировать. Существующие на данный момент реквизиты электронных документов, такие как «название», «дата создания», «владелец», «объем» и «атрибуты», которые могут быть легко изменены или подделаны «без следов», не позволяют идентифицировать информацию. Зафиксировать компьютерную информацию – это распечатать на принтере, но тогда она перестанет быть компьютерной.

Для установления доказательственной силы машиночитаемого документа или документированной информации необходим такой механизм записи информации на магнитном диске, который, с одной стороны, исключал бы возможность неправомерного доступа постороннего лица с целью искажения или подделки, а с другой – позволял бы конкретному лицу ставить на этом документе некоторую отметку, аналогично его подписи на бумаге, которую было бы невозможно подделать, а экспертиза могла бы надежно подтвердить принадлежность такой отметки – подписи данному лицу.

С целью выполнения поставленных условий появилась «электронная цифровая подпись», которая посредством программно-аппаратного комплекса обеспечивает надежное подтверждение оригинальности сведений,

реквизитов документа и факта его подписания конкретным лицом. Федеральный закон «Об электронной цифровой подписи» дает следующее определение:

Электронная цифровая подпись - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе [10].

Все это направлено на обеспечение надежного и эффективного протекания информационных отношений. За глобальную составляющую информационных отношений возьмем термин «компьютерная информация», под которой будем понимать всю информацию, циркулирующую на компьютере и вычислительной сети. Не смотря на то, что это утверждение на первый взгляд несколько конфликтует с определением компьютерной информации, но будет правильным считать именно так из-за двойственности самой информации на компьютере. Например, программное обеспечение также является компьютерной информацией. Это правильно подметил В.В. Крылов определивший, что программа для ЭВМ: …с одной стороны, служит инструментом воздействия на информацию; с другой стороны, сама как совокупность команд и данных является информацией [44]. К тому же программное обеспечение, как обеспечивающее правильную работу компьютерной техники, также может быть предметом преступного воздействия. Итак, будем считать, что предмет преступного посягательства преступлений в сфере компьютерной информации должен выглядеть так:

- Компьютерная информация - вся информация, циркулирующая на компьютере или в вычислительной сети, как записанная на машинных носителях, так и загруженная в оперативную память компьютера.

- Информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах, циркулирующая на компьютере и вычислительной сети.

В связи с широким проникновением во все сферы человеческой деятельности современных информационных технологий назрела острая необходимость не только в научном осмыслении последствий их создания и практического использования, но и в содержательном анализе проблем, возникающих в сфере информатизации общества и обеспечения информационной безопасности.

В основе производства, распространения, преобразования и потребления информации лежат информационные процессы – создания, сбора, обработки, накопления, хранения, поиска, получения, распространения и потребления информации в государстве и обществе, а также процессы создания и применения информационных систем, информационных техноло-

гий и средств их обеспечения, средств и механизмов информационной безопасности. Социальные (общественные) отношения, подлежащие правовому регулированию, возникают при выполнении именно этих информационных процессов. Такие общественные отношения называют информационными отношениями, а деятельность по осуществлению и обеспечению информационных процессов – информационной деятельностью.

Результатом бурных информационных процессов, охватывающих все сферы общественных и производственных отношений, является постепенный переход развитых стран мира к постиндустриальному «информационному обществу», которое характеризуется изобилием циркулирующей по коммуникационным каналам связи информации, а также наличием всех необходимых средств для ее хранения, передачи, обработки, использования и защиты.

Процесс формирования информационного общества в каждой стране происходит от какого-то начального рубежа и основывается на сложившихся политических, культурных и социально-экономических условий. В свою очередь, необходимо указать, сто современное общественное развитие рассматривается как информационное пространство, к основным компонентам которого можно отнести:

- информационные ресурсы, хранящиеся в базах данных и логических средствах управления ими;
- развитость телекоммуникационной инфраструктуры, и, как следствие, взаимодействие со всемирными информационными сетями;
- систему массовой информации.

В последнее время протекает процесс перехода общества от индустриального к информационному и, как следствие, мир переживает информационный бум. Процесс текущего развития можно охарактеризовать такими тенденциями как глобализация и развитие информационных технологий, что превращает информацию в стратегический ресурс, а также, инструмент управления и власти.

В жизни современного общества происходят существенные изменения, связанные с успехами внедрения информационных технологий в повседневную жизнь. Определенная информация, управляющая практически каждым компонентом цивилизации, объединяется в информационные потоки, которые, в свою очередь, образуют информационные процессы. То есть, информация о практически любом человеке практически постоянно собирается, обобщается и пересылается по назначению.

Серьезные изменения в развитии общества происходят на фоне научно-технической революции, в процессе протекании которой возникали, накаливались и использовались информационные ресурсы. При этом, следует отметить, что они коренным образом отличаются от природных, сырьевых и других ресурсов, которые традиционно используются человечеством в ходе развития. В настоящее время информационные ресурсы

становятся национальным богатством, а экономическая мощь страны зачастую определяется эффективностью их промышленного использования.

Информационные ресурсы можно охарактеризовать рядом отличительных черт к основным из которых целесообразно отнести:

- непотребляемость и подверженность моральному износу;
- нематериальность, то есть они не могут быть отнесены к физическому носителю;
- экономия средств, так как использование информационных ресурсов позволяет значительно сократить потребление сырьевых, энергетических и других ресурсов;
- циркуляция, то есть создание и использование осуществляется с помощью средств вычислительной техники.

Сегодня любое информационное подразделение является элементом системы обеспечения безопасности государства и, следовательно, владеет информацией (секретной, служебной, конфиденциальной), подлежащей защите. Объем подобной информации огромен и поэтому в интересах информационных подразделений создаются специализированные банки данных с целью информационного обеспечения деятельности. Средний объем одного интегрированного банка данных регионального уровня составляет до 3-4 миллионов документов. Такой объем информации требует автоматизации системы обеспечения повседневной деятельности.

Постоянное совершенствование информационного обеспечения требует расширения сфер применения систем информатики, их использования на всех стадиях интеграции систем в информационно-вычислительные сети и обеспечения их взаимодействия с системами других государственных органов.

Внедрение информационных технологий создало новые возможности для ускорения и повышения эффективности информационных процессов, повысило качество информационного обслуживания, и по сути дела совершила революцию в информационной коммуникации. Были созданы новые материальные носители информации, существенно отличавшиеся от существовавших, новые механизмы ее тиражирования и распространения, что, в свою очередь, повлекло за собой возникновение новых отношений, связанных с особенностями автоматизированной обработки информации.

Интегрированные банки данных являются объективной потребностью и обусловлены необходимостью комплексного решения проблемы совершенствования информационного обеспечения повседневной деятельности.

Совместное функционирование в рамках единой информационной вычислительной сети интегрированных банков данных общего пользования разных уровней управления призвано обеспечить единство информационной поддержки основных стадий развития и становления информационного общества.

Практика показывает, что создание условий для более эффективного использования информационных ресурсов позволяет существенного повысить информированность каждого работника. Информационные массивы регионального, федерального и межгосударственного уровня зачастую используются в виде «электронного досье», при этом данные об объекте содержатся в виде основных установочных данных и, конечно, их целесообразно использовать в справочном режиме. В этом случае в результате запроса к банку данных он, по совокупности признаков, предоставляет точную и компетентную информацию об объекте учета. В результате происходит значительное сокращение времени в связи с сужением направления поиска информации, что практически невыполнимо при ручном ведении учетов.

При использовании банков данных необходимо применять все традиционные и нетрадиционные режимы хранения и обработки информации. Реализация подобных режимов должна основываться на использовании специальных систем безопасности. Одной из основных задач подобных систем (охранных, сигнальных, сторожевых запросов и т.д.) заключается в автоматическом фиксировании и обобщении различных фактов, в том числе криминогенных. Таким образом, программное обеспечение, установленное на персональном компьютере, должно самостоятельно, без вмешательства оператора, выявлять совокупность фактов и автоматически их фиксировать с последующим извещением пользователя о результатах. В частности, используемой сигнальной системе целесообразно работать в таких основных режимах, как:

- контроль за циркуляцией информации;
- постоянный поиск новых фактов, которые могут корректировать уже имеющуюся информацию.

Но, кроме того, эта система должна обеспечивать регистрацию обращений за информацией и таким образом позволять:

а) выявлять возможные каналы утечки информации или попытки модифицировать (удалить) информацию;

б) активизировать надзорно-профилактическую деятельность.

Данные, хранящиеся в информационных системах («Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств» [5]), довольно часто связаны с информацией, которая отнесена к различным видам тайн, то есть является информацией ограниченного доступа.

Порядок обращения с подобными данными ориентирован на бумажные носители, несмотря на то, что все больший объем сведений переносится в компьютерную среду. Порядок допуска к данной информации законодательно не определен и, следовательно, наиболее оптимально приблизить

организацию защиты подобных сведений к уровню защиты государственной тайны, в тех случаях, когда это возможно.

Прогресс в области информационных технологий привел к тому, что в развитых странах начала формироваться информационная среда, основными элементами которой являются банки данных, информационные сети и системы. Характерной особенностью этой среды является усиление интеграционных тенденций.

Современная ситуация в сфере применения информационных технологий характеризуется наличием:

- информационно-вычислительных сетей, программное обеспечение которых подвержено поражению вредоносными программами;
- различных групп пользователей, объединенных в рамках этих сетей, интересы которых могут быть прямо противоположными, а действия трудно поддающимися контролю;
- информационно-вычислительной среды, в которой злоумышленники могут действовать в интересах различных преступных групп.

Необходимость борьбы с незаконными деяниями в области вычислительных сетей во многом обусловлена стремительным развитием научно-технического прогресса. Глобальная компьютеризация современного общества, затрагивающая практически все стороны деятельности людей, предприятий и организаций, государства породила новую сферу общественных отношений, которая, к сожалению, нередко становится объектом противоправных действий.

Применение современных информационных технологий вызвало негативные последствия – появление новых видов преступлений (компьютерных), ранее не известных праву, основанных, прежде всего, на возможностях неправомерного доступа к информации.

Практика борьбы с преступлениями в сфере компьютерной информации весьма невелика, поскольку информационные технологии стали внедрятся в повседневную жизнь сравнительно недавно. Не смотря на это, общественная опасность преступных посягательств в указанной сфере становится все более очевидной.

Преступления в сфере компьютерной информации чрезвычайно Разнообразны и подразделяются на несколько сегментов, в числе которых одно из основных мест занимает понятие «компьютерное преступление». В качестве примеров подобных видов преступлений можно привести следующие:

- неправомерный доступ к информации, хранящейся на рабочей станции;
- создание и распространение вредоносного программного обеспечения, задача которого заключается в порче или выведении из строя программного или аппаратного обеспечения рабочей станции и т.д.;
- кража компьютерной информации.

Необходимо учитывать, что объектами преступных посягательств могут являться как сами технические средства (рабочие станции, периферийное оборудование, каналы связи), так и программное обеспечение или информационные ресурсы.

Существующие в настоящее время меры противодействия преступлениям в сфере компьютерной информации можно подразделить на: технические, организационные и правовые.

К техническим мерам можно отнести защиту от неправомерного доступа, резервирование важных компонентов вычислительной сети, принятие конструкционных мер защиты от хищений и диверсий, обеспечение резервным электропитанием, разработку и реализацию специальных программных и аппаратных комплексов безопасности и многое другое. Средств технического обеспечения информационной безопасности, в настоящее время, существует достаточное количество, и они постоянно модернизируются.

К организационным мерам относятся охрана вычислительных сетей, подбор персонала, исключение случаев проведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра после выхода его из строя, универсальность средств защиты от всех пользователей (включая высшее руководство), возложение ответственности на лиц, которые должны обеспечить безопасность центра, выбор места расположения центра и т.п. Все эти вопросы рассматривались и рассматриваются в федеральном законодательстве, местных нормативных правовых актах, кроме этого существуют внутриведомственные нормативные документы.

К правовым мерам следует отнести разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства. К правовым мерам относятся также вопросы общественного контроля за разработчиками программного обеспечения, компонентов вычислительных сетей и принятие соответствующих международных нормативных правовых актов. Только в последние годы появились работы по проблемам правовой борьбы с преступлениями в сфере компьютерной информации, и относительно недавно отечественное законодательство встало на путь борьбы с компьютерной преступностью. Поэтому, представляется весьма важным расширить правовую и законодательную информированность специалистов и должностных лиц, заинтересованных в борьбе с преступлениями в сфере компьютерной информации.

В мире и нашей стране техническим и организационным вопросам посвящено большое количество научных исследований и технических изысканий. Что касается правовой защиты информации, то до сравнительно недавнего времени, а именно до 1 января 1997 года, даты вступления в

действие нового Уголовного Кодекса Российской Федерации (УК РФ) [3], в России отсутствовала возможность эффективно бороться с преступлениями в сфере компьютерной информации. Несмотря на явную общественную опасность, данные посягательства не были противозаконными, т.е. они не упоминались нашим уголовным законодательством. Хотя, еще до принятия нового УК в России была осознана необходимость правовой борьбы с преступлениями в сфере компьютерной информации, был принят ряд законов, которые внесли правовую определенность в явление компьютеризации нашего общества вообще и проблему компьютерной преступности в частности и вместе с другими правовыми актами сформировали пласт, именуемый «законодательством в сфере информатизации», охватывающий в настоящее время несколько сотен нормативно-правовых актов [23].

Непосредственно законодательство России в области информатизации начало формироваться с 1991 года и включало до 1997 года десять основных законов. Это закон «О средствах массовой информации», Патентный закон РФ, закон «О правовой охране топологий интегральных микросхем», закон «О правовой охране программ для электронных вычислительных машин и баз данных», Основы законодательства об Архивном фонде РФ и архивах, закон «Об авторском праве и смежных правах», закон «О государственной тайне», закон «Об обязательном экземпляре документов», закон «О связи», закон «Об информации, информатизации и защите информации» (отменен), закон «Об участии в международном информационном обмене». В данных законах определяются основные термины и понятия в области компьютерной информации (например, такие как компьютерная информация, программа для ЭВМ, ЭВМ (компьютер), сеть ЭВМ, база данных), регулируются вопросы ее распространения, охраны авторских прав, имущественные и неимущественные отношения, возникающие в связи с созданием, правовой охраной и использованием программного обеспечения и новых информационных технологий. Также осуществлено законодательное раскрытие понятий информационной безопасности и международного информационного обмена [23].

Таким образом, до 1 января 1997 года на уровне действующего законодательства России можно было считать в достаточной степени урегулированными вопросы охраны исключительных прав и частично защиту информации (в рамках государственной тайны). Не получили достойного отражения в законодательстве права граждан на доступ к информации и защита информации, т.е. то, что напрямую связано с преступлениями в сфере компьютерной информации.

Часть указанных пробелов в общественных отношениях в области компьютерной информации была ликвидирована после введения в действие с 1 января 1997 года нового Уголовного Кодекса, принятого Государственной Думой 24 мая 1996 года. Сведения по данным вопросам изложе-

ны в главе 28 «Преступления в сфере компьютерной информации», содержащей три статьи №№ 272 «Неправомерный доступ к компьютерной информации», 273 «Создание, использование и распространение вредоносных программ для ЭВМ», 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» [23].

Уголовно-правовая защита компьютерной информации в российском уголовном законодательстве введена впервые. Ранее в этих законах предусмотрен комплекс мер по защите ЭВМ, баз данных, сетей и в целом компьютерной информации. В ст. 20 Закона «О правовой охране программ для электронно-вычислительных машин и баз данных» от 23 сентября 1992 г. содержалось положение о том, что выпуск под своим именем чужой программы для ЭВМ или базы данных либо незаконное воспроизведение или распространение таких произведений влечет за собой уголовную ответственность в соответствии с законом. Однако соответствующие уголовно-правовые нормы тогда не были приняты. Очевидно, посчитали достаточной ст. 141 УК РСФСР, хотя она ответственности за упомянутые деяния не предусматривала.

Включение ст.ст. 272, 273 и 274 УК, в раздел о преступлениях, посягающих на общественную безопасность и общественный порядок, определяет объект рассматриваемых преступлений. Но это был бы слишком общий подход. Конкретно эти преступления направлены против той части установленного порядка общественных отношений, который регулирует изготовление, использование, распространение и защиту компьютерной информации. Выяснение данного обстоятельства важно для того, чтобы отграничить преступления, предусмотренные ст.ст. 272 – 274 УК, от других преступлений, связанных с использованием ЭВМ, системы ЭВМ и их сети для совершения других преступлений.

Предметом правонарушений в сфере компьютерной информации является непосредственно компьютерная информация, ЭВМ или их сеть.

1.2. Процессы информационного обмена в телекоммуникационных сетях

Появившейся сравнительно недавно высокоэффективный способ обмена информацией между пользователями возник благодаря повсеместному развитию и внедрению сетей передачи данных. В период своего возникновения они использовались, в основном, для проведения научных исследований и повышения обороноспособности страны, а затем уже стали проникать во все сферы деятельности человечества. Решая задачи отдельных групп пользователей они существовали обособлено и независимо, а для решения конкретных задач выбиралось соответствующие аппаратное и программное обеспечение. Существовавшее типовое аппаратное обеспечение просто не позволяло построить универсальную вычислительную сеть для удовлетворения потребностей потенциальных пользователей. Связано это с тем, что одним необходима высокая скорость обмена данными в пределах здания, а другим обеспечение надежного соединения на значительные расстояния. Для решения этих задач, в последствии, появилась идея объединения существовавших вычислительных сетей в глобальную вычислительную сеть. Соединение рабочих станций, в этом случае, происходило бы на физическом уровне с использованием определенного набора специальных «соглашений» или протоколов. Под протоколом, обычно, понимаются правила, согласно которым функционирует вычислительная сеть.

Целый ряд правительственных организаций США стали работать в этом направлении, осознавая важность и необходимость создания крупных локальных вычислительных сетей и, создания на их основе, глобальной вычислительной сети. Агентство Defense Advanced Research Projects Agency (DARPA) добилось наибольшего успеха, создав стек протоколов TCP/IP. В настоящее время данный протокол, возникший как проект объединения нескольких исследовательских организаций, стал наиболее популярным для обеспечения сетевого взаимодействия, а также, стандартом для реализации глобальных сетевых соединений.

DARPA начало работу над созданием глобальной вычислительной сети середине 70-х годов, а уже в 1977-1979 гг. протоколы TCP/IP приобрели современный вид и была разработана ее структура. К этому времени агентство DARPA уже стало одним из лидеров в исследовании и разработке сетей с коммутацией пакетов и реализовало немало новых идей в этой области в своей сети ARPANET. Бурное развитие разнообразных сетевых технологий, в том числе беспроводных радиосетей и спутниковых каналов связи, стимулировало активность DARPA в исследовании проблем межсетевого взаимодействия и реализации принципов internet в ARPANET [39, 51,68].

В процессе своей работы DARPA не пыталось обеспечивать тайну своей деятельности и, поэтому, рабочие группы, занимавшиеся данной проблематикой, активно интересовались процессом исследования. Особенно это касалось тех, кто уже имел опыт использования принципов коммутации пакетов в сети ARPANET. По инициативе агентства было проведено несколько неформальных встреч, на которых была предоставлена возможность всем заинтересованным лицам провести обмен новыми идеями и обсудить результаты. В результате, в создание протокола TCP/IP были вовлечены значительные силы, результатом чего стало создание неформального комитета для координации и руководства процессом разработки протоколов и архитектуры сети Internet. Данная группа, существовавшая до 1983 г., получила название Internet Control and Configuration Board (ICCB).

Время зарождения «Всемирной паутины» (WWW), как еще называют глобальную вычислительную сеть, относится к началу 80-х гг., а окончательный переход к данной технологии произошел в 1983 году. В этот период по инициативе DARPA начали перевод вычислительных машин своих вычислительных сетей на использование стека TCP/IP. Для многочисленных экспериментов с TCP/IP использовалась ARPANET, которая, на тот момент, уже являлась магистральной сетью Internet. При этом она была разбита на такие независимые части как:

- ARPANET, предназначенная для исследовательских целей;
- MILNET, предназначенная для обеспечения военных коммуникаций.

DARPA обеспечило реализацию TCP/IP, предлагая ее за низкую цену, что стимулировало адаптацию и использование новых протоколов в университетских кругах. В этот период основная масса подразделений институтов, занимавшихся исследования в области средств вычислительной техники, использовали различные версии операционной системы (ОС) Unix от Berkeley Software Distribution (Berkeley Unix, или BSD Unix) университета штата Калифорния в Беркли. DARPA, в результате своей деятельности добилось того, что большинство подразделений университетов адаптировали для себя новую сетевую технологию. Это стало возможным после субсидирования компании Bolt Beranek and Newman (BBN), которая реализовывала протоколы TCP/IP для использования вместе с Unix. Общим стандартом для реализации модификаций протокола TCP/IP стала версия BSD, приобретшая свою популярность благодаря большим возможностям по сравнению с базовыми internet-протоколами. Помимо стандартных прикладных программ TCP/IP, BSD предоставляет набор сетевых утилит, сходных с Unix-службами, используемыми на автономном компьютере. Сейчас поддержку разных модификаций протокола TCP/IP встраивают в свои операционные системы компании-разработчики, а многие независимые поставщики работают над продуктами обеспечивающими рас-

ширение возможностей TCP/IP. К подобным возможностям можно отнести поддержку интерактивных приложений, электронную и голосовую почту, средства коллективной работы и, конечно, средства обеспечения информационной безопасности.

В результате развития средств вычислительной техники научные исследования в области сетевых коммуникаций становятся критически важной составляющей с начала 80-х годов XX века. В результате, National Science Foundation стало принимать активное участие в процессе популяризации и внедрения вычислительных сетей, при этом основная задача заключалась в популяризации и доступности протокола TCP/IP для максимального числа исследовательских организаций. С 1985 г. NSF реализовывала программу создания сетей вокруг шести своих суперкомпьютерных центров. В 1986 г. была создана магистральная сеть NSFNET, которая в конце концов, объединила все эти центры и связала их с ARPANET [51,68].

В настоящее время глобальная вычислительная сеть объединяет множество мелких сетей по всему миру, а к ней кроме научных институтов подключаются различные компании и крупные корпорации нефтяной, автомобильной и электронной индустрии, не остались в стороне и телефонные компании. Internet уже приник практически во все сферы жизнедеятельности, и некоторые всерьез говорят о том влиянии, которое оказывает всемирная сеть на мировоззрение и восприятие каждого человека. Не стоит оставлять без внимания, что многие организации используют протокол TCP/IP для построения своих локальных и региональных вычислительных сетей, не имеющих подключения к Internet.

Глобальная вычислительная сеть строится посредством объединения различных физических сетей, рабочие станции которых используют одну из таких технологий как Ethernet, Token Ring, FDDI, ISDN, а также соединение типа «точка-точка». В последние годы к этому списку присоединилась сеть ATM и, конечно, современные беспроводные технологии. В стык между используемыми прикладными системами и способами коммутации, в зависимости от физических сетей, встраивалось специальное программное обеспечение, функции которого заключались в обеспечении соединения различных компонентов друг с другом. При этом пользователю предоставляется возможность работать в крупной вычислительной сети, не зная процедуры и детали соединения. Подобный способ соединения, в последующем, получил название internet. Следует обратить внимание на тот факт, что для обеспечения процесса соединения вычислительных сетей используются маршрутизаторы (routers), которые передают пакеты между рабочими станциями различных сетей соединенных на физическом уровне с использованием специального программного обеспечения.

Современная глобальная вычислительная сеть не обязывает для подключения использовать конкретное межсетевое соединение или топологию и, следовательно, подключение новых рабочих станций не подразумевает

необходимость прямого физического соединения со всеми компьютерами, уже подключенными к сети или подсоединения к некоей центральной точке коммутации. Используемый маршрутизатор, основываясь на адресе и знании топологии сети, передает отправляемый пакет по конкретному адресу используя тот или иной маршрут. Объясняется это тем, что каждая рабочая станция имеет конкретный универсальный идентификатор (IP-адрес) позволяющий компьютерам, даже находясь на значительном удалении, взаимодействовать друг с другом. Коме того, благодаря независимости интерфейса пользователя от физической сети появляется достаточнго много способов установления соединений и передачи данных, одинаковых для всех сетевых технологий.

Построение глобальной вычислительной сети основывается на таком фундаментальном принципе, как равнозначность объединенных рабочих станций. То есть, система коммуникаций, как таковая, представляется компонентом сети, при этом отсутствует зависимость от физических параметров, географического масштаба и, конечно, объемов передаваемых пакетов данных [51,68,69].

Серия протоколов TCP/IP обычно предоставляется пользователям бесплатно или за символическую цену, при этом спецификации и реализации протокола общедоступны, что является достаточно ярким примером открытой системы. Благодаря этой особенности практически любой разработчик программного обеспечения может его использовать для взаимодействия в вычислительной сети. Сам по себе, протоколов TCP/IP предоставляет равные возможности для глобальных, региональных и локальных вычислительных сетей и привлекает разработчиков своей масштабируемостью.

Сетевой интерфейс, а особенно его уровень, способствует установлению соединения между компьютерами в любой вычислительной сети, прокол TCP/IP позволяет построить универсальную сеть. Для обеспечения взаимодействия различных устройств в современных программно-аппаратных комплексах используются драйвера, чья установка предусмотрена в операционной системе. В свою очередь, сетевое взаимодействие между устройствами, на основе протокола TCP/IP, организуется с использованием сетевой платы, которая обеспечивает маршрутизацию пакетов, под которыми следует понимать некоторый объем полезной и необходимой информации. Тут следует указать на тот факт, что рассматриваемый протокол отвечает только за передачу данных, но не обеспечивает их гарантированную доставку адресату, то есть направленные пакеты могут быть переданы в неправильном порядке или вообще потеряны полностью или частично. Причина этого кроется в том, что передача происходит без установления соединения, а пакеты обрабатываются независимо друг от друга, хотя именно на этом уровне определяется маршрут пакета.

Для обеспечения надежной передачи пакетов между рабочими станциями был разработан следующий уровень получивший название транспортный, который работает на основе двух основных протоколов TCP и UDP.

Остановимся более подробно на протоколах нижних уровней и обеспечивающих работу приложений типа клиент-сервер. Подобные протоколы занимаются не способами передачи данных, а деталями конкретного приложения. Причина этого кроется в том, что многие детали физических соединений в вычислительных сетях не доступны приложениям, работа которых не зависит от наличия подключения к Ethernet или Token Ring. В целом, между отправителем и адресатом может быть множество маршрутизаторов и различных типов промежуточных физических сетей, но используемое приложение воспринимает этот конгломерат как единую сеть.

Несмотря на то, что TCP/IP называется целый стек протоколов, TCP и IP не являются единственными, хотя и важнейшими, представителями этого семейства. Каждый уровень коммуникаций обслуживается несколькими протоколами [84,51,68,69,70].

Сами по себе протоколы транспортного уровня TCP (Transmission Control Protocol) и UDP (User Datagram Protocol) важны для приложений верхнего уровня как организующие поток данных между конечными системами и, что важно, имеют значительные различия между собой.

Существование сразу двух транспортных протоколов TCP и UDP объясняется предоставлением разных услуг прикладным процессам, хотя основная часть прикладных программ использует только один из них. Выбор типа протокола зависит от потребностей программиста. То есть, при необходимости высокой эффективности на быстрых сетях с короткими соединениями используется протокол UDP, а при необходимости гарантированной доставки по длинному и ненадежному каналу передачи данных используется протокол TCP.

Кроме обеспечения надежной передачи данных между хостами, протокол TCP позволяет устанавливать логическое соединение между клиентом и сервером, а затем использовать его для передачи информационных массивов. Рассматриваемый протокол позволяет выполнять задачи по дроблению информационного потока, получать подтверждение доставки отправленных пакетов и т.д. Использующие TCP приложения могут игнорировать детали передачи, но при этом транспортный протокол будет обеспечивать доставку отправляемой информации.

Еще одним протоколом семейства TCP/IP, достаточно давно используемым в сетях связи, является FTP (File Transfer Protocol) имеющий много версий для различных взаимодействующих операционных систем. Используя штатные служебные команды протокола FTP, пользователь имеет возможность ознакомиться с тем или иным каталогом удаленной рабочей станции, осуществить копирование файлов.

Следующим протоколом семейства TCP/IP является SMTP (Simple Mail Transfer Protocol), который отвечает за передачу сообщений между рабочими станциями сети internet. Рассматриваемый протокол допускает возможность разных транспортных служб, а также, для повышения гарантированности доставки информации, использует механизмы промежуточного хранения. Протокол SMTP может функционировать в любых информационных сетях, даже не использующих TCP/IP, но при этом обеспечивает и группирование сообщений, и, при необходимости, создает несколько копий для передачи в несколько адресов.

Другой рассматриваемый протокол транспортного уровня UDP (User Datagram Protocol) обеспечивает невысокую надежность доставки из-за отсутствия логического соединения. Он обеспечивает простую отправку дейтаграмм (datagrams), как еще называют пакеты данных, между рабочими станциями без предоставления гарантий и подтверждения доставки адресату. Для повышения надежности доставки сообщений необходимо функции надежной передачи встраивать в прикладное программное обеспечение.

Не смотря на перечисленные недостатки, протокол UDP имеет и определенные преимущества перед TCP. Установление логического соединения требует определенное время и дополнительных ресурсов на рабочей станции для хранения информации о состоянии соединения, UDP же использует системные ресурсы только в моменты отправки и получения информации.

На основании сказанного можно сделать вывод, что вид используемого транспортного протокола во многом зависит от потребностей конкретного пользователя. В случаях необходимости обмена данными межу рабочими станциями и сервером в режиме реального времени использование для связи транспортного уровня TCP является более оптимальным. В случаях периодической связи между хост-компьютерами предпочтительнее пользоваться проколом UDP.

Теперь обратимся к сетевой файловой системе NFS (Network File System), разработанной компанией Sun Microsystems Inc. Данная система позволяет объединить файловые системы рабочих станций, с установленной операционной системой UNIX, используя транспортные услуги UDP. В этом случае, созданные бездисковые рабочие станции, могут получить доступ к серверу как локальные диски, но при низкой пропускной способности каналов вычислительной сети использование данной файловой системы неэффективно. В противном случае, использование NFS, позволяет несетевым программам работать с удаленными файлами, как с хранящимися на локальных дисках, что значительно упрощает и повышает эффективность работы пользователей.

Еще одним протоколом, работающим на базе UDP, используемым сетевыми управляющими станциями, является SNMP (Simple Network

Management Protocol). Данный протокол позволяет управляющим стациям обобщать информацию о сети internet, определять формат данных, а вот обработка и интерпретация выполняются по требованию управляющих станций или администратора.

TCP и UDP идентифицируют приложения по 16-битным номерам портов, которые заранее предназначены для серверов приложений. Например, в каждой реализации TCP/IP, которую поддерживает сервер FTP, этот протокол передачи файлов получает для своего сервера 21 номер TCP-порта. Каждый Telnet-сервер имеет TCP-порт 23, а сервер протокола TFTP (Trivial File Transfer Protocol) - UDP-порт 69. Службам, которые могут поддерживаться любой реализацией TCP/IP, назначаются номера портов в диапазоне от 1 до 1023 [84,51].

Назначением номеров портов занимается организация под названием Internet Assigned Numbers Authority (IANA), а пользователю важен только факт того, что номер используемого порта уникален для данного хоста. При работе с сервером уникальные номера клиентам присваиваются только на время соединения. Для присвоения краткосрочных номеров, при использовании семейства TCP/IP, используется диапазон от 1024 до 5000.

Теперь обратимся к Internet Protocol (IP) являющимся основным протоколом сетевого уровня и позволяющим реализовывать межсетевые соединения с использованием протоколов транспортного уровня. IP определяет IP-дейтаграмму, указывая единицу передачи данных и формат всей циркулирующей в internet информации. На основе адреса вычислительной сети, при помощи специальных таблиц, определяется маршрут передачи данных отдельно для каждого пакета, но без гарантии доставки в нужном порядке. Протокол IP реализует высокоэффективную доставку пакетов, задавая отображение данных на физическом уровне.

Протоколы разрешения адресов ARP (Address Resolution Protocol) и RARP (Reverse Address Resolution Protocol) используются на нижнем уровне сетевого интерфейса. Они применяются для преобразования адресов сетевого и физического уровня только в определенных типах физических сетей (Ethernet и Token Ring).

Рассмотрим более подробно, как происходит адресация в вычислительной сети.

Если используемая коммуникационная система предоставляет возможность хостам взаимодействовать, то она считается универсальной. Добиться такой универсальности позволяет глобальный метод идентификации. Схема идентификации в семействе протоколов TCP/IP аналогична адресации в физических сетях. В этом случае каждый сетевой интерфейс получает уникальный 32-битный адрес, называемый также IP-адресом, и использует его для всех коммуникаций в вычислительной сети. Предоставляемый компьютеру IP-адрес имеет строгие требования и в нем, в обязательном порядке, содержится информация об идентификации вычисли-

тельной сети, в состав которой входит рабочая станция, и уникальный идентификатор самого компьютера. Кроме адресов для одного хоста (unicast), используются еще широковещательные (broadcast) и групповые (multicast) адреса

Широковещательные адреса, в поле идентификатора хоста которых входят только единицы, позволяют обмениваться данными со всеми хостами сети. В этом случае существует возможность широковещательной передачи информации, но гарантированная доставка зависит от характеристик данной физической сети. Например, в Ethernet подобная передача может выполняться достаточно эффективно, но есть сети, которые по ряду причин имеют ограниченные возможности либо не поддерживают такой тип передачи.

В случае необходимости отправки информации определенному количеству рабочих станций адресатов (multicasting) используют групповые адреса. Такая возможность требуется, например, для проведения видеоконференций, отправки новостей или конфиденциальной информации определенной группе получателей. В этом случае для обеспечения групповой передачи используют протокол IGMP (Internet Group Management Protocol), который предоставляет информацию о принадлежности рабочей станции к конкретной группе в данный момент.

Вследствие бурного развития во всем мире современных вычислительных сетей32-битная схема адресации нынешней версии Internet Protocol (IPv4) уже не удовлетворяет насущным потребностям. В новой версии протокола IPv6 реализуется 128-битный формат IP-адреса и поддерживать автоматическое назначение адресов [84,85].

Семейство протоколов TCP/IP предоставляет возможность работать с именами компьютеров, а не с их адресами, что значительно упрощает взаимодействие операторов. Преобразование IP-адресов в имена хостов осуществляется при помощи распределенной базы данных DNS (Domain Name System) и практически любое приложение может обратиться для преобразования IP-адреса в соответствующее имя хоста. Причина распределенности этой базы кроется в том, что всей информацией об именах не обладает ни один объект в internet. DNS обеспечивает протокол взаимодействия клиентов и серверов.

Таким образом, протокол TCP/IP широко применим, т.к. имеет ряд существенные преимущества.

Как протокол передачи данных, он не зависит от физической среды передачи. Это означает, что протокол TCP/IP может использоваться для передачи информации, по оптоволоконной или спутниковой линии или коммутируемой/выделенной линии с равным успехом.

Требование универсальности [84] вынуждает строить многоуровневую модель передачи данных, встраивая протокол TCP/IP в промежуток между физическим уровнем (к нему относятся сетевые карты, модемы, ка-

бели и их протоколы передачи данных) и уровнем прикладных программ (почтовая программа) (рисунок 1.1).

Протокол TCP/IP является открытым, с его официальным описанием (RFC-791, RFC-793) может познакомиться в Интернет любой желающий.

Неудивительно, что существуют программные реализации этого протокола практически для любой операционной системы. Например, Microsoft TCP/IP для Windows, Berkly TCP/IP для Unix линии BSD и т.д. И, хотя этот протокол не стандартизован ни одним государством мира, он стал фактически международным стандартом для вычислительных сетей.

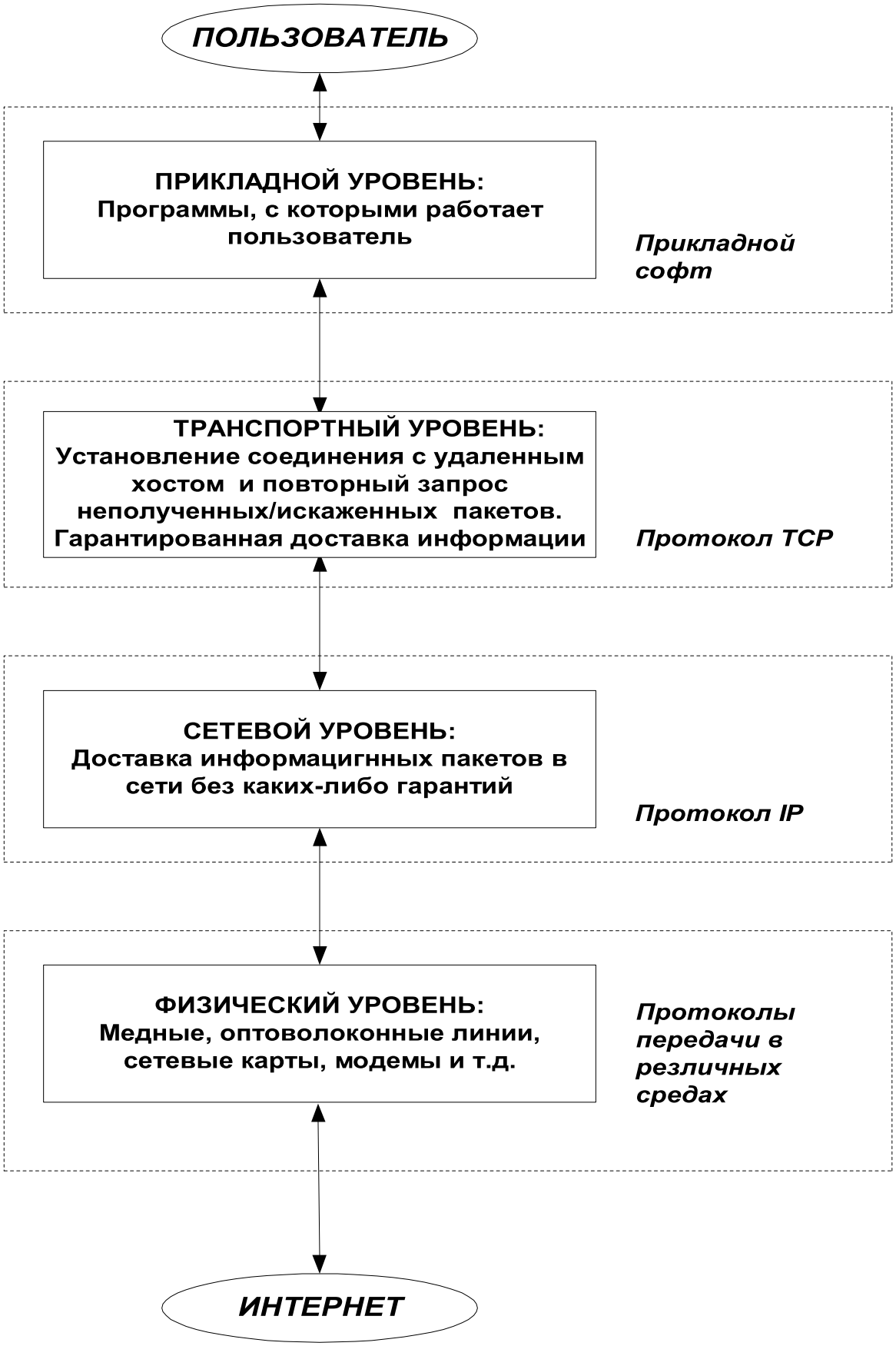

Рисунок 1.1. Универсальность протокола TCP/IP

1.3. Деструктивные воздействия в среде информационного обмена

Повсеместное использование высоких технологий приводит к тому, что любая деятельность тесно связана с получением, накоплением, хранением, обработкой и использованием информационных потоков. Следствием этого является высокая цена информации в современном обществе и постоянные попытки получения данных о структуре, состоянии и деятельности объекта интересов. Научно-техническая революция и формирование информационного общества порождают совершенствование процедур направленных на модификацию компьютерной информации. Подобные деяния могут привести к дезинформации в различных сферах деятельности современного общества.

Анализ уязвимостей современных вычислительных систем указывает на их существенное превышение уязвимостей, связанных с неправомерным доступом к компьютерной информации, по сравнению с автономными компьютерами. Это различие связано, прежде всего, с масштабностью, неоднородностью и открытостью вычислительных сетей.

Приступать к рассмотрению признаков неправомерного доступа к компьютерной информации, хранящейся на рабочих станциях в вычислительных сетях, нецелесообразно без определения и классификации возможных угроз информационной безопасности.

Под фактором и угрозой (вообще) обычно понимают потенциально возможное событие, действие (воздействие), процесс или явление, которое можно привести к нанесению ущерба чьим-либо интересам. В вычислительной сети возможны все традиционные способы неправомерного вмешательства в обработку и доступа к информации. Угрозой информационным ресурсам можно считать потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию может прямо или косвенно привести к нарушению безопасности информации, к возникновению угроз целостности и неприкосновенности.

Нарушением безопасности информации (или просто нарушением) можно считать реализацию угрозы. Угрозы по природе их возникновения можно разделить на два типа:

- естественные (объективные);
- искусственные (субъективные).

Естественные угрозы – это угрозы, вызванные воздействиями на информацию и ее элементы объективных физических процессов или стихийных природных явлений, не зависящих от человека (К таковым можно отнести стихийные бедствия, аварии, террористические акты, сбои и отказы оборудования (технических средств) вычислительной сети). Последствия воздействия данных угроз заметны невооруженным глазом и действия работников в случае их возникновения предписаны соответствующими нормативными актами и инструкциями.

Искусственные угрозы – это угрозы информации, вызванные деятельностью человека. Учитывая мотивацию действий их можно разделить на:

- непреднамеренные;
- преднамеренные.

Непреднамеренные угрозы – это неумышленные угрозы, вызванные возможными ошибками при проектировании и разработке компонентов компьютерной сети, ошибками в программном обеспечении или действиях персонала. К основным непреднамеренным искусственным угрозам информации следует отнести действия работников, совершаемые случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла. Они проявляются в неумышленных, неправомерных или неосторожных действиях.

Неумышленные действия – это действия, приводящие к:

- частичному или полному отказу, потере работоспособности сети или разрушению аппаратных, программных, информационных ресурсов (Например, неумышленная порча оборудования, удаление, искажение файлов с важной информацией, в том числе системных, или программ и т.п.);
- физической порче носителей информации;
- опасности для работоспособности сети и безопасности информации в результате ошибок в проектировании архитектуры системы, технологии обработки данных, разработка прикладных программ, в авторизации пользователей и предоставлении им излишних прав;
- заражению компьютерными вирусами.

Неосторожные или неправомерные действия это действия, приводящие к:

- изменение режимов работы устройств и программ или необоснованному включению оборудования;
- разглашению или общедоступности информации ограниченного доступа;
- разглашению, утрате или передаче атрибутов разграничения доступа;
- игнорированию организационных ограничений (установленных правил) в сети, пересылке данных по ошибочному адресу абонента (устройства);
- уменьшение эффективности защиты информации в результате некомпетентного использования, настройки, неправомерного отключения или входа в сеть в обход средств защиты работниками;
- повреждению каналов связи.

Следы непреднамеренных угроз, в основном, обнаруживаются по истечении времени, но не обладают свойствами преднамеренного неправо-

мерного доступа к компьютерной информации и не представляют серьезной угрозы безопасности информации.

Преднамеренные угрозы – это угрозы, связанные с корыстными устремлениями людей (злоумышленников).

Уязвимыми с точки зрения неправомерного доступа к информации являются следующие элементы вычислительной сети:

- рабочие станции – отдельные электронно-вычислительные машины или удаленные терминалы информационной сети, на которых реализуются автоматизированные рабочие места пользователей (операторов, диспетчеров, администраторов удаленных кластеров);
- серверы;
- межсетевые экраны (порты, мосты, маршрутизаторы) – элементы, обеспечивающие соединение нескольких сегментов одной и той же сети, имеющие различные протоколы взаимодействия;
- каналы и линии связи.

Рабочие станции являются наиболее доступными компонентами, и именно с них могут быть предприняты наиболее многочисленные попытки совершения неправомерных действий. С рабочих станций осуществляется управление процессами обработки информации, запуск программ, ввод и корректировка данных, на дисках рабочих станций могут размещаться важные данные и программы.

Признаки совершения противоправных деяний, связанных с неправомерным доступом к компьютерной информации представляют собой следы неправомерного доступа, оставленные злоумышленником. Чаще всего используется не один метод доступа, а совокупность методов для достижения цели. При этом действия правонарушителя могут быть разделены на активные и пассивные воздействия.

Под пассивным воздействием нарушителя понимаются действия, направленные на получение сведений о характеристиках информационных процессов в вычислительной сети. Эти воздействия проявляются в возможности нарушителя подключиться к линии связи для съема циркулирующей информации или получать ее вследствие побочного электромагнитного излучения технических средств при передаче, приеме и обработке. Следы пассивного воздействия нарушителя обнаруживаются при помощи специальной аппаратуры, предназначенной для выявления пассивных каналов утечки информации.

Под активным воздействием нарушителя стоит понимать случайные или преднамеренные изменения информации в передаваемых сообщениях или заданных характеристиках информационного процесса, приводящие к осуществлению угрозы безопасности информации. Наиболее явно данные случаи отражаются в базовом протоколе передачи данных TCP-IP.

Противоправные действия правонарушителя связанные с неправомерным доступом в сфере информационных технологий определяются их криминалистической характеристикой.

Криминалистическая характеристика правонарушений в сфере информационных технологий – это совокупность элементов состава преступления, позволяющих квалифицировать преступные деяния в оперативно-розыскных, уголовно-правовых и судебных аспектах.

Неправомерный доступ, хищение, модификация компьютерной информации с использованием электронно-вычислительной техники, скрытными способами, а также комплексными действиями, порождено возможностью практически безнаказанного совершения подобных противоправных действий. Причем скрытный способ хищения компьютерной информации в свою очередь тоже не может обойтись без использования средств электронно-вычислительной техники и, следовательно, состав преступления необходимо рассматривать в совокупности с правонарушениями, рассматриваемых в главе 28 Уголовного кодекса РФ [3].

Одной из главных особенностей расследования неправомерного доступа в сфере информационных технологий является необходимость определения рабочей станции, с которой осуществлялся доступ. Специфика вычислительных сетей заключается в предоставлении доступа к информации определенных пользователей и вынуждает оставлять следы своего пребывания за рабочей станцией, как традиционные, так и информационные.

В то же время, кроме времени, места и орудия совершения преступления в компьютерных сетях немаловажную роль в раскрытии играют способы совершения и сокрытия. Используемые в настоящее время информационные технологии защиты информации обуславливают такие уязвимости информации как [97]:

1. Возможность случайной или злоумышленной неправомерной модификации;
2. Подверженность физическому или логическому искажению или уничтожению;
3. Опасность случайного или преднамеренного неправомерного получения информации посторонними лицами.

Отсюда вытекают угрозы информационной безопасности в вычислительных сетях, которые обусловлены [97]:

1. степенью надежности функционирования средств обработки информации;
2. непреднамеренными, случайными, действиями обслуживающего персонала;
3. преднамеренными действиями, целью которых является незаконное ознакомление, хищение, модификация или уничтожение обрабатываемой информации.

Одним из основных и особенно важных, при расследовании преступлений в сфере компьютерной информации, элементов криминалистической характеристики является способ совершения правонарушения. Использование средств вычислительной техники, и особенно, содержащейся на ней информации, оказывает существенную помощь и позволяет сократить время обработки и поиска информации. Но кроме помощи, хранимая информация, в случае ее утечки, может оказать и вред. Несмотря на существующие проблемы, поиск с научной и практической точки зрения, перспективы совершенствования информационной безопасности информационных систем представляются совершенно неизбежным, так как в конечном итоге это напрямую влияет на безопасность общества и государства.

По мнению В.А. Минаева и других авторов, появление Федеральной целевой программы (ФЦП) «Электронная Россия» кажется весьма своевременным. Основные направления ее реализации разработаны с учетом Программы действий Европейской комиссии по созданию «Электронной Европы», среди которых можно выделить следующие:

- новая концепция предоставления услуг в сфере электронных коммуникаций с акцентом на создание правовой базы;
- создание высокоскоростной инфраструктуры;
- электронное обучение с предоставлением учебным заведениям доступа в Интернет, адаптацией учебных программ и переподготовкой преподавательского состава, поддержкой исследований в этой области;
- разработка стандарта на электронную цифровую подпись и системы разрешения конфликтов, а также кодекса поведения в вычислительной сети;
- обеспечение безопасности сетей связи – поддержка исследований и технологических разработок в области сетевой безопасности и создание «компьютерных групп быстрого реагирования» и др.

Таким образом, возрастающие требования к управлению системами жизнеобеспечения в современном обществе, построение информационных сетей и распределённая обработка данных приводят к глобализации информационных систем. В связи с этим постоянно возрастает число случаев неправомерного доступа к компьютерной информации в вычислительных системах. В целом спектр правонарушителей и преступлений очень широк – от шуток до международного терроризма.

Рассмотрим более подробно, какими техническими возможностями (специальными техническими средствами) может располагать потенциальный нарушитель, который преследует цель совершения неправомерного доступа к защищаемой информации. Практически все специальные технические средства, под которыми целесообразно понимать различные устройства, приборы, системы, программно-аппаратные комплексы, реализующие специальные информационные технологии существуют в двух видах: первые – «оборонительные» (технологии защиты информации огра-

ниченного доступа), вторые – «атакующие» разведывательные технологии, как правило предназначенные для скрытого, негласного получения информации. Оба вида активно используются как правоохранительными органами в целях решения установленных законом задач, так и криминальными и другими структурами в преступных намерениях [97].

Согласно классификации данной в учебнике криминалистики она объединяет неправомерный доступ к компьютерной информации в три основных группы [43]:

1. способы непосредственного доступа;
2. способы опосредованного (удаленного) доступа;
3. смешанные способы.

Способ опосредованного доступа основан на получении компьютерной информации методом аудиовизуального и электромагнитного перехвата при помощи устройств внешнего пользования, широко практикуемого в оперативно-розыскной деятельности. Этот способ можно разделить на две составляющие пассивный и активный перехват.

Пассивный перехват с применением устройств внешнего пользования осуществляется путем дистанционного перехвата электромагнитных излучений исходящих при работе средств вычислительной техники. В своей книге Д. Айков и др., рассматривая компьютерные преступления, выделяют и использование электромагнитных излучений для перехвата информации. Так, электронные излучения компьютерного оборудования представляют собой риск, о котором пользователь ЭВМ должен полностью отдавать себе отчет (в первую очередь это касается военных и разведывательных данных). Компьютеры, так же как и все остальные электрические приборы – от фенов до стереоаппаратуры, излучают электромагнитные волны. Всякий раз, когда нажимается клавиша компьютера, в окружающее пространство посылается электромагнитный сигнал. Иностранные разведывательные службы, коммерческие предприятия и даже взломщики-тинэйджеры могут следить за этими излучениями, перехватывать и расшифровывать их. Из этих устройств, следует выделить три, принципиально характеризующие основные группы таких средств [97].

К первой группе относятся *лазерные датчики*. Луч направляется на окно, а отраженный сигнал принимается специальным блоком, расшифровывается и направляется на магнитный носитель или на распечатку. Максимальное расстояние уверенного приема составляет до 300 метров. При благоприятных условиях информация считывается даже при окнах с двойными рамами. Но в силу сложности и очень высокой стоимости, при низкой помехоустойчивости в условиях города, вероятность их применения крайне мала [97].

Представителем второй группы приборов внешнего использования являются *направленные микрофоны*, позволяющие распознавать речевой сигнал на расстоянии до 100 метров в условиях города. Их особенностью

является способность фиксировать звуковые колебания узконаправленным лучом.

Стереоскопические датчики составляют третий тип рассматриваемых устройств. Они представляют собой приборы для приема акустических сигналов через строительные конструкции (стены, окна, двери).

Кроме того, распространен перехват электромагнитных сигналов, распространяющихся по техническим каналам основных и вспомогательных средств и систем в виде паразитных информативных физических полей (побочные электромагнитные излучения и наводки, паразитные модуляции высокочастотных сигналов, паразитные информационные токи и напряжения, образуемые за счет эффекта электроакустического преобразования сигналов в сетях электросвязи) [67].

Наиболее простой способ опосредованного доступа (внутреннего использования) – это перехват электромагнитного излучения и использование подслушивающих радиопередающих устройств.

Особенностью устройств *âíóòðåííåãî èñïîëüçîâàíèÿ* является необходимость их установки в контролируемом помещении. К ним относятся лазерные и радиомикрофоны или, как их еще называют, радиозакладки, радиобаги, радиокапсулы. Они являются самыми распространенными средствами съема информации, что объясняется удобством их оперативного использования, простотой применения, относительной дешевизной и малыми габаритами. Как правило, они имеют автономное электропитание, что ограничивает время их использования. Интересными являются случаи оформления в виде настольных электронных часов, калькуляторов с питанием от электросети, а также электрических удлинителей, тройников, розеток и т. д., что позволяет использовать их продолжительное время. Кроме того, имеются типы акустических закладок с питанием от телефонной линии. Также к устройствам внутреннего использования относятся *äàò÷èêè ýëåêòðîìàãíèòíûõ èçëó÷åíèé*, служащие для съема информации. Примером может быть имевший место факт, когда Терминалы HealthKit H19 излучали такие сильные радиосигналы, что они могли улавливаться расположенным неподалеку обычным телевизором. Когда на терминале появлялись символы, на экране телевизора также возникали отчетливые образы, которые могли быть расшифрованы [97].

Это объясняется тем, что «всякое электронное устройство, телефон и факс, а также линии связи излучают в открытое пространство высокие уровни поля в диапазоне частот вплоть до 150 МГц и на определенном расстоянии можно уловить устойчивый сигнал при помощи измерительной установки, включающей обычную дипольную антенну и телевизор [55].

Таким образом, из-за угрозы перехвата информации в излучениях все компьютеры, используемые для хранения и обработки информации ограниченного распространения, должны иметь специальное физическое экранирование.

Оперативные возможности нарушителя определяются тем, имеется ли у него позиции на самом объекте преступных устремлений (режимное помещение, организация, рабочий кабинет и пр.) или необходимо на объект проникать. От этого зависит, к каким именно техническим средствам съема информации может прибегнуть контрпартнер. В первом случае он, вероятнее всего, применит устройства внутреннего использования, рассмотренные выше [97].

Активный перехват осуществляется путем непосредственного подключения к средствам вычислительной техники или системе передачи данных при помощи различных штатных оперативно-технических или специально разработанных, изготовленных, приспособленных, запрограммированных средств негласного получения информации.

Довольно серьезную опасность при использовании активного перехвата представляет способ, который получил название «уборка мусора». Физический вариант включает в себя осмотр содержимого банальных мусорных корзин для поиска выброшенных за ненадобностью распечаток, вышедших из строя электронных носителей информации, так как велика вероятность их восстановления [97].

Особенность совершения неправомерного доступа к компьютерной информации при помощи способов непосредственного доступа заключается в том, что для его реализации необходим прямой доступ непосредственно к компьютеру или вычислительной сети, содержащей информацию ограниченного распространения. Осуществить доступ к подобной информации может не только лицо, работающее или имеющее отношение к производству работ с информацией, но и лицо, целенаправленно проникшее в контролируемую зону или место обработки и хранения информации. Практически безнаказанно данные правонарушения в вычислительных сетях может совершать сотрудник данной организации, так как в этом случае он оставляет минимум физических следов неправомерного доступа к компьютерной информации. При этом злоумышленник может не только знакомиться с охраняемой законом компьютерной информацией, но и проводить ее модификацию, оказывать влияние на процессы обработки, нарушать работу ЭВМ, системы ЭВМ или их сети, то есть совершать деяния, предусмотренные 28 главой УК РФ.

В вышеперечисленных случаях немаловажное значение имеет то, как организован доступ к рабочим станциям. Имеются ли системы идентификации (аутентификации), наличие или отсутствие лиц, способных оказать содействие в проникновении постороннего специалиста на объект. При отсутствии возможности проникновения нарушитель вынужден будет обратиться к устройствам внешнего использования. Таким образом, решение проблемы защиты информационного пространства от различного рода нарушителей, пользующихся специальными техническими средствами, мо-

жет быть только комплексным, т.е. необходимо обеспечение технологической, логической и физической безопасности [97].

Долгое время организаторы, администраторы и пользователи вычислительных сетей при организации защиты основное внимание и, как следствие, средства, сосредотачивали на противодействии внешним угрозам и злоумышленникам, совершенствовали системы доступа, устанавливали межсетевые экраны и другие мощные инструменты, направленные на предотвращение процедур нарушения информационной безопасности извне. Подобное совершенствование привело к тому, что, в настоящее время, осуществить проникновение в вычислительную сеть, содержащую информацию ограниченного распространения, извне может только высококвалифицированный нарушитель обладающий, к тому же, серьезными познаниями в области информационных технологий и программного обеспечения.

Однако современная действительность указывает на то, что в погоне за повышением эффективности противодействия внешним нарушителям была упущена другая немаловажная проблема. Она заключается в том, что в настоящее время наибольшую угрозу представляют не внешние, а внутренние злоумышленники. Это вызвано тем, что они знакомы с системой защиты и могут реально оценить ценность данных содержащихся на рабочих станциях и серверах вычислительной сети. Наибольшую опасность представляют обиженные работники, научившееся работать на персональных компьютерах на уровне пользователей и продолжающие свое самосовершенствование, работники занимающиеся обеспечением работы локальных вычислительных сетей.

Исследование рассматриваемой проблемы Deloitte Touche Tohmatsu указывает на активизацию именно второй категории. Так в 2006 году в канадских банках зафиксированы утечки информации от сотрудников, нанесшие ущерб не менее 1 млн $. При этом необходимо указать, что более половины нарушителей являлись действующими или недавно уволенными сотрудниками. Необходимо отметить, что это только вершина айсберга, в реальности ситуация намного плачевнее. Конечно, это не является причиной недоверия ко всем работающим сотрудникам и не указывает на необходимость проводить в отношении них профилактические действия, основываясь на том, что они являются потенциальными нарушителями безопасности информации. Но, в свою очередь, подобная вероятность нарушения указывает на необходимость развития средств обеспечения защиты компьютерной информации от внутренних угроз посредством использования программных и аппаратно-программных средств.

Практически всех сотрудников организации можно разделить на несколько типов: обычные работники, нарушители-любители и предатели-агенты.

«Обычные работники» являются самой многочисленной категорией, к которой относятся сотрудники которые, в основном, выполняют предъявляемые требования. Данные лица лишь изредка совершают незначительные нарушения, наиболее часто заключающиеся в самовольной установке или удалении программного обеспечения, перенастройке параметров рабочих станций вычислительной сети, злоупотреблении доступом к Интернету. Если рассматриваемая категория и нарушает информационную безопасность, то это связано с недостаточными знаниями в области программного или аппаратного обеспечения и связанных с этим процессов функционирования вычислительных и телекоммуникационных сетей.

Относящиеся ко второму типу «нарушители-любители» менее многочисленны и их нарушения довольно часто заключаются в отклонениях от предъявляемых требований по обеспечению информационной безопасности. Они злоупотребляют не только доступом к Интернету, устанавливают и удаляют различные программы и приложения, но и, преследуя определенные цели, целенаправленно вносят изменения в конфигурацию рабочих станций тем самым, создавая угрозы информационной безопасности. Кроме того, рассматриваемая категория может, время от времени, разглашать информацию ограниченного распространения посторонним лицам, в ряде случаев преследуя корыстные цели.

Третий тип «предатели-агенты», являющийся самым немногочисленным, потенциально наиболее опасен. Их противоправные действия, в основном, направлены на получение информации ограниченного распространения и предоставлении ее третьим лицам. К подобному типу следует отнести лиц, целенаправленно внедренных в организацию или же работников преследующих, по различным причинам, цель нанести ей максимальный вред различными способами.

Однако следует указать на необходимость определения не только типов сотрудников, но и причин по которым они совершают те или иные действия. Это конечно не относится к целенаправленно внедренным лицам, задача которых заключается в осуществлении вредоносных воздействий в вычислительных и телекоммуникационных сетях организации.

Остановимся в первую очередь на лицах, которые могут быть отнесены к первому типу. Это, наиболее часто, сотрудники, халатно относящиеся к своим обязанностям или подвергающиеся неявному воздействию, использованию вслепую, манипуляции со стороны «предателей-агентов».

Халатно относящиеся к своим обязанностям сотрудники, относящиеся к «обычным работникам», как правило, преследуют цель расширения возможностей своего доступа к Интернету или использования рабочего времени с «большей пользой», то есть, играя в компьютерные игры. Для претворения подобных желаний в жизнь они могут самолично устанавливать или удалять различное, в том числе системное, программное обеспе-

чение тем самым, создавая угрозы информационной безопасности, не преследуя каких-либо корыстных целей.

Более опасна категория «обычные работники» подвергающиеся манипуляционному воздействию со стороны «предателей-агентов». Они обычно подвергаются различным видам воздействия, в том числе, психологического и даже не знают, о том, чье задание и с какой целью выполняют. Подобные деяния выполняются без умысла и преследования корыстных целей.

Ко второму типу «нарушители» следует отнести в первую очередь сотрудников обиженных на определенные действия администрации. К подобному типу нарушителей можно отнести также лиц преследующих корыстные цели личного обогащения. Примеры подобных деяний встречаются часто и приводить их можно достаточно долго.

К третьему типу «предатели-агенты» можно отнести лиц, целенаправленно внедренных или подкупленных другими организациями. Их действия носят следы преступного умысла и выполняются целенаправленно по поступившему заданию.

Процесс постоянного совершенствования средств вычислительной техники вызывает необходимость изменения и улучшения характеристик средств обеспечения информационной безопасности с целью предотвращения неправомерных деяний в сфере информационных технологий. Преобладающая часть подобных инцидентов связана с нарушением безопасности информации заключающейся в ознакомлении, модификации или уничтожении данных, хранящихся на рабочих станциях в вычислительных и телекоммуникационных сетях. Одним из наиболее эффективных способов противодействия неправомерному доступу в сфере информационных технологий является своевременное выявление подобных попыток, определение рабочего места и конкретного виновника инцидента.

Степень опасности происшедшего инцидента зависит от способа воздействия на сеть, которая, в свою очередь, может быть различно от ознакомления с данными или проникновения вредоносных программ до модификации или кражи информации. На определении способа совершения атаки основываются особенности реагирования на нее. Для разработки эффективной методики противодействия вредоносным воздействиям на информацию вычислительной сети необходимо определить:

- степень ценности украденной или модифицированной информации;
- произошло ли разглашение информации ограниченного доступа;
- степень квалификации виновника инцидента;
- степень опасности воздействия на систему.

Способы непосредственного неправомерного доступа к информации можно условно разделить на три группы [97]:

1. Способы, препятствующие нормальной обработке информации;

2. Способы, направленные на неправомерное чтение копирование и распространение компьютерной информации;

3. Способы, видоизменяющие и разрушающие компьютерную информацию.

Неправомерное использование компьютерной информации, в свою очередь, обычно заключается в:

- незаконном использовании программ для получения информации с целью сбыта ее третьим лицам;
- незаконном распространении программного обеспечения;
- считывании данных из массивов других пользователей;
- копировании информации с преодолением мер защиты;
- считывании информации, оставшейся в памяти системы после выполнения санкционированных запросов.

В качестве иллюстрации приведем несколько способов совершения неправомерного доступа к информационным ресурсам вычислительных сетей различного уровня.

Для совершения неправомерного доступа связанного с ознакомлением и распространением компьютерной информации можно применять любые методы, начиная от беглого просмотра и заканчивая наиболее действенным методом, получившим название «неспешный выбор» [100]. Этот метод заключается в осуществлении неправомерного доступа к охраняемой законом компьютерной информации через слабые места в защите одиночных средств вычислительной техники или их сети. Злоумышленник, самостоятельно или с чьей-то помощью, обнаружив такие места, может, не торопясь исследовать и анализировать информацию ограниченного доступа, обрабатываемую или хранящуюся в компьютерной сети, при необходимости копируя или осуществляя модификацию. Найти следы такого преступления, даже без попытки их сокрытия, довольно сложно без наличия определенных знаний и навыков работы, так как преступник обычно старается оставить все реквизиты в исходном состоянии [97].

Еще один метод неправомерного доступа, получивший название «аварийный» или «склад без стен» [100], применяется при возникновении аварийных ситуаций в компьютерной сети. Злоумышленник либо дождавшись возникновения аварийной ситуации или системной неисправности в сети, либо инициировав ее, проводит необходимые мероприятия. В этом случае нарушитель может осуществить однократный неправомерный доступ к информации. Кроме того возможна организация доступа для последующего использования при помощи специальных программ, применяемых в случаях возникновения сбоев в работе компьютерной сети. Определение лица осуществившего неправомерный доступ к компьютерной информации затруднено, так как во время аварии отключаются основные системы, отвечающие за защиту информации в сети.

На современном этапе для получения информации необходимо проникнуть в компьютерную сеть, при этом, желательно, для сокрытия следов противоправных действий, произвести проникновение под видом другого законного пользователя. Такие действия получили название «маскарад», «самозванство» и «мистификация» [100], так как получить идентифицирующие данные другого сотрудника не составляет труда. Это является следствием того, что пользователи при выборе паролей обращаются к событиям и датам, связанным с их личной жизнью, что позволяет злоумышленнику при помощи определенного анализа определить значения символов. Если для обозначения пароля используются нейтральные обозначения, то их могут записать на листе бумаги и оставить на видном месте [97].

Что же касается уборки электронного мусора, то, как известно, при хранении компьютерных данных на внешних носителях прямого доступа выделяется несколько уровней иерархии: сектора, кластеры и файлы. Сектора являются единицами хранения информации на аппаратном уровне. Кластеры состоят из одного или нескольких подряд идущих секторов. Файл — это множество кластеров, связанных по определенному закону.

Работа с электронными документами, как правило, сводится к выполнению таких манипуляций с файлами, как:

- создание;
- хранение;
- коррекция;
- уничтожение.

Защищаемая компьютерная информация обычно шифруется, но основная угроза утечки информации происходит не от того, что используются нестойкие алгоритмов шифрования или несовершенные криптографические ключи как это может показаться на первый взгляд), а от банального прикладного программного обеспечения (текстовые редакторы, базы данных), применяемого для создания или коррекции документов. Причина подобной опасности кроется в том, что используемое программное обеспечение создает в оперативной или внешней памяти средства вычислительной техники временные копии документов, с которыми они работают. Результатом является выпадение подобных файлов из поля зрения любых программ шифрования, что может быть использовано злоумышленником для составления представления о содержании данных хранимых в зашифрованном виде.

Необходимо напомнить тот факт, что в случаях редактирования информации ее объем зачастую уменьшается, а записывается она в те же кластеры, где находилась изначально. В результате остаются «хвостовые» кластеры, где исходная информация полностью сохраняется. В этом случае, при использовании специализированного программного обеспечения осуществляющего шифрование, подобные кластеры не только не зашифровываются, но и остаются в исходно состоянии даже при использовании

средств гарантированного уничтожения информации. Конечно, рано или поздно, в зависимости от интенсивности работы, информация из «хвостовых» кластеров затирается данными из других файлов, однако по оценкам специалистов из них через сутки можно извлечь до 85%, а через десять суток — до 25—40% исходной информации [97].

Пользователям и операторам информационной системы необходимо учитывать, что команда удаления файла (DEL) не изменяет содержания файла, и возможность его восстановления остается высока до тех пор, пока поверх удаленных файлов не записана другая информация. Средства гарантированного уничтожения файлов, не помогают, полной мере, решить указанную проблему, так как записывают на место файла, удаленного стандартными средствами, константу или случайные числа. Однако, даже подобное программное обеспечение оказывается неспособным противостоять программам закладкам, которые нацелены на увеличение количества остающихся в виде «мусора» фрагментов информации. Например, можно инициировать статическую ошибку, пометив один или несколько кластеров из цепочки, входящей в файл, меткой «сбойный». В результате при удалении файла средствами операционной системы или средствами гарантированного уничтожения та его часть, которая размещена в сбойных кластерах, останется нетронутой и впоследствии может быть восстановлена с помощью стандартных утилит.

Осуществление смешанных способов доступа к информации заключается в использовании смешанного воздействия способами предыдущих групп.

Современная концепция создания вычислительных сетей предполагает использование программных средств различного назначения в едином комплексе. К примеру, типовая система автоматизированного документооборота состоит из операционной среды, программных средств управления базами данных, телекоммуникационных программ, текстовых редакторов, антивирусных мониторов, средств для криптографической защиты данных, а также средств аутентификации и идентификации пользователей. Главным условием правильного функционирования подобной вычислительной сети является обеспечение защиты от вмешательства в процесс обработки информации тех программ, присутствие которых не обязательно. Среди подобных программ, в первую очередь, следует упомянуть компьютерные вирусы особенно такие как «троянский конь» или «бомба» [100].

Так, установка и активация компьютерного вируса «троянский конь», позволяет получать информацию ограниченного доступа с одной или нескольких рабочих станций, не расшифровывая своего интереса и местоположения благодаря командам управления, заложенным в данную программу. При этом она будет самостоятельно отправлять всю вызывающую интерес информацию по указанному адресу.

«Бомба» или «логическая бомба» имеет несколько иное предназначение. Набор команд, содержащихся в программе, направлен на уничтожение информации, находящейся на рабочей станции или на уничтожение компьютера, однажды или каждый раз, при определенных условиях или в определенное время.

В последнее время получила распространение форма вредоносных программ, связывающая эти два способа. В этом случае вредоносная программа, попадая на компьютер, начинает работать как «троянский конь» и передавать добытую информацию по заданному адресу, а через какой-то промежуток времени или по полученной команде приступает к разрушению штатного программного обеспечения и отдельных файлов в памяти компьютера.

Однако, следует обратить внимание еще на один тип вредоносных программ от которых, как и от вирусов, необходимо защищаться и тщательно отчищать свои вычислительные сети. К подобному типу относятся программы закладки, выполняющие хотя бы одно из следующих действий [97]:

- внесение произвольных искажений в коды исполняемых программ, то есть находящихся и оперативной памяти компьютера (программная закладка первого типа);
- перенос фрагментов обрабатываемой информации из одних областей памяти в другие (программная закладка второго типа);
- искажение информации, выводимой на внешние устройства или каналы связи, которая получена в результате работы других программ (программная закладка третьего типа).

Программные закладки можно классифицировать и по методу их внедрения в компьютерную сеть [48]:

- программно-аппаратные закладки, ассоциированные с аппаратными средствами компьютера (их средой обитания, как правило, является BIOS — набор программ, записанных в виде машинного кода в постоянном запоминающем устройстве — ПЗУ);
- загрузочные закладки, ассоциированные с программами начальной загрузки, которые располагаются в загрузочных секторах (из этих секторов в процессе выполнения начальной загрузки компьютер считывает программу, берущую на себя управление для последующей загрузки самой операционной системы);
- драйверные закладки, ассоциированные с драйверами (файлами, и которых содержится информация, необходимая операционной системе для управления подключенными к компьютеру периферийными устройствами);
- прикладные закладки, ассоциированные с прикладным программным обеспечением общего назначения (текстовые редакторы, утилиты, антивирусные мониторы и программные оболочки);

- исполняемые закладки, ассоциированные с исполняемыми программными модулями, содержащими код этой закладки (чаше всего эти модули представляют собой пакетные файлы, т. е. файлы, которые состоят из команд операционной системы, выполняемых одна за одной, как если бы их набирали на клавиатуре компьютера);
- закладки-имитаторы, интерфейс которых совпадает с интерфейсом некоторых служебных программ, требующих ввод конфиденциальной информации (паролей, криптографических ключей, номеров кредитных карточек);
- замаскированные закладки, которые маскируются под программные средства оптимизации работы компьютера (файловые архиваторы, дисковые дефрагментаторы) или под программы игрового и развлекательного назначения.

Одним из условий выполнения программной закладки является начало выполнения процессором исполнению команд, входящих в состав кода вредоносной программы. Подобное возможно только при наступлении некоторых событий, таких как:

- программная закладка должна попасть в оперативную память компьютера, то есть необходимо, чтобы она была загружена до начала работы программного обеспечения являющего целью воздействия или во время работы этой программы;
- программная закладка, находящаяся в оперативной памяти, приступает к выполнению своих функций при наступлении определенного перечня условий, называемых активизирующими.

В модели искажение программная закладка изменяет информацию, которая записывается в память компьютерной системы в результате работы, либо подавляет или инициирует возникновение ошибочных ситуаций в сети.

Можно выделить статическое и динамическое искажение. Статическое искажение происходит всего один раз, и при этом модифицируются параметры программной среды компьютерной сети, чтобы впоследствии в ней выполнялись нужные злоумышленнику действия.

Динамическое искажение заключается в запуске заранее активизированных закладок, в результате чего могут быть изменены параметры системных или прикладных процессов. Подобное деяние целесообразно разделить на искажение на входе, заключающегося в попадании на обработку уже искаженного документа, и искажение на выходе, заключающееся в искажении отображаемой информации как для оператора, так и для других программ.

Практика использования в системах электронного документооборота электронной цифровой подписи отражает ее подверженность таких программных закладок как «динамическое искажение», которые, используя свои особенности, могут осуществить проводки неправомерных записей в

базы данных и вмешаться в процесс разрешения споров по фактам неправомерного применения цифровой подписи. Например, в одной из программных реализаций широко известной криптосистемы PGP электронный документ, под которым требовалось поставить цифровую подпись, считывался блоками по 512 байт, причем процесс считывания считался завершенным, если в прочитанном блоке данные занимали меньше 512 байт. Работа одной программной закладки, выявленной специалистами, основывалась на навязывании длины файла. Эта закладка позволяла считывать только первые 512 байт документа, и в результате цифровая подпись определялась на основе только этих 512 байт. Такая же схема действовала и при проверке поставленной под документом цифровой подписи. Следовательно, оставшаяся часть этого документа могла быть произвольным образом искажена, и цифровая подпись под ним продолжала оставаться «корректной» [97].

Существуют четыре основных способа воздействия программных закладок на цифровую подпись [101]:

- искажение входной информации (изменяется поступающий на подпись электронный документ);
- искажение результата проверки истинности цифровой подписи (вне зависимости от результатов работы программы цифровая подпись объявляется подлинной);
- навязывание длины электронного документа (программе цифровой подписи предъявляется документ меньшей длины, чем на самом деле, и в результате цифровая подпись ставится только под частью исходного документа);
- искажение программы цифровой подписи (вносятся изменения в исполняемый код программы с целью модификации реализованного алгоритма).

При использовании модели «искажение» тоже используются вредоносные программные закладки, при этом их действие основывается на инициировании или подавлении сигнала о возникновении ошибочных ситуаций в вычислительной сети. В этом случае исполняемая программа может быть завершена отлично от порядка предписанного соответствующей документацией.

Инициирование статической ошибки заключается в создании на устройстве хранения информации области, при любом обращении к которой возникает ошибка. В этом случае происходит блокирование или значительное усложнение действий оператора, системных пли прикладных программ, которые могут осуществлять нежелательные для злоумышленника действия. К таким действиям относятся, например, уничтожение информации на жестком диске, проведение корректной модификации.

Особенностью инициирования динамической ошибки является генерация ложного сообщения о ошибке из числа тех, которые могут возникать

при выполнении используемой программы. Например, для блокирования приема или передачи информации в компьютерной сети может постоянно инициироваться ошибочная ситуация «Линия занята». Или при прочтении первого блока информации длиной 512 байт может устанавливаться соответствующий флажок для того, чтобы не допустить прочтения второго и последующих блоков и в итоге подделать цифровую подпись под документом.

Злоумышленник, для маскировки ошибочной ситуации, зачастую использует подавление статической или динамической ошибки. Подобные действия предпринимаются для блокирования нормального функционирования телекоммуникационной сети или желания заставить ее неправильно работать. В этом случае необходима адекватная реакция вычислительной сети на все возникающие ошибки, так как отсутствие адекватной реакции на практически любую ошибку может быть использовано злоумышленником для нарушения безопасности информации.

Выполнять функции с разновидностью искажения может вредоносная программа получившая название «троянский конь». В этом случае происходит встраивание вредоносной программы в используемое программное обеспечение и она может вызвать сбой в вычислительной сети, будучи активирована по какому-то событию. Тем самым злоумышленник парализует работу всей системы, а обеспечив себе доступ для устранения неисправности, может, например, извлечь из нее данные, перехваченные заранее внедренными программными закладками. Активация рассматриваемого программного обеспечения может происходить при наступлении определенного момента времени или состояние некоторых счетчиков (например, счетчика количества запусков программы). Кроме того, сам пользователь может спровоцировать запуск исполняемого файла, содержащего код программной закладки.

Так как для выполнения программной закладки необходима загрузка в оперативную память вычислительной машины, следует выделить резидентные закладки, которые выполняются с момента включения вычислительной машины, и нерезидентные, которые загружаются в оперативную память аналогично резидентным, но могут прекратить свое выполнение по истечении некоторого времени или при выполнении особых условий).

Существуют три основные группы деструктивных действий, которые могут осуществляться программными закладками [106]:

- копирование информации пользователя вычислительной сети (паролей, криптографических ключей, кодов доступа, информации), находящейся в оперативной или внешней памяти;
- изменение алгоритмов функционирования системных, прикладных и служебных программ (например, внесение изменений в программу разграничения доступа может привести к тому, что она разрешит вход в

систему всем без исключения пользователям вне зависимости от правильности введенного пароля);

- навязывание определенных режимов работы (например, запись на диск при удалении информации, при этом информация, которую требуется удалить, не уничтожается и может быть впоследствии скопирована).

У всех программных закладок (независимо от метода их внедрения в вычислительную сеть, срока их пребывания в оперативной памяти и назначения) имеется одна важная общая черта: они обязательно выполняют операцию записи в оперативную или внешнюю память системы. В противном случае никакого негативного влияния она оказать не может. Ясно, что для целенаправленного воздействия программа закладка должна выполнять и операцию чтения, иначе в ней может быть реализована только функция разрушения (например, удаление или замена информации в определенных секторах жесткого диска).

Рассмотренные примеры способов совершения неправомерного доступа к вычислительной сети указывают на то, что основную опасность для информации представляют внутренние злоумышленники, которые знакомы с системой защиты и могут реально оценить стоимость информации. Следует всегда помнить, что любые данные, не носящие массового характера и предназначенные для ограниченного круга лиц, попадая в руки злоумышленника, могут быть использованы им во вред обществу и государству.

Несмотря на определенную, и в большинстве случаев успешную, работу российских правоохранительных органов, запрещенные законом техническая разведка и промышленный шпионаж, экономически подпитываемые недобросовестной конкуренцией, как в международном масштабе, так и внутри нашей страны, продолжают оставаться одним из самых опасных видов информационных угроз, в том числе влияющих и на безопасность информационной сферы. Таким образом, целесообразно, прежде всего, на законодательном уровне выработать чёткую целевую Федеральную Программу противодействия источникам угроз в сфере информационной безопасности.

К основным угрозам в сфере информационной безопасности следует отнести [48]:

- 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;
- 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 свете рассмотренных деструктивных воздействий на информационные ресурсы в вычислительных сетях встает вопрос о повышении эффективности противодействия и предупреждения противоправных деяний в сфере информационных технологий. Далее целесообразно перейти к рассмотрению некоторых принципов обеспечения информационной безопасности в информационной сфере.

Глава 2. Обеспечение безопасности в среде информационного обмена

Внедрение автоматизированных систем обработки информации приводит к появлению «безбумажных» технологий и документооборота. Для обеспечения нужд обработки и передачи данных используют средства вычислительной сети. До недавнего времени информация и средства управление ею были сосредоточены в одном месте и централизованы. Сейчас вычислительные сети логически и физически рассредоточили информацию, а также вычислительную мощность и службы обмена сообщениями. В последнее десятилетие год от года увеличивается число правонарушений с использованием электронно-вычислительных машин, необходимых для осуществления неправомерного доступа к компьютерной информации. Одновременно с этим, довольно часто, информация, обрабатываемая и хранящаяся на компьютере, относится к информации ограниченного доступа и становится объектом правонарушения. Причем все чаще они совершаются не отдельными гражданами, а лицами, состоящими в преступных сообществах.

Неправомерный доступ с целью хищения, модификации компьютерной информации с использованием электронно-вычислительной техники, скрытными способами, а также комплексными действиями, порождено возможностью практически безнаказанного совершения подобных противоправных действий и обладает высокой латентностью. В этой связи целесообразно обратить серьезное внимание на вопросы обеспечения безопасности информационных ресурсов в вычислительных сетях.

2.1. Анализ уязвимости в базовом протоколе передачи данных информационной системы

Постоянное совершенствование средств вычислительной техники и внедрение их в различные области повседневной деятельности выявило потребность пользователей в более оперативном обмене информацией, в том числе на значительном удалении рабочих станций друг от друга. Для обеспечения возникших потребностей начали прокладывать линии связи, объединяющие рабочие станции, что послужило началом создания вычислительных сетей различного уровня. В настоящее время существует три типа сетей локальные, региональные и глобальные.

Изначально вычислительные сети создавались для развития открытой коммуникации между правительственными исследовательскими центрами, а не для обмена закрытыми финансовыми данными или как безопасная инфраструктура для е-коммерции. Так как правоохранительные органы хорошо знают, что преступления двигаются вслед за деньгами, то никто не был удивлен, что как только жизненно важная информация и коммерция попали в локальные сети и Интернет, тут же было совершено преступление. Сегодня никто не сомневается, что сетевой трафик необходимо контролировать, чтобы предотвратить потерю жизненно важной информации, поддерживать секретность, доступное рабочее время машины и защищать ценные сведения своей организации.

Для успешного контроля сетевого трафика, необходимо иметь хорошее понимание сетевой коммуникации, а также соответствующее снаряжение для выполнения того, что называется сетевым судебным рассмотрением — изучение сетевого трафика для подтверждения неправомерной, неавторизованной, или неприемлемой активности. Множество коммерческих и несколько бесплатных утилит автоматизируют процесс контроля и обнаружения неправомерных действий в информационной среде, но, в то же самое время, хорошее понимание работы TCP/IP и протоколов обмена также позволит распознавать незаконный, неавторизованный и зловредный трафик вычислительной сети, независимо от используемых утилит мониторинга.

Как было отмечено ранее протокол управления передачей (TCP/IP) является языком вычислительной сети. В свою очередь, используя протокол TCP/IP, мы подчиняемся набору принятых правил, которые сообщают вычислительной системе, как получить доступ к информационным ресурсам и локальным сетям на основе TCP/IP (LAN). При перемещении в Web, пересылке файла, отправке или получении e-mail, или использовании онлайн-чата, мы применяем протоколы TCP/IP.

Понимание TCP/IP позволит повысить эффективность обнаружения, мониторинга или поиска злоумышленников, которые атакуют сети, крадут информацию, создают черные ходы или тайные каналы, а также запускают

атаки типа «отказ в обслуживании». Профессионалы сетевой безопасности хорошо знакомы с основными особенностями сетевых протоколов представленных в таблице 2.1.

Теперь обратимся к понятию «инкапсуляция», которое широко известно в среде соответствующего круга специалистов в области IT- технологий.

Итак, «инкапсуляция» является методом реализации слоев в сетевых протоколах [38]. Идея состоит в том, что несколько слоев программного обеспечения служат определенным целям во время создания сетевого трафика и каждый слой модели добавляет информацию, или заголовки, к пакетам, которые посылаются по сети.

Хорошим примером концепции слоев является модель взаимодействия открытых систем, называемая также модель OSI (см. рис. 2.1), которая никогда не была реализована в реальности, но мы используем ее здесь для иллюстрации взаимодействия сетей. Каждый уровень модели обслуживает только свои смежные уровни. Таким образом, программное обеспечение, которое реализует уровень транспорта, получает входные данные с уровня сеанса или с уровня сети.

Таблица 2.1. Особенности протоколов TCP/IP

Протокол	Сокращение	Назначение
Протокол передачи гипертекста	HTTP	Используется при перемещении в WWW
Простой протокол передачи электронной почты	SMTP	Используется при отправке e-mail
Протокол почтовой службы	POP	Применяется для извлечения e-mail
Протокол пересылки файлов	FTP	
Протокол управляющих сообщений Интернета	ICMP	Применяется системами для согласования трафика
Telnet	нет	Используется для доступа на командном уровне к
Протокол управления передачей	TCP	Используется практически всеми приложениями для обеспечения надежной коммуникации
Протокол датаграмм пользователя	UDP	Применяется приложениями для передачи голоса, музыки и мгновенных сообщений
Протокол Интернета	IP	Конверт, который содержит почти каждый пакет
Протокол разрешения адреса	ARP	Используется для разрешения физической адресации сетевого адаптера (адресации MAC) в адреса Интернета
Двухточечный протокол	PPP	Используется в основном для коммутируемого доступа

Следует отметить, что термин пакет используется для обозначения датаграмм IP, сегментов TCP и Ethernet или других кадров уровня канала данных, посредством которых представляются различные стадии создания пакета данных [82].

Рисунок 2.1. Модель OSI

При вводе e-mail для отправки почты, создается адрес на уровне приложений. Нажимая кнопку отправки сообщения, приложение, которое используется для его создания (Netscape, Outlook, Eudora, cc:Mail и т.д.), передает программе метод представления, используемый на рабочей станции. Программа уровня представления, которая обрабатывает сообщение некоторым образом, передает управление уровню сеанса, который дальше его обрабатывает и посылает следующему уровню. Это продолжается, пока сообщение не обработается уровнем канала данных и пересылается по сетевому соединению. Практически все это невидимо конечному пользователю, который просто нажимает кнопку отправки. Это «невидимое» или прозрачное программное обеспечение, которое создает много заголовков,

называется стеком протоколов [26]. Хотя мы интересуемся, прежде всего, стеком протоколов TCP/IP, необходимо знать, что стеки протоколов существуют для множества других сетевых протоколов, включая протоколы Novell IPX, AppleTalk, DECNet, IBM System Network Architecture и Microsoft NetBIOS, которые выполняют аналогичные задачи.

Применим рассмотренную концепцию слоев к TCP/IP. На рисунке 2.2 показано, как инкапсуляция TCP/IP благоприятствует трафику между двумя различными сетями. Далее следует пошаговое рассмотрение действий, которые происходят при создании сетевого трафика TCP/IP в процессе отправки сообщения, что аналогично и для множества других типов приложений:

1. По окончании ввода сообщения, нажимается кнопка отправки.
2. Приложение, которое использовалось для создания сообщения, создает свой собственный заголовок и затем передает информацию транспортному уровню, где его обработает программное обеспечение TCP или UDP. Клиенты электронной почты обычно запрашивают соединение службы TCP; поэтому программное обеспечение TCP, реализованное на транспортном уровне, обработает данные и создаст заголовок TCP.
3. После того как заголовок TCP был создан и добавлен перед сообщением на транспортном уровне, программное обеспечение TCP передает управление сетевому уровню, где оно обрабатывается программным обеспечением IP.
4. После создания заголовка IP и добавления его перед сообщением на сетевом уровне, программное обеспечение IP передает управление сетевой плате на уровне канала данных, которая создает заголовок уровня канала данных и создает электрические или оптические единицы и нули, используемые в сетевой среде.
5. Рабочая станция, которая получает этот пакет на физическом уровне, удаляет по очереди каждый заголовок в обратном порядке на каждом соответствующем уровне. Таким образом, заголовок IP удаляется на сетевом уровне, заголовок TCP — на транспортном уровне, а данные передаются по стеку на уровень приложений получающего пользователя.

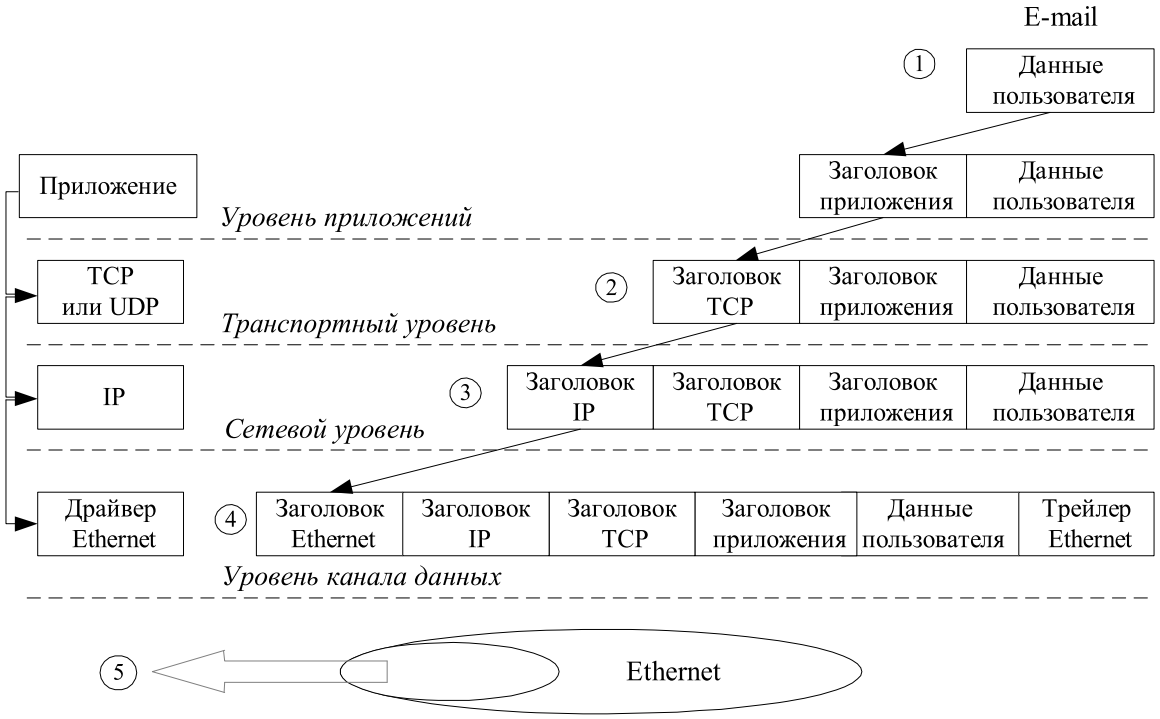

Рисунок 2.2. Реализация инкапсуляции в TCP/IP

Отметим, что TCP/IP не реализует все семь уровней модели OSI, но концепция уровней все равно сохраняется. Атакующие утилиты, которые «разрушают стек», являются программами, которые создают свою собственную заголовочную информацию, чтобы «обмануть» (создать поддельные адреса IP), выбрать свои собственные порты источника и заполнить поля заголовка значениями, которые нужны атакующему.

Для продолжения в качестве иллюстрации рассмотрим некоторые примеры атак в базовом протоколе передачи данных.

Перехват транзакционных данных

В случаях, когда злоумышленник не авторизован для перехвата всего содержимого коммуникации, они могут быть авторизованы для перехвата так называемой транзакционной информации, которая включает заголовки пакетов TCP/IP. Рассмотрение реализации инкапсуляции (рис. 2.2) показывает, что мониторинг всего содержимого требует перехвата данных пользователя, но транзакционный перехват для определения источника и места назначения коммуникации является просто перехватом заголовков TCP и IP.

Крайне важно знать и понимать поля, которые формируют заголовок IP, так как брандмауэры, системы IDS и сетевые анализаторы могут фильтровать трафик на основе любого из полей в заголовке IP. Заголовки обычно содержат всю информацию, которая понадобится для фильтрации сетевого трафика, чтобы сделать инспектирование сети менее навязчивым, более целенаправленным и более эффективным [38].

IP работает на сетевом уровне модели OSI и отвечает за доставку пакетов от источника по месту назначения. Протокол IP содержит или инкапсулирует другой протокол, такой как ICMP (Протокол управляющих сообщений Интернета), TCP или UDP. Заголовок IP включает как минимум 12 полей, все из которых могут содержать значения, на основе которых создаются схемы фильтрации. Конструкция заголовка IP описана в RFC791 (Североамериканский стандарт для передачи данных – аналог Российского ГОСТа)[26]. Компоновка заголовка IP показана на рисунке 2.3 и мы остановимся на ней подробнее.

Версия (Version) является 4-битовым полем, которое идентифицирует версию пакета IP. В настоящее время в вычислительных сетях используется IP версии 4 (IPv4), который представляет собой общий способ указания адресов, но уже в некоторых случаев можно встретить также IP версии 6.

Длина (Length) является 4-битовым полем, которое идентифицирует число 32-битовых (4-байтных) слов, которые составляют заголовок IP, а его максимальный размер равен 60 байтам. Размер всегда является кратным 32 битам. Наиболее распространенное значение поля длины - 5 (заголовок IP без дополнительных опций).

TOS обозначает тип обслуживания (type of service). Это - 8-битовое поле, представляющее тип обслуживания, которое должен получить пакет, и оно имеет, как говорит RFC [58], «неустойчивую историю». RFC791 первоначально определил байт TOS в заголовке IP, позже, 8-битовое поле TOS было переопределено в RFC 1122, 1349, 1455 и 2481.

Общая длина (total length) является 16-битовым полем, представляющим общую длину IP-пакета в байтах. Наибольший пакет в Интернете имеет 2^{16} или 65535 байтов в длину. Многие системы IDS создают сигнал тревоги, когда получен IP-пакет с полем протокола в заголовке IP, заданным как 1 (ICMP) и общей длиной, заданной числом больше 1024. Например, «Ping of Death» («Пинг смерти») представляет собой эхо-запрос ICMP (ping) IP фрагмента, в котором общий восстановленный пакет будет больше 65535 байт.

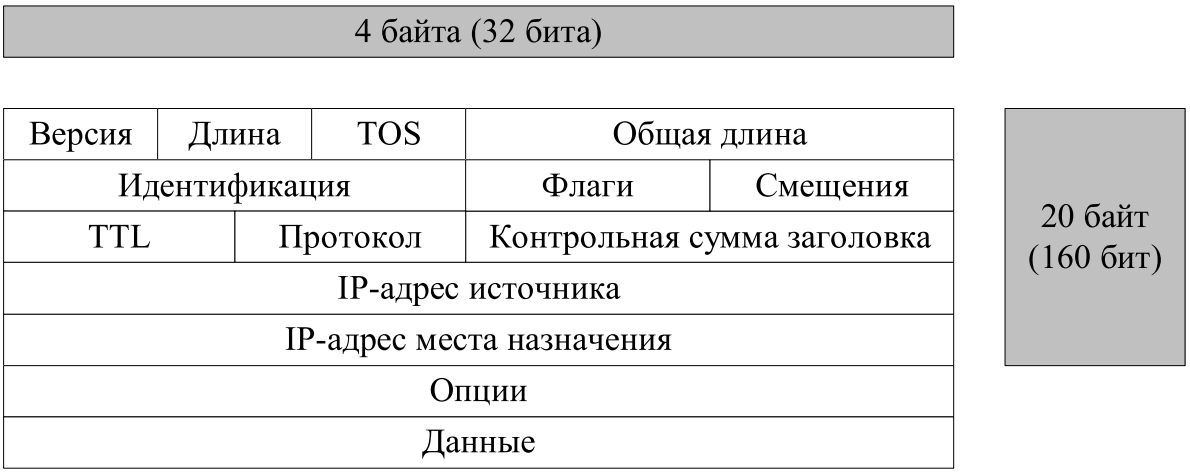

Рисунок 2.3. Компоновка протокола Интернета (IP версии 4)

Следующие три поля - идентификация (identification), флаги (flags) и смещение (offset) - необходимы для фрагментации IP, но прежде чем обсуждать эти поля, необходимо немного познакомиться с фрагментацией.

Не все сети имеют пакеты одинакового размера. Сети Ethernet используют размер MTU (Максимальная единица передачи) равна 1518 байт на пакет. Многие сети token-ring применяют значительно больший размер пакета. В некоторых сценариях маршрутизатор должен фрагментировать входящие пакеты, поскольку они слишком большие для сети, которую обслуживает маршрутизатор. Такая фрагментация IP будет происходить, когда сеть token-ring общается с Ethernet. На рисунке 2.4. показана работа фрагментации IP.

16-битовое поле идентификации в пакете 1 будет иметь значение, идентичное значению в пакетах 2, 3 и 4 (рисунок 2.4.). Пакет в 4048 байт получается маршрутизатором, но это много для Ethernet, поэтому маршрутизатор этот пакет фрагментирует на меньшие пакеты, которыми может управлять Ethernet. Так как пакеты 2, 3, 4 имеют одинаковые значения поля идентификации, получающая машина знает, что данные четыре пакета составляют один пакет, и будет пытаться реконструировать пакеты в одну сущность.

Рассмотрим компоновки заголовка на рисунке 2.3, где 3-битовое поле флагов (биты 0,1,2) обеспечивают управление фрагментами:

- Бит 0 зарезервирован и не используется.
- Бит 1 является битом нефрагментирования. Когда задан бит 1, он приказывает маршрутизатору «не фрагментировать» пакеты. Когда бит 1 не задан, пакет может фрагментироваться.

- Бит 2 является битом последнего фрагмента или дополнительных фрагментов. Он задается для указания, что пакет содержит дополнительные фрагменты.

13-битовое поле смещения (Offset) является счетчиком байтов, который сообщает получающей системе, где располагается пакет в общей схеме всех полученных фрагментов.

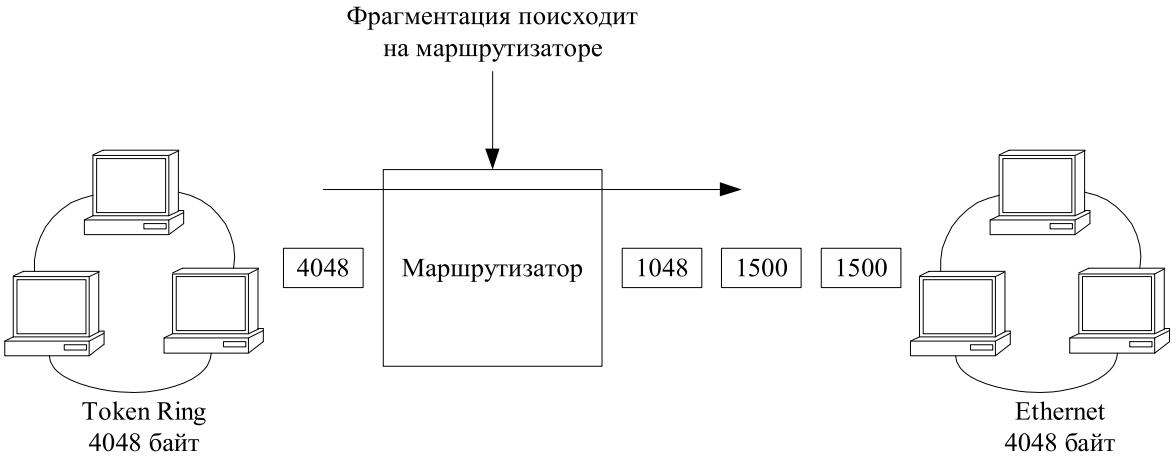

Рисунок 2.4. Работа фрагментации IP

TTL означает time to live (время жизни), 8-битовое поле, определяющее максимальное число переходов (hop), которое может выполнить пакет. Например, если TTL пакета равен 32, то он может пройти или перепрыгнуть через 31 маршрутизатор, прежде чем TTL уменьшится до 0. Когда TTL пакета уменьшается до 0, то посылающей машине возвращается пакет ICMP, сообщающий о превышении времени жизни.

Поле протокола (protocol) является 8-битовым полем, которое указывает, какой тип заголовка следует за заголовком IP. Поле заголовка может содержать одно из определенных значений списка. Вот некоторые из наиболее распространенных значений протоколов:

- 1 Пакет IP содержит пакет ICMP
- 6 Пакет TCP
- 17 Пакет UDP

RFC762 определяет значения и их соответствующие протоколы, а некоторые популярные системы IDS создают тревожный сигнал, когда в поле протокола задано нестандартное значение..

Для обеспечения неизменности данных в заголовке используется поле контрольной суммы заголовка, которое является 16-битовым числом и представляет собой контрольную сумму (числовой уникальный идентификатор) для всего заголовка IP.

IP-адрес источника является 32-битовым IP-адресом системы, посылающей пакет. Важно понимать, что каждая машина в сети TCP/IP имеет IP-адрес, который является «телефонным номером» системы, когда она со-

единяется с сетью. Все вызовы, поступающие или посылаемые компьютером, помечаются IP-адресом соответствующей рабочей станции во время, когда она делает или получает вызов.

Наиболее распространенным способом указать IP-адрес системы является метод десятичных значений с точками, который представляет 4-байтный IP-адрес как четыре значения между 0 и 255, разделенных точкой, такой как 149.16.12.8. Любое значение в IP-адресе является десятичным представлением каждого 8-битового значения в 32-битовом поле адреса.

Программное обеспечение перехвата Ethereal показывает 12 полей заголовка IP в удобном для пользователя формате. Можно выделить любое поле заголовка, а Ethereal укажет, какие шестнадцатеричные значения соответствуют выбранному полю. Шестнадцатеричная система счисления является лучшей системой для просмотра данных, генерируемых компьютерами, так как шестнадцать равно общему числу значений, которые может иметь 4-битовый отрезок данных. Поэтому шестнадцатеричная система позволяет использовать метод представления значения байта с помощью двух алфавитно-цифровых символов, а данные в пакете выводятся в шестнадцатеричном формате. При трансляции в ASCII (удобочитаемом для людей) они получают значительно больше смысла. Уверенное использование шестнадцатеричной распечатки сетевых данных является критически важным для тех, кто должен выполнять сетевой надзор.

Соответствие RFC

Традиционно неиспользуемые зарезервированные поля в заголовках TCP/IP изменяются различными атакующими утилитами для отправки пакетов, не соответствующих RFC, что означает, что пакеты не придерживаются установленных правил и являются плохо сформированными. Пакеты, не соответствующие RFC, могут использоваться для сокрытия устройства каналов или для изучения системных ответов на плохо сформированные пакеты для определения операционной системы рабочей станции.

Чтобы опознавать соответствие самым последним RFC, системы обнаружения вторжения и брандмауэры должны обновляться. Например, недавние изменения в поля типа обслуживания реализуют новые значения, которые могут заставить некоторые системы IDS ложно предупреждать сетевых администраторов, что в их сетях выполняется некая утилита, ощупывающая стек TCP /IP.[38]

Знание полей заголовка IP может помочь при обнаружении, предотвращении и мониторинге атак. Список полей и как их можно использовать:

- Чтобы защитить себя от потока ICMP, «Ping of Death» (фрагментированных пакетов ping, которые превышают максимальный размер пакета IP) и атак «Smurf» (широковещательных пакетов ping) можно заблокировать все пакеты с полем протокола, равным 1 (ICMP).

- Чтобы блокировать все фрагментированные пакеты, можно отбрасывать пакеты IP со значением дополнительного фрагмента поля флат заголовка IP равного 1 биту.
- Для мониторинга трафика, приходящего или уходящего с системы с IP-адресом, например 192.168.0.100, можно перехватывать все пакеты, которые имеют 192.168.0.100 в полях IP-адрес источника и IP-адрес места назначения заголовка IP.
- Чтобы помешать некоторым IP-адресам источника непрерывно сканировать сеть, можно заблокировать все пакеты с IP-адресом источника инициирующей сети.

Заголовок TCP

TCP отвечает за предоставление надежной доставки пакетов и является, вероятно, самым распространенным протоколом в вычислительной сети. Заголовок TCP содержит известные номера портов, которые определяют, какие службы должны обрабатывать пакет при его получении, и функционирует на транспортном уровне модели OSI. Конструкция заголовка подробно описана в RFC793, а компоновка показана на рисунке 2.5.

Знание полей заголовка TCP помогает в обнаружении, предотвращении и мониторинге атак. Для предотвращения передачи файлов с ваших серверов ftp неавторизованным пользователям, целесообразно заблокировать все входящие пакеты со значением порта назначения TCP, равным 21.

4 байта (32 бита)	
Порт источника	Порт места назначения
Порядковый номер	
Подтверждение	
Информация заголовка	Размер окна
Контрольная сумма TCP	Указатель срочности
Опции	
Данные	

20 байт (160 бит)

Рисунок 2.5. Компоновка заголовка TCP

Например, чтобы помешать сотрудникам, тратить дорогостоящие рабочие часы на использование IRC (Internet Relay Chat), можно заблокировать пакеты, исходящие из сети с портом места назначения в диапазоне от 6665 до 7000. Или, если нужно, выполнять мониторинг сообщений, которые посылают сотрудники, можно сконфигурировать систему для перехвата всего трафика из сети, уходящего на порт места назначения 25.

Конечно, можно использовать и другие решения для всех этих ситуаций, такие как сервер ftp, использующий порт, отличный от используемого по умолчанию порта 21, и блокирование известных портов службы.

Порт источника является 16-битовым полем, которое ссылается на посылающее приложение. Порт места назначения является 16-битным полем, которое ссылается на получающее приложение. Когда вы соединяетесь с удаленной машиной, ваша операционная система выбирает порт источника, часто описываемый как эфемерный порт, так как он существует в течение короткого времени (обычно только во время данного соединения). Эти эфемерные порты являются произвольными. Номера портов бывают больше 1024. Если для соединения с сервером используется браузер, то он выберет эфемерный порт источника и пошлет пакеты в используемый по умолчанию порт места назначения, который будет портом 80. Когда сервер отвечает и передает данные на вашу машину, он будет посылать данные на эфемерный порт, который выбрала система для этого конкретного сеанса telnet. На рисунке 2.6. показано, как это работает.

Поля порядкового номера и подтверждения на рисунке 2.5 являются 32-битовыми счетчиками. Данные поля показывают, сколько байтов было послано и получено во время соединения, так как TCP является дуплексным коммуникационным каналом.

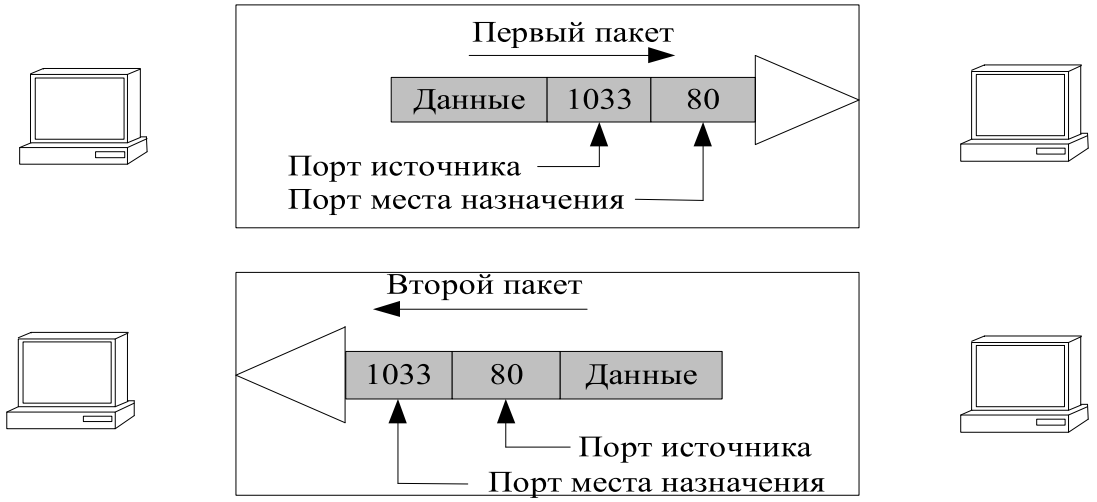

Рисунок 2.6. Типичное соединение Web

Это означает, что информация может перемещаться между отправителем и получателем в обоих направлениях. Таким образом, каждая сторона соединения должна поддерживать различный порядковый номер, считающий число байтов, которое он посылает. Номер подтверждения является следующим порядковым номером, который отправитель подтверждения ожидает получить. Ваш порядковый номер указывает, сколько байтов по-

слала система. Система также посылает номер подтверждения, который предвосхищает следующий порядковый номер от удаленной машины.

Поле информации заголовка является 16-битовым полем, которое содержит длину заголовка TCP, несколько резервных битов и шесть битов флагов. Необходимо хорошо понимать значение этого поля, так как многие методы опознания цели, которые используют атакующие, включают переключение различных битов (сканирование портов и ощупывание стека TCP/IP) в поле информации заголовка [38]/ На рисунке 2.7 показана конфигурация битов поля информации заголовка.

		Биты					
Длина	Зарезервировано	URG	ACK	PSH	RST	SYN	FIN

Рисунок 2.7. Резервные биты в заголовке TCP

Биты 0-3 представляют длину заголовка в 32-битовых словах (максимально 60 байт).

Биты 4-9 являются зарезервированными для будущего использования. Они обычно заданы как 0, хотя протокол ECN (Explicit Congestion Notification — Уведомление о явной скученности) (RFC2481) предложил использование битов 8 и 9. Если ECN реализован, бит 8 становится битом сокращения окна скопления, а бит 9 — битом ECN-Echo.

Биты с 10 по 15 являются управляющими битами. Эти шесть битов указывают, какой тип пакетов TCP передается:

- Бит 10 является флагом URG. Он задается для активации поля указателя срочности, которое обозначает конец срочных данных в пакете.
- Бит 11 является флагом ACK (Acknowledgement — подтверждения). ACK задается всякий раз, когда данные успешно принимаются удаленным хостом.
- Бит 12 является флагом PSH (push — выталкивания). Он задается, чтобы разрешить приложению избежать буферизации TCP. Стек TCP/IP буферизирует пакеты и ожидает дополнительных данных, прежде чем передать пакеты получающему приложению. Флаг выталкивания посылает пакеты непосредственно ожидающему процессу, предполагая, что приложение может обработать окно пакетов, доставленных ему. Однако сегодня стек TCP/IP хоста определяет, когда задавать этот бит.
- Бит 13 является флагом RST (reset — сброс в исходное состояние). Он задается при получении пакета, который кажется неправильным

пакетом. Это может происходить, когда одно из шести полей, которые составляют сеанс TCP/IP, будет не тем, что ожидается.

- Бит 14 является флагом SYN (синхронизация). Он задается для инициализации порядковых номеров в начале соединения.
- Бит 15 является флагом FIN (конец). Он задается, чтобы указать, когда отправитель закончил передачу информации.

Вернемся к рисунку 2.5. Следующее поле в заголовке TCP является 16-битовым полем размера окна, представляющим собой число байтов, которое способна получить рабочая станция во время каждой транзакции пакетов. Создатели TCP решили, что никто не будет посылать по одному пакету за раз и ждать подтверждения, прежде чем посылать другой пакет, так как в этом случае сети просто работали бы слишком медленно. Поэтому поле размера окна позволяет машине принимать несколько пакетов и посылать только один подтверждающий пакет в ответ.

Поле контрольной суммы TCP является 16-битовой контрольной суммой для всей полезной нагрузки пакета, включая заголовок TCP, а также данные [38].

Последним полем в заголовке TCP, помимо различных опций TCP, является 16-битовое поле указателя срочности.[82] Когда используется указатель срочности, посылающая система сообщает получающей системе, что срочные данные некоторого вида были помещены в поток данных сеанса. Указатель срочности должен использоваться во время передачи большого файла. Если вы решите прервать передачу, клиент протокола передачи файла будет задавать указатель срочности.

Соединения на основе TCP всегда начинаются с так называемого трехходового квитирования. Важно понимать этот обмен, так как каждое завершенное трехходовое квитирование обозначает начало нового сеанса соединения.

Для того, чтобы обмануть брандмауэры, которые фильтруют порты, порт источника часто изменяется утилитами хакеров. Хорошим примером такого инструмента хакера является бесплатно доступная, мощная утилита сканирования портов программа Nmap, которая имеет параметр -g, позволяющий произвольно выбрать порт источника. Атакующие обычно сканируют с порта источника 53 (отвечает DNS), 80 (отвечает Web-сервер), 20 (отвечает FTP), или 110 (отвечает сервер почты). Эти порты-источники редко фильтруются брандмауэрами или маршрутизаторами; поэтому сканирование не блокируется, когда оно инициируется с данных портов.

Следует понимать, что соединения, которые не завершают трехходовое квитирование, могут выполнять полусканирование системы для определения, какие порты в данный момент открыты. Полусканирование позволяет атакующему перенумеровать выполняемые службы скрытым образом, так как полусканирование редко фиксируется в журнале на хосте. Когда атакующий знает, какие порты были открыты, он лучше подготовлен

для успешной атаки системы. Поэтому важно, чтобы персонал, обеспечивающий информационную безопасность, идентифицировал те пакеты, которые не имеют намерения соединиться с системой, так как такое сканирование портов является предшественником полноценной сетевой атаки.

Еще одними уязвимыми местами базового протокола передачи данных TCP/IP являются черные ходы на младших портах.

Многие случаи можно превратить из проступка в уголовное преступление в зависимости от объема повреждения и/или доступа, которого добился атакующий. Если вы обнаруживаете незаконный сервер на порте 999, то вы знаете, что атакующий имеет доступ административного уровня в некотором месте, так как порт 999 является зарезервированным портом. Злоумышленник не сможет открыть службу на порте меньше 1024, если не имеет доступ административного уровня, следовательно он представляет значительно большую угрозу для жертвы и может читать, писать или удалять любую информацию в сети.

Еще одним слабым местом является Сетевой анализатор, который представляет собой оборудование или программу, которые пассивно перехватывают пакеты во время их прохождения в сети. Наиболее распространенными сетевыми анализаторами являются программы, которые позволяют сетевой интерфейсной плате (NIC) обрабатывать пакеты, предназначенные для множества различных рабочих станций. Система, выполняющая сетевой анализатор, может перехватывать сообщения, пароли, пересылки файлов, перемещение и любые другие виды трафика в сети [82].

Программные сетевые анализаторы работают, переводя сетевой адаптер в неразборчивый режим, называемый так потому, что он будет принимать весь трафик, с которым он вступает в контакт. Обычно вычислительная среда отвечает на два типа пакетов: которые предназначены IP-адресам системы и которые имеют сетевой адрес широковещания.

Если IP-адрес компьютера 147.7.4.11, сетевой адрес 147.7.4.0 и маска сети 255.255.255.0, машина будет обычно обрабатывать пакеты, предназначенные для IP-адреса 147.7.4.11 (вашего IP-адреса) и 147.7.4.255 (адрес широковещания вашей сети). Когда сетевой интерфейс переведен в неразборчивый режим, сетевой адаптер не подавляет пакеты, предназначенные для других компьютеров, но вместо этого направляет их в стек TCP/IP для дополнительной обработки. Пакеты по-прежнему приходят своим назначенным получателям, но отправитель не знает о том, что вы также получили информацию.

Представим некую сеть из 4х ЭВМ, а концентратор является широковещательным или «тупым» и будет пересылать весь трафик по каждому присоединенному к нему кабелю. В этом случае весь трафик, идущий к машине A, будет также проходить к машинам B, C и D. Так как все сетевые адаптеры видят один и тот же трафик, то говорят, что эти четыре рабочие станции находятся в одном сегменте. Если сеть имеет сегмент с 40

отдельными хостами, то значит, что все они «видят» один и тот же трафик и следовательно сетевой анализатор атакующего на одном из хостов потенциально компрометирует все остальные. С другой стороны сетевой анализатор службы безопасности может выполнять мониторинг всего сетевого трафика 40 рабочих станций.

Отсюда можно сделать вывод о важности реагирования на случаи нарушения информационной безопасности узла, поиска и идентификации всех сетевых анализаторов на рабочих станциях-жертвах. Если на ПЭВМ найден действующий сетевой анализатор, необходимо определить общее число скомпрометированных узлов как весь сегмент, а не как единственную рабочую станцию.

Когда вы ищете транзакционную информацию («не относящуюся к содержимому»), можно использовать в сети то, что правоохранительные органы называют автоматическим самописцем/ловушкой и трассировкой. В вычислительных сетях применение ловушки и трассировки означает мониторинг заголовков IP и TCP (или других заголовков протоколов транспортного уровня) без выполнения мониторинга содержимого пакетов пользователя. Это ненавязчивый способ определения источника атаки на основе сети или обнаружения аномалий сетевого трафика, таких как программы черного хода, которые невозможно обнаружить обычными системами обнаружения вторжений. Мониторы, создающие ловушки и выполняющие трассировку, можно реализовать с помощью бесплатно доступных, стандартных утилит, таких как tcpdump, snoop, snort, или утилит с графическим интерфейсом пользователя (GUI), таких как netmon (Windows) [108,103,104].

Так как мониторы tcpdump и snoop являются старыми промышленными стандартами (snoop доступен для машин Solaris), мы будем использовать их в качестве примеров. Утилита tcpdump для Windows, называемая WinDump, полностью совместима с tcpdump и может использоваться для наблюдения и диагностики сетевого трафика согласно тем же правилам, что и tcpdump. Файлы захвата утилит имеют одинаковый двоичный формат - поэтому можно захватывать трафик с помощью tcpdump и просматривать его с помощью WinDump. Следующая командная строка инициирует ловушку и трассировку без фильтрации и печатает вывод на экране:

```
[root@linux taps]# tcpdump
tcpdump: listening on eth0
```

Если вы работаете в занятой сети, то увидите многочисленные повторы строки заголовка tcpdump. Данная программа является достаточно удобной для создания заголовка с многочисленными полями, перенесенными из заголовка IP и TCP [38].

Основной заботой при использовании ловушки и трассировки является уклонение от вторжения в чьи-либо секреты при перехвате каких-либо передаваемых пользователем данных. Важно помнить, что многие

утилиты захватывают некоторое количество байтов по умолчанию, и можно случайно захватить содержимое пакета. Заголовки IP и TCP используют обычно всего 40 байт, но различные опции могут увеличить это значение. По умолчанию программы tcpdump определяют для захвата 68 байт на пакет, но если необходимо выводить результат на экран, то может получиться ненавязчивый просмотр трафика в сети.

При выполнении ловушки и трассировки лучше создавать постоянный файл вывода, а не просматривать текущие данные на консоли. Без создания файла вывода информация теряется в тот момент, когда прекращается процесс tcpdump, snoop или WinDump [110,108,103,104].

Следующая командная строка будет запускать процесс захвата информации заголовка на всем трафике, который воспринимает сетевой адаптер на анализирующей сеть рабочей станции:

i[root@homer /root]# tcpdump > traptracel

Если анализируемая сеть активно используется, то желательно быстро остановить процесс tcpdump, так как файл traptracel может стать очень большим за короткий период времени.

Достаточно часто возникает необходимость записывать файлы в двоичный файл вывода — единственный способ сохранить постоянную запись данных. Для этого можно использовать параметр *-w* с утилитой tcpdump или WinDump. При использовании snoop применяется параметр -o.

Следующая командная строка создает двоичный файл вывода, называемый trapfflel, в текущем рабочем каталоге, где выполняется tcpdump. [rootelinux taps]# tcpdump -x -v -i ethO -w trapfilei tcpdump: listening on ethO

Так как параметр *-s для* определения длины снимка не специфицирован, tcpdump использует по умолчанию первые 68 байт информации каждого пакета, что может оказаться слишком большим значением для ловушки и трассировки. Некоторые протоколы содержат данные пользователя в первых 68 байтах, такие как userid (идентификатор пользователя) или пароль. Если длины заголовка IP и заголовка TCP вместе составляют 40 байт (что часто бывает), tcpdump будет захватывать дополнительно 28 байт информации пользователя.

Так как tcpdump, snoop и WinDump сохраняют свои файлы вывода в двоичном формате, мы не можем просто прочитать их как обычные текстовые файлы. Чтобы просмотреть перехваты, сделанные с помощью параметра *-w,* используется параметр - r с помощью той же утилиты следующим образом: [root§lmux taps]# tcpdump -x -v - r trapfilei | less [root§solaris]# snoop -i trapfile2 | more.

Многие атаки типа «отказ в обслуживании» используют поддельные значения фрагментации IP для «замораживания» системы-жертвы. Если вы встретите систему, которая постоянно зависает, необходимо выполнить ловушку и трассировку, чтобы определить, связана ли проблема с атакой

«отказ в обслуживании» на основе сети или просто система имеет какие-то проблемы с аппаратом или программой.

Рассмотрим фрагмент из ловушки и трассировки. (номера строк были добавлены автором):

1) 16:07:40.872940 192.168.0.200.domain > 192.168.0.210.netbios-ns: 0 [0q] (10) (frag 242:18@0+)

2) 16:07:40.872945 192.168.0.200> 192.168.0.210: (frag 242:116(348)

3) 16:07:40.872986 [|udp] (frag 242:224@0+)

Пакет 1 является IP-пакетом из 18 байт, прибывшим из порта 53 *(domain)* в порт 139 *(netbios-ssn)*. Общая длина пакета равна 38 байт. Порт источника 53 предполагает ответ на запрос DNS. Но запросы DNS обычно бывают меньше 150 байт, но смещение равно 0 и знак + указывает, что ожидаются дополнительные фрагменты. Следующее смещение должно быть 38, так как первый фрагмент имел 18 байт.

Пакет 2 имеет тот же самый идентификатор фрагмента (ID), что и пакет 1. Предполагается, что это фрагмент исходного пакета. Так как за смещением в 48 байт не следует знак плюс, то можно предположить, что это последний фрагмент для идентификатора пакета (ID) 242. Но затем идет пакет 3 с тем же самым идентификатором фрагмента (ID).

Пакет 3 имеет смещение 0, но предположительно это третий фрагмент. Рассматриваемый здесь пример, является атакой отказа в обслуживании Nestea, которая была преобладающей в начале 1998 г. Эта атака могла «заморозить» почти любую операционную систему в то время, когда она появилась.

Теперь вы видите, что знание того, как осуществляется коммуникация сети, является жизненно важным для любого профессионала сетевой безопасности. Хорошее понимание заголовков TCP/IP является критически важным для соответствующего перехвата данных, фильтрации и блокирования специфических типов трафика, распознавания атак и защиты сетей от атак.

2.2. Методы и способы обнаружения признаков преступных посягательств

На современном этапе развития общества сохраняется устойчивая тенденция к нарушению безопасности информации на всех стадиях ее обработки, хранения и передачи. Причины постоянного совершенствования процедур неправомерного доступа в сфере компьютерной информации кроются в высокой латентности этого вида преступлений.

Анализ статистики преступлений в сфере компьютерной информации с 1997 по май 2009 года указывает на постоянный существенный рост числа подобных противоправных деяний.

Противоправные деяния в сфере компьютерной информации совершаются в целях получения информации ограниченного доступа и последующей продажи ее третьим лицам, при этом содержание информации может быть различным. Изучение проблем расследования правонарушений в сфере компьютерной информации выступает одной из острейших задач современной криминалистической науки [60].

В сложившейся ситуации просматривается глобальная тенденция по совершенствованию средств обнаружения, противодействия и предотвращения попыток неправомерного доступа в вычислительных сетях любого уровня.

Информационная безопасность общества, государства и личности характеризуется степенью их защищенности и, следовательно, устойчивостью основных сфер жизнедеятельности (экономики, науки, техносферы, управления, военного дела, общественного сознания и т.д.) по отношению к опасным, дестабилизирующим, деструктивным, ущемляющим интересы страны информационным воздействиям на уровне как внедрения, так и извлечения информации. Информационная безопасность определяется способностью нейтрализовать такие воздействия [35].

Данный процесс достаточно динамичен, так как постоянное совершенствование процедур неправомерного доступа влечет за собой адекватное совершенствование и повышение надежности средств и методов обнаружения атак, аналитической обработке сообщения о подобных воздействиях. Система защиты компьютерной сети и обнаружения атак должна быть интегрирована во всей локальной вычислительной сети и обязательна для исполнения. Пользователи должны быть уверены в том, что информация адекватно защищена.

Построение эффективной системы обеспечения информационной безопасности невозможно без анализа известных процедур неправомерного доступа, что, в том числе, напрямую связано с трасологическими исследованиями. Следы неправомерного доступа к компьютерной информации, в силу специфики рассматриваемого вида преступлений, редко остаются в виде изменений внешней среды, однако, это не означает, что ма-

териальных следов не остается вообще. Прежде всего, они остаются на магнитных носителях и отражают изменения, по сравнению с исходным состоянием, в хранящейся в них информации.

Следы неправомерного доступа к компьютерной информации целесообразно разделить на два типа: традиционные и нетрадиционные следы.

Традиционные следы – следы отображения, следы вещества, следы предметы довольно полно рассматриваются классической трасологией и, как правило, могут находить проявления при совершении преступлений связанных с неправомерным доступом к компьютерной информации. Следами могут являться какие-либо рукописные записи, распечатки, свидетельствующие о приготовлении к совершению преступления и оставленные на месте преступления. Следы пальцев рук, микрочастицы на клавиатуре, дисководах, принтере, вычислительной технике, магнитных носителях и CD-ROM дисках.

К подобным следам можно отнести физическое разрушение объектов вычислительной сети (например, следы взрыва, поджога), вывод из строя отдельных наиболее важных компонентов (Устройств, носителей важной информации, лиц из числа персонала, владеющих ключевой информацией и т.п.), отключение или вывод из строя подсистем обеспечения функционирования (например, электропитания, охлаждения и вентиляции, линий связи и т.п.), действия по дезорганизации функционирования компьютерной сети (например, постановка мощных активных радиопомех на частотах работы устройств системы), применение подслушивающих устройств, дистанционная фото- и видеосъемка, перехват побочных электромагнитных излучений и т.п. И конечно же наиболее опасные – это внедрение агентов в число персонала компьютерной сети и вербовка (путем подкупа или шантажа) сотрудников. Обнаружением следов подобных преступлений занимаются специальные подразделения в составе правоохранительных органов.

Следы неправомерного доступа к компьютерной информации, в силу своей специфики, редко остаются в виде изменения внешней среды. Однако, это не означает, что следов не остается вообще. Прежде всего, они остаются на магнитных носителях и отражают изменения, по сравнению с исходным вариантом, в хранящейся в них информации.

Нетрадиционные следы остаются благодаря осуществлению неправомерного доступа к компьютерной информации и представляют собой любые изменения исходной компьютерной информации. В первую очередь на неправомерный доступ указывают:

✓ изменения в заданной ранее конфигурации компьютера (например, изменение картинки и цвета экрана при включении, изменение порядка взаимодействия с периферийным оборудованием, появление новых и удаление прежних устройств);

✓ необычные проявления в работе электронно-вычислительной машины (например, замедленная загрузка операционной системы, замедленная реакция компьютера на ввод с клавиатуры, замедленная работа компьютера при записи и считывании информации с дисковых накопителей, неадекватная реакция на команды пользователя).

Наиболее явными, следами доступа постороннего лица к охраняемой законом информации, обрабатываемой в вычислительных сетях, могут являться изменение стандартных реквизитов, размеров и содержимого файлов (изменение статуса файла, например, только чтение, архивный, скрытый, системный) и переименование существующих или появление новых каталогов и файлов.

В свою очередь более скрытыми, для неспециалиста, следами неправомерного доступа к охраняемой законом компьютерной информации являются результаты работы антивирусных программ (например, результаты работы распространенной антивирусной программы «DrWeb» отображаются в файле «report.web», содержимое которого легко просмотреть), программного обеспечения и в случае подозрения на неправомерный доступ их обнаружение не занимает много времени.

Признаки совершения противоправных действий, связанных с неправомерным доступом к компьютерной информации представляют собой следы, оставленные злоумышленником. Чаще всего преступник использует не один метод неправомерного доступа, а их совокупность для достижения поставленной цели.

Проявлениями подобного опосредованного доступа могут являться [98]:

✓ физические следы разрушения компьютерной сети, такие как следы взрыва, поджога и т.д.;

✓ вывод из строя отдельных компонентов компьютерной сети, устройств, носителей информации;

✓ воздействия на лиц из числа персонала владеющих ключевой информацией;

✓ отключение или умышленный вывод из строя подсистем обеспечения функционирования компьютерной сети, таких как, электропитание, охлаждение, линии связи и т.д.;

✓ постановка активных помех на частотах работы устройств и другие действия по дезорганизации работоспособности вычислительной сети;

✓ применение подслушивающих устройств, дистанционная фото-, видеосъемка, перехват побочных электромагнитных излучения;

✓ подключение к линиям связи вычислительных систем и т.д.

Обнаружением подобных признаков преступлений занимаются специализированные подразделения с применением специальной аппаратуры.

На непосредственный неправомерный доступ к компьютеру указывают следующие изменения [65]:

✓ в заданной конфигурации. Например, изменение картинки и цвета экрана при включении, изменение порядка взаимодействия с периферийным оборудованием, появление новых и удаление прежних устройств;

✓ стандартных реквизитов, размеров и содержимого файлов. Например, изменение такого статуса файла, как только чтение, архивный, скрытый, системный;

✓ переименование существующих и появление новых каталогов;

✓ необычные проявления в работе электронно-вычислительной машины.

Например, замедленная загрузка операционной системы, замедленная реакция компьютера на ввод с клавиатуры, замедленная работа при записи и считывании информации с дисковых накопителей, неадекватная реакция на команды пользователя.

Постоянный рост информационной составляющей общества вызывает развитие программных средств обеспечения безопасности. Причина этого заключается в том, что происходит все большее совершенствование процедур осуществления неправомерного доступа к компьютерной информации. Любая подобная процедура состоит из трех этапов: сбор информации, реализация и завершение атаки.

На первом этапе происходит изучение нарушителем топологии сети, идентификация узлов и операционных систем, роли узла, уязвимостей и сканирование портов.

На втором этапе осуществляется непосредственное проникновение в узел и установление контроля над ним.

На завершающем этапе производится чистка логов и устранения физических следов неправомерного доступа. Анализ популярных средств обеспечения информационной безопасности на уровне сети показывает, что они, в качестве источника данных, используют сетевой трафик или журналы регистрации сетевого программно-аппаратного обеспечения. Оно фиксирует обрабатываемый трафик и анализирует его на наличие признаков атак.

В настоящее время для обеспечения требуемого уровня безопасности, чаще всего, используются межсетевые экраны, функционирование которых основано на правилах разрешения или запрещения прохождения трафика.

Межсетевые экраны определяются как «локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в или выходящей из автоматизированной системы. Межсетевые экраны обеспечивает защиту посредством фильтрации информации, то есть ее анализа по совокупности критериев и принятия решения о распространении на основе заданных правил, проводя, таким образом, разграничение доступа субъектов. Каждое правило запрещает или разрешает пе-

редачу информации определенного вида между субъектами и объектами. Как следствие, составляющие компоненты сети получают доступ только к разрешенным информационным объектам. Интерпретация набора правил выполняется последовательностью фильтров, которые разрешают или запрещают передачу данных (пакетов) на следующий фильтр или уровень протокола» [20].

Обычно межсетевые экраны защищают внутреннюю сеть от атак («вторжений»), но могут использоваться и для защиты от «нападений» извне. В этом случае вырабатывается конкретная политика безопасности определяющая тип трафика, который будет восприниматься брандмаузером как «авторизированный». Например, необходимо решить, будет ли ограничен доступ пользователей к определенным службам на базе наиболее используемого протокола TCP/IP, и если будет, то до какой степени. Выработка политики безопасности позволит выяснить, какие компоненты брандмауэра необходимы и как их сконфигурировать, чтобы обеспечить ограничения доступа.

Межсетевые экраны реализуются на базе подобных Unix-систем, таких как Solaris, BSDI, Linux и т.д., а также Windows. При этом настоятельно рекомендуется использовать для установки firewall отдельную станцию с соответствующими аппаратными требованиями, кроме того, в ядро операционной системы для межсетевых экранов вносятся некоторые изменения, повышающие защищенность. Например, запрещается иметь на шлюзе разделы пользователей, так как некоторые из них работают только в однопользовательском режиме и формируют специальные коды для отслеживания целостности программного обеспечения.

Передаваемые по сети данные представляют собой набор пакетов использующих для передачи данных набор протоколов TCP/IP. Каждый такой пакет имеет исходящий и входящий IP-адрес, а также указание на службу TCP/IP, которая будет его обрабатывать.

Модель OSI, разработанная Международной организацией по стандартизации (International Standards Organization — ISO), определяет семь уровней, на которых рабочие станции вычислительной сети взаимодействуют друг с другом, — начиная с уровня физической среды передачи данных и заканчивая уровнем прикладных программ, используемых для коммуникаций. В общем случае, чем выше уровень модели OSI, на котором брандмауэр фильтрует пакеты, тем выше и обеспечиваемый им уровень защиты.

Большинство из существующих коммерческих систем межсетевых экранов предусматривает сокрытие внутренней структуры IP-сети организации (так называемый network address translation). Обычно экраны настраивается как минимум на два интерфейса: внутренний — для локальной сети и внешний. Кроме того, существует вариант интерфейса для подключения так называемых демилитаризованных зон — Web и FTP серверов.

Коммерческие продукты межсетевых экранов зачастую обладают графическим интерфейсом и мощными средствами администрирования, позволяющими формировать гибкие правила фильтрации. Однако производители продуктов утверждают, что использование графического интерфейса замедляет работу системы, и советуют запускать ее из командной строки. Кроме того, серьезный межсетевой экран должен иметь возможность удаленного конфигурирования и управление системой, а также протоколирования событий, например, попыток неправомерного доступа и т.д. [54].

Общеизвестно, что межсетевые экраны настраиваются специалистами в сфере защиты информации, а им, как и всем людям, свойственно ошибаться. Настроенный экран фильтрует трафик и принимает решения о пропуске или блокировании сетевых пакетов на основе информации об используемом протоколе. Проверка на соответствие осуществляется на основании установленных правил.

Если вернуться к этапам осуществления неправомерного доступа, то можно обратить внимание на то, что используемые механизмы защиты вычислительных сетей, реализованные на основе межсетевых экранов, серверов аутентификации или систем разграничения доступа работают только на втором этапе.

То есть, по существу, они являются средствами блокирующими, а не упреждающими атаки. В абсолютном большинстве случаев они защищают от атак, которые уже находятся в процессе осуществления. И даже если они смогли предотвратить ту или иную атаку, то намного более эффективным было бы упреждение, т.е. устранение самих предпосылок реализации вторжений. Комплексная система обеспечения информационной безопасности должна работать на всех трех этапах осуществления атаки. И обеспечение адекватной защиты на третьем, завершающем, этапе не менее важно, чем на первых двух. Ведь только в этом случае можно реально оценить ущерб от «успешной» атаки, а также разработать меры по устранению дальнейших попыток реализовать аналогичную атаку.

На современном этапе требуется специальное программное обеспечение, которое в результате анализа файлов отчета о работе вычислительной сети позволяет установить:

1. Компьютер, с которого был произведен неправомерный доступ;
2. Время и продолжительность соединения одной рабочей станции с другой;
3. Протокол выхода в вычислительную сеть, который автоматически ведется на каждом компьютере;
4. Данные, о пользователе, определяемые по адресу его электронной почты, назначенном системным администратором;
5. Содержание переговоров через вычислительную сеть, информация о которых автоматически сохраняется во временных файлах, которые,

как говорилось ранее, даже после стирания могут быть частично восстановлены.

Соответствующее программное обеспечение следует разделить на две категории, направленные на:

- обнаружение злоупотреблений;
- обнаружение аномалий.

К злоупотреблениям следует отнести типы атак, которые используют известные уязвимости вычислительной сети и, как следствие, легко обнаруживаются. Система обнаружения злоупотреблений содержит описание существующих видов вторжений и ищет соответствие этим описаниям в проверяемом потоке данных.

К достоинствам системы обнаружения злоупотреблений следует отнести незначительное количество ложных тревог и как следствие уменьшение времени необходимого для анализа работы вычислительной сети. Это в свою очередь, является и ее недостатком, так как она работает только с известными видами и не может определять ранее неизвестные типы и принципы атак.

К аномалиям следует отнести любую необычную деятельность, которая может оказаться атакой. Обнаружение аномалий использует модели предполагаемого поведения пользователя и приложений, интерпретируя отклонения от «нормального» поведения как потенциальное нарушение защиты. Например, определенную деловую активность пользователей можно смоделировать достаточно точно. Конкретный пользователь обычно регистрируется в системе в определенное время, выполняет транзакции баз данных, другие действия, совершает незначительное количество ошибок и т.д. Если этот пользователь выходит в сеть в другое время и совершает большое количество ошибок при доступе к файлам, то система пометит эту деятельность как подозрительную.

Главное преимущество систем обнаружения аномалий заключается в том, что они позволяют обнаружить ранее неизвестные атаки. Определив «нормальное» поведение, можно обнаружить любое нарушение, предусмотрено оно или нет.

Главным недостатком систем обнаружения аномалий является наличие большого количества ложных тревог и необходимость постоянного анализа функционирования вычислительной сети.

Традиционно эта задача обеспечения безопасности вычислительных сетей рассматривается с позиций защиты от неправомерного доступа, разрушающих воздействий и решается, прежде всего, за счет внедрения межсетевых экранов, частных виртуальных сетей и использования средств шифрования, контролирующих доступ и защиту от воздействий извне.

Используемые в настоящее время традиционные системы обнаружения злоупотреблений и аномалий (IDS) основаны на модели, предложенной Деннингом в 1987 году [74]. Эта модель поддерживает набор профи-

лей для пользователей, согласовывает записи подсистемы контроля с соответствующим профилем, при необходимости обновляет профиль, сообщает обо всех аномалиях и не зависит от платформы, уязвимостей операционной системы и типа атаки. Для обнаружения злоупотреблений используется другой компонент, набор правил.

Существующие системы реализуют эту модель с помощью различных методов [75]. Наиболее часто для определения аномальности поведения используют статистические методы, то есть осуществляется сравнение с известным заранее для определения нормального режима работы.

Автономные системы обнаружения злоупотреблений и аномалий запускаются периодически, и, как следствие, довольно часто обнаруживают атаки уже после их прохождения на основе записей в журналах регистрации.

Анализ популярных сегодня систем обнаружения атак на уровне сети показывает, что все они, в качестве источника данных, используют сетевой трафик или журналы регистрации сетевого программно-аппаратного обеспечения (маршрутизатор, межсетевой экран, анализатор протоколов), фиксирующие обрабатываемый трафик, анализируя его на наличие признаков атак.

Целесообразно использовать программное обеспечение системы обнаружения атак, которое состоит из следующих частей:

- Ядро, обеспечивающее захват данных и осуществляющее взаимодействие с сетевым адаптером, частью сетевого оборудования или журналом регистрации, хранящим сетевой трафик. В тех системах обнаружения атак, где используется захват с сетевой карты, драйвер системы защиты подменяет драйвер операционной системы, отвечающий за взаимодействия устройств, что повышает эффективность работы. Подобная замена, кроме того, позволяет реализовать такие функции, как, например, stealth-режим, которая не позволяет обнаружить и атаковать систему обнаружения атак. Менее сложные системы (более дешевые или созданные самостоятельно) используют и анализируют данные, получаемые от драйвера операционной системы, что, по решаемым задачам, практически идентична ядру анализатора протоколов.
- Программное обеспечение, декодирующее и анализирующее протоколы, с которыми работает сетевой адаптер, позволяет также реализовывать определенную логику работы системы обнаружения вредоносных воздействий и обеспечение реагирование на них.

Механизм функционирования системы обнаружения атак на уровне сети состоит из четырех этапов:

- захват пакетов;
- фильтрация и сборка фрагментов;
- распознавание атак;
- реагирование на них.

Механизм захвата пакетов заключается в обработке трафика, получаемого с сетевой карты, которая может работать в двух режимах:

- в обычном режиме, в котором сетевая карта обрабатывает только пакеты, предназначенные именно ей;
- в «смешанном» или «беспорядочном» (promiscuous) режиме, в котором сетевая карта обрабатывает все пакеты, передаваемые в сетевом сегменте.

Самым важным этапом в системе обнаружения атак является распознавание атаки и от качества реализации этого модуля зависит эффективность всей системы. Модуль распознавания атаки, в общем случае, использует три широко известных метода:

- Сигнатуры, основанные на шаблоне (pattern-based signatures), выражении или строке, характеризующих практически любую подозрительную деятельность. Подобные сигнатуры имеют словарь, содержащий ключевые слова или выражения, при обнаружении которых можно информировать о совершаемой атаке. Например, фрагмент «cwd ~root» в FTP-сеансе однозначно определяет факт обхода механизма аутентификации на FTP-сервере и попытке перейти в корневой каталог FTP-сервера. Другим примером является обнаружение апплетов Java в сетевом трафике на основе шестнадцатиричного фрагмента «CA FE BA BE». Эти же сигнатуры позволяют обнаруживать многих троянских коней, если последние используют стандартные значения портов.
- Сигнатуры, действие которых основано на контроле частоты происходящих событий, а также превышении пороговой величины. В этом случае осуществляется контроль за происходящими событиями и контролируются заданные заранее показатели. Примером такой сигнатуры является обнаружение сканирования портов или обнаружение атаки SYN Flood. В первом случае осуществляется контроль за числом портов, просканированных в единицу времени, а во втором контролируется число попыток соединения с узлом за заданную единицу времени.
- Обнаружение аномалий. Посредством использования подобного типа сигнатур появляется возможность выявлять события даже незначительно отличающиеся от заранее заданных. Например, если система обнаружения атак фиксирует вход сотрудника в сеть в нестандартное время, то это, в ряде случаев, может свидетельствовать о том, что пароль этого пользователя украден или подобран и его использует злоумышленник для неправомерного проникновения.

Необходимо отметить, что при создании своей собственной системы обнаружения атак с помощью утилит и библиотек можно запрограммировать, в основном, сигнатуры первого типа.

Система обнаружения и распознавания атак не может функционировать без базы сигнатур. Все атаки или иные неправомерные действия построены на стандартных фильтрах, которые являются основой любой сис-

темы обнаружения атак. Рассмотрим два типа фильтров. Первый - на примере утилиты TCPdump, второй - на примере межсетевого экрана Check Point VPN-1&Firewall-1. В большинстве случаев - это решение компании Check Point [100]. Этот межсетевой экран обладает замечательным механизмом - языком описания сетевых событий INSPECT, который позволяет оперировать любыми полями (включая поле данных) сетевых пакетов. Используя этот язык можно построить достаточно эффективную систему обнаружения атак, встроенную в так полюбившийся российским пользователям межсетевой экран. Достоинство этого решения в том, что на единую консоль администратора выводятся сообщения и от межсетевого экрана и от системы обнаружения атак.

Напрашивается вывод, что контроль работы вычислительной сети не имеет никакого смысла без последующего анализа полученной информации. Можно выделить две основные категории методов обнаружения неправомерного доступа к компьютерной информации – это обнаружение аномалий и злоупотреблений. Такие системы имеют право на существование, и технологии их создания используются при создании своей системы обнаружения атак.

Кажется целесообразным построение системы обнаружения атак на следующих общих методах:

1. Анализ журналов регистрации.
2. Анализ «на лету».
3. Использование профилей нормального поведения.
4. Использование сигнатур атак.

Необходимо заметить, что все данные методы не являются взаимоисключающими и наиболее оптимально использовать комбинацию нескольких методов.

Метод анализа учета регистрации заключается в анализе журналов, создаваемых операционной системой, прикладным программным обеспечением, маршрутизаторами и т.д. Записи журнала регистрации анализируются и интерпретируются системой обнаружения атак.

К достоинствам этого метода относится простота его реализации. Однако имеется немало недостатков и, как правило, анализ журналов регистрации является дополнением к другим методам обнаружения атак, в частности, к обнаружению атак «на лету». Использование этого метода позволяет проводить разбор уже после того, как была зафиксирована атака, для того чтобы выработать эффективные меры предотвращения аналогичных атак в будущем.

Метод анализа «на лету» заключается в мониторинге сетевого трафика в реальном или близком к реальному масштабу времени и использовании соответствующих алгоритмов обнаружения. Очень часто используется механизм поиска в трафике определенных строк, которые могут характеризовать неправомерную деятельность.

Использование метода обнаружения атак в сетевом трафике дает два основных преимущества. Во-первых, один агент системы обнаружения атак может просматривать целый сегмент сети с многочисленными хостами, в то время как для предыдущего метода необходимо на каждый анализируемый узел устанавливать свой агент. Этот метод позволяет обнаруживать атаки против всех элементов вычислительной сети, начиная от атак на маршрутизаторы и заканчивая атаками на прикладные приложения. Во-вторых, системы, построенные с учетом этого метода, могут определять атаки в реальном масштабе времени и останавливать атаки до достижения ими цели.

Профили нормального поведения используются для наблюдения за пользователями, системной деятельностью или сетевым трафиком и, в последующем, сравниваются с ожидаемыми значениями профиля нормального поведения, который строится в период обучения системы обнаружения атак.

Метод использования сигнатур атак очень часто сопоставляют с анализом «на лету» и он заключается в описании атаки в виде сигнатуры (signature) и поиска данной сигнатуры в контролируемом пространстве (сетевом трафике, журнале регистрации и т.д.). В качестве сигнатуры атаки, которые хранятся в базе данных, аналогичной той, которая используется в антивирусных системах, может выступать шаблон действий или строка символов, характеризующие аномальную деятельность. Антивирусные резидентные мониторы являются частным случаем системы обнаружения атак.

Эффективность системы обнаружения атак во многом зависит от применяемых методов анализа. В самых первых системах, разработанных в начале 80-х годов, использовались статистические методы. Сейчас к статистическому анализу добавилось множество новых методик, начиная с нечеткой логики и заканчивая использованием нейронных сетей.

Обнаружение атак остается областью активных исследований в течении последних лет. Считается, что начало этому направлению положено в 1980 году статьей Джеймса Андерсена «Мониторинг угроз компьютерной безопасности» [72]. Несколько позже, в 1987 году это направление было развито в публикации статьи «О модели обнаружения вторжений» Дороти Дейнинг [74]. Она обеспечила методологический подход, заложивший основу для создания продуктов в области систем обнаружения атак, которые используются в качестве средств предотвращения неправомерного доступа.

Система обнаружения атак - это совокупность программных и программно-аппаратных средств, обеспечивающая автоматизированный контроль процессов, с целью анализа состояния ее защищенности, выявления попыток или фактов вмешательства в ее работу, определения источника

(источников) вмешательства и реагирования на вмешательства с целью их нейтрализации в информационной вычислительной сети любого масштаба.

Технология систем обнаружения атак молода и, динамична и сегодня в этой сфере идет активное формирование рынка, информация быстро устаревает, что затрудняет сравнительный анализ характеристик [95].

Система обнаружения атак включает:

- сенсоры - программные или программно-аппаратные источники информации о процессах, протекающих в вычислительной сети;

- анализаторы - программные или программно-аппаратные средства, обрабатывающие получаемую от сенсоров информацию, принимающие решение о наличии факта вмешательства в работу вычислительной сети или подготовки к нему, выявляющие источник или источники угрозы, а также выбирающие вариант реагирования на них;

- компоненты реагирования - наборы действий, которые выполняют системы обнаружения атак, при обнаружении факта вмешательства в работу вычислительной сети или подготовки к нему.

Принцип работы системы обнаружения атак основывается на том, что поведение взломщиков, вторгающихся в работу вычислительной сети, значительно отличается от действий зарегистрированных пользователей. При этом производится анализ отчетов о функционировании операционной системы, приложений и сравнение системных событий с заранее известной базой процедур нарушений безопасности. Располагающиеся на сетевых рабочих станциях компоненты системы обнаружения атак следят за различными аспектами безопасности, и в случае взлома или отклонений от нормального режима функционирования реагируют на это. Системой регистрируется факт произошедшего, предупреждается администратор, а в отдельных случаях производится полная остановка рабочих станций, изменение настроек межсетевых экранов или маршрутизаторов.

Повысить эффективность систем обнаружения атак позволяет захват сетевого трафика непосредственно с сетевой карты, минуя операционную систему, что может реализовываться на обычных, специализированных компьютерах или интегрировано в маршрутизаторы или коммутаторы. При реализации подобных систем на компьютерах информация собирается посредством захвата и анализа пакетов, используя сетевые интерфейсы в беспорядочном (promiscuous) режиме. В маршрутизаторах или коммутаторах захват трафика осуществляется с шины сетевого оборудования.

Системы сетевого уровня не требуют установки на каждом хосте программного обеспечения необходимого для обнаружения атаки, так как число мест контроля сети невелико. Кроме того, для контроля сетевого сегмента, необходим только один сенсор, независимо от числа узлов. Системы, функционирующие на сетевом уровне, используют живой трафик при обнаружении атак в реальном масштабе времени. В результате сетевой пакет, ушедший с компьютера злоумышленника, не может быть возвращен

назад и он теряет возможность сокрытия следов противоправной деятельности. Анализируемая информация не только описывает метод атаки, позволяет идентифицировать правонарушителя, но и позволяет использовать ее в качестве доказательной базы в суде. Эффективность использования специального программного обеспечения на сетевом уровне основывается на то, что многие хакеры хорошо знакомы с механизмами системной регистрации и знают, как манипулировать этими файлами для сокрытия следов своей деятельности.

Системы обнаружения атак, функционирующие на уровне сети, позволяют обнаруживать противоправные деяния на фазе подготовки и, по сравнению с системами, анализирующими журналы регистрации, обеспечивают своевременное уведомление и реагирование. Например, хакер, инициирующий сетевую атаку типа «отказ в обслуживании» на основе протокола TCP, может быть остановлен системой обнаружения атак сетевого уровня, посылающей TCP-пакет с установленным флагом Reset в заголовке для завершения соединения с атакующим узлом, прежде чем атака вызовет разрушения или повреждения узла.

Часто используемые системы анализа журналов регистрации не распознают атаки до момента соответствующей записи в журнал и предпринимают ответные действия уже после того, как была сделана запись. К этому моменту наиболее важные системы или ресурсы уже могут быть скомпрометированы или нарушена работоспособность системы.

Уведомление в реальном масштабе времени позволяет, в соответствии с предварительно определенными параметрами, своевременно среагировать. Диапазон этих реакций изменяется от разрешения проникновения в режиме наблюдения для того, чтобы собрать информацию об атаке и злоумышленнике, до немедленного прекращения вторжения.

Системы обнаружения атак, функционирующие на сетевом уровне, не зависят от операционных систем, установленных в сети, так как они оперируют сетевым трафиком, которым обмениваются все узлы. Данному программному продукту обеспечения информационной безопасности все равно, какая операционная система сгенерировала тот или иной пакет, если он соответствует стандартам, поддерживаемым системой обнаружения. Например, в сети могут работать операционные системы Windows, Netware, Linux, MacOS, Solaris и т.д., но если они общаются между собой по протоколу IP, то любая из систем обнаружения атак, поддерживающая этот протокол, сможет обнаруживать атаки.

Обеспечение адекватного реагирования на производимые атаки невозможно без использования системы поддержки и принятия решений, накопления знаний и опыта в области расследования правонарушений и преступлений в сфере компьютерной информации. Этой связи целесообразно использовать нейросетевые методы анализа, что позволит выполнять вы-

шесказанное и обеспечивать информационную безопасность на должном уровне.

Экспериментальная оценка показывает, что нейронная сеть может обучаться с целью идентификации пользователей просто по командам и частоте их использования, и такая идентификация может быть применена для обнаружения атак против информации в вычислительной сети. Нейросетевые методы позволяют легко обучаться, не требуют значительных затрат работая в автономном режиме позволяют ежедневно создавать регистрационные записи.

Предложенный в данном параграфе материал позволяет нам определиться с основными методами обнаружения преступных посягательств на информацию в вычислительных сетях. Далее перейдем к рассмотрению основных способов обнаружения аномальных явлений в среде циркуляции информационных ресурсов.

2.3. Управление процессами информационного обмена и способы обнаружения аномальных процессов и явлений

В целях защиты внутренних механизмов вычислительной сети от перегрузок и удержать характеристики передачи в желаемых пределах при доступе сообщений в транспортную компоненту сети, организуется управление потоком данных. При этом в используемом протоколе TCP/IP применяется механизм «скользящего окна», когда не все поступающие в транспортную компоненту сообщения сразу отправляются на передачу. Одна транспортная станция может одновременно вести передачу ограниченного числа сообщений (количество сообщений - размер «окна»), остальные поступившие сообщения ожидают передачи в очереди к «окну». При установлении соединения счетчики последовательностей сегментов у отправителя и получателя устанавливаются в одинаковые состояния. Получатель, приняв несколько подряд следующих сегментов, в ответном сообщении-квитанции передает отправителю номер следующего байта данных, который он намерен принять (номер последнего байта, в последнем корректно принятом сегменте, плюс единица).

Управление квитированием (способом с использованием квитанций по отправке и приему сообщений) методом «скользящего окна» предоставляет возможность управления потоком в целях повышения качества приема пакетов в сети. Изменяя размер окна для множества источников информации, можно не только эффективно управлять перегрузками на отдельных участках сети, но и манипулировать числом сегментов в ней [87,31].

Модуль TCP/IP может использовать алгоритм «медленного старта», формируя при установлении соединения окно перегрузки, размер которого изначально равен размеру одного сегмента. Это окно показывает, сколько сегментов TCP-модуль, с его собственной точки зрения, может отправить без получения подтверждения. Скользящее же окно, рассмотренное выше, показывает, какой объем неподтвержденных данных модулю разрешено отправить с точки зрения получателя его данных. После прихода подтверждения о доставке окно перегрузки увеличивается на 1 сегмент, и отправитель может выслать уже два сегмента, не дожидаясь подтверждения. Такой подход позволяет постепенно увеличивать нагрузку на сеть. Если окно перегрузки становится больше объема скользящего окна, объявляемого получателем, ограничение на передачу неподтвержденных данных устанавливает уже его скользящее окно (рисунок 2.8) [90].

Основная задача оптимизации заключается в изменении таких параметров протокола, которые не требуют внесения модификаций в аппаратную часть. Среди таких параметров тайм-ауты на передающей и принимающей стороне (необходимые временные отрезки получения и приема сообщений), максимальное число повторных попыток передачи, размер

ограничивающего окна. Критерием оптимизации может служить среднее время доставки сообщений или удовлетворение требованиям на вероятность доставки. Таким образом, одна из задач оптимизации заключается в нахождении таких значений размера окна и величины тайм-аутов, при которых среднее время доставки сообщений является наименьшим. Однако, центральная проблема стека протоколов TCP/IP заключается в их низкой надежности, вызванной появлением логических ошибок. Поэтому основной задачей оптимизации становится такое преобразование протокола, которое ведет к повышению вероятности доставки сообщения.

При всех преимуществах протокола TCP/IP, он имеет следующие существенные недостатки:

1. Применяемый в TCP/IP метод AIMD (метод линейного изменения) предписывает постоянное линейное увеличение нагрузки на сеть с целью определения момента начала перегрузки. Вследствие этого среда постоянно находится либо в состоянии перегрузки, либо в состоянии выхода из нее. Это отрицательно сказывается на соединениях в виде увеличенного среднего RTT.

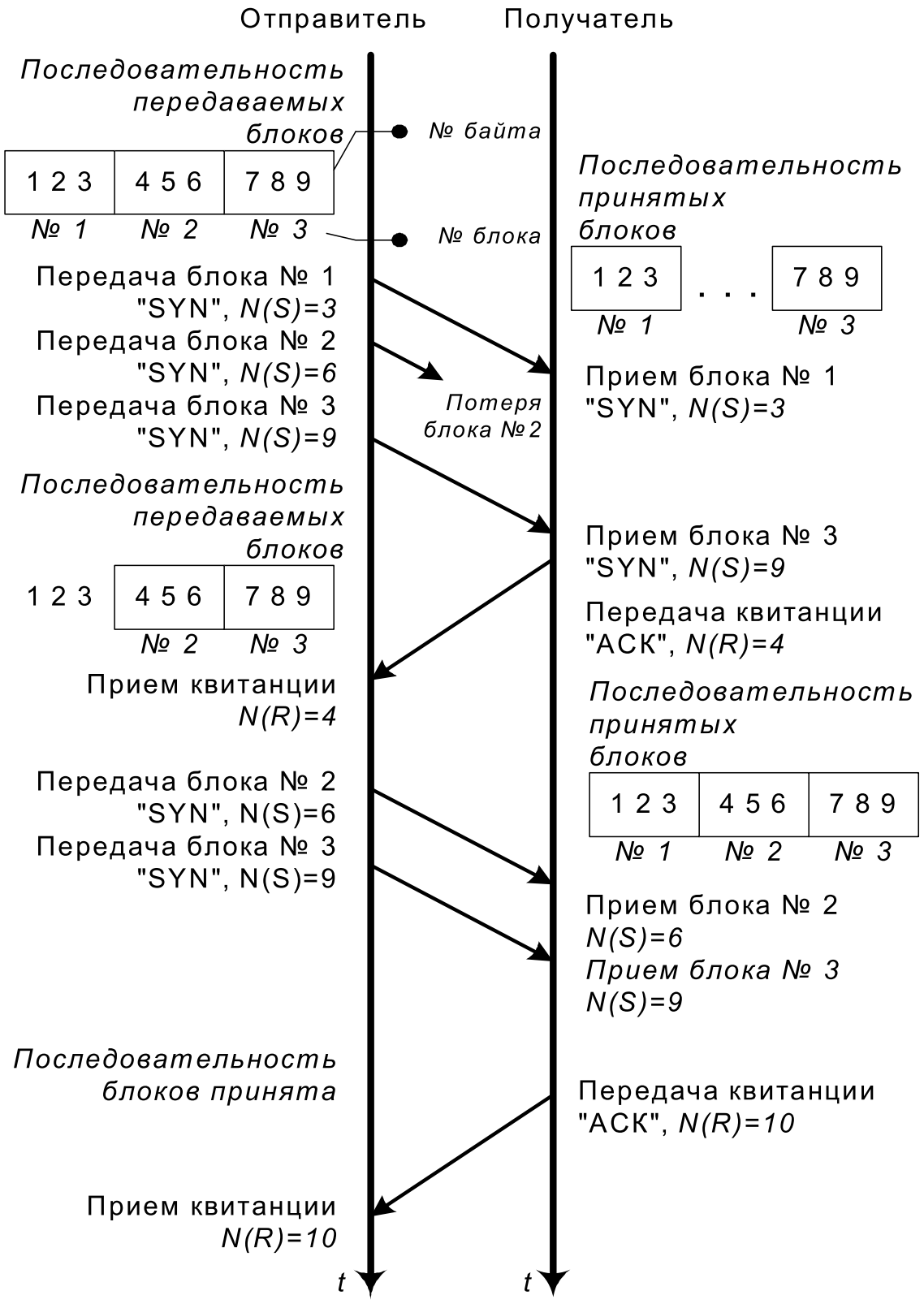

Рисунок 2.8. Фаза передачи данных (группового квитирования)

(*Round trip time* – время двойного прохода, т.е. промежуток времени от отправки пакета, до получения квитанции, подтверждающей прием), большой дисперсии измеряемых значений RTT, постоянном наличии потерь, с помощью которых сеть сигнализирует о начале перегрузки.

2. Эффективность работы протокола TCP резко падает при возникновении логических ошибок. Это связано с тем, что при получении неверного пакета, приемник сообщает об ошибке и передатчик повторяет всю последовательность данных из окна. Такой алгоритм действий ведет к явной избыточности передаваемых данных, поскольку необходимо передать только фрагмент сообщения, следующий за последним корректно принятым блоком. Соответственно увеличивается время, затрачиваемое на доставку сообщения, а некоторые сообщения теряются из-за превышения размеров тайм-аута.

Первая проблема решается, если отправлять пакеты в транспортную компоненту, разделенные временными промежутками, длительность которых определяется текущим значением скорости. Скорость потока регулируется следующими темпоральными характеристиками: измерением длительности межпакетных интервалов у получателя и изменении времени RTT. При увеличении значения $\frac{(\text{длительность межпакетных интервалов у получателя})}{(\text{длительность межпакетных интервалов у отправителя})}$ скорость потока следует уменьшить, в противном случае – увеличить. Таким образом, модифицированному протоколу не требуется доводить среду до состояния перегрузки, чтобы определить доступную долю пропускной способности, поэтому исключены потери пакетов, связанные с этим процессом. Под пропускной способностью понимается: максимальная скорость передачи информации (в Кбит/с), на которую способен канал связи и при которой обеспечивается необходимая вероятность ошибок при приеме сообщений на принимающей стороне.

Вторую проблему можно разрешить, преобразовав алгоритм следующим образом:

Пусть мы имеем логически завершенный протокол профиля информационного обмена, воплощаемый процессами $P_1', P_2', \ldots, P_n'$.

1. При не получении, или получении некорректного блока данных процессом P_i', квитанция о получении пакета не высылается.

2. При превышении тайм-аута ожидания квитанции, процессу P_i' посылается сообщение «фиксация». После этого процесс сообщает о своем текущем состоянии (какие пакеты были правильно приняты).

3. Вводится объединенное состояние $<S_0^1, S_0^2, \ldots, S_0^n>$, включающее частные состояния процессов, не получивших пакеты.

4. Для каждого процесса из этого объединенного состояния посылается сообщение «восстановление», после которого идут блоки информации, которые не были получены данным процессом. В течение некоторого промежутка времени ожидается подтверждение правильного приема. Если в течение этого времени подтверждение не получено, то шаг 4 повторяется.

5. При достаточно большом увеличении размера объединенного состояния $<s_0^1, s_0^2, \ldots, s_0^n>$, считается, что сеть перегружена, и всем процессам, чьи частные состояния входят в объединенное посылается квитанция «сброс», сигнализирующая об очистке объединенного состояния. Процесс, получивший квитанцию сброс, считает, что передача сообщения не была успешна, и начинает прием заново.

Такой механизм будет более эффективен, чем стандартный механизм протокола.

Для того чтобы устранить недостатки, свойственные TCP/IP, необходимо было найти способ получения информации о состоянии сети, отличный от применения в этих целях потерь сегментов. [31] Наиболее хорошо на роль индикатора состояния сети подходят временные характеристики потока: время RTT и межсегментные интервалы. С использованием межсегментных интервалов можно также определить долю пропускной способности канала. Для этого требуется запоминать межсегментные интервалы потока у отправителя и измерять их у получателя. Сравнение значений интервалов характеризует состояние сети, а минимальное значение измеряемых интервалов у получателя позволяет определить доступную долю пропускной способности.

Таким образом, реализуя вышеизложенное, происходит модернизация протокола TCP/IP (собственно модернизированный протокол - MTCP/IP). Он функционирует по следующей схеме: установка скорости потока отправителем посредством тщательной диспетчеризации сегментов (отслеживание каждого информационного пакета), измерение скорости прибытия потока у получателя и передача этой информации отправителю вместе с остальной контрольной информацией. Разность старого и нового значений скорости отправки потока протокола на каждом шаге задается случайной переменной, однако, при наличии сигнала о перегрузке сети вероятность снижения скорости должна превышать вероятность ее увеличения на каждом новом шаге.

Параметры и переменные. Пусть τ временной интервал между последовательными трансляциями пакетов. Задача функции диспетчеризации сегментов в том, чтобы задерживать отправку очередного сегмента на время τs, после начала передачи предыдущего сегмента. Обозначим все переменные, относящиеся к отправителю индексом S, и R - относящиеся к получателю. Итак, τ_S временной интервал между моментами начала отправки

в среде сегмента i+1 и i-го, а τ_R интервал между последовательно прибывшими к получателю сегментами.

Пусть скорость канала связи, непосредственно к которому подключен отправитель R_{lS}, тогда время уходящее на отправку одного сегмента (с момента начала передачи до момента ее окончания) $t_{lS}=S/R_{lS}$, где S - размер передаваемого сегмента. Очевидно, что максимально возможная скорость потока $R_{maxS}= R_{lS} =S/\tau_{minS}$.

Минимальное значение межсегментного интервала в этом случае будет $\tau_{minS}=t_{lS}$, когда пакеты отправляются в транспортную компоненту среды без задержек с максимальной скоростью канального уровня. Путем изменения τ_S в пределах $[\tau_{Smin},\infty)$, MTCP/IP может контролировать скорость потока в пределах $[R_{lS}, 0)$.

Задержка отправки готовых сегментов производится с помощью системного таймера. Например, для полного использования пропускной способности канала в 512 Кб/с при размере сегмента в 1000 байт каждый сегмент необходимо отправлять с задержкой τ_S =0.015625 с, чтобы скорость потока составила 64 пакета/с.

В таблице 2.2 приведен список параметров и переменных используемых алгоритмом управления потоком протокола MTCP/IP.

Формат сообщений используемых MTCP должен в точности совпадать с форматом пакета TCP/IP, который предусматривает наличие дополнительных полей в заголовке сегмента между стандартным заголовком и полем данных. MTCP/IP может передавать дополнительную информацию в этих полях, что будет гарантировать совместимость с TCP.

Всего протокол MTCP/IP требует использования лишь двух новых полей: значения предыдущего порядкового номера «PS» в направлении от отправителя к получателю и значения скважности «TI» в направлении от получателя к отправителю.

Значение «TI» можно передавать в виде опции временной метки [91], а значение «TI» требует поля, позволяющего поместить порядковый номер сегмента.

Таким образом в протоколе MTCP полностью переработаны все механизмы управления потоком, а механизм коррекции ошибок передачи в MTCP не влияет на скорость передачи. От TCP сохраняется оконный механизм для управления загрузкой получателя, алгоритмы определения RTT и установки таймера ТПП.

Признаком потери сегмента служит срабатывание ТПП или приход двух последовательных подтверждений одного сегмента. Алгоритм управления скоростью включает в себя: функции диспетчеризации сегментов, измерения и адаптации скорости. Далее рассмотрим эти функции подробно.

Таблица 2.2. Переменные и параметры модели MTCP

S	Размер кадра канального уровня содержащего сегмент
τ_S	Временной промежуток между последовательными трансляциями сегментов первого бита до первого бита
τ_R	Временной промежуток, измеренный между последовательными моментами прибытиями сегментов (от последнего бита до последнего бита)
$R_S(t)$	Скорость потока, устанавливаемая отправителем
$R_R(t)$	Скорость потока, вычисляемая получателем
$R_e(t)$	Оценка доступной пропускной способности в момент t-RTT
R'_S	Первая производная скорости по времени, устанавливается отправителем
R_{pe}	Значение оценки доступной пропускной способности в момент i-1
A_C	Площадь области компенсации
SSGR	Параметр экспоненциального роста R'_S в режиме SS
RTT	Временной промежуток между моментом отправки сегмента и моментом прихода его подтверждения
ERTT	Взвешенное скользящее среднее RTT
SmoothedR_e	Взвешенное скользящее среднее Re
MaxERTT	Максимальное значение сглаженного RTT
MinERTT	Минимальное значение сглаженного RTT
MDFACTOR	Коэффициент, используемый при мультипликативном снижении $R_S(t)$
R_{Samd}	Значение скорости отправки данных непосредственно на выходе режима MD1
R_{Sbmd}	Значение скорости отправки данных непосредственно перед входом в режим MD1
R_{eamd}	Значение оценки доступной пропускной способности в режиме MD1
speedup	Коэффициент, определяющий вероятность увеличения скорости в режиме FT
slowdown	Коэффициент, определяющий вероятность снижения скорости в режиме FT
Midpoint	Точка отсчета скорости на каждом шаге в режиме FT
sR_S	Взвешенное скользящее среднее значение R_S
K	Коэффициент критерия осуществления перехода 6
BER	Резидентное значение ошибки передачи
R_{Smin}	Начальное минимальное значение скорости, с которого начинается рост в состоянии SS

Алгоритм адаптации скорости передачи сообщений

В задачи функции диспетчеризации сегментов входит отправка сегментов в транспортной компоненте среды со строго заданной скоростью, которая выражается в значениях межсегментных временных интервалов.

Функция измерения скорости определяет скважность потока поступающего к получателю и информирует отправителя о темпоральных параметрах прибывающего потока. Кроме того, отправитель сам производит измерение времени RTT (в рамках стандартной функциональности протокола TCP/IP).

Значения скважности потока измеренной получателем и времени RTT измеренного отправителем поступают на вход функции адаптации, которая определяет новое значение скорости отправки потока в соответствии с полученными на вход значениями и своим состоянием в этот момент времени.

MTCP/IP использует два признака начала перегрузки среды, когда средняя скорость прибытия запросов сравнивается со средней скоростью обслуживания и началом роста очереди: начало роста RTT и стабилизацию $R_R(t)$ при увеличении $R_S(t)$. Получатель MTCP/IP в сегментах с подтверждениями указывает значение скорости прибытия потока. Получая подтверждение сегмента спустя время RTT после его отправки, источник MTCP/IP получает информацию о значении скорости, с которой поток, содержащий этот сегмент, прибыл к получателю и использует $R_R(t)$ в качестве оценки $R_e(t)$ пропускной способности транспортной составляющей.

Очевидно, что скорость приема потока получателем не может быть выше скорости обслуживания потока на участке с наименьшей пропускной способности, через который проходит соединение. Таким образом, зная скорость прибытия потока к получателю, можно определить доступную пропускную способность среды. Для корректного измерения скорости необходимо не учитывать выпавшие из потока, т.е. потерянные сегменты, а также сегменты, доставляемые транспортной компонентой в измененном порядке. Для выполнения этого условия в поле «PS» каждого отправляемого сегмента записывается порядковый номер (или смещение) от предыдущего.

Получив сегмент i, получатель вычисляет разницу текущего времени и времени прибытия предыдущего (j) сегмента τ_R и в случае, если поле «PS» i-го содержит значение j, помещает $R_R=S/\tau_R$ в поле «TI» подтверждения следующего в противоположном направлении. Получатель извлекает значение поля «TI» из получаемых подтверждений и использует его для управления скоростью передачи.

Способ управления потоком должен достичь, во-первых, быстрой реакции потока на изменяющиеся условия соединения и, во-вторых, стабилизировать скорость передачи, когда она равна максимальной скорости сети [93]. Алгоритм управления потоками MTCP/IP функционирует в нескольких режимах.

Работа MTCP/IP начинается с режима быстрого увеличения скорости, аналогичной механизму замедленного старта стандартного TCP/IP, для максимально быстрого достижения соединением верхнего предела доступной пропускной способности. После того, как верхний предел достигнут, алгоритм MTCP/IP переходит в режим точной настройки, в течение которой удерживает скорость на уровне доступной пропускной способности. При определении ее уменьшения, MTCP/IP совершает мультипликативное (резкое) снижение скорости, которое в случае продолжительного состояния перегрузки продолжается экспоненциально. Итак, адаптация скорости передачи потока протоколом MTCP/IP происходит в пяти режимах (рисунок 2.9)[90].

Режим ускоренного старта (SS) имеет цель максимально быстро увеличить скорость потока от минимального значения до значения, равного или превосходящего пропускной способности канала, сразу после инициализации соединения. Для этого скорость увеличивается экспоненциально:

$$R'_S\,(t + RTT) = R_S(t) \times SSGR$$

$$R_S\,(t_i) = R_S(t_{i-1}) + R'_S(t_{i-1}) \times (t_i - t_{i-1})$$

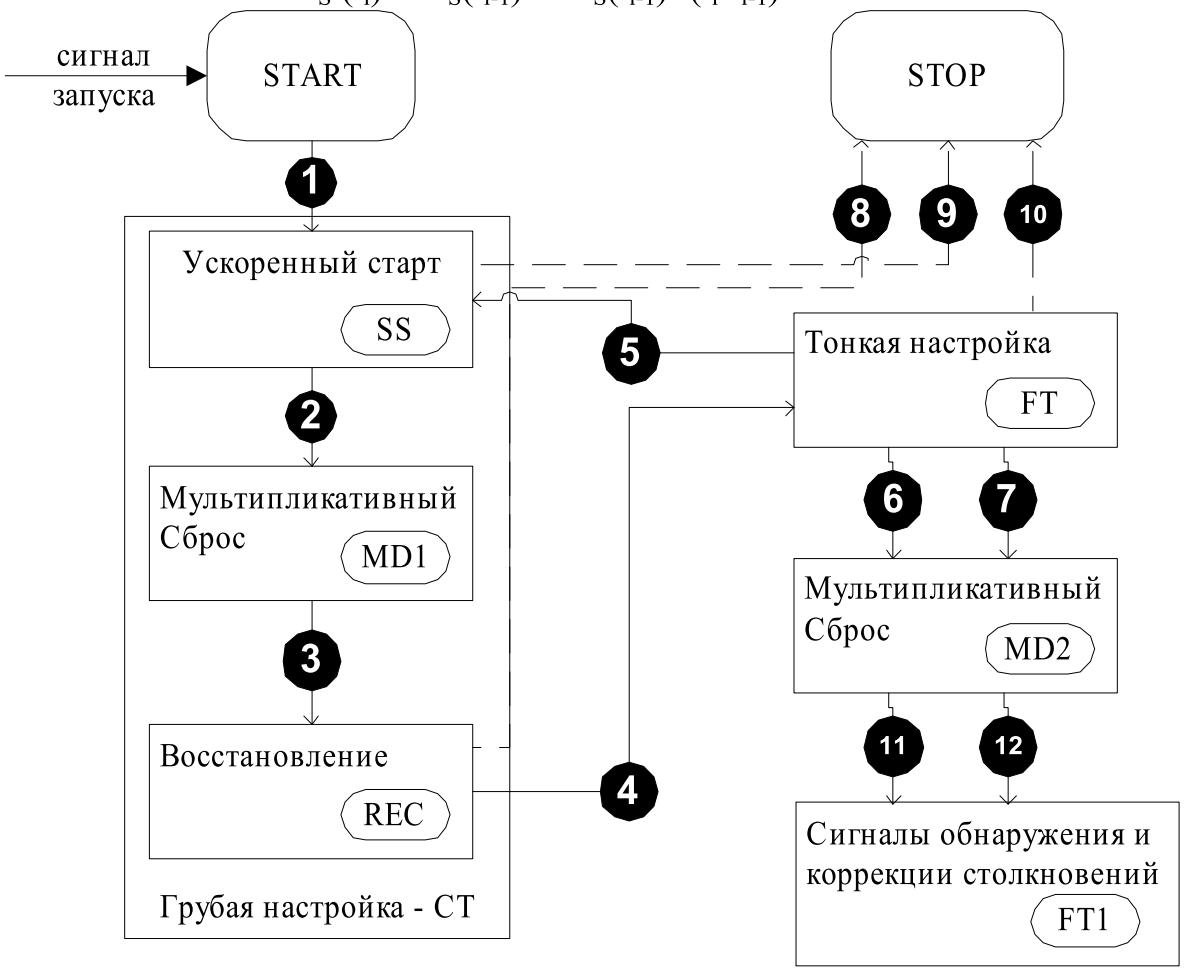

Рисунок 2.9.Алгоритм адаптации скорости передачи сообщений
(Штрихованные линии обозначают возможные переходы
в состояние остановки системы)

Начальное значение скорости устанавливается после синхронизации соединения как:

$$R_s^{\min} = \frac{SEGSIZE}{\min RTT}$$

Выход из режима SS происходит, когда $R_e(t_i)<(1-\varepsilon)\times R_S(t_i\text{-}RTT)$. После реализации перехода 2, алгоритм переходит в состояние мультипликативного сброса MD1.

Режим мультипликативного сброса (MD1) следует за режимом SS. После выхода из SS значение $R_S(t)$ будет превышать $R_e(t)$, поэтому в режиме MD1 скорость потока скачкообразно устанавливается заведомо ниже $R_e(t)$:

$$R_S(t_i) = R_e(t_i)\text{-}MDFACTOR\times(R_S(t_{i-1})-R_e(t_i))$$

После снижения скорости алгоритм переходит в режим восстановления.

Режим восстановления (REC) имеет целью, линейно увеличивая скорость, довести ее до уже известного значения пропускной способности канала: $R_e(t)$, компенсируя возникшую в режиме SS перегрузку. В режиме REC вычисляется значение площади области компенсации $A_C(t_i)$ как площади фигуры, образованной значениями $R_S(t)$ над прямой $R_e(t_i)$ за время, пока $R_S(t_i) > R_e(t_i)$ в режиме SS:

Значение площади области компенсации равно сумме площадей набора трапеций образованных значениями Rs(t) над прямой Re(ti). Площадь каждой трапеции

$$S_T = \Delta t_i / 2 \,(2R_S(t_i) - R'_S(t_i)\times\Delta t_i - 2R_e(t_i))$$

где Δt_i время, в течение которого не происходило изменений значения $R'_S(t_i)$.

$$R_S(t_i) - \frac{R'_S(t_i)}{SSGR^N} > R_e(t_i)$$

Итак, первое слагаемое приведенной формулы есть площадь трапеции с высотой меньшей RTT, последнее слагаемое - площадь треугольника, слагаемые от 2 до N-1 площади трапеций с высотой равной RTT.

Например, в случае, приведенном на рисунке 2.10, $A_C(t_i)$ равна сумме площадей трапеции DGBE и треугольника ABE. Δt_0 равно отрезку ED.

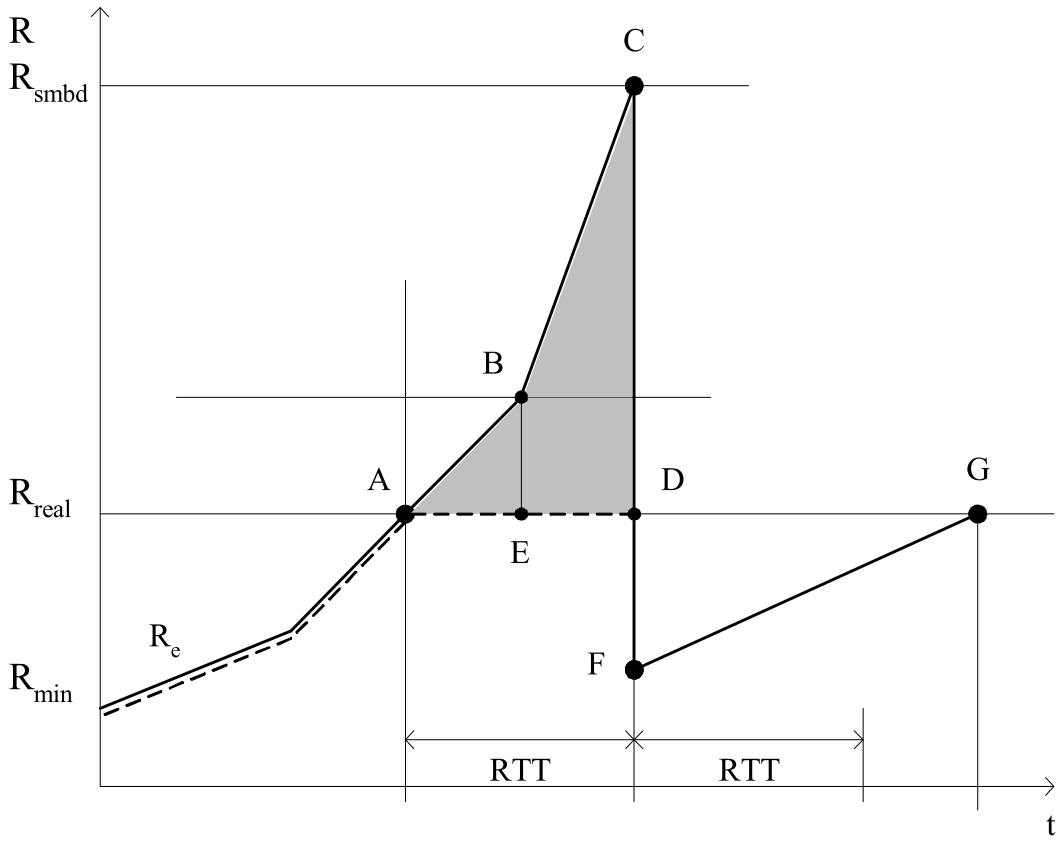

Рисунок 2.10.Зависимость скорости от времени в фазе грубой настройки MTCP

Значение $A_C(t_i)$ применяется для определения величины $R'_S(t_i)$ в состоянии восстановления REC. Идея в том, что из-за задержки информации о состоянии среды на время RTT, в состоянии быстрого увеличения скорости отправки сегментов поток вызовет наполнение буферов среды. Пакеты будут накапливаться в течение времени, когда скорость отправки сегментов превышает пропускную способность среды (отрезок AD на рис. 3.3). Пребывание соединения в состоянии восстановления необходимо для того, чтобы транспортная компонента справилась с возникшей до уменьшения скорости отправки перегрузкой. Очевидно, что количество данных, накопившихся в буферах среды, определяется площадью области $A_C(t_i)$, поэтому скорость отправки сегментов в состоянии REC должна быть снижена таким образом, чтобы площадь фигуры DFG была равна $A_C(t_i)$. Скорость в состоянии REC меняется линейно и определяется значением

$$R'_S(t_i) = \frac{[R_{pe}(t_i) - R_S(t_i)]^2}{2A_c(t_i)}.$$

В состоянии REC скорость отправки данных возрастает линейно от значения полученного в предшествующей стадии MD1 по закону

$$R_S(t_i) = R_S^{amd} + t \times R'_S(t_i)$$

Выход из состояния REC (переход 4) осуществляется в том случае, когда

$$R_S(t) \geq R_c^{amd}$$

Режим тонкой настройки (FT) следует за режимом REC, в режиме FT скорость отправки данных медленно подстраивается под пропускную способность канала. Отношение коэффициентов speedup и slowdown в состоянии FT определяет вероятность снижения или повышения скорости на каждом шаге. Коэффициент speedup, отвечающий за повышение скорости обратно пропорционален скорости данного соединения. Коэффициент slowdown, отвечающий за снижение скорости, пропорционален отношению измеряемого RTT к минимальному значению RTT. Значение speedup больше при меньших значениях Rs(t), что дает медленным соединениям преимущество для получения доступа к большей относительной доле пропускной способности. Значение slowdown одинаково для всех соединений и растет при росте RTT. Таким образом, вероятность повышения скорости для медленных соединений больше, а вероятность снижения скорости одинакова для всех соединений. Выход из режима FT происходит в случае скачкообразного изменения измеряемого RTT.

В состоянии FT значения скорости передачи определяются по закону:

$$R_s(t_i) = \text{midpoint} + \left[2 \times Rand - \frac{slowdown}{speedup}\right] \times \frac{speedup}{slowdown} \times INTERVAL \times \text{midpoint} \quad (1),$$

где rand - равномерно распределенная случайная величина, генерируемая функцией drand48 с областью значений [0;1]. После попадания в состояние FT (реализации перехода 4) значение midpoint устанавливается равным R_e^{amd}, в дальнейшем значение midpoint устанавливается равным sR_S. Переменные speedup и slowdown определяют направление изменения скорости отправки данных в зависимости от изменения времени RTT.

Коэффициенты slowdown и speedup для использования в формуле (1) определяются по следующим формулам:

$$speedup = \left[1 + \frac{S}{\text{minRTT} \times sR_S}\right]^2,$$

где второе слагаемое представляет собой отношение минимального количества данных в транзите по соединению (S байт за время RTT) к реальному их количеству (произведение минимального времени RTT на среднюю скорость отправки потока). Соответственно рост реальной скорости потока выражается в уменьшении значения коэффициента speedup, таким образом, при прочих равных условиях вероятность роста R_S для соединения с меньшей скоростью будет больше. За счет этого устраняется неравномерность использования ресурсов разными соединениями.

Коэффициент slowdown вычисляется следующим образом:

Если RTT > minERTT * (1 +PRECISION),

то $slowdown = 2 \times \left(\frac{RTT}{\text{minERTT}} \right) \times speedup,$

иначе slowdown = 1.

Отношение speedup/slowdown определяет знак отклонения мгновенного значения скорости от среднего. Если speedup>slowdown то отклонение от среднего значения для мгновенного значения скорости будет положительным, т.е. скорость потока будет увеличиваться, в противном случае speedup<slowdown скорость потока будет снижаться. Также, в состоянии FT максимальное отклонение мгновенного значения скорости отправки пакетов от среднего за предыдущий период, согласно формуле (1), пропорционально среднему значению скорости. В связи с этим поток, совершая переход 4 в состоянии FT при большем значении оценки доступной ПС, приспосабливается к небольшим изменениям пропускной способности более интенсивно.

Условием перехода из FT в режим мультипликативного сброса MD2 (переход 6) является:

$$ERTT > K * \left(FT \max RTT - \min ERTT \right) \quad (2)$$

Режим мультипликативного сброса (MD2) необходим для быстрого снижения скорости при условии резкого роста RTT:

$$\text{midpoint}_i = \text{midpoint}_{i-1} \times MDFACTOR$$

После этого протокол переходит в состояние FT, реализуя переход 7. В том случае, если условие (2) продолжает оставаться истинным, то мультипликативное уменьшение продолжается, поскольку последовательность переходов 6-7 реализуется неоднократно, выражаясь в экспоненциальном уменьшении скорости передачи данных.

Завершение работы протокола может произойти из любого состояния (SS, REC, FT} - переходы (8, 9, 10).

Ожидаемое поведение алгоритма управления скоростью потока в различных режимах изображено на рисунке 2.11 [90].

Для сравнения эффективности протокола TCP/IP и модифицированного протокола (M TCP/IP), учитывающего неэффективность обработки ошибок протоколом TCP, разработаны упрощенные модели, реализованные на языке GPSS [93].

Основная идея состоит в следующем: с интенсивностью Q сообщений/секунду процесс-отправитель посылает сообщения процессу-получателю. При передаче сообщение разбивается на M пакетов. Время от момента отправки сообщения до получения подтверждения о приеме равно

RTT секунд. Размер окно равен K пакетам. С вероятностью P происходит ошибка при передаче пакета. Рассчитать количество дошедших сообщений, долю потерь, коэффициент использования канала для протокола TCP/IP P и MTCP/IP.

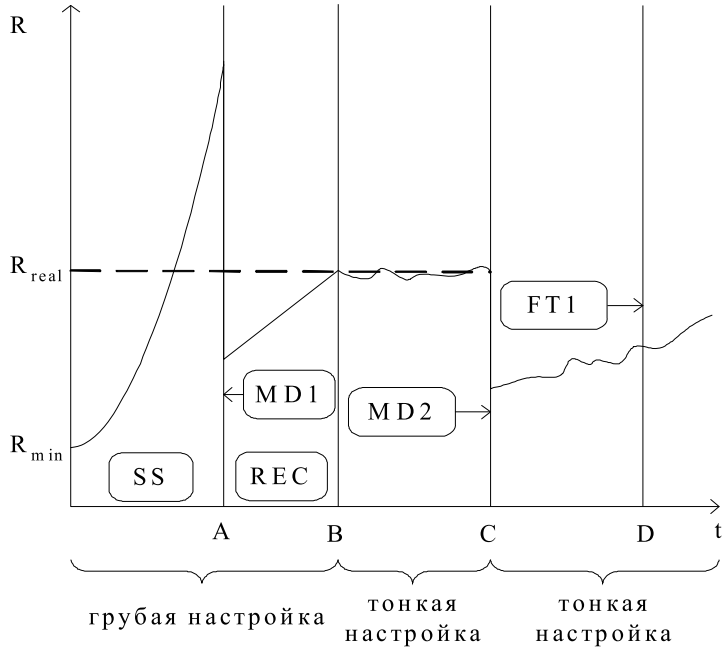

Рисунок 2.11. Ожидаемое поведение алгоритма управления скоростью потока (зависимость скорости от времени). Значения t в точках A,B,C обозначают моменты перехода в среды новый режим

Исходные данные для моделирования:
Q = 1,25 сообщений/с
M = 16 пакетов
RTT = 0,2 с
P = 0.05
K = 4 пакета
Время моделирования 10 000 секунд.

Центральной задачей данного этапа является выбор критерия оценки функционирования системы. В качестве критерия оценки эффективности функционирования выбраны показатели надежности системы, то есть доля потерь, коэффициент использования канала. [90]

Для рассматриваемой системы в качестве основных параметров, от которых зависит характеристика работы системы, можно считать время передачи сообщений, общее количество сообщений, количество удачно переданных сообщений, количество пакетов переданных повторно.

Для возможной оценки качества функционирования моделируемой системы заданы доля потерь и коэффициент использования канала. [93]

В результате исследования установлено, что количество удачно отправленных сообщений для протокола TCP/IP равно 5280, а для протокола MTCP/IP – 5449.

Проанализировав получившиеся данные, подмечено, что доля заново переданных пакетов в протоколе TCP/IP составила 11,1%, а в протоколе MTCP/IP составила 4,6%.

Коэффициент использования каналов в моделируемой системе, использующей протокол TCP/IP равен 0.866, а MTCP/IP – 0.901.

В итоге, по сравнению со своим предшественником, модернизированный протокол MTCP/IP обладает следующими преимуществами:

1. MTCP/IP не требуется доводить транспортную компоненту информационной среды до состояния перегрузки, чтобы определить доступную долю ПС, поэтому исключены потери пакетов связанные с этим процессом.

2. MTCP/IP существенно снижает требования к межсетевым устройствам. Во-первых, для нормального функционирования данного протокола требуется меньший объем буферного пространства, чем для TCP/IP, поскольку режим передачи является сглаженным. Во-вторых, MTCP/IP не требует и не зависит от наличия каких либо механизмов диспетчеризации или управления очередями, таких как RED или WFQ.

3. В отличие от TCP/IP новый протокол не полагается целиком на поток подтверждений в обратном направлении для синхронизации процесса передачи. В связи с этим возможна реализация MTCP/IP с меньшей частотой подтверждений, которая не ограничивала бы скорость в асимметричных системах. Работоспособность методики управления потоком данных в режиме восстановления после сбоев экспериментально подтверждена [91].

Таким образом, управление процессом информационного обмена является действенным способом повышения надежности в базовом протоколе передачи данных TCP/IP. Которая в свою очередь непосредственно оказывает влияние на обеспечение безопасности в сфере информационных технологий [90].

2.4. Некоторые особенности фиксирования деяний, связанных с неправомерным доступом к компьютерной информации

Обнаружение попытки неправомерного доступа должно повлечь за собой не только быстрый и продуманный ответ, преследующий цель предотвращения дальнейших потерь, но и использование специальных процедур для получения доказательной базы, преследования и идентификации злоумышленника. Работу по поиску следов и идентификации злоумышленника должен выполнять эксперт-криминалист, являющийся специалистом в области выявления неправомерных действий в сфере компьютерной информации.

Анализ места совершения преступления в сфере информационных технологий преследует цель определения механизма совершения и поиска следов неправомерного доступа к информации. Представляется целесообразным, для повышения эффективности, разбить подобный процесс на несколько этапов, которые заключаются в реализации трех фаз:

1. Сохранения системы;
2. Поиска следов противоправного деяния;
3. Реконструкция событий.

На этапе сохранения системы необходимо произвести консервацию места совершения преступления. Задача данного этапа заключается в сведении к минимуму всех возможных потерь улик необходимых для проведения последующего анализа. Исключением могут являться преступления определяемые ст. 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ» [3].

Любое вредоносное воздействие на вычислительную или телекоммуникационную сеть представляет собой атаку на информацию, состоящую из нескольких этапов. Подобное деяние, чаще всего, как уже говорилось ранее, состоит из трех этапов: подготовка атаки, реализация атаки и заметание следов. В этап подготовки атаки может входить выбор хоста и изучение инфраструктуры атакуемой системы, перехват и анализ сетевого трафика с целью получения имен пользователей, паролей, определение доступных служб и сервисов и т.д. На втором этапе происходит непосредственно реализация атаки и на завершающем этапе заметаются следы. В зависимости от метода воздействия на систему и ценности утраченных данных можно сделать вывод о степени опасности воздействия и квалификации злоумышленника.

1. Обнаружение попытки неправомерного доступа должно повлечь за собой не только быстрый и продуманный ответ, с целью предотвращения дальнейших потерь, но и эффективное использование специальных процедур для преследования и идентификации злоумышленника. Осуществлять формирование доказательной базы инцидента должен специально подготовленный специалист в области информационной безопасности, так

как в противном случае может быть случайно модифицировано ценное доказательство или неидентифицирован важный признак неавторизированной, незаконной активности в течение анализа процесса совершения неправомерного доступа к компьютерной информации [50].

Как уже говорилось ранее, любая попытка совершения подобных деяний включает в себя три этапа: подготовка, реализация и завершение атаки. На основании этого можно предложить способ вычисления степени опасности атаки S_A:

$$S_A = S_П + S_Р + S_З \qquad (1)$$

где $S_П$ - подготовка атаки,

$S_Р$ - реализация атаки,

$S_З$ - завершение атаки

В абсолютном большинстве случаев традиционные механизмы защищают от атак, которые уже находятся в процессе реализации или завершения. В этом случае $S_A = S_Р + S_З$ и даже если удается предотвратить ту или иную атаку, то намного более эффективным было бы упреждение и устранение самих предпосылок реализации вторжений. Комплексная система обеспечения информационной безопасности должна работать на всех трех этапах осуществления атаки, так как защита на этапах подготовки и завершения атаки не менее важна, чем в период ее реализации. Ведь обнаружение вторжения во время подготовки позволяет своевременно предотвратить ее, а правильное сохранение следов противоправного деяния позволяет разработать рациональные меры по устранению дальнейших попыток реализовать аналогичную атаку. Эффективность системы обеспечения информационной безопасности $C_Р$ должна быть выше опасности инцидента связанного с неправомерным доступом к компьютерной информации.

$$C_Р > S_A = S_П + S_Р + S_З \qquad (2)$$

Если принять эффективность обеспечения информационной безопасности за 1, то, следовательно, вероятность возникновения успешной атаки должна быть значительно меньше 1. Отсюда следует, что реакция на инцидент, связанный с неправомерным доступом к компьютерной информации, является сложной задачей, которую можно решить с использованием специально разработанной методики с учетом предполагаемых действий правонарушителя (рис. 2.12).

На первом этапе осуществляется подготовка к неправомерным действиям и формирование алгоритма реагирования на инцидент на основе информации о его процедурах. Доскональная проработка этого вопроса позволяет наиболее эффективно противодействовать рассматриваемым попыткам.

Обнаружение инцидентов, связанных с неправомерным доступом к компьютерной информации, осуществляется при содействии установленного на объектах информационно-телекоммуникационной сети программного обеспечения. Системы обеспечения информационной безопасности должны не только обнаруживать известные атаки и предупреждать о них, но и распознавать непонятные источники информации об атаках, при этом, снижая нагрузку на персонал, давая возможность управления собой не экспертами в данной области. К подобным системам целесообразно отнести системы обнаружения атак. [50]

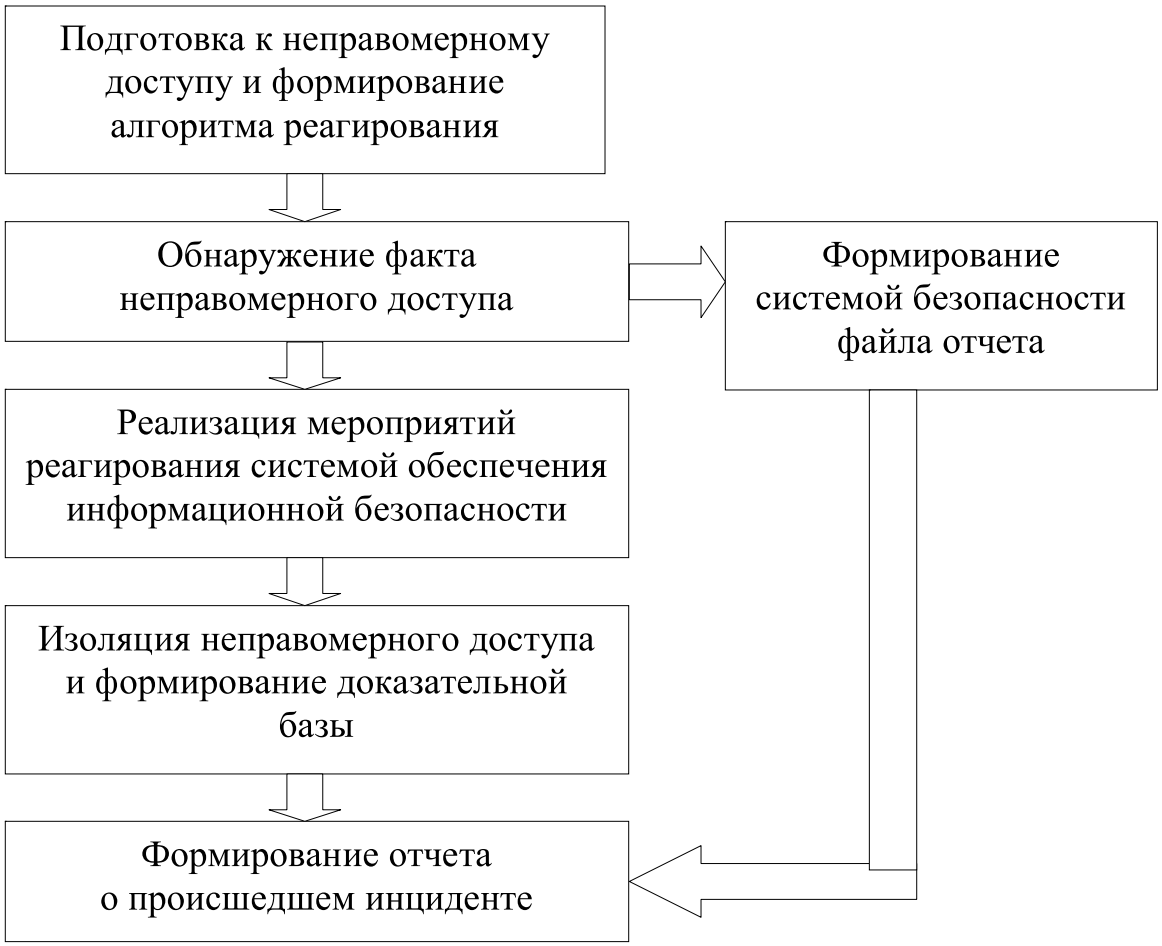

Рисунок 2.12. Реагирование на инцидент связанный с неправомерным доступом к компьютерной информации

Факт неправомерного доступа может быть обнаружен различными программно-техническими и организационными средствами. К программно-техническим можно отнести систему обнаружения атак и брандмауэры (firewall), формирующими сообщения об опасных ситуациях в файлах отчета (журналах регистрации). В течение этого процесса происходит фиксирование даты и времени, природы инцидента, оборудования и про-

граммного обеспечения, участвующем в нем. То есть, осуществляется обнаружение и регистрация факта неправомерного доступа к компьютерной информации, формируется файл отчета.

Следующим этапом является реализация мероприятий реагирования на инцидент. Использование в информационно-телекоммуникационной сети системы обнаружения атак позволяет производить ответные действия в режиме реального времени, так как в ней уже сформирован примерный алгоритм реагирования на нештатные ситуации, включающий в себя несколько этапов (рис. 2.13). На первом проверяется информация об инциденте и сетевые журналы, а на втором этапе осуществляется реализация мероприятий безопасности и изоляция инцидента.

На основе зарегистрированного факта осуществляется предупреждение администратора сети, а в отдельных случаях системой принимается решения на полную остановку обмена данными. Происходит реализация мероприятий по реагированию на нарушение информационной безопасности, изоляция попытки неправомерного доступа, фиксирование доказательной базы [50].

Целью заключительного этапа является создание как можно более полного набора документов. Применение системы обнаружения атак позволяет формировать необходимые документы, начиная с первой фазы вторжения и формировать отчет о происшедшем инциденте. Основываясь на файлах отчета есть возможность осуществить поиск и наказание лица или группы лиц виновных в инциденте, выработать рекомендации по совершенствованию мер защиты в используемой информационно-телекоммуникационной сети.

Эффективность использования методики реагирования на инцидент напрямую зависит от качества проведения анализа и выявления следов уже совершенных деяний. Он заключается в определении закономерностей проявления механизма неправомерного доступа, собирания, исследования, оценки и использования следов, а также совершенствовании средств, приемов, методов анализа и предотвращения в последующем подобных противоправных деяний. На основании отчета, предоставленного системой, необходимо провести проверку процедуры неправомерного доступа, по следам, оставленным злоумышленником. С учетом необходимой степени сохранности объекта исследования при проведении экспертизы могут быть использованы следующие методы [58]:

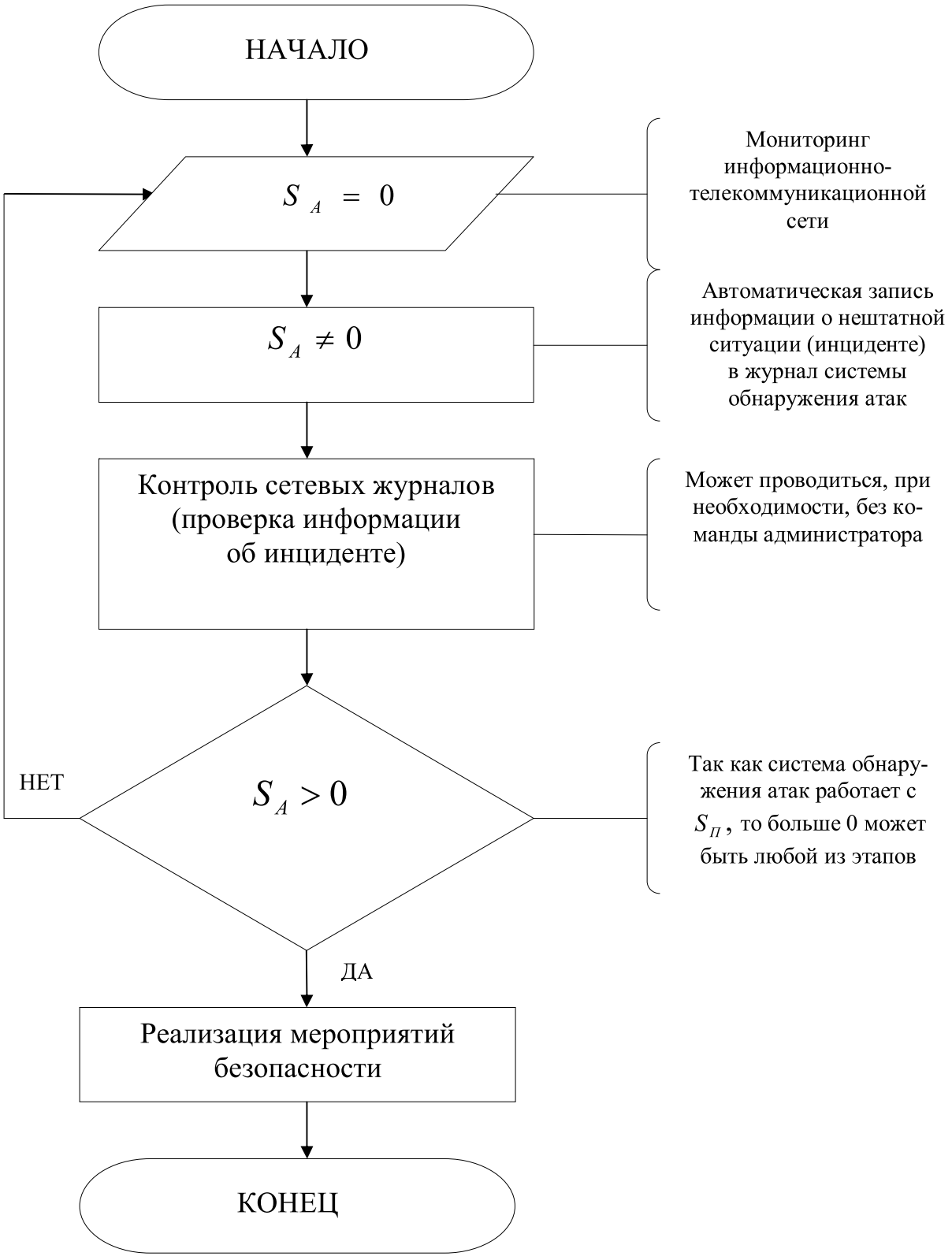

Рисунок 2.13. Примерная блок-схема алгоритма реагирования системы обнаружения атак на нештатные ситуации

- исследование компьютерных средств и систем, никак не влияющие на объект компьютерно-технической экспертизы и не требующие реализации процедур пробоподготовки;
- исследование компьютерных средств и систем, не разрушающие объект компьютерно-технической экспертизы, но изменяющие его состав, структуры или отдельные свойства;
- исследование компьютерных средств и систем, не разрушающие образец, но требующие для его изготовления разрушения или видоизменения объекта;
- исследование компьютерных средств и систем, полностью или частично разрушающие объект компьютерно-технической экспертизы или образец.

Естественно, что наиболее целесообразными являются методы, никак не влияющие на объекты информационно-телекоммуникационной сети. В этом случае есть возможность наиболее полно оценить процедуру неправомерного доступа, вред, нанесенный данным деянием, и выработать методику противодействия.

Поиск следов неправомерного доступа к компьютерной информации и анализ компьютерных сетей невозможен без обращения к данным, хранящимся на жестком диске. Подобный анализ может проводиться в как «живых» системах – «Прямой анализ», то есть продолжающих функционировать в составе информационно-телекоммуникационных сетей, так и при помощи «автономного анализа» («мертвая» система) в целях исключения модификации или утраты хранящейся на жестком диске информации, для чего производится их копирование на внешний носитель в целях последующего исследования (рис. 2.14).

Наибольшую сохранность следов обещает второй вид анализа, но при этом порядок его проведения зависит от средств обеспечения информационной безопасности в данной информационно-телекоммуникационной сети.

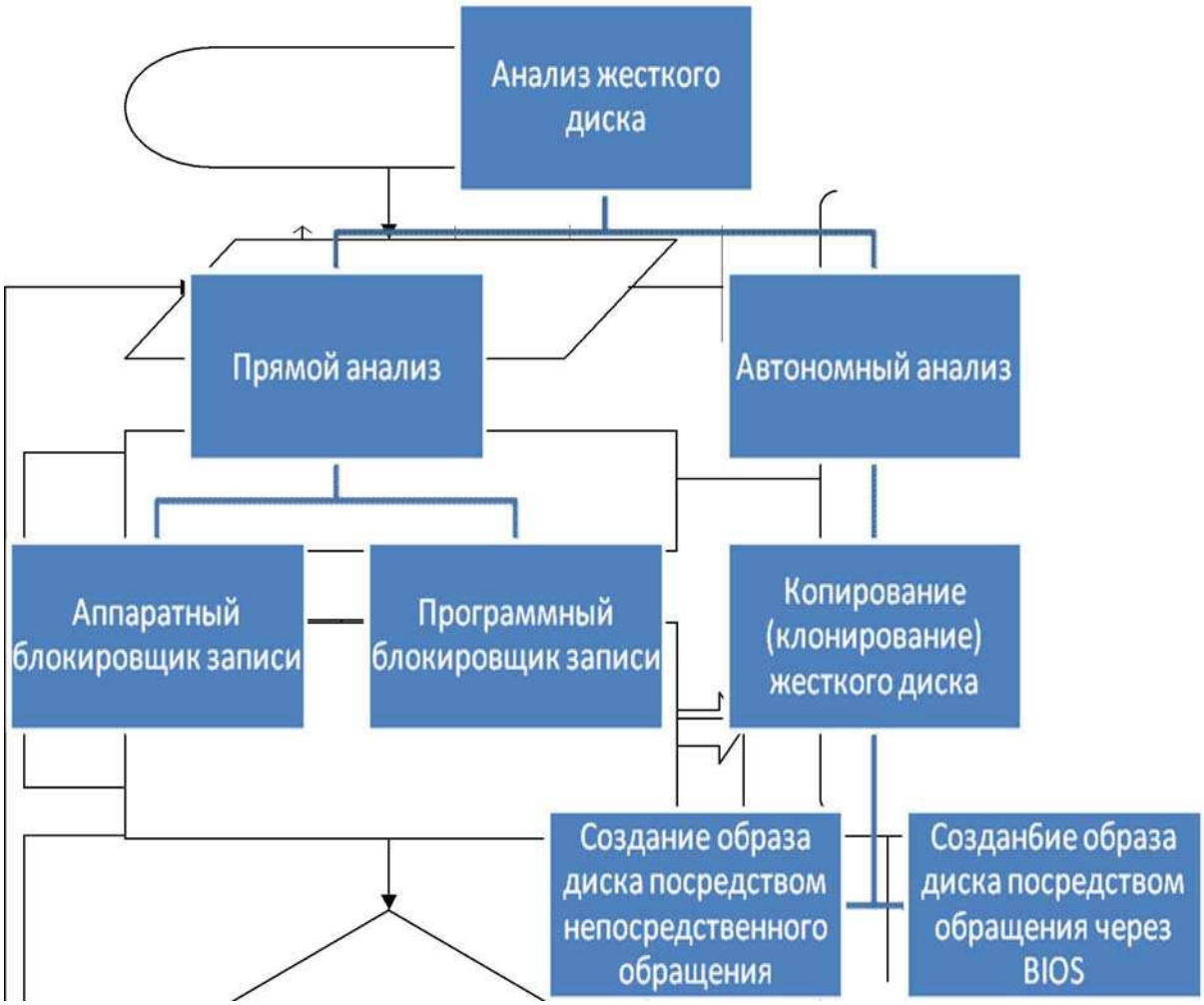

Рисунок 2.14. Порядок анализа жесткого диска

В том случае если производится исследование рабочей станции компьютерной сети с действующей системой обнаружения атак достаточно простого копирования файлов, так как в ней имеется журнал регистрации, содержащий информацию о действиях злоумышленника. При уверенности эксперта в том, что она не изменялась, все необходимые следы находятся на файловом уровне и достаточно произвести копирование журналов для последующего анализа.

Это можно объяснить принципом работы системы обнаружения атак основанном на том, что поведение взломщиков, вторгающихся в работу сети, отличается от действий зарегистрированных пользователей. При этом производится анализ отчетов о функционировании операционной системы, приложений и сравнение системных событий с заранее известной базой процедур нарушений безопасности. Располагающиеся на сетевых рабочих станциях компоненты системы обнаружения атак следят за различными аспектами безопасности, и в случае взлома или отклонений от нормального режима функционирования реагируют на это. Системой регистрируется подозрение на факт неправомерного доступа, предупреждается админист-

ратор, а в отдельных случаях производится полная остановка рабочих станций, изменение настроек межсетевых экранов или маршрутизаторов. Следовательно, система производит запись в журнал регистрации любых аномальных действий [94].

При использовании в компьютерных сетях иных средств обеспечения информационной безопасности необходимо проводить копирование информации, содержащейся на жестком диске. Для повышения эффективности данного процесса его необходимо проводить путем сохранения каждого байта на внешний носитель, так как при проведении этой работы на более высоких уровнях (диски, тома, файлы, приложения) теряется часть данных необходимых для объективного анализа. Например, если произведено копирование только существующих файлов, то в этом случае невозможно восстановление удаленных файлов, недоступны временные данные, служебная информация, скрытая в структурах и разделах исследуемой файловой системы.

В целях обеспечения безопасности копирования информации, содержащейся на диске, национальным институтом стандартов и технологий США (NIST, National Institute of Standards Technology) в рамках проекта CFTT (Computer Forensic Tool Testing) был разработан перечень требований для создания образов дисков. Спецификации приведены на http://www.cftt.nist.gov/disk_imaging.htm [50].

Существуют два способа обращения к диску:

1. Операционная система или программа копирования обращается к жесткому диску напрямую;
2. Операционная система или программа копирования обращается к жесткому диску через BIOS (Basic Input/Output System).

На первый взгляд второй способ удобнее, так как BIOS владеет всеми аппаратными тонкостями компьютера, но на самом деле все несколько сложнее. Если BIOS считает, что размер диска 300 Гбайт, а не фактические 500 Гбайт, то функция INT 13h предоставит доступ только к 300 Гбайтам и, как следствие, 200 Гбайт не будут скопированы для исследования и анализа [83].

В целях избежание подобных проблем эксперты, в настоящее время, загружают исследуемую рабочую станцию с компакт диска Linux, конфигурация которого не предусматривает модификации данных, и приступают к копированию информации, в процессе которого используемая программа должна обрабатывать возникающие ошибки. Кроме того, ей необходимо обнаруживать защищенную область диска, так как в противном случае хранящаяся в этой области данные не будут обнаружены.

При обнаружении на диске защищенной области требуется изменить его конфигурацию для получения доступа к скрытой информации. Для достижения этих целей необходимо чтобы максимальный сектор, адресуемый экспертом, был равен максимальному сектору на диске, но при этом

существует вероятность потери данных. Во избежание подобных случайностей предварительно целесообразно создать образ диска, а факт вскрытия защищенной области эксперту необходимо отразить в записях.

Одной из составляющих успешного проведения экспертизы является сведение к минимуму вероятности любых изменений исходных данных. Для эффективного достижения поставленных целей, возможно, использовать блокировщик записи, устройство, подключенное между компьютером и носителем информации, с задачей недопущения записи в регистр команд ничего способствующего изменению первоначальных данных.

К подобным устройствам можно отнести NoWrite компании My Key Technologies, которое выполняет функцию посредника между контроллером и жестким диском.[78] Оно позволяет записывать в регистр только заведомо безопасные команды. Блокировщик записи должен проходить специальное тестирование. Группа CFTT при NIST опубликовала спецификацию подобных устройств на сайте http://www.cftt.nist.gov/hardware_write_block.htm.

Кроме аппаратных блоков записи находят широкое применение и программные в основу работы которых заложена модификация таблицы прерываний. Он изменяет таблицу так, что в записи прерывания 0x13 хранится адрес кода блокировщика вместо адреса кода BIOS. Группа CFTT при NIST разработала требования к программным блокировщикам записи и поместила их на сайте http://www.cftt.nist.gov/software_write_block.htm.

При любом предложенном виде анализа необходимо определить криптографический хеш-код, который может понадобиться для доказательства целостности данных и отсутствия в процессе проведения экспертных действий следов модификации на носителе информации.

Криптографический хеш-код (MD5, SHA-1 или SHA-256) [81] представляет собой очень большое число, вычисляемое по математической формуле для набора входных данных. Изменение хотя бы одного бита во входных данных приводит к заметному изменению выходного числа. Для процедур хеширования разработаны специальные алгоритмы, при которых получение одинакового результата для двух разных входящих данных крайне маловероятно. Неизменность хеш-кода свидетельствует о том, что информация не подверглась модификации.

На этапе поиска следов совершения противоправного деяния осуществляется поиск, необходимый для подтверждения или опровержения выдвинутых на первоначальном этапе гипотез о происшедшем неправомерном доступе, в случае известности типа которого круг поиска сужается и начинается со стандартных мест.

Процесс поиска заключается, в первую очередь, в определении общих характеристик искомого объекта. На основании данных характеристик происходит выделение предмета и объекта поиска. Второй этап дол-

жен заключаться в поиске непосредственно в выделенном наборе данных, что позволяет сузить круг и сократить время поиска.

По мере проведения анализа требуется найти подтверждение или опровержение выдвинутых гипотез по обнаруженным следам совершения противоправного деяния. При проведении данного процесса эксперту для проведения объективного анализа следует искать не только следы, подтверждающие выдвинутую гипотезу, но и опровергающие ее.

Для выполнения подобных задач существует множество программ, используемых при проведении анализа цифровых систем, функции которых, в основном, сосредоточены в фазах сохранения и поиска следов. При этом компьютеры могут функционировать под управлением различных операционных систем. Существует множество видов программного обеспечения, используемого при анализе неправомерных действий в сфере информационных технологий. Например, в бесплатно распространяемом пакете TSK (The Sleuth Kit), содержатся следующие комплексы программам:

1. EnCase (Guidance Software), Forensic Toolkit (Access Data), ProDiscover (Technology Pathways) предназначенные для работы на платформе Windows.
2. SMART (ASR Data) предназначенная для работы на платформе Linux.
3. The Sleuth Kit/Autopsy предназначенная для работы на платформе UNIX.

Практика расследования неправомерного доступа в сфере компьютерной информации показывает, что большинство следов находятся в файловой системе. В этом случае к стандартной методике поиска следует отнести поиск ключевой комбинации в названии файла или поиск по шаблонам. Часто необходимо осуществлять поиск определенного слова в содержании файла или по его временным параметрам (время последнего обращения или записи), если анализ проводится по «горячим следам».

В некоторых случаях поиск можно осуществлять простым сравнением хеш-кодов содержимого файлов. Как правило, они вычисляются по алгоритмам MD5 или SHA и сравниваются с базой данных хеш-кодов для поиска заведомо хороших или заведомо вредоносных файлов. Для этих целей может использоваться National Software Reference Library [109].

Другой метод поиска основан на сигнатурах, присутствующих в содержимом файлов по которым часто удается найти все файлы заданного типа, даже если они были переименованы.

В случаях, когда требуется анализ сетевого трафика, возможен поиск всех пакетов, отправленных с некоторого исходного адреса, или всех пакетов, адресованных конкретному порту. Кроме того, при необходимости, можно найти все пакеты с заданными ключевыми словами.

При выполнении фазы реконструкции событий на основе найденных следов производится реконструкция событий происходивших в системе.

Для осуществления данной задачи эксперт должен на достаточно высоком уровне работать с операционной системой и приложениями, установленные на данном компьютере, чтобы провести правильную реконструкцию происходивших событий [50].

На основании предложенного порядка проведения анализа места совершения противоправного деяния в сфере информационных технологий следует привести некоторые общие рекомендации.

В первую очередь целесообразно осуществить сохранение исследуемой системы. Эксперт должен исключить любую вероятность модификации или уничтожения данных, которые могут послужить следами, то есть изолировать среду анализа от анализируемых данных и внешнего мира. Необходимость выполнения подобных действий объясняется тем, что неизвестно назначение и скрытые задачи исследуемых файлов. Порядок выполнения данной рекомендации зависит от метода проведения анализа. Предлагается различать, как указывалось ранее, два типа «мертвый анализ» и «живой анализ» [50].

При использовании метода «мертвого анализа» необходимо:

1. Провести копирование важных данных на аналогичный носитель и поместить оригинальный носитель исследуемой информации в надежное место. Исследование копии необходимо для исключения возможности модификации или удаления данных на протяжении всего процесса анализа и наличия сохраненных данных в случае модификации их копии программами с заранее заготовленными сценариями.

2. В процессе проведения исследования необходимо произвести вычисление хеш-кодов при помощи алгоритмов MD5 и SHA для данных, необходимых для проведения анализа.

При использовании метода «живого анализа» необходимо:

1. Воспользоваться устройствами блокирования записи во время любых действий, в особенности способных привести к изменениям данных во время анализа.

2. Свести к минимуму количество файлов, создаваемых в период проведения анализа способствующих стиранию следов на свободном пространстве диска, так как по оценкам специалистов из «хвостовых» кластеров через сутки можно извлечь до 85%, а через десять суток – до 25 – 40% исходной информации.

3. Проявлять осторожность при открытии файлов, так как данное событие может в свою очередь привести к модификации или удалению необходимых следов. Анализируемый файл может произвести запуск удаления данных, форматирования диска или осуществить попытку связаться с удаленной системой, а HTML-файл – инициировать свой заготовленный сценарий или запустить его с удаленного сервера.

Проведенное исследование позволяет сделать вывод о том, что проведение «живого анализа» является «рискованным предприятием».

Эксперту необходимо проверять анализируемые данные по независимым источникам, что снижает риск использования при проведении анализа модифицированных данных.

Кроме того, документирование всех действий, совершаемых во время проведения анализа, позволяет избежать повтора проводимого исследования и производить учет полученных результатов.

По окончании краткого рассмотрения фаз анализа места совершения противоправного деяния в сфере информационных технологий целесообразно приступить к рассмотрению способов и методике проведения анализа.

Современные базы данных имеют многоуровневую архитектуру, при этом обладая необходимой гибкостью и масштабируемостью для эффективного хранения и обработки информации циркулирующей в персональных компьютерах и информационно-телекоммуникационных сетях [73]. Воспользуемся аналогичной структурой для определения типов анализа, которая должна включать в себя две независимые области. Первая основывается на устройствах хранения информации, а вторая – на устройствах обмена данными.

Иерархия последовательности анализа производится на основании архитектуры цифровых данных. После проведения анализа физических носителей информации необходимо переходить к анализу томов и файловой системы с последующим выходом на прикладной уровень. В рамках данного исследования не рассматривается обращение к таким видам анализа, как анализ файлов подкачки, баз данных, анализ ячеек памяти, сетевой анализ.

Анализ физических носителей информации относится к исследованию низкоуровневых данных и требует наличия надежного метода чтения физических носителей (жесткие диски, карты памяти и т.д.). Это объясняется тем, что при необходимости долгосрочного хранения информации она организуется в виде томов, где под томами понимается совокупность ячеек доступных для обращения и записи со стороны приложений. Несколько мелких томов объединяются в более крупные, которые в свою очередь объединяются в разделы. Примером данной категории могут служить таблицы разделов Apple и массивы RAID. Анализ на уровне томов позволяет точно определить местонахождение файловой системы, данных и место хранения скрытой информации.

Самым распространенным содержимым томов являются файлы и файловые системы, созданные различными программами прикладного программного обеспечения, кроме того, они могут содержать базы данных или использоваться как временное пространство подкачки.

Файловые системы являются набором структур данных, которые позволяют приложениям производить различные действия с файлами. Анализ подобных систем необходим для поиска файлов, их восстановления в

случае удаления и в первую очередь должен быть направлен на поиск скрытой информации.

Для определения содержания файла необходимо перейти на прикладной уровень, который определяет структуру файла в зависимости от создавшего его приложения или операционной системы. Например, реестр Windows не отличается от обычной HTML-страницы и в тоже время они оба являются файлом, но, в то же время, они имеют разную структуру и для анализа должен использоваться разный инструментарий.

Анализ прикладного уровня играет важную роль, так как основываясь на анализе конфигурации файлов можно определить программы выполнявшиеся в системе и выявить скрытое содержание графических файлов, которое может создаваться при помощи специальных программ.

Можно сделать вывод о том, что поток байтов, полученный в результате анализа жесткого диска, в последующем анализируется на уровне томов, а дальнейший анализ происходит на уровне файловой системы и прикладном уровне. При этом необходимо учитывать, что данные об имени файла и его местоположении (адресе) обязательны. Если они не верны или отсутствуют, то, в этом случае, прочитать содержимое файла не представится возможным или будет получено ошибочное содержание. Кроме того, такой показатель как время последнего обращения к файлу может быть изменено умышленно или по неосторожности и опираться на подобные данные не следует.

На современном этапе развития общества и научно-технической революции сохраняется устойчивая тенденция к нарушению безопасности информации на всех стадиях ее обработки, хранения и передачи. Причины постоянного совершенствования процедур этого процесса кроются в высокой латентности случаев неправомерного доступа к информации в информационных сетях. В сложившейся ситуации просматривается глобальная тенденция по совершенствованию средств обнаружения, противодействия и предотвращения попыток неправомерного доступа в информационных сетях любого уровня [95].

Главная цель любой системы информационной безопасности 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 РФ [3], обеспечении нормальной производственной деятельности всех подразделений объекта. Все это указывает на то, что построение системы информационной безопасности на достаточно высоком уровне требует не только организационных, но и материальных издержек.

Глава 3. Особенности организационного обеспечения и определения экономической целесообразности информационной безопасности

На сегодняшний день ни у кого не вызывает сомнения необходимость обеспечения безопасности в сфере информационных технологий. Одним из основных критериев обоснования использования подобных средств является определение экономической целесообразности использования той или иной системы защиты информации. При этом необходимо помнить об общих принципах построения организационной защиты информации, что, также, оказывает существенное влияние на весь процесс обеспечения безопасности информации.

Созданию проекта системы обеспечения информационной безопасности, обычно, предшествует всесторонний анализ, который включает в себя экономическое обоснование. Следует указать на тот факт, что в процессе анализа необходимо опираться на методы бюджетного планирования, прогнозные показатели и перспективные сценарии развития организации.

Немаловажно проведение информационно-аналитической работы, которая позволяет прогнозировать проблемные ситуации в сфере обеспечения информационной безопасности и разрабатывать предложения по предположительным нарушениям безопасности информации.

3.1. Общие принципы организационной защиты информации

В настоящее время в нашей стране во многих, если не во всех государственных и частных структурах уделяют существенное внимание разработке и введению в эксплуатацию разнообразных систем обеспечения информационной безопасности. При этом необходимо учитывать, что подобные системы являются составными частями общегосударственной системы и должны соответствовать действующим нормативным документам и законодательным актам в данной области. Отечественный законодатель определил основные положения и принципы в Федеральном Законе «О безопасности» и «Доктрине национальной безопасности». В процессах построения систем обеспечения информационной безопасности немаловажную роль играет определение ее общей модели и основных принципов организационной защиты информации, что, в свою очередь, позволяет определить объемы последующих затрат на всех этапах разработки.

Построение модели системы защиты информации требует ее соответствия специальным нормативным документам по обеспечению информационной безопасности, принятым в Российской Федерации, международному стандарту ISO/IEC 15408 «Информационная технология - методы защиты - критерии оценки информационной безопасности», стандарту ISO/IEC 17799 «Управление информационной безопасностью» и учитывает тенденции развития отечественной нормативной базы (в частности, ФСТЭК РФ) по вопросам защиты информации.

Модель защиты – абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа [19].

Сама по себе модель системы обеспечения информационной безопасности заключается в стремлении владельца информации сохранить свой информационный ресурс в неприкосновенности и избежать неправомерного доступа. Для достижения поставленных целей владелец использует определенные меры противодействия, которые обладают некоторыми уязвимостями, приводящими к повышению рисков потери информационных ресурсов.

Злоумышленник, в свою очередь, предпринимает попытки преодоления системы защиты информации с целью получения неправомерного доступа. Для достижения поставленных целей он создает определенные угрозы, воздействующие на уязвимости, тем самым увеличивающие риск потери информационных ресурсов.

Отсюда можно сделать вывод о том, что модель системы обеспечения информационной безопасности должна являться совокупностью объективных внешних и внутренних факторов и их влияния на состояние информационной безопасности на объекте и на сохранность материальных или информационных ресурсов.

Общая структура модели системы обеспечения информационной безопасности должна включать основные цели, уязвимости и угрозы безопасности систем обработки данных, и, конечно, субъектов, участвующих в циркуляции информационных потоков.

Цели, преследуемые данной моделью, включают в себя несколько составляющих и проистекают из нескольких нормативно-правовых документов. В Конституции, УК РФ и ФЗ «Об информации, информационных технологиях и о защите информации» определяется разделение содержимого информационных ресурсов на общедоступную информацию и ограниченного доступа. В свою очередь, информация ограниченного доступа подразделяется, в соответствии с ФЗ «О государственной тайне», на содержащую государственную тайну и конфиденциальную.

К информации, содержащейся в информационных ресурсах, как объекту защиты, предъявляются три важных требования: конфиденциальность, целостность и доступность.

В Федеральном Законе «Об информации, информационных технологиях и о защите информации» даются следующие определения [5]:

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Доступ к информации - возможность получения информации и ее использования

При этом необходимо учитывать необходимость обеспечения **целостности** информации и предотвращения ее модификации либо блокирования.

Каждое требование разделяется на уровни, соответствующие критериям реальных пользователей (Таблица 3.1).

Таблица 3.1

<table>
<tr><th colspan="3">Требования к обеспечению информационной безопасности</th></tr>
<tr><th>конфиденциальность</th><th>целостность</th><th>доступность</th></tr>
<tr><td rowspan="2">контроль доступа</td><td>контроль и анализ защищенности</td><td>физическая и техническая защита</td></tr>
<tr><td>контроль активности пользователей</td><td>аутентификация</td></tr>
<tr><td rowspan="3">шифрование</td><td>отслеживание событий</td><td rowspan="3">идентификация</td></tr>
<tr><td>проверка</td></tr>
<tr><td>резервное хранение</td></tr>
</table>

Соблюдение режима требований к обеспечению информационной безопасности невозможно без использования программно-технических средств.

Признаки совершения противоправных действий, связанных с неправомерным доступом к информации представляют собой следы, оставленные злоумышленником. Чаще всего преступник использует не один метод неправомерного доступа, а их совокупность для достижения поставленной цели.

Проявлениями подобного опосредованного доступа могут являться [98]:

- ✓ физические следы разрушения, такие как следы взрыва, поджога и т.д.;
- ✓ вывод из строя отдельных компонентов, устройств, носителей информации;
- ✓ воздействия на лиц из числа персонала владеющих ключевой информацией;
- ✓ отключение или умышленный вывод из строя подсистем обеспечения функционирования объектов защиты, таких как, электропитание, охлаждение, линии связи и т.д.;
- ✓ постановка активных помех на частотах работы устройств и другие действия по дезорганизации работоспособности объекта;
- ✓ применение подслушивающих устройств, дистанционная фото-, видеосъемка, перехват побочных электромагнитных излучения;
- ✓ подключение к линиям связи и т.д.

Обнаружением подобных признаков преступлений занимаются специализированные подразделения с применением специальной аппаратуры.

В процессе обеспечения конфиденциальности и целостности составляющих информационных ресурсов необходимо учитывать уязвимости существующей системы обеспечения информационной безопасности, которые могут включать в себя технологические, физические, организационные и человеческие факторы.

Технологические уязвимости подразумевают возможность нарушения конфиденциальности или целостности информации посредством опосредованного доступа к системе обработки данных и представляют собой искусственные угрозы. Кроме того, подобные уязвимости проявляются в случаях возникновения естественных угроз.

Физические и организационные уязвимости подразумевают возможность проникновения на охраняемую территорию посторонних лиц, в обход используемых средств ограничения доступа, с целью получения возможности непосредственного доступа для нарушения конфиденциальности или целостности данных.

Немаловажную роль в процессе организации функционирования системы обеспечения информационной безопасности играет человеческий фактор. Это обуславливается тем, что любой сотрудник может создать искусственную внутреннюю угрозу преднамеренно или непреднамеренно. Кроме того, возможно банальное разглашение информации ограниченного

доступа третьим лицам с целью получения финансовой выгоды или в качестве мести организации (руководству).

В целях эффективного использования уязвимостей для осуществления неправомерного доступа к информации ограниченного распространения злоумышленник старается создавать и реализовывать угрозы, которые подразделяются на внешние (опосредованные) и внутренние (непосредственные). Каждая из них, в свою очередь, может подразделяться на естественные и искусственные, что уже было рассмотрено в предыдущем параграфе.

Существующие, в настоящее время, меры противодействия попыткам неправомерного воздействия на информационные процессы можно подразделить на программно-технические, организационные и правовые.

К правовым мерам следует отнести разработку норм, устанавливающих ответственность за разглашение информации ограниченного распространения, защиту авторских прав, совершенствование уголовного и гражданского законодательства, а также судопроизводства, вопросы контроля и надзора за разработчиками систем обработки информации, баз данных, приведение их в соответствие с нормами международного права.

В Российской Федерации нормативно-правовая база и структура законодательных актов имеет четкую иерархию. Все нормативно-правовые документы принимаются в строгом соответствии с подобными международными правовыми актами и, естественно, указы Президента, постановления правительства и другие документы принимаются в соответствии с нормативными правовыми актами федерального уровня (рис. 3.1).

Рисунок 3.1. Структура нормативных правовых актов в области информационной безопасности

Можно выделить четыре уровня правового обеспечения информационной безопасности. Первый уровень образуют международные договоры, к которым присоединилась Российская Федерация, и федеральные законы России.

Второй уровень правового обеспечения информационной безопасности составляют подзаконные акты, к которым относятся указы Президента РФ и постановления Правительства РФ, а также письма Высшего Арбитражного Суда РФ и постановления пленумов Верховного Суда РФ. Примерами таких актов могут являться Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 06.03.97 № 188 или Постановление Правительства РФ «О перечне сведений, которые не могут составлять коммерческую тайну» от 05.12.91 № 35.

Третий уровень правового обеспечения информационной безопасности составляют государственные стандарты (ГОСТы) в области защиты информации, руководящие документы, нормы, методики и классификаторы, разработанные соответствующими государственными органами.

Четвертый уровень правового обеспечения информационной безопасности образуют локальные нормативные акты, положения, инструкции, методические рекомендации и другие документы по комплексной защите информации в вычислительной сети конкретной организации. В соответствии с требованиями нормативных правовых актов Российской Федерации, а также Международного сообщества осуществляется построение структуры органов участвующих в организации и обеспечении информационной безопасности (рис. 3.2). Ведущую роль в данной структуре играет Президент Российской Федерации, а далее ветви власти разделяются на законодательную и исполнительную, включающие, в свою очередь, различные немаловажные составляющие.

К программно-техническим мерам можно отнести защиту от неправомерного доступа к информации ограниченного распространения, связанную с резервированием важных компонентов систем обработки информации, принятие конструкционных мер защиты от хищений и диверсий, обеспечение резервным электропитанием, разработку и реализацию специальных программных и аппаратных комплексов безопасности и многое другое. Средств технического обеспечения информационной безопасности, в настоящее время, существует достаточное количество, и они постоянно модернизируются.

Рисунок 3.2. Структура органов по организации и обеспечению информационной безопасности

К программно-техническим мероприятиям системы обеспечения информационной безопасности можно отнести:

- разграничение территориальных, частотных, энергетических, пространственных и временных в режимах использования технических средств подлежащих защите;
- разработка технических решений и элементов защиты информации при создании и эксплуатации вооружения и военной техники, при проектировании, строительстве (реконструкции) и эксплуатации объектов, систем и средств информатизации и связи;
- разработка средств защиты информации;
- создание и применение информационных и автоматизированных систем управления в защищенном исполнении;
- применение специальных методов, технических мер и средств защиты, исключающих перехват информации, передаваемой по каналам связи.

К организационным мерам относятся охрана систем обработки информации, подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности системы после выхода из строя. Универсальность средств защиты от всех пользователей (включая высшее руководство), возложение ответственности на лиц, которые должны обеспечить безопасность информации и т.п. Все эти вопросы должны иметь отражение в федеральном законодательстве, нормативных правовых актах, а также внутриведомственных нормативных документах. В первую очередь необходимо определить основные направления работ, что позволит эффективнее построить работы в данной области.

Основные направления работ позволяют вывести основные организационные и технические мероприятия позволяющие повысить эффективность системы обеспечения информационной безопасности.

К организационным мероприятиям целесообразно отнести:

- лицензирование деятельности предприятий в области защиты информации;
- сертификация средств защиты информации и контроля за ее эффективностью, систем и средств информатизации в части защищенности информации от утечки по техническим каналам;
- аттестование объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности;
- обеспечение условий защиты информации при подготовке и реализации международных договоров и соглашений;

- введение территориальных, частотных, энергетических, пространственных и временных ограничений в режимах использования технических средств подлежащих защите;
- категорирование вооружения и военной техники, предприятий (объектов) по степени важности защиты информации в оборонной, экономической, политической, научно-технической и других сферах деятельности государства;
- внедрение технических решений и элементов защиты информации при создании и эксплуатации вооружения и военной техники, при проектировании, строительстве (реконструкции) и эксплуатации объектов, систем и средств информатизации и связи;
- контроль за эффективностью средств защиты информации (специального и общего применения) и их использования.

Из вышеперечисленного можно сделать вывод о том, что работы по обеспечению информационной безопасности начинаются с определения перечня сведений ограниченного распространения циркулирующей в организации. На следующем этапе необходимо провести анализ реальной опасности перехвата информации различными средствами. Основываясь на проведенном анализе, следует провести разработку организационных и программно-технических мероприятий по защите информации и приступить к их реализации. На заключительном этапе с целью обеспечения эффективного управления системой обеспечения информационной безопасности следует проводить работы по организации и проведению контроля состояния системы.

Общие принципы организации защиты информации должны строиться в соответствии с требованиями данной организации и включать в себя:

- организацию и координацию работ по защите информации;
- определение информации ограниченного распространения и перечня лиц, имеющих к ней доступ;
- принятие в пределах компетенции соответствующих нормативно-правовых актов, регулирующих действия в области защиты информации;
- организация и координация работ по обеспечению информационной безопасности в соответствии с единой технической политики России;
- организацию сил и создание средств обеспечения информационной безопасности;
- обеспечение противодействия утечки информации ограниченного распространения по различным каналам;
- анализ системы обеспечения информационной безопасности, процедур противодействия неправомерному доступу и прогнозирование возможных каналов утечки;

- создание системы контроля за эффективностью функционирования системы обеспечения информационной безопасности.

Перечисленные требования определяют основные направления при проведении работ по обеспечении информационной безопасности. При этом необходимо прикладывать максимальные усилия по обеспечению защиты информации от различных процедур неправомерного доступа.

В первую очередь необходимо четко определить информацию ограниченного распространения, циркулирующую в организации.

На следующем этапе необходимо провести анализ рисков преднамеренного воздействия на сведения посредством перехвата информации техническими средствами разведки, неправомерного доступа, совершаемого с целью разрушения или модификации информации, и т.д.

Основываясь на проведенном анализе необходимо разработать организационно-технические мероприятия и определить пути их реализации.

На заключительном этапе необходимо приступить к организации контроля системы обеспечения информационной безопасности и определить способы его проведения.

На основании сказанного можно сделать вывод о достаточно сложном процессе построение системы обеспечения информационной безопасности объекта. При этом немаловажно учитывать условия необходимые для обеспечения организационной защиты информации.

Достаточно важным моментом в процессе обеспечения безопасности организации является допуск сотрудника к конфиденциальной информации. Свободный доступ к данным ограниченного распространения закрывается с целью защиты конфиденциальной информации и физической защиты ее носителей. В повседневной деятельности постоянный доступ к конфиденциальной информации имеет руководитель, что связано с тем, что он наиболее заинтересован в ее сокрытии от посторонних лиц.

Допуск к конфиденциальной информации оформляется в случае служебной необходимости и на основании заявления работника, с указанием причины получения данных. В случае необходимости, предусматривается изготовления копий с документов с использованием технических средств и оговаривается порядок обращения с подобными данными. Право на доступ и изготовление копий может быть оформлено в виде персональной карточки с указанием необходимых направлений деятельности сотрудника.

Руководитель вправе разрешить любому сотруднику или постороннему лицу использование конфиденциальных сведений, если в их отношении не установлены ограничения со стороны контрагентов (рис.3.3.)

Рисунок 3.3. Определение перечня лиц имеющих доступ к конфиденциальной информации

Штатные работники получают доступ к конфиденциальной информации и обеспечиваются ей в объеме, необходимом для качественного и своевременного выполнения порученных работ. При этом, допуск происходит только при исполнении условия о неразглашении подобных данных. При устройстве на работу или перед началом работы с конфиденциальной информацией, каждый сотрудник обязан пройти соответствующую проверку. Порядок проведения проверки указан на рисунке 3.4.

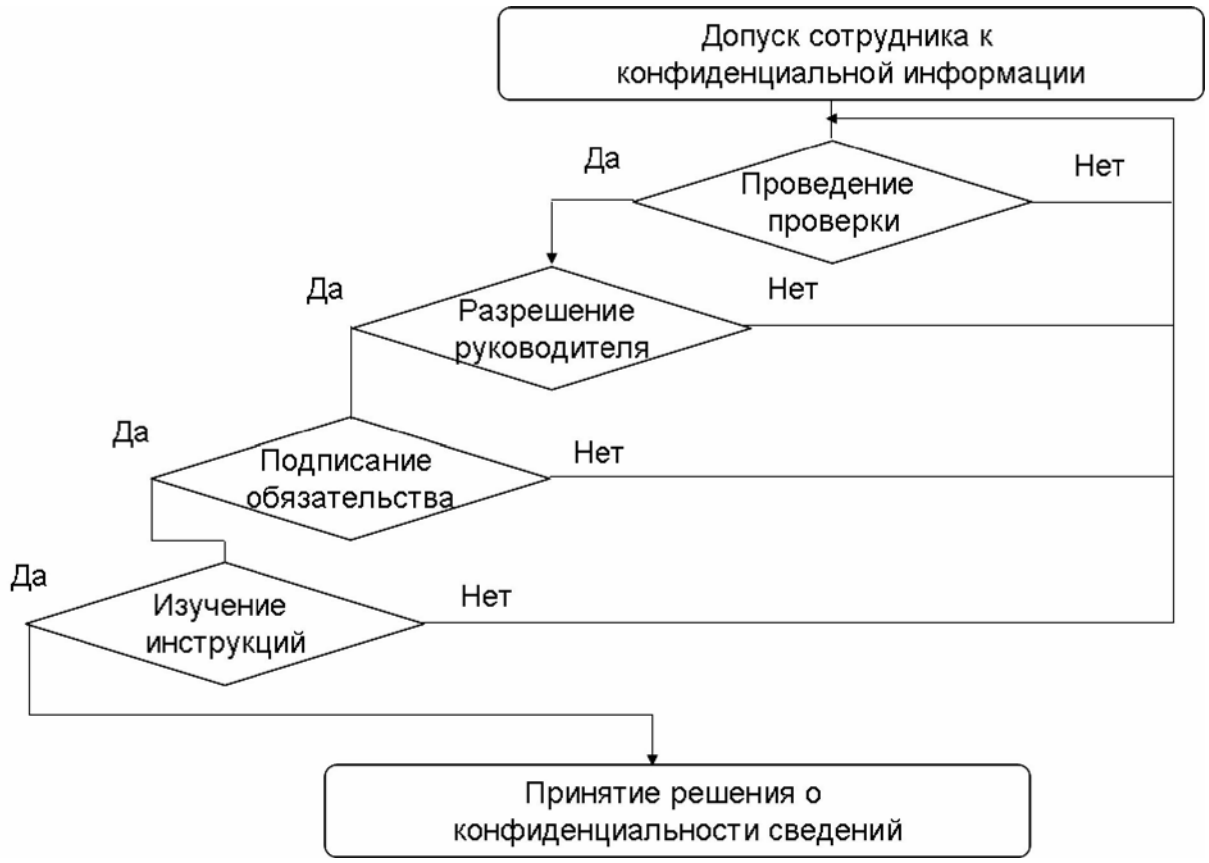

Рисунок 3.4. Порядок допуска к работе с конфиденциальной информацией

Цель, преследуемая проверкой, состоит в выявлении обстоятельств, которые препятствуют получению доступа к сведениям ограниченного распространения. Проверка осуществляется сотрудниками службы безопасности организации путем сбора информации различными средствами.

По результатам проверочных мероприятий сотрудниками службы безопасности готовится, оформленное соответствующим образом, заключение о результатах проверки с выводами о пригодности и возможности допуска работника или кандидата к сведениям ограниченного распространения.

В случае выявления обстоятельств, дающих основание для отказа в допуске к информации ограниченного распространения, возможен отказ в приеме на работу или прекращение действия трудового договора. Следует также указать, что решение о прекращении доступа сотрудника к конфиденциальной информации принимается также в случае нарушения установленных обязательств.

Окончательное решение о допуске принимает руководитель, и оно оформляется соответствующим приказом. Материалы проверки обычно хранятся в личном деле сотрудника.

Необходимо указать на недопустимость ознакомления исполнителя с конфиденциальной информацией, не имеющей отношения к исполняемой работе.

Не стоит оставлять без внимания процесс увольнения сотрудника или работника, что может нести серьезную опасность для обеспечения информационной безопасности предприятия или организации. Немаловажную роль в возникновении подобных потенциальных рисков играет поведение отдельных руководителей, которые мало интересуются внутренним состоянием и чувствами персонала попадающего под сокращение или причинами возникшего желания покинуть организацию. Практика показывает, что подобный подход может привести к достаточно серьезным негативным последствиям.

Существующие в настоящее время психологические подходы к процедуре увольнения позволяют выработать один из основных принципов, который заключается в том, что не смотря на причины увольнения сотрудник должен уходить без оставшегося чувства обиды или раздражения. Только в этом случае существует высокая вероятность того, что увольняемый не предпримет из чувства мести противоправных деяний.

В случаях увольнения сотрудника по собственной инициативе, представители кадровых подразделений и служб безопасности должны быть четко ориентированы на выяснение истинных мотивов увольнения всех категорий сотрудников. Часто встречаются случаи, когда причины, на которые ссылается сотрудник при увольнении, и подлинные мотивы, побудившие его к такому шагу, существенно отличаются друг от друга. Отсюда вытекает задача представителей кадровых подразделений, заключающаяся в необходимости точного определения причины увольнения, ее правильной оценки и принятия решения о целесообразности предпринятия попыток к искусственному удержанию данного лица в коллективе. В противном случае необходимо отработать и реализовать процедуру спокойного и бесконфликтного увольнения.

При обращении работника в устной или письменной форме с просьбой об увольнении целесообразно провести с ним беседу сотрудниками кадрового подразделения с обязательным участием представителя руководства. Но предварительно, перед этим, необходимо осуществить некоторые мероприятия по выяснению такой информации о сотруднике, как:

- уровень профессионализма;
- отношение к работе;
- взаимоотношения с коллегами;
- наличие служебных и неслужебных конфликтов;
- доступ и владение информацией, являющейся конфиденциальной, а также период ее устаревания и потери ценности;
- высказывания или пожелания о смене места работы, а также предполагаемое в будущем трудоустройство.

Построение самой беседы во многом зависит от предполагаемого результата и она может проводиться как в форме доверительной беседы, так и в официальном тоне. Необходимо обратить внимание на то, что вне зависимости от планов в отношении сотрудника он, в процессе встречи и беседы, не должен испытывать чувств обиды или унижения. Если уже принято решение об увольнении сотрудника располагающего доступом к конфиденциальной информации, то заинтересованным лицам необходимо отработать несколько вариантов ее сохранения в тайне.

В последнее время нередки случаи увольнения сотрудников по инициативе работодателя. В этом случае не следует спешно и необдуманно реализовывать принятое решение, особенно если это касается лиц имеющих доступ к конфиденциальной информации. В этом случае данное лицо необходимо предварительно, под благовидным предлогом, перевести в подразделение, не использующее в своей работе конфиденциальной информации. Кроме того, подобных сотрудников традиционно стремятся сохранить до тех пор, пока не будут найдены адекватные процедуры обеспечения информационной безопасности или не будут приняты меры по минимизации возможного ущерба.

Только после этого подлежащего увольнению сотрудника целесообразно приглашать для беседы с объявлением принятого решения и озвучивания причин отказа от его услуг. В процессе проведения этой беседы необходимо внимательно выслушать все аргументы и замечания сотрудника о стиле руководства, характере работы и т.д. Подобные высказывания, если их рассматривать объективно, могут быть достаточно эффективно использованы в дальнейшем.

В любом случае целесообразно поблагодарить увольняемого сотрудника за работу, а также, независимо отличных характеристик, взять с него подписку о неразглашении конфиденциальной информации. Кроме того, после увольнения осведомленных сотрудников, необходимо, в ряде случаев, проводить за ними контроль на новом месте работы с использованием возможностей собственной службы безопасности ил сторонних организаций специализирующихся на данной деятельности.

3.2. Методика расчета экономической целесообразности

Сегодня от утечек конфиденциальной информации страдают не только большие корпорации и маленькие фирмы, но и отдельные граждане. При этом многие руководители считают, что потеря нескольких никому не нужных документов не причинит сколько-нибудь значимого вреда и не снизит доверия к организации. Однако, в дальнейшем это может обернуться сотнями тысяч и даже миллионами долларов ущерба.

Еще одним заблуждением руководителей является уверенность, что наибольшая опасность исходит извне. Однако опасность, исходящая от своих нелояльных работников, так называемых инсайдеров, несоизмеримо выше в силу их посвященности во многие внутренние дела организации, знания скрытых механизмов и специфики работы. Именно на долю внутренних угроз приходится 71 % инцидентов (против 29 % внешних угроз) [77].

Организация Ponemon Institute опросила 450 экспертов по ИТ-безопасности в рамках исследования National Survey on Managing the Insider Threats, результаты которого показали, что 89 % респондентов считают атаки инсайдеров наиболее серьезной угрозой [79]. Однако, только 50 % руководителей компаний согласны со своими подчиненными и придают ключевое значение защите от внутренних утечек. В то же время, результаты другого исследования (2005 FBI Computer Crime Survey) показывают, что 44 % компаний в течение года пострадали от инсайдерских инцидентов, утечки или искажения данных. По сведениям The G1oba1 State of Information Security — 2005, средний ущерб от инсайдерских атак, составляет сотни тысяч долларов. И это при том, что по вине инсайдеров происходит около 60 % от общего числа инцидентов ИТ-безопасности.

По мнению многих экспертов, специализированные средства предотвращения утечек позволяют закрыть большинство каналов утечки, существенно снизить влияние «человеческого фактора», заблокировать потенциально опасных инсайдеров. Стоимость такого рода мероприятий (в среднем 300 тыс. долл.) ниже предполагаемых потерь в результате утечки конфиденциальной информации [54].

В настоящее время во многих подразделениях безопасности хозяйствующих субъектов эксплуатируются мощные информационные системы, обладающие значительными объемами накапливаемой информации и сложными логическими связями. Данные системы отличаются сложной технической инфраструктурой, с помощью которой они решают задачи оперативного сбора информации, ее первичной обработки, а также информационного взаимодействия с другими информационными системами через коммуникационные сети.

При этом, несмотря на то, что львиная доля мероприятий по обеспечению информационной безопасности возлагается на ИТ-подразделения,

ущерб может быть нанесен сотрудником, работающим в совершенно другом подразделении и негативно повлиять на деятельность всех подразделений организации. И это не говоря уже о подрыве репутации, что, даже на фоне огромных издержек на ликвидацию последствий утечек и возмещения ущерба пострадавшим, выглядит более угрожающим в стратегической перспективе [30].

Все выше сказанное не означает отсутствия необходимости защиты от внешних угроз, но указывает на целесообразность использования комплексного подхода к построению устойчивой системы обеспечения информационной безопасности.

Для решения задач противодействия неправомерному доступу в сфере информационных технологий также требуется широкий спектр профессионалов, являющихся специалистами по вычислительной технике, средствам связи, передачи данных в телекоммуникационных системах и программированию, системные и информационные аналитики, специалисты по защите информации, операторы-технологи, оперативные работники. Естественно, что потребности в этих специалистах по мере становления и развития рыночной экономики в России будут только расти [56].

Российская высшая школа ранее никогда не занималась подготовкой специалистов по обеспечению экономической безопасности и в том числе специалистов по противодействию неправомерному доступу в сфере информационных технологий в частности. Однако на сегодняшний день проблема подготовки специалистов, которые могут обеспечивать принятие оптимального решения в условиях системной неопределенности, связанной с различными предпринимательскими рисками, встала кардинально. Не менее кардинально встала проблема подготовки специалистов в сфере обеспечения информационной безопасности [49].

Сегодня по ряду причин система российского высшего образования находится в состоянии кризиса, поэтому и стратегия подготовки специалистов по противодействию неправомерному доступу в сфере информационных технологий должна формироваться, исходя из сложившейся реальной ситуации на двух уровнях.

Первый уровень:

- необходимо ввести в учебные планы ряда специальностей хотя бы установочные курсы по экономической безопасности и информационно-аналитической работе;
- необходимо организовать сеть курсов переподготовки и повышения квалификации специалистов смежных областей.

Второй уровень:

- целесообразно начать планомерную и фундаментальную подготовку высококвалифицированных молодых специалистов в области экономической безопасности и информационно-аналитической работы;

- целесообразно развернуть исследовательскую работу и аспирантскую подготовку в данном направлении на базе академических институтов и вузов [30].

Также в целях улучшения качества подготовки высококвалифицированных специалистов по противодействию неправомерному доступу в сфере информационных технологий необходимо внести изменения в действующие учебные планы, причем эти изменения должны носить адекватный текущему моменту характер. В качестве обязательных компонентов должны рассматриваться системотехнические знания в данной предметной области; знание средств связи и передачи данных, вычислительной техники, системного администрирования (в особенности знание методов, способов, средств и системной организации защиты информации), программирования; владение различными способами и видами информационно-аналитической деятельности; теоретические и практические знания по моделированию рисковых ситуаций и процессов; а также способов, типологий и алгоритмов информационного нападения и защиты.

Очевидно, что данный перечень неизбежно будет уточняться и расширяться по мере развития технологий информационно-аналитической работы, подобно тому, как будут меняться требования, предъявляемых к специалистам различного уровня квалификации.

Если обратиться к зарубежному опыту, то, например, в Федеративной Республике Германии уже с 1973 года на базе торговой и промышленной палаты готовятся квалифицированные кадры в области экономической безопасности и противодействия неправомерному доступу в сфере информационных технологий. По окончании этих курсов претенденты на различные должности в негосударственной системе безопасности сдают квалификационные экзамены [52].

В условиях рыночной экономики любая коммерческая структуры стремится к получению максимальной прибыли. Это – базовый, основной принцип работы любой коммерческой структуры. При этом практически всегда объективно существует возможность понести убытки, а следовательно, рисковая составляющая является неустранимым элементом управленческого решения любого уровня.

С управленческой, да и с экономической точки зрения риск – это величина, характеризующая убытки (потери), вызванные неправильными управленческими решениями, принимаемыми в результате мониторинга экономических, политических и социальных параметров ситуации, в которой протекает деятельность. Оптимальное управленческое решение подразумевает высокую достоверность и качество прогнозов тенденций развития, которые, в свою очередь, базируются на качественном анализе текущей ситуации.

Можно выделить четыре основные категории рисков: стратегический, экономический, природный и политический [37].

Стратегический риск представляет собой совокупный результат динамики политических, экономических и социальных факторов, то есть так называемую системную неопределенность. В данном контексте организация должна постоянно адаптировать стратегию и тактику своего развития к постоянно изменяющимся условиям рыночной конъюнктуры, что возможно только при проведении активной и эффективной работы по сбору и анализу информации, т.е. постоянного текущего мониторинга оперативной обстановки.

При этом ключевая задача обеспечения безопасности в сфере информационных технологий состоит в превентивном мониторинге и оперативном выявлении источников внешних и внутренних угроз, что способствует максимальному снижению неопределенности стратегического риска. Подобного рода деятельность должна оперативно выявлять угрозы, своевременно обеспечивать их нейтрализацию, проводить комплексную диагностику информационных систем на предмет потенциальной возможности неправомерного доступа и утечки информации. Кроме того, система информационной безопасности призвана обеспечивать руководство хозяйствующего субъекта по возможности полной и достоверной информацией об истинных намерениях действительных и потенциальных партнеров, о слабых и сильных сторонах конкурентов, контролировать «узкие места» в информационной безопасности, своевременно сигнализировать о возможном возникновении кризисных ситуаций.

Помимо прочего, система информационной безопасности должна позволять контролировать ход реализации и соблюдения партнерами достигнутых ранее договоренностей, выявлять потенциальные каналы утечки конфиденциальной информации о предприятии [30].

Современный этап развития можно охарактеризовать такой особенностью, как принятие априори принципиальной обоснованности необходимости создания систем обеспечения безопасности информации. На сегодняшний день никакая стратегия, производственная и коммерческая политика, а, следовательно, и капиталовложения, научно-исследовательские работы, структурные изменения и т.д., не представляются возможными без накопления и углубленного изучения информации в период создания информационного общества.

По оценкам западных экспертов, затраты на обеспечение информационной безопасности составляют значительную долю бюджета транснациональных корпораций.

В России ситуация значительно сложнее, и допустимые затраты на «информированность» руководства для каждого хозяйствующего субъекта - дело сугубо индивидуальное. Но, в любом случае, своевременное обеспечение безопасности в сфере информационных технологий позволяет значительно облегчить процесс сохранения конфиденциальной информации от неправомерного доступа, не допустить использования данной информа-

ции при гринмейле – корпоративном шантаже и при осуществлении стратегического планирования конкурентов.

Широкое и повсеместное использование различных информационных ресурсов выводит на передний план проблемы их защиты от неправомерного доступа. В этой связи следует указать, что если инструментарий противодействия внешним угрозам разработан достаточно тщательно (есть методы и средства борьбы с хакерами, спамом, вирусами), то с внутренними угрозами дело обстоит сложнее. Причина подобной ситуации кроется в том, что руководители, достаточно часто, просто недооценивают опасность внутренних угроз. Кроме того, немаловажную роль играет недостаточная квалификация сотрудников службы безопасности в вопросах выявления и документирования противоправных действий со стороны нелояльных работников.

Здесь можно привести данные исследования, проведенного компанией Info Watch - Annual Study: Cost of a Data Breach. Суммировав все убытки 31 компании исследователь получили сумму в 148 млн долл., т.е. в среднем 4,8 млн долл. на компанию, что является весьма значительной величиной.

Исследовав инциденты по утечке информации, специалисты пришли к выводам, что в руки злоумышленников попали конфиденциальные данные от 2,5 до 263 тыс. чел. из каждой пострадавшей организации. В среднем из расчета на одну фирму – 26,3 тыс. записей, суммарно же это персональные данные почти 815 тыс. граждан. Таким образом, легко вычислить средние убытки организации на каждую единицу информации – 182 долл. Таким образом, налицо экономическая целесообразность защиты информации, которая будет стоить гораздо дешевле и прослужит не один год [77].

Для наглядности приведем структуру прямых издержек представленных в таблице 3.2.

Таблица 3.2. Прямые средние издержки на каждую потерянную запись

Статья расходов	**Расход, долл.**
Бесплатные услуги и поддержка	24
Уведомления по почте, телефону, Интернету и/или через СМИ	13
Услуги по найму адвокатов	7
Судебные издержки, расходы на аудит и бухгалтерию	4
Расходы на call-центры	3
Связи с прессой	1
Внутренние расследования	1

Обратимся теперь к прибыли, которую компания недополучила вследствие нанесенного марке вреда, потери имевшихся клиентов и возникновения трудности в привлечении новых, то есть к упущенной выгоде. Средняя упущенная выгода (согласно данным исследования 2006 Annual Study: Cost of a Data Breach), составила $98 на одну приватную запись, или $2,6 млн на компанию. Это на 31 % больше показателя предыдущего года. Теперь детализируем вышеперечисленные данные в таблице 3.3 и на диаграмме 3.5 [77].

Таблица 3.3

	средние косвенные издержки	средние общие издержки	средние прямые издержки	средняя упущенная выгода
млн $	0,8	4,8	2,6	1,4
$/запись	30	182	98	54

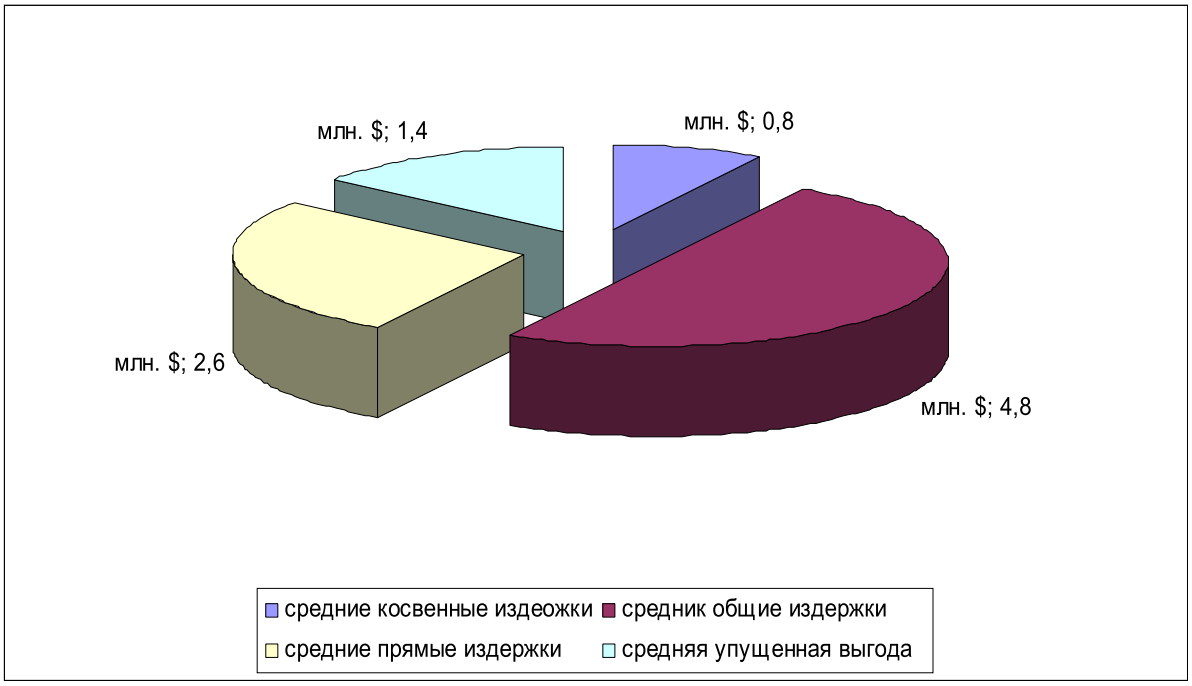

Рисунок 3.5. Средние издержки, приходящиеся на одну компанию

Как видно из приведенных в диаграмме данных, общие издержки на одну компанию составили $4,8 млн.

Приведенные в таблице и на диаграмме данные — всего лишь непосредственные затраты на ликвидацию последствий утечек. В то же время можно с уверенностью констатировать, что в стратегической перспективе ущерб бренду с большой долей вероятности обернется более значительными потерями, величина которых существенно превысит текущие расходы на ликвидацию последствий утечек.

По результатам проведенного в ходе исследования опроса среди населения выяснилось, что около 12 % из 9 тыс. ответивших граждан получили уведомления об утере их персональной информации. Учитывая данную пропорцию, можно предположить, что кража личностных данных затронула около 23 млн совершеннолетних американцев. Результатом данной ситуации стал тот факт, что немногим менее двух третей пострадавших либо планируют разорвать отношения со скомпрометировавшими либо себя компаниями в ближайшее время, либо уже сделали это. При этом еще 27 % обеспокоены кражей личностных данных, и лишь 14 % респондентов не выказали озабоченности в связи с инцидентами (таблица 3.4 и рисунок 3.6) [77].

Таблица 3.4

Обеспокоены утечкой	Прервали сотрудничество	Собираются прервать сотрудничество	Не обеспокоены
27%	19%	40%	14%

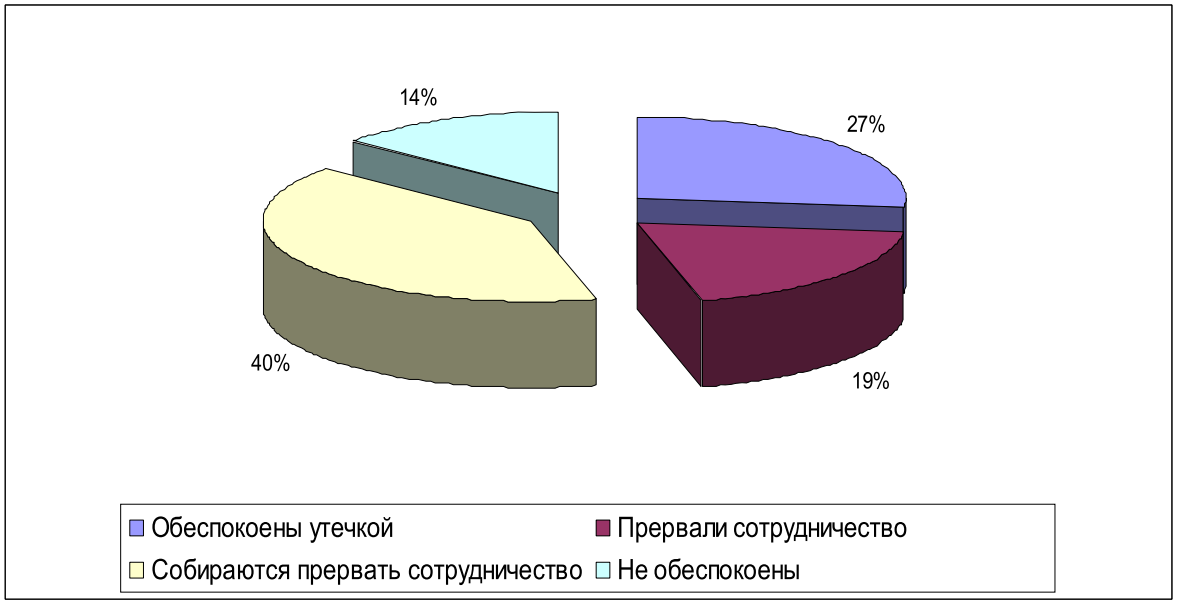

Рисунок 3.6. Реакция граждан на утечки их персональных данных

По мнению экспертов InfoWatch, последняя цифра была бы значительно меньше, если бы все граждане осознавали возможные последствия утечек. Так как некоторые граждане просто до конца не осознавали всей опасности незаконного использования их личных данных [35].

Как уже отмечалось выше, потеря клиентской базы влечет за собой не только прямые издержки и потерю упущенной прибыли. Негативное отношение со стороны потребителей и контрагентов будет еще длительное время оказывать самое отрицательное влияние на фирму, вплоть до поте-

ри доверия к ней, а восстановить подорванное доверие граждан, по мнению аналитического центра Info Watch, будет очень непросто.

На приведенных ниже таблицах и диаграммах представлены следующие данные: на первых (таблица 3.5 и рисунок 3.7) представлены подразделения, на которые приходятся наибольшие траты при возмещении ущерба от утечек, а на вторых (таблица 3.6 и рисунок 3.8) показана степень ответственности за потерю конфиденциальной информации [77].

Таблица 3.5

Поддержка клиентов	ИТ-безопасность	Маркетинг	Право, аудит управление рисками
34%	0%	55%	11%

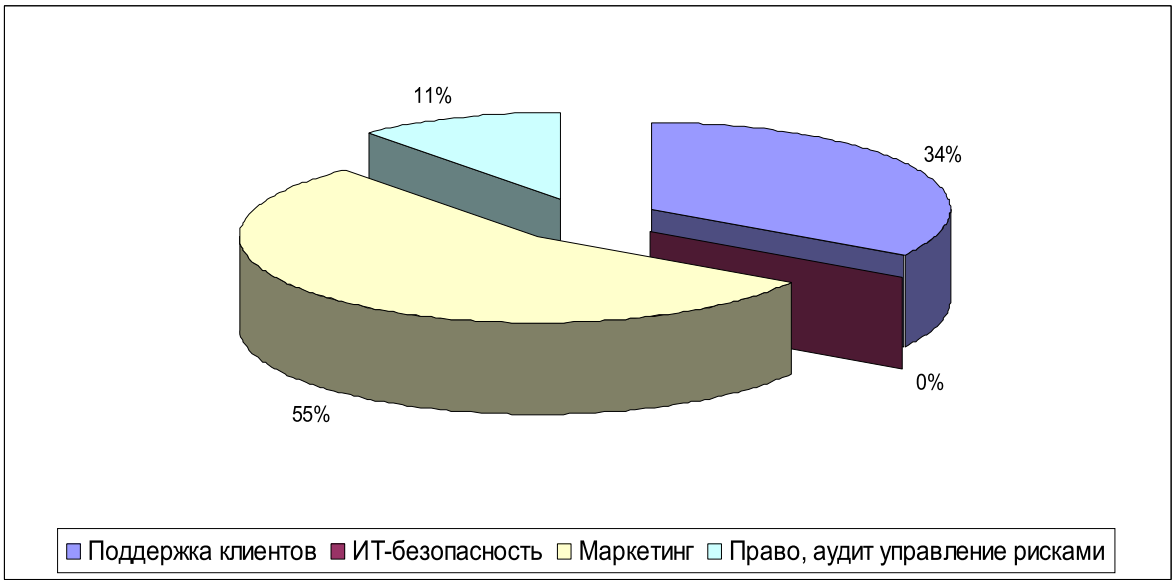

Рисунок 3.7. Затраты при возмещении ущерба по подразделениям

Таблица 3.6.

Деловой сектор	Служба безопасности	Нормоконтроль	ИТ-исполнители	ИТ-безопасность	Совместная вина
7%	7%	3%	33%	20%	30%

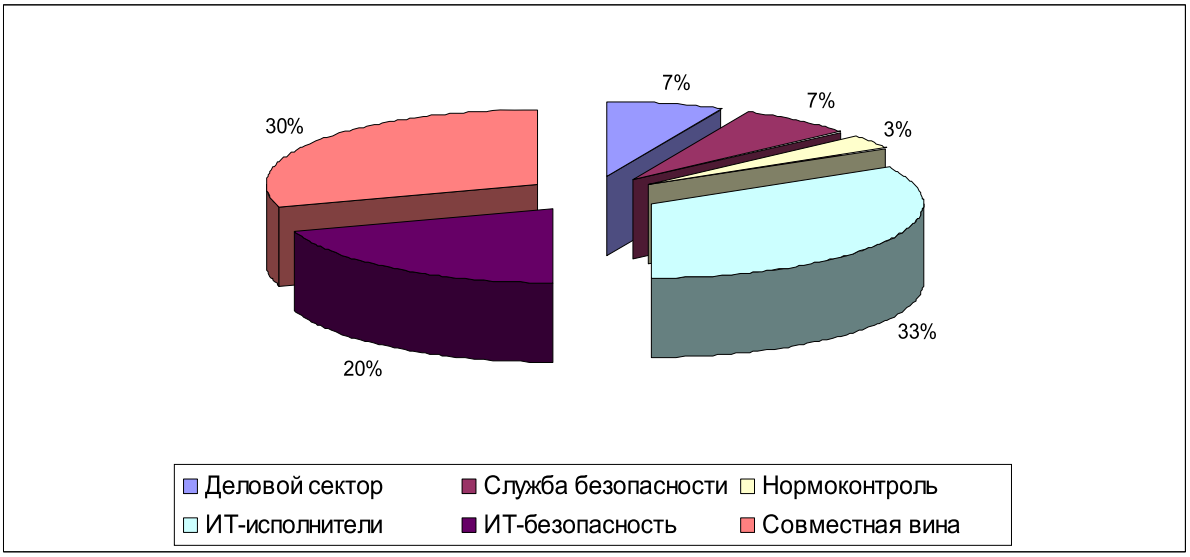

Рисунок 3.8. Разделение ответственности за утечку информации

На основе анализа данных вышеприведенных таблиц и диаграмм можно сделать следующие обобщающие выводы: с одной стороны, сотрудники ИТ-подразделений несут наибольшую ответственность (всего более половины: 20% ИТ - безопасность и 33% ИТ - исполнители) за утечки данных. Это закономерно, так как именно они наиболее осведомлены об электронных угрозах и именно на них возложены задачи сохранении информации. В то же время, ИТ - службы не несут никаких затрат при возмещении ущерба. При этом вся тяжесть последствий ложится на отделы маркетинга (55 %), службы поддержки клиентов (34%), а также подразделения аудита и управления рисками (11 %). И это при том, что нередко в краже данных повинны сотрудники сразу нескольких секторов (почти треть в опросе) [54].

Данное обстоятельство следует учесть как при установлении ответственности работников за утрату конфиденциальных данных, так и при мероприятиях компенсационного характера, направленных на скорейшее восстановление организации после понесенных убытков, так и при мероприятиях, направленных на недопущении подобной ситуации в будущем [30].

Как и любая другая деятельность, сопряженная с использованием материальных, интеллектуальных и прочих ресурсов, деятельность по противодействию неправомерному доступу в сфере информационных техно-

логий требует составления детального бюджетного плана, являющегося по своему содержанию точным и полным описанием всех затрат, которые возникают в процессе этой деятельности. Он призван дать доходчивое представление лицам, принимающим решение, о величине расходов, которые предстоит понести, а также доказать необходимость этих расходов, сравнив их с материальными и нематериальными дивидендами, получаемыми от деятельности системы обеспечения безопасности в сфере информационных технологий [59].

Таким образом при расчете затрат по противодействию неправомерному доступу в сфере информационных технологий применяется затратная методика бюджетного планирования.

Зачастую доход от осуществления мероприятий по противодействию неправомерному доступу в сфере информационных технологий не отображает всех выгод от использования системы безопасности, а сводится лишь к измерению выгоды в денежном выражении, кроме того, во многом носит прогнозный, сдвинутый во времени характер. Затратная же методика значительно приближена во времени, показывая затраты, которые понесет организация уже сейчас. Для реализации этой методики служит бюджетный план.

Бюджетный план, как правило, бывает многоуровневый и состоит из:

- первоначальных затрат на создание самой структуры и минимальных информационных массивов, необходимых для начала ее работы;
- ежемесячных расходов на обеспечение повседневной информационно-поисковой и информационно-аналитической работы;
- годового бюджета (обычно связанного с закупкой дорогостоящей техники), с разбивкой по кварталам и месяцам.

Процесс же согласования этого документа может занять приличный временной промежуток [30].

На основании предлагаемого бюджетного плана попробуем представить примерную структуру предполагаемых затрат**:**

1. Заработная плата оперативного состава и аналитиков ($З_п$) - ...
2. Затраты на технику (компьютеры, периферия, охранная сигнализация, спецтехника и т.д.) ($З_Т$) -...
3. Затраты на программное обеспечение (системы управления базами данных, специальные программы, необходимые для функционирования спецтехники, и т.д.) ($З_{ПО}$) -...
4. Затраты на официальную закупку информации ($З_И$):

- Интегрум-техно, Публичная интернет-библиотека и т.д. - ...
- пресса в электронном виде - ...
- местная пресса - ...
- базы данных - ...

5. Оплата услуг доверительных источников («девятка») ($З_{ДИ}$):

- регулярные выплаты - ...

- разовые выплаты -...

- резервный фонд на премирование при чрезвычайных ситуациях и предотвращении крупных ЧП -...

6. Представительские расходы (подарки, спиртное и угощения, необходимые для завязывания и поддержания деловых и доверительных контактов) ($З_{ПР}$) - ...

7. Командировочные расходы (оплата гостиниц, проездных билетов, суточные и т.д.) ($З_К$) - ...

8. Услуги связи ($З_С$):

- затраты на покупку средств связи - ....

- лимиты на услуги операторов связи - ... -
аренда частот-...

- оплата услуг Интернет-провайдеров - ...

9. Оплата услуг сторонних организаций (сторонние информационные компании, привлекаемые для выполнения особо сложных заданий; государственные структуры, выполняющие информационные запросы на платной основе; технические фирмы, располагающие дорогостоящей техникой и богатым опытом, оказывающие услуги в области информационной безопасности) ($З_{СО}$)

10. иные затраты ($З_{проч}$).

Данный перечень затрат можно считать примерным, но отнюдь не исчерпывающим, поскольку мероприятия по противодействию неправомерному доступу в сфере информационных технологий могут быть различны как по суммарным затратам, так и по целям. Обобщенно же формула суммарных затрат по противодействию неправомерному доступу в сфере информационных технологий имеет вид:

$$\sum З_{ОБЩ} = З_п + З_Т + З_{ПО} + З_И + З_{ДИ} + З_{ПР} + З_К + З_С + З_{СО} + З_{проч}$$

В качестве приложения отражается и утверждается то, что планируется приобрести в течение года, а одним отдельным документом - ежемесячные затраты.

В идеале деятельность по обеспечению безопасности в сфере информационных технологий должна вестись параллельно с разведывательной и контрразведывательной деятельностью, дабы своевременно выявлять потенциальные угрозы безопасности информации и адекватно на них реагировать.

Расходы на систему обеспечения безопасности информации, как и на другие расходы предприятия, планируются в рамках утверждаемого бюджета хозяйствующего субъекта с разбивкой по соответствующим статьям. В целях обеспечения безопасности отдельные статьи расходов могут детализироваться или легендироваться под проведение маркетинговых исследований, рекламных или консалтинговых услуг.

В обязательном порядке должны быть определены должностные лица, имеющие право выделять конкретные суммы на оперативные расходы при проведении мероприятий, требующих дополнительных затрат, и организована строгая система контроля за соблюдением финансовой дисциплины. В противном случае возникают ситуации, иллюстрируемые приведенным ниже примером нецелевого использования денежных средств.

При этом отчет по всем затратам в рамках проведенных операций с максимальной степенью детализации и в обязательном порядке должен сопровождаться финансовым отчетом, который утверждается лишь после его скрупулезной оценки компетентными лицами.

При образовании остатка денежных средств при проведении оперативных мероприятий целесообразно направлять его на премирование наиболее отличившихся сотрудников соответствующих подразделений. Кроме того, здоровая стимуляция за успехи в служебной деятельности при выполнении заданий руководства обязательно должна найти свое отражение в нормативных документах службы безопасности [30].

Теперь рассмотрим более подробно структуру потерь при ликвидации последствий утечки информации (таблица 3.3).

Таблица 3.7. Средние издержки на возмещение ущерба утечек на каждую запись, $

Мероприятие	**Прямые издержки**	**Потери от снижения производительности**	**Упущенная прибыль**	**Всего**
Обнаружение и изучение инцидента	**5,76**	**5,51**	**-**	**11,28**
Внутреннее расследование	1,38	4,10	-	5,48
Правовые, аудиторские и консультационные услуги	4,38	1,41	-	5,80
Уведомление	**13,03**	**12,16**	**-**	**25,19**
Почтой	5,30	1,11	-	6,41
Электронными письмами	0,34	0,53	-	0,86
По телефону	7,30	10,47	-	17,76
Через печатные издания	0,03	-	-	0,03
На веб-сайтах	0,06	0,06	-	0,12
Последующие мероприятия	**35,42**	**11,97**	**-**	**47,39**
Почта	0,13	0,10	-	0,23

Мероприятие	**Прямые издержки**	**Потери от снижения производительности**	**Упущенная прибыль**	**Всего**
Электронные письма	0,15	0,86	-	1,00
Звонки на внутренний call-центр	1,88	3,28	-	5,16
Звонки на внешние call-центры	1,40	4,62	-	6,03
Услуги адвокатов	5,51	1,12	-	6,63
Судебное расследование	1,38	1,10	-	2,48
Общение с прессой и инвесторами	1,16	0,89	-	2,05
Бесплатные услуги	23,80	-	-	23,80
Ущерб бренду	**-**	**-**	**98,32**	**98,32**
Потеря лояльных клиентов	-	-	4,70	4,70
Потеря клиентов	-	-	93,62	93,62
Сумма затрат на компенсацию утечки	**54,22**	**27,96**	**98,32**	**182,17**
Последующие затраты на ИТ	6,85	-	-	6,85

В первую очередь следует выделить величину затрат на элементарное уведомление клиента о потере или утечке его персональных данных. По американскому законодательству это нужно делать обязательно, по российскому - всего лишь желательно. Вместе с тем, получение подобной информации способно побудить гражданина сможет предпринять самостоятельные шаги в направлении самостоятельного обеспечения собственной информационной безопасности и минимизации возможного ущерба от действий мошенников.

В данном аспекте самыми затратными выходят телефонные звонки (по $17,76 на запись), немного отстают от них почтовые уведомления ($6,41). В то же время, способы уведомления, основанные на современных технологиях, выглядят более привлекательно в силу их относительной дешевизны: стоимость электронного письма всего $0,86, а использование интернет-сайтов еще дешевле — $0,12. Суммарно на извещение клиента уходит $25,19. Это довольно много по сравнению с расходами на внутреннее расследование инцидента ($11,28): собственно на расследование — $5,48 и правовые, аудиторские и консультационные услуги — $5,80 [54].

Как видно из данных таблицы, сумму расходов на уведомление и расследование превышают траты на ликвидацию последствий, что на наш взгляд еще раз говорит в пользу превентивных мер по обеспечению информационной безопасности. Цифра в $47,39 на учетную запись – довольно значительна в масштабах организации, поскольку она возрастает в геометрической прогрессии в зависимости от масштабов организации. Данная величина складывается из бесплатных услуг клиентам ($23,80), телефонных звонков (в сумме $ 11,19) и услуг адвокатов ($6,63). Это наиболее значительные статьи расходов, прочие затраты существенно ниже.

В то же вышеперечисленные статьи расходов даже суммарно уступают перспективным убыткам в $98,32 от ущерба репутации. Большую часть здесь составляет потеря текущих пользователей ($93,62). Напомним, что данная величина с течением времени имеет тенденцию к увеличению, поскольку негативный имидж компании, помноженный на информационные коммуникации потерянных пользователей будет способствовать росту отрицательной величины.

Последняя строка табл. 3.7 — уже упоминавшиеся расходы ИТ-подразделений на укрепление защиты от утечек. Они составляют весьма скромные $6,85 на запись, что почти в три раза меньше затрат на телефонное уведомление клиентов [54].

Таким образом, экономический эффект от своевременной и надежной защиты налицо, поскольку превентивная защита позволит избежать значительных материальных и репутационных потерь компании в будущем, в то время как затраты на защиту, окупятся многократно за счет предотвращения наступления неблагоприятных последствий в будущем и отклонения от кризисного сценария развития.

3.3. Анализ целесообразности использования систем обеспечения информационной безопасности

Как показывает практика, решение задачи обеспечения безопасности в сфере информационных технологий комплексное, требующее консолидации усилий органов власти, местного самоуправления, правоохранительных органов. В то же время, сами организации, должны более пристальное внимание уделять созданию собственных информационных ресурсов и их защите.

Государство же, в свою очередь, должно организовать максимально открытый доступ к имеющейся у него не секретной информации. В обязательном порядке должна быть разработана комплексная программа по использованию имеющихся у государства информационных ресурсов (возможно даже, на возмездной основе). Ведь потери в случае провала инвестиций значительно превышают затраты на получение предварительной информации.

По нашему мнению целесообразно скорректировать законодательство, регулирующее отношения между субъектами информационного рынка, поскольку ранняя диагностика криминальных схем и мошеннических афер – это не только пополнение бюджета за счет выплаченных налогов, но и одно из первоочередных направлений оздоровления национальной экономики.

Еще одним препятствием, стоящим на пути массового внедрения систем обеспечения безопасности в сфере информационных технологий в России является нехватка квалифицированных кадров, свободно ориентирующихся на отечественном и международном информационных рынках, владеющих новыми информационными технологиями, а также способных генерировать и развивать далее методологию информационно-аналитической деятельности [40].

При оценке целесообразности использования систем обеспечения информационной безопасности следует учитывать достаточно высокую степень использования ресурсов глобальной телекоммуникационной сети.

В то же время американские правительственные агентства давно сместили акцент с использования глобальной телекоммуникационной сети на более мощные и дорогостоящие ресурсы. По соображениям безопасности каждое разведывательное ведомство США в свое время создавало свои собственные системы сбора и распределения информации (АНБ - КРИТИКОМ, РУМО - ДЖЕЙВИКС, ДОДИИС, АМХС). С течением времени назрела и актуализировалась острая необходимость в их интеграции в специальную закрытую сеть, невидимую для большинства пользователей. Непосредственный доступ к секретной информации в этой секретной сети, получившей название Интерлинк, осуществляется через специальный протокол HTTPS при наличии специального браузера с набором

криптографических алгоритмов, поставляемого только для зарегистрированных пользователей Интерлинк [30,40].

Специфика и интегрированный характер сети Интерлинк наложили свой отпечаток на ее структуру: данная сеть имеет четыре уровня доступа к разведывательной информации по степени секретности: «…первый уровень составляет особо важная информация для принятия политических решений, которую готовит и распределяет только ЦРУ через специальную сеть ПОЛИСИНЕТ для Президента и Совета безопасности; второй - информация, имеющая гриф «совершенно секретно», к которой имеют доступ около 50 тыс. пользователей; третий - секретная информация, связанная с планированием военных операций, к которой имеют доступ 265 тыс. пользователей сети СИПРНЕТ; четвертый - несекретная информация из открытых источников (печать, Интернет, телевидение, радио), которая составляет свыше 95% всей добываемой разведкой информации…» [52].

Все это привело к тому, что на сегодняшний день одним из самых перспективных направлений работы службы безопасности многих организаций является аналитическая разведка, заключающаяся в поиске информации средствами Интернета, или как этот комплекс мероприятий обозначают многие специалисты в сфере информационной безопасности – компьютерную разведку. Ее сущность заключается в поиске и передаче информации из компьютерных систем и сетей «всемирной паутины» с последующей верификацией и аналитической обработкой.

Поскольку в Интернете содержатся огромные объемы сведений, представляющих оперативный интерес как для государственных, так и негосударственных спецслужб, большой интерес к методам аналитической разведки проявляют и те, и другие.. Поэтому во многих странах, в частности в правоохранительных органах России (МВД и ФСБ), США (ФБР) и Германии (ВКА), созданы специальные подразделения аналитической разведки в открытых телекоммуникационных сетях и организована подготовка сотрудников соответствующего профиля [30].

Сфера деятельности этих госструктур - легальная разведка в глобальной сети, организация каналов связи с агентурой, сбор материалов по оперативно значимым ситуациям, проведение в сети активных мероприятий, изучение личностных характеристик политиков, ученых, военных, а также сбор и анализ информации, представляющей интерес с точки зрения государственной безопасности.

Аналогичные подразделения функционируют в транснациональных корпорациях, которые все больше и больше превращаются в государства в государстве.

Помимо этого существуют самостоятельные исследовательские центры, специализирующиеся на сборе и анализе информации.

Целесообразность использования систем обеспечения информационной безопасности возрастает еще и в связи с растущим числом пользовате-

лей социальных сетей. Еще нет комплексных исследований данной проблемы, но уже ясно, что многие сотрудники осознанно или не осознанно разглашают конфиденциальные сведения именно в рамках общения в таких социальных сетях, как «Одноклассники», «В контакте» и т.п.

В большинстве стран мира сбор информации средствами Интернета давно уже превратился в весьма прибыльный бизнес. Причем сама информация носит разноплановый характер и касается как маркетинговых исследований, исследований стратегически важных отраслей экономики (только во Франции в настоящее время работает более десятка компаний, задачей которых является изучение документов, в том числе таблиц и рисунков, существующих в Интернет-пространстве), так и информационно-аналитические центры со схожими задачами, работающими на правительства и спецслужбы.

В качестве примера можно привести компанию MAAC, работающую в сфере лингвистической инженерии. Данная компания официально ориентирована на информационно-аналитическое обеспечение таких ключевых отраслей французской экономики, как транспорт, энергетика и аэрокосмическая промышленность [66], но по нашему предположению может поставлять полученные данные и спецслужбам. Подобная многопрофильность и широкое распространение методов и инструментария работы – еще один довод в пользу противодействия неправомерному доступу в сфере информационных технологий.

Также следует отметить, что для глобальных исследований в Интернете используются специальные «процессоры сбора данных» - часть программы, которая определяет, каким образом сама программа управляет и манипулирует данными, перехватывают любую запрашиваемую информацию, как только она появится в Интернете. Данный процессор использует программное обеспечение, получившее название «робот», извлекающее нужную информацию, с использованием целого арсенала средств статистического, лингвистического, а также семантического анализа.

Как пример можно отметить французский процессор «Taiga» (Traitement automatique d'information geopolitique d'actualite - «автоматическая обработка актуальной геополитической информации») - программный комплекс, разработанный для нужд французской разведки, где он длительное время эффективно использовался, после чего был передан для коммерческого использования с сохранением части первоначальных задач, например поиска по Интернету и извлечение ценной информации из баз данных о патентах, сообщений информационных агентств и публикаций о научных конференциях [61]. Обрабатывая материалы открытого доступа, имеющиеся в Интернете, программа статистического анализа составляет так называемые карты работы в различных отраслях науки, что позволяет аналитикам устанавливать наиболее перспективные научные разработки в областях, где конкуренция пока что сравнительно невелика. При этом дан-

ные количественного и качественного анализа результатов работы научных лабораторий позволяют оценить , хотя и косвенно состояние морально-психологического климата в исследовательских коллективах, что позволит выявить. перспективных «летунов», - исследователей, за сравнительно короткое время поменявших в качестве места работы ряд представляющих интерес научных центров, и как следствие знакомых не понаслышке с методами и результатами их работ.

Следует сказать и о другой работе французов, которая была разработана компанией «Acetic» совместно с учеными Парижского университета для проведения семантического анализа крупных информационных массивов. Речь идет о пакете прикладных программ «Tropes», в котором отбор требуемой информации происходит в соответствии с ключевыми словами и понятиями, связанными по смыслу (к примеру, название типа самолета «Мираж» соотносится со словами «самолет», «истребитель», а сочетание слов «госсекретарь США» автоматически ассоциируется со словами «министр», «политик»).

Названное программное обеспечение обладает высокой производительностью и позволяет одновременно анализировать два текстовых информационных массива объемом в несколько десятков книжных томов. Также вышеуказанный «Tropes» дает возможность создавать необходимые для информационные рабочие сценарии, на основе которых осуществляется не только автоматический поиск, но и группировка требуемых массивов данных по определенным параметрам и критериям [55].

То, что подобные разработки попадают в руки гражданских специалистов, однозначно свидетельствует о том, что спецслужбы на сегодняшний день располагают более мощными техническими средствами. К примеру, «Noemic», пришедший на смену «Taiga», помимо сканирования автоматически осуществляет «объединение источников», обрабатывая полученную информацию со скоростью 1 млрд. знаков в секунду независимо от массива поиска и того, представляется ли она в виде готовой структурированной базы данных или передается по каналам электронных СМИ на любом языке в виде целостного текста.

Этот семантический процессор сбора данных способен также обрабатывать информацию по отдельным критериям, совокупностям идей, концепциям и метафорам. Если перед данным процессором будет стоять задача по выявлению, скажем всех случаев установления контактов между российскими и американскими фирмами, действующими в области микроэлектроники, за последние пять лет, то для ее выполнения ему хватит всего нескольких часов. [59]

Американский аналог этих программных комплексов, «Topic», также является результатом длительных исследовательских работ, финансировавшихся в свое время ЦРУ. Данный аналог в настоящее время использу-

ется в коммерческих целях мировым лидером по сбору документальных данных калифорнийской фирмой «Verity».

Конкуренты данной фирмы также не уступают своих позиций: например, другая американская фирма «Intelligent Search Solutions» выпустила на рынок пакет программного обеспечения «InfoTracer», предназначенный для сбора разведывательной информации экономического характера в сети Интернет. Поиск в данной системе идет по ключевым словам и фразам, после чего автоматически составляются отчеты, в которых результируются данные по запросу пользователя и составляется отчет, к примеру, о фондовых операциях конкретной компании и ее партнеров, их ценовой, кадровой политике и т.д. [44].

На примере использования указанных технологий и устройств можно сделать вывод о том, что в настоящее время именно быстрота поиска и правильный анализ полученной информации, а не доступ к ней определяют победителя в конкурентной борьбе.

На сегодняшнем витке развития информационных технологий экономическую разведку можно вести без компьютерных взломов, просто обрабатывая по специальному алгоритму огромные массивы информации, доступные каждому пользователю Интернета.

По оценкам специалистов, в настоящее время только в США насчитывается около 150 фирм, которые специализируются на анализе данных, полученных из Интернета. Причем количество их постоянно растет [30].

Все приведенные выше факты свидетельствуют о том, что интерес к получению конфиденциальной информации только возрастает (отсюда и рост организаций, специализирующихся на получении конфиденциальных данных). Наряду с возрастанием интереса совершенствуется инструментарий для получения информации, возрастает степень использования утечек информации, в том числе инсайдерских, в конкурентной борьбе.

Приведенный ниже пример наглядно иллюстрирует один из типичных на сегодняшний день алгоритмов утечки информации в условиях острой конкурентной борьбы.

26 июня 2003 года два крупнейших оператора сотовой связи России «Вымпелком» и «МобильныеТелеСистемы» (МТС) в один голос объявили о практически одной и той же маркетинговой инициативе.

Если «Вымпелком» дал возможность своим абонентам «Би+» увеличить срок действия платежей по препейд-картам до десяти и более лет, то МТС ввели тарифный план «Супер Джинс», по которому платежи его подписчиков стали действовать бессрочно.

«Вымпелком» и МТС и ранее заимствовали друг у друга удачные маркетинговые ходы: посекундную тарификацию, безлимитные пакеты услуг. Копировали популярные тарифные планы. Но здесь получилось так, что операторы выступили с новой и, казалось бы, оригинальной идеей день в день.

«Вымпелком» с целью проверки версии об утечке конфиденциальной информации инициировал внутреннее расследование. В МТС принципиально не стали ничего делать.

Расследование, проведенное службой безопасности «Вымпелкома» длилось недолго, уже к исходу третьего дня виновник утечки был установлен. Им оказался один из сотрудников компании, поделившийся этой информацией со своим другом, который в свою очередь решил обсудить планы «Вымпелкома» в сети.

Так что данные о грядущих нововведениях для абонентов «Би+» в путевой книге сайта www.cells.ru появились уже 19 июня 2003 года [102].

Нетрудно представить, чего стоили разглашение оригинальной идеи и утечка информации о ней в период острой конкурентной борьбы между двумя крупнейшими операторами сотовой связи России: утрата конкурентного преимущества, переход инициативы к конкурентам, снижение прибыли и т.д.

Однако всего этого можно было бы избежать, если бы в организации «Вымпелком» существовала и эффективно работала система информационной безопасности, подобная той, которая использовалась другой организацией - ОАО «ГидроОГК».

Динамичное развитие и постоянный рост рынка энергоресурсов поставили перед ОАО «ГидроОГК» вопросы ИТ-безопасности на первое место. Нельзя сказать, что до этого компания не уделяла достаточного внимания данным вопросам, - в ней уже существовала система защиты от внешних угроз, которая впрочем не решала проблем инсайдеров и утечек, в то время как характеристики внутренней среды организации свидетельствовали о том, что она критически уязвима именно с точки зрения внутренних атак.

Потенциально более 10 тыс. компьютеризированных рабочих мест, сотни серверов и различных каналов связи находились в распоряжении инсайдеров и в любой момент могли стать источником утечки конфиденциальной информации.

Внедренная на ОАО «ГидроОГК» система защиты от инсайдеров и утечек удовлетворяет следующим требованиям [34]:

■ Создаваемая система информационной безопасности должна эффективно защищать как от внутренних (нарушение целостности и непрерывности бизнес-процессов, утечка, искажение, уничтожение конфиденциальной информации; со стороны инсайдеров), так и от внешних угроз (со стороны конкурентов, преступных сообществ, структур, специализирующихся на промышленном шпионаже и сборе конфиденциальной информации, рейдеров и т.д.).

■ Внедряемое решение в целях защиты от внутренних угроз должно иметь комплексный характер и предусмотреть защиту всех каналов утечки конфиденциальной информации из организации (социальные сети, элек-

тронную почту и Интернет, принтеры и сменные накопители на рабочих станциях, беспроводные сети и мобильные устройства).

■ Система внутренней информационной безопасности не должна затруднять деятельность компании, существенно снижать скорость документооборота и принятия управленческих решений, то есть должна быть максимально прозрачной.

■ Система защиты от инсайдеров и утечек должна быть полностью контролируемой и способной конструктивно интегрироваться в комплексную корпоративную систему информационной безопасность. При этом корпоративный процесс управления информационной безопасностью должен соответствовать европейскому стандарту ISO 17799.

Внедрению системы защиты от инсайдеров и утечек предшествовала кропотливая аналитическая работа: рассматривались рынок систем защиты от инсайдеров и утечек, техническая функциональность продуктов, спектр сопроводительные услуг, оказываемых различными поставщиками, то есть детальнейшим образом анализировались показатели экономической целесообразности. Таким образом, после детального анализа различных вариантов экспертами выбор был сделан в пользу российской компании Info Watch. – поставщика комплексного решения Info Watch Enterprise Solution, которое анализирует весь спектр внутренних угроз (утечка, искажение, уничтожение, саботаж и т. д.) и покрывает все используемые в компании коммуникационные каналы.

Наиболее важными аргументами в пользу Info Watch Enterprise Solution были следующие [34]:

■ Компания Info Watch имеет опыт реализации проектов в крупнейших корпорациях и госструктурах, специализируется именно на защите от утечек и инсайдеров.

■ Решение Info Watch Enterprise Solution покрывает каналы электронной почты и Интернета, всевозможные порты рабочих станций (USB, COM, LPT, FireWire, IrDA, Bluetooth и т. д.), защищает от утечки через принтеры и т. д.

■ В состав комплексного решения входит модуль Info Watch Storage, собирающий и архивирующий всю корпоративную корреспонденцию и весь сетевой трафик. Данный модуль интегрирован в систему защиты от утечек и не имеет конкурентных аналогов. Кроме того, данное решение в отличие от других обладает возможностью произведения развернутого ретроспективного анализа.

Помимо прочего активной комплекс способен вести текущий мониторинг манипуляций с информацией: абсолютно все операции служащих с конфиденциальной информацией протоколируются и складываются вначале в журнал событий, а потом в базу данных.

С другой стороны, используемое в решении Info Watch разделение ролей позволяет набежать проблемы суперпользователя и минимизировать

проблему человеческого фактора и злонамеренных действий инсайдеров, обладающих широкими должностными полномочиями.

В то же время, комплексное решение InfoWatch Enterprise Solution является полностью централизованным и управляемым, это значительно снижает затраты на администрирование решения.

К перечисленным достоинствам следует добавить также и то, что компания InfoWatch поставляет широкий спектр сопроводительных и консалтинговых услуг как в сфере обеспечения соответствия нормативным актам, так и в области построения эффективной системы защиты от инсайдеров и утечек, а также инжиниринговые услуги.

Все вышеперечисленные факторы склонили руководство ОАО «ГидроОГК» к выбору данного продукта и поставщика как наиболее экономически целесообразного [34].

Перед компанией InfoWatch стояла задача разработки и внедрения системы информационной безопасности ОАО «ГидроОГК» — крупной территориально распределенной компании с большим набором разнообразных информационных систем, в том числе производственных.

На момент начала работ процессы управления информационной безопасностью заказчика находились на начальном уровне модели зрелости в соответствии со стандартом COBIT.

Данный уровень применительно к конкретной компании характеризовался тем, что в компании уже имелись документально зафиксированные свидетельства осознания руководством и персоналом того факта, что в ней существуют проблемы обеспечения информационной безопасности. Также были вскрыты текущие проблемы: используемые процессы управления не стандартизованы, применялись эпизодически и бессистемно, в то время как общий подход к управлению информационной безопасностью не был выработан.

Ниже представлен график выполнения работ и соответствии с требованиями и пожеланиями заказчика, который представлен (см. табл. 3.8) [54], который основан на детальном и скрупулезном анализе сферы информационной безопасности в ОАО «ГидроОГК».

Таблица 3.8. План работ компании InfoWatch по созданию в ОАО «ГидроОГК» системы защиты конфиденциальной информации от утечек и инсайдеров

№ этапа	Описание этапа	Сроки выполнения
1	Производится аудит ИТ-систем заказчика на соответствие стандарту по управлению ИТ-безопасностью ISO 17799. В результате аудита эксперты InfoWatch получают общую картину состояния ИТ-систем, степень влияния их на бизнес-процессы организации, состоянии процессов управления ИТ-безопасностью	1,5-2 месяца
2	Выработка общих принципов и подходов к обеспечению ИТ-безопасности и закрепление их в специальном документе «Политика ИТ-безопасности». Созданная Политика должна учитывать производственную специфику заказчика и результаты аудита. Жизненный цикл Политики должен включать в себя механизмы принятия решений и постоянной актуализации положений документа. Кроме того, Политика должна охватывать все без исключения подразделения заказчика	3-4 месяца
3	Разработка Плана защиты — документа, необходимого для внедрения Политики ИТ-безопасности. В Плане зашиты поэтапно, придерживаясь принципа «сверху — вниз», должны быть описаны шаги по интеграции Политики в управленческие и бизнес-процессы заказчика. Придерживаясь Плана защиты и в тесной кооперации с соответствующими службами заказчика, разработать такие документы, как Положение о конфиденциальности информации, Политика реагирования на инциденты ИТ-безопасности, Политика работы с мобильными компьютерами, и еще более 10 документов	4-5 месяцев
4	При необходимости приобретение нескольких новых программных продуктов, отвечающих отраслевым требованиям заказчика и необходимых для внедрения	4-5 месяцев

В результате реализации плана работ должна быть построена система защиты от внутренних угроз и система управления ИТ-безопасностью, удовлетворяющая требованиям нормативных актов [54].

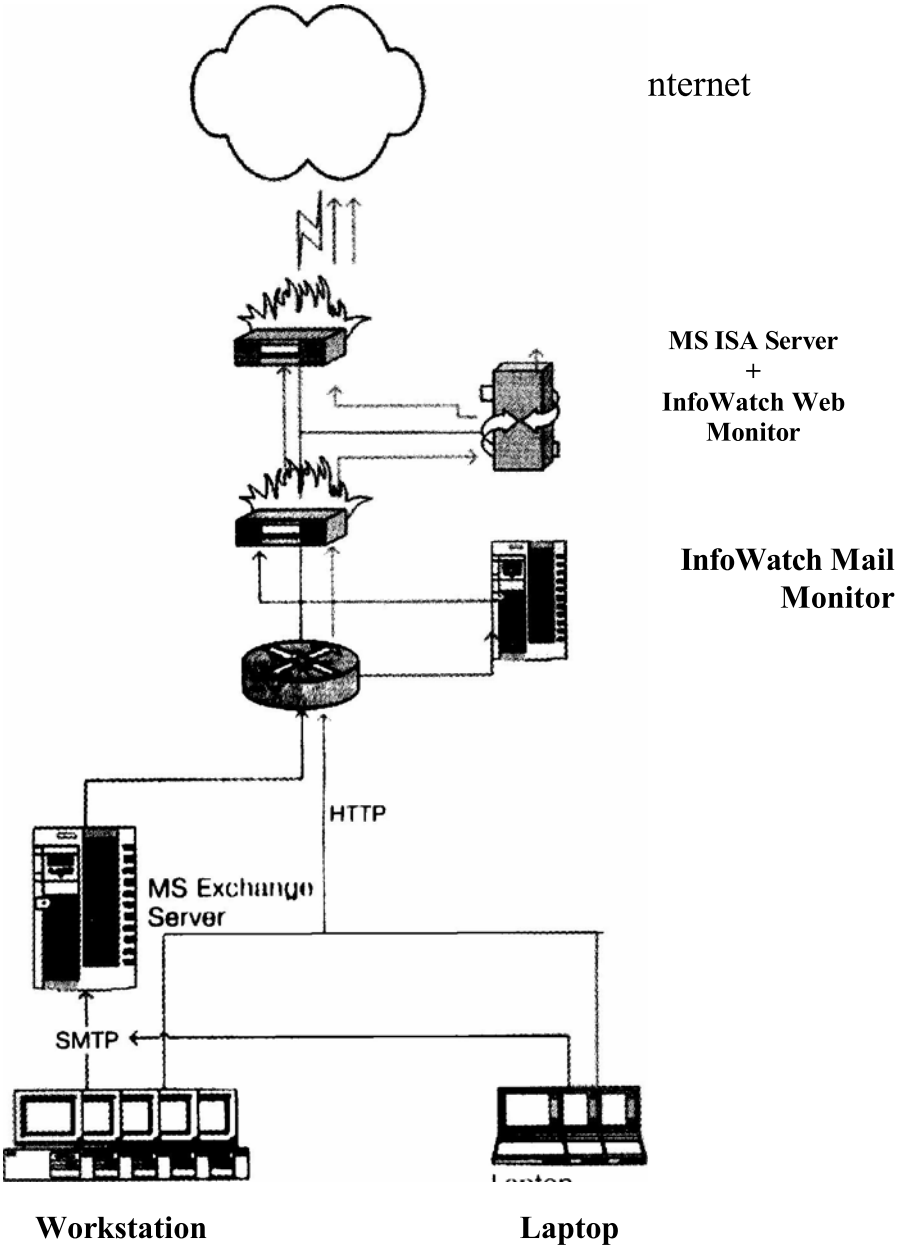

Рисунок 3.9. Система защиты от утечек и инсайдеров
в ОАО «ГидроОГК»

Приведенная на рис. 3.9. система управления ИБ обеспечивает мониторинг и оценку соответствия используемых в организации процессов; при выявлении низкой эффективности реализуемых процессов управления ИБ

обеспечивается их оптимизация; процессы управления находятся в стадии непрерывного совершенствования, используются средства автоматизации управления ИБ.

Помимо прочего, данная система безопасности позволила выявить целый ряд неправомерных действий инсайдеров, нарушающих политику безопасности организации. В то же время практически все неправомерные действия были в режиме реального времени блокированы с последующей отправкой соответствующих уведомлений. Таким образом, использование комплексного решения InfoWatch позволило минимизировать самый опасный риск – нарушение конфиденциальности информации, а также искажение финансовой отчетности, саботаж, утечку информации через социальные сети и другие инсайдерские угрозы, одним словом доказала свою экономическую целесообразность и эффективность [34].

3.4. Организация информационно-аналитической работы по предупреждению утечки информации

В современных условиях значительно возросла роль информационно-аналитической деятельности при управлении организацией. Руководители достаточно остро нуждаются в аналитических моделях, позволяющих оценить текущее состояние, спрогнозировать перспективы развития и последствия принятых решений. Аналитические подразделения, на сегодняшнем этапе, являются одним из эффективных элементов системы поддержки принятия решения.

Как уже указывалось ранее, организационная структура службы безопасности должна включать в свой состав подразделения информационно-разведывательной и аналитической деятельности. При этом необходимо указать на то, что функции рассматриваемых подразделений службы безопасности включают в себя две составляющие: добывание информации и ее аналитическая обработка. Следует обратить внимание на неукоснительное соблюдение действующего законодательства в процессе добывания информации независимо от способа ее получения (проведение оперативно-розыскных мероприятий, изучение открытых источников информации и т.д.).

К числу наиболее значимых процессов информационно-аналитической работы целесообразно отнести следующие:

1. Четкое формулирование целей и задач аналитического исследования;

2. Эффективный и адаптивный сбор информации в условиях постоянно меняющейся ситуации;

3. Анализ и оценка полученной информации в свете сущности наблюдаемых процессов.

4. Определения объекта исследования, построение модели исследования и проверка ее адекватности.

5. Доведение результатов аналитической работы до лица принимающего решение.

Остановимся более подробно на некоторых понятиях определяющих информационно-разведывательную и аналитическую деятельность. В первую очередь обратимся к информационной составляющей и некоторым предъявляемым требованиям.

Информация - сведения (сообщения, данные) независимо от формы их представления. [5]

Информационная работа — деятельность по обеспечению должностных лиц сведениями, необходимыми для решения возложенных на них задач [62].

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов [5].

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств [5].

Процесс информационной работы — это последовательная совокупность операций (регистрация, передача, накопление, хранение, обработка, выдача информации), позволяющая быстро найти в полном объеме нужные сведения, затребованные конкретными потребителями [62].

Накопление информации — это результат интеграции, систематизации, уточнения и учета информации в определенных системах [62].

Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель [5].

После определения информационной составляющей деятельности подразделений занимающихся информационно-разведывательной и аналитической работой обратимся к определениям разведывательной деятельности.

По аналогии с Федеральным законом от 10 января 1996 г. № 5-ФЗ «О внешней разведке» [13], а также в соответствии с комментарием [45] к указанному закону можно дать определение разведывательной деятельности.

Разведывательная деятельность подразделений службы безопасности организации, осуществляющих информационно-разведывательную и аналитическую деятельность, является комплексом мероприятий, проводимых с целью оценки реальных и потенциальных возможностей, действий, планов и намерений организаций и лиц. Она заключается в сборе и обобщении любой информации, которую можно добыть[45].

Правовой базой разведывательной деятельности является совокупность законодательных и иных нормативных актов, регламентирующих отношения, возникающие в сфере этой деятельности.

Одним из основных способов получения информации посредством разведывательной деятельности является оперативно-розыскная деятельность.

Оперативно - розыскная деятельность - вид деятельности, осуществляемой гласно и негласно оперативными подразделениями государственных органов, уполномоченных на то настоящим Федеральным законом (далее - органы, осуществляющие оперативно-розыскную деятельность), в пределах их полномочий посредством проведения оперативно-розыскных мероприятий в целях защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств [8].

Следующим этапом является исследование полученных данных, которое должно начинаться с определенного предварительного отбора и документирования информации, где немаловажную роль играет ее качество и достоверность.

Качество информации — это степень развитости свойств информации, определяющая ее практическую пригодность для исследования. Качество информации зависит от следующих характеристик:

- достоверность;
- относимость;
- своевременность;
- полнота;
- важность [62].

Отбор информации — это результат просмотра материалов и документов, уточнения, дополнения и формализации информации [62].

Способы отбора и рамки информационного поиска определяются с учетом:

- структуры и содержания изучаемой проблемы с выделением конкретных задач, подлежащих анализу;
- наличия смежных областей и проблем, в которых может находиться нужная информация;
- глубины ретроспективного поиска;
- видов документальных источников, необходимых для исследования [62].

Полученные данные, обычно, подвергаются аналитической обработке, на основании которой выносятся определенные рекомендации или строится прогноз. Непосредственно аналитическая деятельность требует творческий подход и направлена на обработку информации с целью подготовки, на ее основе, принятия решения руководителем или лицом принимающим решение. Остановимся на некоторых понятиях используемых в процессе проведения информационно-аналитической работы.

Аналитическая работа — составная часть творческой деятельности. Она предназначена для оценки информации и подготовки принятия решений. Составляет основное содержание повседневной работы каждого руководителя и работника [62].

Аналитическая работа, как процесс познания объективной реальности, осуществляется по законам диалектики, формальной логики, с применением общенаучных методов исследования.

Содержание аналитической работы — приведение разрозненных сведений в логически обоснованную систему зависимостей (пространственно-временных, причинно-следственных и иных), позволяющих дать правильную оценку, как всей совокупности фактов, так и каждому из них в отдельности [62].

Исследования в повседневной деятельности проводятся по мере накопления проблем. Исследуются: актуальность, важность, объективность, перспективность. Предметом исследования становятся события и процессы, развитие которых может повлиять на выбор форм и методов деятельности на определенном участке и в определенное время.

Формы аналитической работы — организационные особенности осуществления аналитической работы, обусловленные целями, средствами и результатами ее проведения, образующие систему аналитического слежения за состоянием и развитием обстановки [62].

Средства аналитической работы — это законы и методы мыслительной деятельности, а также иные технические средства, на основе и с помощью которых осуществляется обработка фактических данных с более высоким качеством, позволяющим извлечь из нее все, что она может дать [62].

Процесс аналитической работы — совокупность мыслительных операций, осуществляемых в определенной последовательности с использованием аналитических средств, приводящих к достижению целей и задач исследования [62].

Наибольшая эффективность подразделений занимающихся информационно-разведывательной и аналитической деятельностью достигается при включении их в состав службы безопасности организации. Подобное включение объясняется тем, что основным потребителем аналитически обработанных данных является сама служба безопасности как подразделение, наиболее нуждающееся в аналитически обработанной информации, работающее на опережение и прогнозирование событий. Кроме того, в ходе аналитической работы очень часто используются конфиденциальные сведения, что также подтверждает рациональность размещения подразделений занимающихся информационно-разведывательной и аналитической деятельности в службе безопасности [99].

Исходя из сказанного, можно сделать вывод о том, что основной задачей подразделений информационно-разведывательной и аналитической деятельности становится информационно-аналитическое обеспечение принятия решений по вопросам основной деятельности организации. Руководитель практически любого подразделения может заказать аналитический отчет по интересующему вопросу для принятия более рационального и взвешенного решения.

Отсюда следует необходимость обеспечения информационной безопасности информационных массивов, составляющих ценный информационный ресурс организации, включающих в свой состав аналитически обработанные данные. В то же самое время, защита информации внутри подразделений информационно-разведывательной и аналитической деятельности представляет собой крайне сложную задачу, так как специфика аналитической работы в ряде случаев вступает в прямое противоречие с нор-

мами защиты информации. Подобные нарушения часто связаны с тем, что соблюдение такого важного принципа, как дробление информации в работе практически невозможно, так как это тормозит работу всего информационно-аналитического подразделения, где сотрудники должны иметь представление обо всей картине событий. Соблюдение требований по ограничению доступа к информации в ходе работы может привести к ложным выводам и заключениям.

Из сказанного можно сделать вывод о том, что информационно-аналитическая деятельность представляет собой системное получение, анализ и накопление информации с элементами прогнозирования по вопросам, относящимся к безопасности, и подготовка рекомендаций руководству о правомерной защите от противоправных посягательств. Аналитическая работа проводится не только с целью предотвратить утрату собственной информации, но и с целью получения информации о других участниках информационных процессов. Аналитическая обработка информации позволяет получать по различным оценкам от 80 до 90% необходимой информации при использовании только открытых источников [57].

При выполнении информационно-аналитической работы необходимо решить следующие задачи [57]:

- обеспечить своевременное поступление надежной и всесторонней информации по интересующим вопросам;
- описать сценарии действий конкурентов, которые могут затрагивать текущие интересы;
- осуществлять постоянный мониторинг событий во внешней среде, которые могут иметь значение для интересов организации;
- обеспечить безопасность собственных информационных ресурсов;
- обеспечить эффективность и исключить дублирование при сборе, анализе и распространении информации.

Таким образом, деятельность подразделений информационно-разведывательной и аналитической деятельности должна быть направлена на прогнозирование ситуаций, а также формирование соответствующих информационных комплексов, необходимых для эффективного принятия оптимальных решений.

К основным направлениям аналитической работы можно отнести анализ объекта защиты, угроз, каналов неправомерного доступа к информации, вопросов комплексной безопасности, нарушений режима конфиденциальности, а также анализ подозрений утраты конфиденциальной информации. Направления информационно-аналитической работы могут быть постоянными, периодическими и разовыми (рис.3.10).

Рис. 3.10. Направления аналитической работы

Постоянные направления информационно-аналитической работы являются наиболее важными. Это связано с тем, что сбор информации и последующее ее исследование, по поставленной проблеме, не допускают прерывания даже на небольшие промежутки времени. В противном случае результат аналитических выводов может быть ошибочным, так как существует возможность упустить достаточно важные детали.

Периодические и разовые направления информационно-аналитической работы напрямую зависят от постоянных направлений. Промежутки времени, через которые проводятся исследования в области периодических направлений, всецело зависят от результатов анализа по постоянным направлениям.

Периодические направления информационно-аналитической работы проводятся через определенные промежутки времени с целью контроля эффективности и возможности внесения улучшений в действующую в организации систему обеспечения информационной безопасности. К такому виду направлений, прежде всего, относится анализ степени безопасности. Очевидно, что постоянная и каждодневная аналитическая работа по данному направлению не имеет смысла. Вполне достаточно проводить анализ через определенные, специально установленные промежутки времени. Это направление работы находится в прямой зависимости от анализа состава угроз – постоянного направления аналитической деятельности.

Разовые направления информационно-аналитических исследований также являются очень важными в силу того факта, что бывают, вызваны чрезвычайными обстоятельствами, происшествиями, неожиданно появившимися проблемами и требуют проведения исследований в кратчайшие сроки. Кроме того, разовые задачи могут появляться в процессе проведения постоянных исследований по заданной проблематике. Типичным примером разового направления аналитической работы анализ нарушения режима конфиденциальности.

Каждая организация ведет индивидуальные направления информационно-аналитической работы и самостоятельно решает, следует ли разрабатывать их постоянно, периодически или только по мере надобности. Направления аналитической работы могут быть различными, но логика взаимодействия и система связей между направлениями исследований должны сохраняться. Принципиально важными являются ключевые направления, работа по которым ведется постоянно.

Обнаружение каналов и способов совершения неправомерного доступа к конфиденциальной информации организации входит в число постоянных направлений аналитической работы и в общем виде включает в себя [57]:

- анализ источников конфиденциальной информации;
- анализ каналов объективного распространения информации;
- аналитическую работу с источником угрозы информации.

Рассмотрим данные направления более подробно:

Аналитическое исследование источников конфиденциальной информации предусматривает:

• выявление и классификацию существующих криминальных структур и отдельных преступных элементов;

• выявление и классификацию максимально возможного числа источников конфиденциальной информации организации;

• выявление, классификацию и ведение перечня реального состава циркулирующей в организации конфиденциальной информации;

• изучение данных учета осведомленности сотрудников о циркулирующей конфиденциальной информации;

• ведение и анализ полноты перечня существующих защитных мер.

Выполнение всех перечисленных составляющих позволяет эффективно проводить работу с возможными каналами инсайдерских угроз и осуществлять своевременное противодействие.

Изучение каналов объективного распространения информации в целом схоже с анализом источников конфиденциальной информации и включает в себя:

• выявление и классификацию существующих каналов передачи и распространения конфиденциальной информации;

• выявление, классификацию и ведение перечня сотрудников допущенных к передаче конфиденциальной информации по каналам связи и осведомленных о принципах их функционирования и построения;

• ведение и анализ полноты перечня существующих защитных мер.

Информационно-аналитическая работа с источником угрозы конфиденциальной информации предусматривает:

• выявление и классификацию максимального состава источников угрозы конфиденциальной информации по всем направлениям;

• анализ риска возникновения угрозы;

• разработку превентивных мероприятий по локализации и ликвидации объективных угроз;

• разработку мероприятий по выявлению, противодействию и пресечению попыток совершения неправомерного доступа к конфиденциальной информации.

Анализ возникновения угроз рекомендуют вести по такой схеме: вначале нужно выяснить, кто является потенциальным злоумышленником,

в чем причина подобных действий, какие цели может преследовать злоумышленник. После изучения проблемы, исходя из имеющихся в распоряжении злоумышленника средств и возможностей, значительно упрощается процесс прогнозирования, способа или метода достижения цели.

Анализ угроз является одним из самых важных разделов информационно-аналитической работы и представляет собой ответ на вопрос, от чего или кого следует защищать определенные ранее объекты защиты. Источники угрозы конфиденциальной информации – объективные (естественные) и субъективные (искусственные) события, явления, факторы, действия и обстоятельства, содержащие опасность для ценной информации.

Источники угрозы могут быть внешними и внутренними. Внешние источники находятся вне организации и представлены чрезвычайными событиями, а также организационными структурами и физическими лицами, проявляющими определенный интерес. Внутренние источники угрозы связаны с фатальными событиями в здании организации, а также с персоналом. Однако наличие источника угрозы само по себе не является угрозой. Угроза реализуется в действиях [57].

Таким образом, наличие, ведение и результаты постоянной информационно-аналитической работы определяют структуру и содержание системы защиты информации и направления её совершенствования. При отсутствии серьезной и постоянной информационно-аналитической работы становится практически невозможным выявление и контроль каналов неправомерного доступа к ценной, конфиденциальной информации.

Порядок проведения информационно-аналитических исследований по возникшей проблематике достаточно трудоемкий процесс и его целесообразно разделить на несколько этапов.

1. Общее знакомство с проблемой и уяснение поставленной задачи.
2. Сбор информации по необходимой проблематике.
3. Интерпретация полученной информации.
4. Выделение посторонней информации.
5. Оценка информации и построение рабочей гипотезы.
6. Определение потребности в дополнительной (уточняющей) информации.
7. Подготовка отчетов и рекомендаций.

Выделяют следующие этапы выполнения информационно-аналитической работы (рис.3.11):

Этап 1. Общее знакомство с проблемой включает в себя не только ознакомление с поставленной проблемой, но и изучение логично возникающих смежных вопросов. При этом целесообразно изучить и проанализировать необходимые термины и определения, что необходимо для более точного уяснения поставленной задачи. В заключение данного этапа составляется общий план работы, в котором определяются исполнители каждого пункта, необходимые источники и способы получения информации.

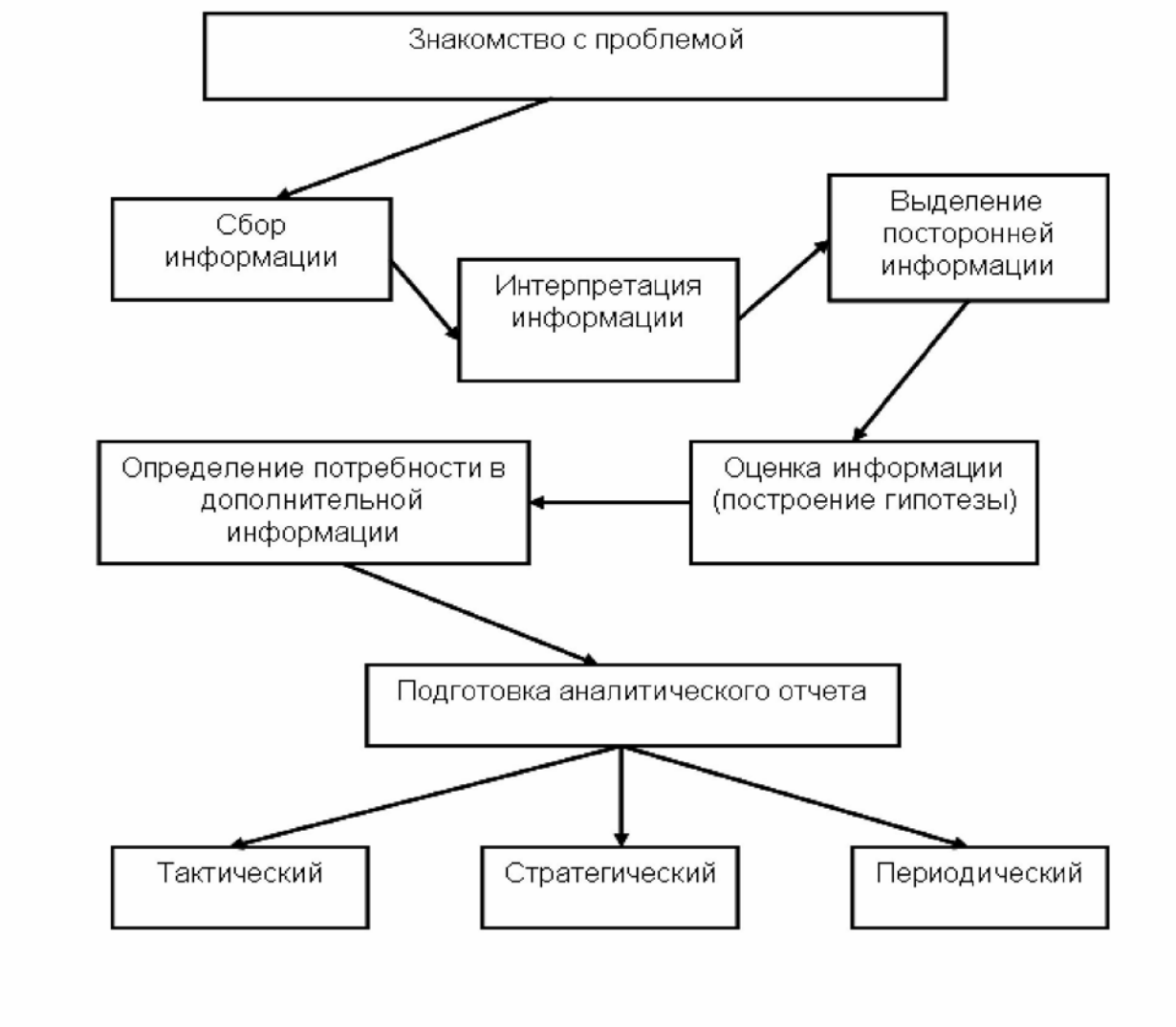

Рисунок 3.11. Этапы выполнения
информационно-аналитической работы

Этап 2. На этапе сбора информации по необходимой проблематике выполняются различные мероприятия по добыванию данных, но не в нарушение действующего законодательства. Следует обратить внимание на то, что информация собирается из различных источников, в том числе открытых. Основу для проведения мероприятий по сбору информации может дать, в части касающейся, Федеральный закон «Об оперативно-розыскной деятельности». Согласно ст. 6 целесообразно использовать следующие мероприятия [8]:

1. Опрос.
2. Наведение справок.
3. Сбор образцов для сравнительного исследования.
4. Исследование предметов и открытых документов.
5. Наблюдение.
6. Отождествление личности.

Порядок проведения указанных мероприятий достаточно полно рассмотрен в действующем законодательстве, а также в некоторых изданных источниках. Остановимся более подробно на традиционном, достаточно трудоемком и наиболее используемом канале получения информации, которым являются средства массовой информации и открытая печать.

Повседневная деятельность профессионального журналиста во многом похожа на работу сотрудника спецслужб и это, как показывает практика необходимо максимально использовать. На мнении журналиста постоянно пишущего об однотипных проблемах, в ряде случаев, можно основываться как на мнении эксперта в соответствующей области. Кроме того, средства массовой информации позволяют получить представление о существующей ситуации на достаточно понятном языке, пусть даже основанной на слухах и ощущениях, что, в свою очередь, позволяет составить из фактов и цифр целостную картину [52].

Служба безопасности организации может получать сведения по очень широкому кругу вопросов из средств массовой информации в случае грамотной организации поиска.

Материалы средств массовой информации позволяют сопоставлять, уточнять и снабжать новыми подробностями уже полученные данные, а также давать новые направления для текущей информационно-поисковой работы [52]. Следует указать на то, что к этому времени целесообразно провести первый этап и ознакомиться с проблемой и уяснить поставленную задачу. В противном случае есть вероятность потратить время и ресурсы на изучение избыточной информации.

Представляется очевидным, что преобразование опосредованной информации в проблемно-ориентированный информационный массив требует целенаправленного подхода по объективному восприятию поступающих информационных потоков. Для достижения поставленных целей совсем необязательно изучать всю подряд печатную продукцию. Вполне достаточно правильно подобрать источники информации, грамотно организовать классификацию, сортировку и хранение отобранной информации на основе принципа «ключевых слов» [52]. Все это связано с тем, что во многих источниках часто дублируется или просто перепечатывается одна и та же информация. Исключения составляют лишь некоторые издания, проводящие некоторые аналитические исследования по проблеме статьи. Так, например, специализированные организации для создания ежедневной сводки объемом в одну страницу с оценочным суждением по одной проблеме обрабатывают информационный массив объемом примерно в 7 млн слов. При этом необходимо из всех проблем, рассматриваемых в публикации, выбрать только отвечающие интересам вашего исследования.

Для оценки качества и анализа пригодности практически для работы любого периодического издания необходимо взять несколько его номеров за определенный период и на основе этих содержания этих номеров соста-

вить список публикуемых материалов. Результатом подобной работы станет выборка именно того сегмента печатных изданий, который наиболее полно совпадает с информационными потребностями исследователя [52].

Необходимо указать, что возможно использовать как собственные, так и сторонние возможности по обработке средств массовой информации. Это связано с тем, что в ряде случаев более целесообразно и менее затратно дать возможность сторонней организации по обработке средств массовой информации, а затем купить аналитический отчет, чем проводить самим.

Более подробно на аналитической обработке средств массовой информации остановимся в следующих параграфах.

Этап 3. Интерпретация полученной информации. Под интерпретацией подразумевается выявление истинного значения той или иной информации. Язык описания информации зачастую может допускать неоднозначность её понимания, поэтому в каждом конкретном случае необходимо выявить истинный смысл поступившей информации. На этом этапе аналитики сталкиваются с проблемой выделения не относящейся к делу информации.

Этап 4. Выделение посторонней информации составляет следующий этап информационно-аналитической работы. Этот процесс является одним из самых сложных и ответственных моментов во всей процедуре. Избыток информации, так же как и ее недостаток, представляет собой серьезную проблему и затрудняет проведение аналитической работы. Так, выделение нескольких ключевых моментов анализа гораздо более эффективно, чем разбрасывание между многими разрозненными данными. Кроме того, на этом этапе существует опасность отбросить важную информацию. это может произойти в случае неправильной интерпретации сведений на предыдущем этапе.

Этап 5. Оценка информации и построение рабочей гипотезы.

Под оценкой понимается метод ранжирования источников информации, самой информации и способов ее получения. Используют такую систему оценок информации, при которой специалист-аналитик может выразить свою точку зрения относительно надежности и достоверности полученных сведений. Так, оценка источника информации осуществляется следующими понятиями: надежный источник, не всегда надежный источник или ненадежный источник.

На этапе оценки необходимо установить, насколько информация может соответствовать истине. При этом нужно учитывать, что можно получить не соответствующую истине информацию следующих типов:

- дезинформацию, доведенную до сведения источника;
- преднамеренно или непреднамеренно искаженную источником.

Для своевременного выявления искаженной информации, а также для успешной борьбы с дезинформацией необходимо различать факты и

мнения, учитывать субъективные характеристики источника и его предполагаемое отношение к выдаваемому сообщению. В качестве страховочных мер всегда нужно иметь дублирующие источники, информации и стараться исключать все лишние промежуточные звенья передачи информации.

После оценки информации обычно приступают к построению рабочей гипотезы. Данный процесс обычно связан с конкретными вопросами, отвечая на которые можно проверить сами гипотезы. По мере изучения данного этапа мы открываем все новые полезные стороны рабочей гипотезы. Первым шагом является составление списка сведений, приготовленных для анализа. Затем необходимо выделить в анализируемых данных ключевые моменты и отделить их от менее важных. Полученные сведения должны быть четко классифицированы по степени достоверности источника, самих сведений и способа их получения.

Далее необходимо выявить все возможные гипотезы, которые могут объяснять ключевые события, и, расположив их по степени вероятности, поочередно проверять на стыкуемость со всеми данными. Если обнаружено значительное расхождение какой-либо предварительной гипотезы с полученными сведениями, то следует переходить к следующей гипотезе. Таким образом, выбираются наиболее вероятные предположения. На этом этапе возникает проблема противоречия в анализируемых сведениях. Для ее преодоления необходимо сравнить оценки информации и источника, даты получения спорных сведений. Решающее же значение имеет интуиция, знания и опыт аналитика, проводящего анализ.

Гипотезу можно рассматривать как положение. Обычно отмечают три полезные стороны гипотезы [62]:

- во-первых, тем самым облегчается уяснение проблемы.
- во-вторых, научное положение является основой для уяснения отдельных фактов или явлений, так как вскрывает существующую между ними связь;
- в-третьих, приемлемое научное положение всегда содержит некоторые моменты, выходящие за его рамки и образующие разумное и плодотворное основание для предвидения новых фактов и явлений.

Этап 6. Следующим этапом является определение потребности в дополнительной (уточняющей) информации, а также выяснение и уточнение, какая именно информация необходима и почему. На этом этапе выявляются пробелы в информации. Часть пробелов может быть быстро установлена и устранена, так как является результатом недостаточного исследования, другая же часть пробелов в информации может и не быть обнаружена аналитиком, потому что упущена на этапе сбора самих сведений. Очевидно, что второй вид пробелов в информации является гораздо более опасным.

Выявив пробелы в информации, нужно определить их важность для дальнейшего анализа. Нельзя до бесконечности откладывать составление

аналитического отчета под предлогом того, что в информации выявлены пробелы, т.к. информация имеет свойство быстро устаревать и достоверность её теряется.

Этап 7. На основе выполнения вышеперечисленных этапов приступают к подготовке аналитических отчетов и рекомендаций по определенному вопросу, выработке конкретных выводов и предложений. Отчеты и рекомендации могут быть представлены в различных формах.

В литературе [57] выделяют три основных вида аналитических отчетов. Первый вид называют тактическим отчетом. К этому типу относятся экстренные отчеты по какому-либо вопросу небольшого объема, которые необходимы для срочного принятия решения. Такие отчеты составляются по разовым направлениям аналитической работы. Второй вид составляют стратегические отчеты. Они содержат более полную информацию и менее ограничены сроками. В них включается подробная предыстория данной проблемы и прогноз ее дальнейшего развития, причем для построения реалистичной гипотезы анализируется вся предшествующая информация по данной теме. Отчеты такого типа соответствуют постоянным направлениям аналитической работы. Третий вид представлен периодическими отчетами, основной отличительной особенностью которых является то, что они готовятся по определенному графику и направлены на анализ основных направлений деятельности.

В настоящее время рекомендуется использовать следующую форму изложения данных аналитического отчета [57]:

1. Заключение. Здесь должны содержаться ответы на вопросы, какова степень важности полученной информации, ее значение для принятия конкретных решений, идет ли речь о каких-либо угрозах, подозрениях, выявленных негативных факторах и т.п., какое отношение имеет предмет отчета к другим областям аналитической работы.

2. Рекомендации. В этом разделе должны быть указаны конкретные направления дальнейших действий службы безопасности и других структурных подразделений для улучшения системы безопасности, предотвращения утраты информации, принятия наиболее эффективных решений и т.п.

3. Обобщение информации. Здесь излагают самую существенную информацию без излишней детализации.

4. Источники и надежность информации. В этом разделе должны быть указаны предполагаемые оценки надежности данных и источника на момент написания отчета, так как для принятия решений необходимо оценить надежность материалов, являющихся их базой.

5. Основные и альтернативные гипотезы. Обязательно должны указываться рассмотренные в ходе анализа наиболее вероятные гипотезы, что

помогает принимать более взвешенные и адекватные решения, а также позволяет еще раз оценить правильность выбранной гипотезы.

6. Недостающая информация. Четко указывается, какая именно дополнительная информация необходима для подтверждения окончательной гипотезы и принятия решения.

Рассмотренная структурная схема проведения аналитического исследования позволяет предоставить в распоряжение специалиста, принимающего решение на его основе, структурированный массив конкретной информации.

Современное развитие общества требует от руководителей быстрого реагирования на резко меняющуюся ситуацию. Адекватная оценка изменений, основывающаяся на выводах информационно-аналитических подразделений, часто становится решающей в процессе принятия решения.

Вся необходимая информация, в основной своей массе, аккумулируется из открытых источников, в качестве которых выступают средства массовой информации и Интернет. В процессе проведения анализа необходимо учитывать, что различные издания зачастую полностью дублируют информацию. Несмотря на это требуется достаточно большой временной промежуток времени на изучение информации открытого доступа, в том числе в связи с тем, что необходимо проводить контекст-анализ, в основе которого лежит количественный подсчет содержательных элементов.

В процессе проведения анализа доминирующими являются следующие компоненты:

1. Четкая формулировка задачи для определения программы и источников исследования.
2. Определение ключевых понятий и единиц исследования.
3. Определение объема информации, достаточного для проведения анализа.
4. Составление инструкций лицу, работающему с текстом.
5. Непосредственная обработка данных.
6. Оформление результатов.

Обычно анализ проводят вручную, с помощью компьютерных программ или смешанным способом. При этом учитывается, что по своей направленности публикации можно разделить на обзорные, дискридитационные, заказные, рекламные и разглашающие информацию ограниченного распространения. Из этого потока можно выделить несколько категорий данных: текущая информация, базовая информация и субъективно-оценочные критерии.

Сравнительный анализ открытых источников зачастую приводит к достаточно неожиданным выводам. Это связано с тем, что профессиональная журналистика зачастую тесно переплетается с вопросами разведки, контрразведки, конкуренции, формированием имиджа и престижа объекта.

Кроме того, средства массовой информации могут использоваться и для организации дезинформации.

Из сказанного можно сделать вывод о необходимости использования определенных аналитических методов, позволяющих провести наиболее полное и объективное исследование.

Основным назначением всех аналитических методов является обработка полученных сведений, установление взаимосвязи между фактами, выявление значения этих связей и выработка конкретных предложений на основе достоверной и полной, аналитически обработанной информации. Существует широкий спектр специальных методов анализа информации [57]: графические, табличные, матричные и т.п., например, диаграммы связи и матрицы участников, схемы потоков данных, временные графики, графики анализа визуальных наблюдений VIA и графики оценки результатов PERT.

С помощью диаграмм связей выявляется наличие связи между субъектами, вовлеченными в конкретную ситуацию, подвергающуюся анализу, а также области общения, соприкосновения этих субъектов. На диаграмме связей отмечают как наиболее прочные, так и вспомогательные связи между субъектами. Анализируются все связи без исключения, так как в ходе развития событий и получения дополнительной информации вспомогательные связи могут выступить на первый план. Для большей наглядности следует также указывать на диаграмме связи должностей (для физических лиц) или род деятельности (для юридических лиц).

Матрицы связей отражают частоту взаимодействия субъектов за определенный период времени. Такой метод анализа дополняет диаграммы связей, позволяет оценить характер взаимодействий между субъектами через частоту таких взаимодействий. При использовании этого метода анализа до его начала необходимо отделить маловажные и не имеющие отношения к делу, пусть даже частые, взаимодействия субъектов.

Схемы потоков информации позволяют оценить то, каким образом происходят события. С их помощью можно анализировать пути движения информации среди субъектов анализа, т.е. оценивать положение каждого субъекта в общей группе и выявлять неустановленные связи между субъектами, используя определенную, специально подготовленную информацию как индикатор.

Временные графики используются для регистрации событий. Такая форма представления данных помогает не только эффективнее анализировать события, но и более рационально планировать меры противодействия.

Графики анализа визуальных наблюдений VIA являются составной частью графиков оценки результатов PERT. Оба графика составляются по принципу разбивки сложной операции на составные элементы. Такой принцип позволяет наглядно отражать ход событий. В зарубежных странах

графики VIA и PERT применяются для анализа тяжких преступлений и террористической деятельности, для повышения эффективности работы.

При проведении аналитической работы можно использовать какой-либо из перечисленных методов или их комбинацию.

В настоящее время в работе информационно-аналитических подразделений широко используют возможности современной вычислительной техники. Это относится к созданию баз данных по тематике аналитической работы и непосредственно к процессу анализа. Статистический анализ не выполняется вручную, для этого применяются специальные программы статистической обработки данных, предназначенные для аналитической работы.

В последнее время для аналитической работы все чаще применяются так называемые экспертные системы. Такие системы представляют собой класс компьютерных программ, которые выдают советы, проводят анализ, выполняют классификацию, дают консультации и ставят диагноз. Экспертные системы не только выполняют все эти функции, но и на каждом шаге могут объяснить аналитику причину той или иной рекомендации и последовательность анализа. В отличие от человека-аналитика у экспертных систем нет предубеждений, они не делают поспешных выводов, не поддаются влиянию внешних факторов. Такие системы работают систематизировано, рассматривая все детали, выбирая наилучшую альтернативу из всех возможных. Несомненным преимуществом экспертных систем является и то, что, будучи введены в машину один раз, знания сохраняются навсегда, как бы обширны они ни были.

В настоящее время в распоряжении сотрудников информационно-аналитических подразделений находится множество методов ведения аналитической работы, среди которых они могут выбрать наиболее эффективный с их точки зрения метод, либо пользоваться своим собственным, уникальным методом. В работу информационно-аналитических подразделений также должны широко внедряться современные компьютерные технологии как в форме современных баз данных и новейших статистических программ, так и в форме практического применения искусственного интеллекта – экспертных систем.

ЗАКЛЮЧЕНИЕ

Современный период развития общества характеризуется периодом перехода от индустриального общества к обществу информационному. Повсеместное внедрение информационных технологий создало новые возможности для активного и эффективного развития экономики, государства, общества и гражданина.

Информация, а равно и процессы, связанные с ее сбором, обработкой и хранением, являются неизменным атрибутом социальной деятельности. Кроме того, информация обладает рядом важных свойств, которые играют немаловажную роль в информационном обеспечении повседневной деятельности.

Анализ существующего понятия «информация» дает представление о ее понимании в общенаучном и философском смысле, когда под информацией понимаются все сведения являющиеся объектом преобразования хранения и передачи. Тем не менее, при рассмотрении информации как предмета правового регулирования информационной безопасности, необходимо оперировать понятием, закрепленным в Федеральном законе «Об информации, информационных технологиях и о защите информации», где под информацией понимаются сведения независимо от формы их представления. Это понятие информации используется для формирования его производных от дефиниций и закрепляется в других нормативных актах.

Рассматривая понятие информации необходимо учитывать ее специфику. Компьютерная сеть может быть представлена как организованная совокупность сведений реализующихся в виде целостного, организационного и технически обеспеченного комплекса информационных процессов. Компьютерная сеть предназначена для сбора, передачи, обработки хранения и выдачи информации по запросам.

Критическими компонентами компьютерной сети являются:

- сотрудники, обеспечивающие функционирование компьютерных сетей;
- информация, обрабатываемая в компьютерных сетях;
- коммуникации;
- носители информации;
- методы и процедуры сбора, передачи, обработки и хранения информации.

Анализ законодательной и терминологической базы, а также процессов развития информационных технологий, позволяет установить:

- понятие документированной информации на двуединстве информации и материального носителя, что определяет специфику требований, касающихся ее правового режима;
- информация в виде электронного документа будет подходить под понятие документальной информации в случае наличия реквизитов, позво-

ляющих ее идентифицировать;

- для установления доказательной силы документальной информации необходим механизм идентификации, исключающий возможность неправомерного доступа и авторизации пользователя. В качестве такого механизма можно использовать электронно-цифровую подпись;
- в основе распространения информационных процессов в компьютерных сетях лежат элементарные акты создания, сбора, обработки, накопления, хранения, поиска, получения, распространения и потребления информации. В результате использования этого в повседневной деятельности формируются информационные ресурсы, то есть отдельные документы и массивы документов в информационных сетях;
- информационные ресурсы и информационное обеспечение компьютерных сетей рассматривается в рамках правового института служебной тайны. В настоящее время механизмы разграничения доступа к информации в отечественной правовой системе не реализованы и регламентируется только порядок доступа к документам на бумажных носителях;
- информационная деятельность рассматривается с точки зрения информационного обеспечения, и в частности, организации доступа к информации, так как именно на несовершенстве доступа основано 80% атак;
- при анализе экономической целесообразности обеспечения безопасности в сфере информационных технологий следует учитывать многомерность экономического эффекта, не только количественные, но и качественные показатели эффективности (работа системы обеспечения безопасности в сфере информационных технологий дает своеобразный мультипликативный эффект, поскольку препятствует хищению различных видов информации начиная от проектов в стадии разработки и заканчивая проектами в стадии завершения и получения прибыли).

В общем смысле под «системой информации» понимается совокупность различных видов информации о конкретных объектах и функциях, соответствующих организации эффективного выполнения оперативно-служебных задач. В последние годы для многих информационных баз созданы средства автоматизированной обработки и идет поэтапный процесс освоения безбумажных технологий информационного обмена. В настоящее время складывается автоматизированный контур системы информационного обеспечения, который полностью реализует системные возможности информационного обеспечения.

Преступные посягательства на информацию в компьютерных сетях базируются на понятии «преступления в сфере компьютерной информации» и мерах по противодействию таковым. В законодательстве России преступления связанные с компьютерной информацией рассматриваются в разделе о преступлениях, посягающих на общественную безопасность и общественный порядок, что определяет объект рассматриваемых преступлений. Конкретно эти преступления направлены против той части уста-

новленного порядка общественных отношений, который регулирует изготовление, использование, распространение и защиту компьютерной информации. Выяснение данного обстоятельства важно для того, чтобы отграничить преступления, предусмотренные ст.ст. 272 – 274 УК, от других преступлений, связанных с использованием ЭВМ, системы ЭВМ и их сети для совершения других видов преступлений.

Преступления в сфере компьютерной информации совершаются в целях получения информации и последующей продажи ее третьим лицам. Содержание информации при этом может быть различным.

На этом фоне вызывает опасение тот факт, что все более проявляется тенденция к совершению преступлений в сфере компьютерной информации в комплексе с другими видами преступлений. В последнее время целью преступлений в сфере компьютерной информации часто выступает манипулирование и модификация, при этом могут быть внесены изменения в электронные реестры, базы данных, средства управления базами данных, системы электронного документооборота.

Среднегодовой показатель роста в числе зарегистрированных преступлений в сфере компьютерной информации составляет 139%. Опасность данной тенденции достаточно велика, так как в силу специфики работы часто следы неправомерного доступа к компьютерной информации обнаруживаются по прошествии определенного времени.

Изучение проблем расследования случаев неправомерного доступа к компьютерной информации выступает одной из острейших проблем. Не смотря на то, что в последние годы в криминалистической литературе уделяется повышенное внимание методике расследования случаев неправомерного доступа к компьютерной информации, при рассмотрении данного вида правонарушений, в проекции на информацию, остается большой ряд нерешенных и дискуссионных вопросов.

По нашему мнению к основным угрозам в сфере информационной безопасности целесообразно отнести:

- критическое состояние отечественных отраслей промышленности;
- неудовлетворительная криминогенная обстановка, которой сопутствует тенденция сращивания государственных и криминальных структур в информационной сфере, постоянные попытки получения доступа к конфиденциальной информации со стороны криминальных структур, понижение защищенности в информационной сфере, а также повышение влияния организованной преступности на жизнь общества в целом;
- недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;

- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, и, как следствие, недостаточная правоприменительная практика;
- недостаточный контроль со стороны государства за развитием информационного рынка, а также неразвитость институтов гражданского общества;
- недостаточное финансирование осуществляемых мероприятий по обеспечению информационной безопасности;
- недостаточное количество специалистов в области обеспечения информационной безопасности, а также снижение уровня эффективности системы образования и воспитания;
- недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, а также в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
- отставание 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;
- нехватка квалифицированных кадров, способных генерировать и развивать далее методологию информационно-аналитической деятельности, наряду с этим владеющих новыми информационными технологиями, а также свободно ориентирующихся на отечественном и международном информационных рынках.

В настоящее время сохраняется устойчивая тенденция к нарушению безопасности информации на всех стадиях ее обработки, хранения и передачи. Причины постоянного совершенствования процедур этого процесса кроются в высокой латентности случаев неправомерного доступа к информации в информационных сетях. В сложившейся ситуации просматривается глобальная тенденция по совершенствованию средств обнаружения, противодействия и предотвращения попыток неправомерного доступа в информационных сетях любого уровня. «Данный процесс достаточно динамичен, так как постоянное совершенствование процедур влечет за собой адекватное совершенствование и повышение надежности средств и методов обнаружения атак, аналитической обработке сообщения о подобных воздействиях» [95]. В связи с этим следует сказать о необходимости создания подразделений, чьей специализацией является проведение информационно-аналитической работы. Наличие и успешное функционирование подобных служб позволяет не только повысить защищенность объектов информатизации, но и проводить постоянную работу по мониторингу процедур неправомерного доступа и эффективно бороться с ними.

Подобные тенденции требуют не только совершенствования средств обеспечения защиты информации и определения места совершения противоправного деяния в сфере информационных технологий, но и проведения эффективного анализа уже совершенных деяний. Он заключается в определении закономерностей проявления механизма неправомерного доступа, собирания, исследования, оценки и использования следов, а также совершенствовании средств, приемов, методов анализа и предотвращения в последующем подобных противоправных деяний.

Библиографический список

Нормативные правовые акты, руководящие документы:

1. Конституция Российской Федерации // Российская газ. - 1993. - 25 дек.

2. Доктрина информационной безопасности Российской Федерации // Российская газ. - 2000. - 28 сент.

3. Уголовный кодекс Российской Федерации. Принят Государственной Думой РФ 24 мая 1996 г. Одобрен Советом Федерации 5 июня 1996 г. (с последующими изменениями и дополнениями). - М. : ТК Велби, 2005. - 192 с.

4. Уголовно-процессуальный кодекс Российской Федерации. Принят Государственной Думой РФ 22 ноября 2001. Одобрен Советом Федерации 5 декабря 2001 года. Подписан Президентом Российской Федерации 18 декабря 2001 года №174-ФЗ. - М., 2001 (с последующими изменениями и дополнениями).

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

6. О государственной тайне : Федеральный закон РФ от 21.07.93 г. № 5485-I.

7. О безопасности : Федеральный закон РФ от 20.12.2010 г. № 390-ФЗ.

8. Об оперативно-розыскной деятельности : Федеральный закон РФ от 12 августа 1995 г. № 144-ФЗ.

9. О связи : Федеральный закон РФ от 16.02.95 г. № 15-ФЗ.

10. Об электронной цифровой подписи : Федеральный закон РФ от 13 декабря 2001 г.

11. Об обязательном экземпляре документов : Федеральный закон РФ от 29.12.94 г. № 77-ФЗ.

12. Об участии в международном информационном обмене : Федеральный закон РФ от 5.06.1996 № 85-ФЗ.

13. О внешней разведке : Федеральный закон РФ от 10 января 1996 г. № 5-ФЗ.

14. О правовой охране программ для электронных вычислительных машин и баз данных : Закон от 23.09.92 г. № 3523-I.

15. О средствах массовой информации : Закон от 27.12.91 г. № 2124-I.

16. Об авторском праве и смежных правах : Закон от 9.07.93 г. № 5351-I.

17. Патентный закон РФ от 23.09.92 г. № 3517-I.

18. Основы законодательства об Архивном фонде РФ и архивах от 7.07.93 г. № 5341-I.

19. Защита от несанкционированного доступа к информации : руководящий документ : утв. решением председателя Гостехкомиссии России от 30 марта 1992 г.

20. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации : руководящий документ ГТК РФ от 25 июня 1997 г.

Монографии, учебники и учебные пособия:

21. Атака из Internet / И.Д. Медведовский, П.В. Семьянов, Д.Г. Леонов, А.В. Лукацкий. - М. : СОЛОН-Р, 2002. - 368 с.

22. Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. - М. : Норма, 2001. - 240 с.

23. Батурин Ю.М. Компьютерная преступность и компьютерная безопасность. - М., 2005. - 390 с.

24. Ветров К.В. Информационная безопасность России в условиях глобального информационного сообщества // Каталог «Системы безопасности, Связи и Телекоммуникаций». - 2003. - № 1 (10).

25. Винер Н. Кибернетика и общество. - М. : Сов. радио, 1958.

26. Глушаков С.В. Секреты хакерства: защита и атаки. - Ростов н/Д: Феникс, Харьков: Фолио, 2005.

27. Грег Хогланд, Гари Мак-Гроу. Взлом программного обеспечения: анализ и использование кода : пер. с англ. - М. : «Вильямс», 2005.

28. Громов Г. Р. Национальные информационные ресурсы: проблемы промышленной эксплуатации. - М. : Наука, 1985.

29. Дворянкин С.В. Передний край обеспечения безопасности информации // Системы безопасности, Связи и Телекоммуникаций. - 2003. - № 1 (10).

30. Доронин А.И. Бизнес-разведка. - М. : Издательство Ось-89, 2006.

31. Еременко В.Т. Основы построения информационно-телекоммуникационных систем : учебное пособие. Часть 2. - Орел : Орловский юридический институт МВД России, 1999.

32. Еременко В.Т., Чистяков М.В. Теоретические основы создания и применения профилей протоколов архитектур безопасности : монография / под общей редакцией В.Т. Еременко. - Екатеринбург : Уральский государственный технический университет, 2000.

33. Зима В.М., Молдавян А.А., Молдавян Н.А. Безопасность глобальных сетевых технологий. - 2-е изд. - СПб. : БХВ – Петербург, 2003. - 368 с.

34. Интервью с директором по ИТ ОАО «Гидро ОГК» Г. Бандуриным.

35. Информационная безопасность России / Ю.С. Уфимцев [и др.]. - М. : Издательство «Экзамен», 2003. - С. 558.

36. Информационная безопасность телекоммуникационных систем (технические вопросы): Учебное пособие для системы высшего профессионального образования России / В.Г. Кулаков, М.В. Гаранин, А.В. Заряев, И.В. Новокшанов, А.Н. Обухов, С.В. Скрыль. - М. : Радио и связь, 2004. - 388 с.

37. Качалов Р.М. Управление хозяйственным риском. - М. : Наука, 2002.

38. Кевин Мандиа, Крис Просис. Защита от вторжений: Расследование компьютерных преступлений. - М. : Издательство «ЛОРИ», 2005.

39. Козлов В.А. Открытые информационные системы. - М. : Финансы и статистика, 1999.

40. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. - М. : «Горячая линия - Телеком», 2002. - 176 с.

41. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов / В.Г. Олифер, Н.А. Олифер. - СПб. : Питер, 2003. - 864 с.

42. Криминалистика / под ред. Н.П. Яблокова. - М. : Юрист, 2001.

43. Криминалистическая характеристика преступлений. - М. : «Щит-М», 1998.

44. Крылов В.В. Информационные компьютерные преступления. - М. : изд. Инфра-М-Норма, 1997.

45. Кузьмин В.А. Комментарий к Федеральному закону от 10 января 1996 г. № 5-ФЗ «О внешней разведке». Материал подготовлен для системы КонсультантПлюс с использованием правовых актов по состоянию на 16 августа 2008 года.

46. Левин М. Фрикинг и хакинг: Методы, атаки, взлом и защита. – М. : МиК, 2001. – 416 с. – (Руководство по работе: Советы, хитрости, трюки и секреты).

47. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. - Воронеж : Изд-во Воронежского государственного университета, 2002. - 408 с.

48. Организационно-правовые основы противодействия неправомерному доступу к информации криминалистических учетов органов внутренних дел / редакционная коллегия: А.Н. Ильяшенко, Д.С. Мишин. - Краснодар : Краснодарский университет МВД РФ, 2008. - 208 с.

49. Основы информационной безопасности : учебник для высших учебных заведений МВД России / под ред. В.А. Минаева и С.В. Скрыль. - Воронеж : Воронежский институт МВД России, 2001. - 464 с.

50. Некоторые особенности выявления, предотвращения и профилактики правонарушений в сфере компьютерной информации / Д.С. Ми-

шин, С.Л. Паньков, О.В. Третьяков // Научный портал МВД России. - 2011. - № 4 (12).

51. Протоколы информационно-вычислительных сетей. Разработка, моделирование и анализ / под редакцией В.А. Мизина. - М. : Финансы и статистика, 1990.

52. Разведывательное и контрразведывательное обеспечение деятельности финансово-хозяйственной деятельности предприятия / А.И. Доронин. Тула : «Гриф и К», 2000. - 116 с.

53. Расследование неправомерного доступа к компьютерной информации : учебное пособие. Изд-е второе, дополненное и переработанное / под ред. д.ю.н. проф. Н.Г. Шурухнова. - М. : Московский университет МВД России, 2004. - 352 с.

54. Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. - СПб. : Питер, 2008.

55. Соколов А.В., Степанюк О.М. Методы информационной защиты объектов и компьютерных сетей. - М. : ООО «Фирма «Издательство АСТ»»; СПб. : ООО «Издательство «Полигон»», 2000. - 272 с.

56. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. - М. : ДМК Пресс, 2002. - 562 с. (Серия «Администрирование и защита»).

57. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: учеб. пособие. - М. : ИНФРА – М, 2001. - 304 с.

58. Усов А.И. Судебно-экспертное исследование компьютерных средств и систем : учебное пособие / под редакцией проф. Е.Р. Россинской. - М. : «Экзамен», 2003.

59. Теоретические основы информатики и информационная безопасность / под ред. В.А. Минаева, В.Н. Саблина. - М. : «Радио и связь», 2000.

60. Теоретические основы развития информационно-телекоммуникационной среды (организационно-правовые и социокультурные аспекты) : монография / Мишин Д.С. [и др.]. - Орел : ОрЮИ МВД России, 2005. - С. 192.

61. Турло С.С., Залдат И.П. Шпионаж. - М. : X-History, 2002.

62. Учебник по информационно-аналитической работе / И.Н. Кузнецов. - М. : ООО Изд-во Яуза, 2001. - 320 с.

63. Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации : учебное пособие. - М. : Издательская группа «Юрист», 2001. - 412 с.

64. Шеннон К. Математическая теория связи // Работы по теории информации и кибернетике. - М. : ИЛ, 1963.

65. Шурухнов Н.Г. Криминалистика : учебник. - М. : Изд-во Эксмо, 2005. - С. 695.

66. Яблоков М. От шпионов до наркобаронов // Тульский молодой коммунар. - 2003. - 24 дек. - №182 (10540).

67. Ярочкин В. Безопасность информационных систем. - М. : «Ось-89», 1996.

68. [GREE] P. Green, ed., Computer Network Architectures and Protocols, Plenum Press, New York, 1982.

69. [ISO 1984a] ISO International Standard 8072, Information Processing Systems — Open Systems Interconnection — Transport Service Definition, International Organization for Standardization, Geneva, 1984.

70. [ISO 1984b] ISO International Standard 8073, Information Processing Systems-Open Systems Interconnection — Transport Protocol Specification, Geneva, 1984; appears in Computer Comm. Rev., vol. 12, nos. 3 and 4, July/Oct. 1982254.

71. [ZIMM] H. Zimmermann, «OSI Reference Model — The ISO Model of Architecture for Open Systems Interconnection», IEEE Trang. on Comm., vol. COM-28, no. 4, April 1980, 425—432; reprinted in [GREE].

72. Anderson, James P. Computer Security Threat Monitoring and Surveillance. Fort Washington, PA: James P. Anderson Go

73. Carrier, Brian and Eugene H. Spafford. «Getting Physical with the Digital Investigation Process». International Journal of Digital Evidence, Fall 2003. http://www.ijde.org.

74. Denning. Dorothy E.(SRI International). An Intrusion Detection Model. IEEE Transaction on Software Engineering (SE-13). 2 (February 1987): 222-232.

75. Frank J. (1994). Artificial intelligence and intrusion detection: Current and future direc-tions. In Proceedings of the National 17th Computer Security Conference. Mukherjee, B., Heberlein, L. T., and Levitt, K. N. (1994). Network intrusion detection. IEEE Network, 26–41.

76. Hartley R.V. Transmission of Information // Bell System Technical Journal. - 1928. - №7 (3). - P. 535-563.

77. Info Watch - Annual Study: Cost of a Data Breach, 2006.

78. My Key Technology, 2003.

79. National Survey on Managing the Insider Threats, 2007.

80. National Survey on Managing the Insider Threats, 2007.

81. Scheier, Bruse. Applied Cryptography. - 2nd ed. - New York : Wiley Publishing, 1995.

82. TCP/IP Illustrated, Volume One: The Protocols, автора W. Richard Stevens (Addison Wesley Professional Computing Series).

83. U.S. Department of Justice, 2003.

Диссертации и научные статьи:

84. Галатенко В.А., Макстенек М.И., Трифаленков И.А. Сетевые протоколы нового поколения // Jet Info. - 1998. - № 7,8.

85. Гуляев Ю.В., Олейников А.Я., Филинов Е.Н. Развитие и применение открытых систем в Российской Федерации // Информационные технологии и вычислительные системы. - 1995. - № 1.

86. Дворянкин С.В. Передний край обеспечения безопасности информации // Системы безопасности, Связи и Телекоммуникаций. - 2003. - № 1 (10). - С. 226.

87. Еременко В.Т. Базовые положения теории профилирования тестирования распределенных управляющих систем // Информационные технологии в науке, образовании и производстве (ИТНОП) : труды международной научно-практической конференции (11-12 мая 2004 г., Орел). - Т. 2.

88. Жаркой В.В., Потанина И.В., Сушков П.Ф., Филиппова Н.В. К вопросу о возможности идентификации противоправных действий в компьютерных сетях // Охрана, безопасность и связь : сборник материалов IV Всероссийской научно-практической конференции. Часть 2. – Воронеж : ВИ МВД России, 2003. - С.114-115.

89. Компьютерные вирусы и противоправное манипулирование информацией / В.А. Минаев, С.В. Скрыль, Е.Г. Геннадиева, И.В. Пеньшин // Технологии безопасности : сборник материалов VII Международного форума. - М. : Пресс-центр Международного форума «Технологии безопасности», 2002. - С. 281-287.

90. Костин С.В. Управление процессом информационного обмена в АСУ на примере горного предприятия : дис. … канд. тех. наук. - Орел : ОрелГТУ, 2006.

91. Костин С.В., Парамохина Т.М., Савенков А.Н. Повышение надежности процессов информационного обмена в распределенной управляющей системе / Правопорядок и безопасность в России: история и современность : материалы региональной конференции молодых ученых, адъюнктов и соискателей (28 мая 2005 г.) // Наука и практика. - 2005. - № 2. - С. 47-49.

92. Костин С.В., Савенков А.Н. Имитационная модель процессов информационного обмена для распределенной управляющей системы // Известия Орловского государственного технического университета. Серия «Информационные системы и технологии». - 2005. - № 1. - С. 106-112.

93. Костин С.В., Савенков А.Н. Методика управления потоком данных транспортного протокола распределенной управляющей системы в режиме возобновления после сбоев // Материалы Всероссийской научно-практической конференции. - 2005. - № 5. - С. 82-84.

94. Мишин Д.С. Культурно-правовые аспекты информационного взаимодействия // «Ломоносовские чтения» МГУ им. М.В. Ломоносова. - 2006.

95. Мишин Д.С., Еременко А.В. Методы и системы обнаружения атак в компьютерных сетях // Вестник информационных и компьютерных технологий. - 2006. - № 10. - С. 35-41.

96. Минаев В.А., Скрыль С.В. Компьютерные вирусы как системное зло // Системы безопасности – СБ-2002 : материалы XI научно-технической конференции Международного форума информатизации. - М. : Академия ГПС, 2002. - С. 18-24.

97. Мишин Д.С. Организационно-правовые основы противодействия несанкционированному доступу к информации криминалистических учетов органов внутренних дел : дис. … канд. юрид. наук. - ВИ МВД России, Орел, 2006.

Информационные Интернет-сайты:

98. URL: BRE_ru Вопросы обеспечения информационной безопасности научных, производственных и финансовых структур на базе программно-технических средств.htm.

99. URL: Www.secur.ru - Российский сервер по безопасности.

100. URL: Www.infosec.ru Научно-инженерное предприятие «ИНФОРМЗАЩИТА».

101. URL: http://bugabooks.com/book/57-zashhita-kompyuternoj-informacii/25-iskazhenie.html.

102. URL: http://mts.ivgsm.ru/news/20030708175734.html.

103. URL: http://netgroup-serv.polito.it/windump/install/default.htm.

104. URL: http://netgroup-serv.polito.it/winpcap.

105. URL: http://technomag.edu.ru/doc/143237.html.

106. URL: http://window.edu.ru/window/library/pdf2txt?p_id=18264&p_page=11.

107. URL: http://www.infosec.ru/produkt/checkpoint/firewall1.html.

108. URL: http://www.tcpdump.org.

109. URL: wspl – http://www.nsrl.nist.gov.

110. URL: www.ietf.org/rfc.

Монография

Авторы:
кандидат педагогических наук **Калиниченко** Игорь Александрович,
кандидат экономических наук **Коробов** Алексей Александрович,
кандидат технических наук **Костин** Сергей Викторович,
кандидат юридических наук **Мишин** Дмитрий Станиславович

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРОТИВОДЕЙСТВИЯ НЕПРАВОМЕРНОМУ ДОСТУПУ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Свидетельство о государственной аккредитации
Рег. № 1300 от 23.12.2011 г.
Подписано в печать_____ Формат 60х90$^{1}/_{16}$.
Усл. печ. л. _____. Тираж _____ Заказ № _____.

Орловский юридический институт МВД РФ им. В.В. Лукьянова.
302027, Орел, Игнатова, 2.