Содержание:

ВВЕДЕНИЕ

Развитие всемирной экономики характеризуется все большей зависимостью рынка от существенного объема информационных потоков, а принятие решений во всех сферах жизнедеятельности компаний или предприятий все в большей степени основывается на информационных процессах. Исследование данных процессов с дальнейшей выработкой управляющих решений выполняется на базе информационных моделей, сформированных на нынешних информационно-телекоммуникационных технологиях.

Информационный ресурс стает одним из основных источников экономической эффективности компаний. Практически наблюдается тенденция, когда любые жизнедеятельности компаний стают зависимы от информационного развития, в процессе которого они сами формируют информацию и сами же ее употребляют. Потому защита информации является самостоятельным и значимым направлением деятельности компании. [3]

Несмотря на все растущие усилия по формированию технологий защиты ее уязвимость информации не только не понижается, а также постоянно повышается. В нынешнее время огромные иностранные компании до 40% прибыли вносят в безопасность. В РФ также увеличивается тенденция повышения ассигнований в обеспечении ИБ. Фактически во всех устойчиво функционирующих компаниях сформированы службы безопасности. Эффективность работоспособности такого типа служб в большинстве зависит от грамотного внесения определенных средств и профессионального подхода в вопросах организации системы защиты данных.

На данном этапе развития ключевыми угрозами безопасности компании представляют собой угрозы в сфере информационного обеспечения. Последствиями эффективного проведения информационных налетов могут стать искажение или компрометация личной информации, навязывание ложной информации, несоблюдение поставленного регламента сбора, передачи и обработки информации, сбои и отказы в работе технических систем, которые вызваны непреднамеренными и преднамеренными действиями, как со стороны преступных сообществ, со стороны конкурентов, так и со стороны сотрудников

организации.

К одной из наиболее основных задач в области обеспеченья безопасности нужно отнести проектирование комплексной системы защиты данных, которая включает создание и введение всех нынешних технологий, средств и методов, которые обеспечивают защиту компании от всех типов угроз, и гарантируют его устойчивое развитие в нынешних условиях.

С появлением информационных технологий появилась и необходимость повышенного внимания к вопросам информационной безопасности. Временная недоступность. Несанкционированное использование или, в худшем случае, разрушение информационного ресурса могут наносить компаниям очень значительный вред, а главное, материальный ущерб.

Без защиты компьютерных информационных систем, внедрение этих систем в компанию может и оказаться экономически невыгодным. Значительные потери данных, что хранятся и обрабатываются в компьютерных сетях, потери конфиденциальности данных - результаты незащищенности компьютерных информационных систем.

В данной работе описана значимая часть информационной безопасности – угрозы. Описаны понятия и виды угроз безопасности в компьютерных информационных системах. Добиться раскрытие темы не возможно без определений и критерий классификации угроз, наиболее распространенных угроз доступности с примерами, описания вредоносного ПО, основных угроз целостности и конфиденциальности.

Объектом в работе выступают угрозы информационной безопасности, предметом – их виды и состав.

Целью работы является исследование видов и состав угроз информационной безопасности.

Для достижения заданной цели в работе необходимо выполнить ряд задач:

- рассмотреть основные определения и критерии классификации;

- выявить состав и виды угроз информационной безопасности (ИБ);

- рассмотреть наиболее распространяемые угрозы конфиденциальности, целостности и доступности;

- рассмотреть статистику угроз ИБ и ее направления деятельности.

При написании работы были применены такие методы научного исследования, как изучение научной литературы по теме исследования, нормативно-правовой базы, аналитический и сравнительный методы.

Глава 1. Теоретические сведения о угрозах информационной безопасности

1.1 Основные определения и критерии классификации угроз

К основным определениям можно отнести само понятие угрозы, а также атаки, злоумышленника, источниками угрозы, уязвимых мест, окна опасности. [1,5,16]

Под угрозой понимают потенциальную возможность нарушить информационную безопасность каким-либо образом.

Атака - это попытка сделать (реализовать) угрозу. А тот кто это хочет сделать называют злоумышленником. Если злоумышленник реализовал угрозу его можно назвать источником угрозы.

Возможность доступа определенных лиц к важному оборудованию или ошибки программного обеспечения, другими словами, это называется уязвимыми местами в компьютерных информационных системах. Именно наличие этих мест чаще всего и является следствием наличия угроз.

Нужно ввести при рассмотрении угроз такое понятие как окно безопасности – это определенный промежуток времени от возможности использовать место компьютерной информационной системы до ликвидации этого места. Т.е., существование окна безопасности равносильно существованию успешных атак на информационную систему.

Ели говорить о программном обеспечении, то окно появляется с появлением ошибки в программном обеспечении и ликвидируется при решении этой ошибки.

Окно безопасности систем может существовать значительно долго –дни и даже недели, и за это время в любой компании должны узнать о средствах использования проблемы в защите, также должны быть выпущены соответствующие заплаты которые должны уже быть установлены в защищаемой ИС.

Угрозы можно классифицировать по аспекту безопасности информационных систем, по компонентам систем, по способу осуществления и по расположению источников угроз.

Аспектами информационной безопасности может быть доступность, целостность, конфиденциальность. Именно против него угрозы направлены в первую очередь.

Угрозы нацелены именно на компоненты информационных компьютерных систем. К ним можно отнести программы, данные, аппаратуру, поддерживающую инфраструктуру.

Способ существования говорит нам что угрозы могут быть не только нацеленными на результат, а могут просто быть случайными. К ним относят случайные угрозы и угрозы преднамеренные. Могут носить как природный так и техногенный характер.

И по расположению источников угрозы можно разделить на внутренние и внешние, так как они могут происходить как внутри информационной системы, так и вне ее.

1.2 Направления обеспечения ИБ

С учетом сформировавшейся практики обеспечения ИБ и в соответствии с условиями руководящих документов в области ИБ, подчеркивают такие типы защиты данных:

Правовая защита данных - защита данных правовыми методами, которая включает в себя создание нормативных и законодательных документов (актов), которые регулируют отношения субъектов по защите данных, использование таких документов (актов), а также контроль и надзор за их исполнением.

Техническая защита данных - защита данных, заключающаяся в обеспечении некриптографическими методами ИБ, подлежащих (подлежащей) защите в соответствии с функционирующим законодательством, с использованием технических, программно-технических и программных средств.

Криптографическая защита данных - защита данных с помощью ее криптографического преобразования.

Физическая защита данных - защита данных путем использования организационных мероприятий и совокупности средств, формирующих препятствия для несанкционированного проникновения или доступа неуполномоченных физ.-лиц к объекту защиты.

Организационные мероприятия по обеспечению физической защиты данных предусматривают постановку режимных, территориальных, временных, пространственных ограничений на условия применения и распорядок работы объекта защиты. При том к объектам защиты информации могут относится: здание (сооружение), охраняемая территория, отдельное помещение, информационные ресурсы и (или) информация объекта информатизации.

Организационная защита информации –регламентация деятельности компании и взаимоотношений сотрудников на нормативно – правовой базе, существенно затрудняющей или исключающей неправомерное освоение конфиденциальными данными и проявление внешних и внутренних угроз.

Только комплексное использование всех типов защиты информации обеспечивает требуемый и достаточный уровень ИБ предприятия. [6,10,21]

1.3 Вредоносное ПО

Внедрение в атакуемые системы вредоносного ПО есть опаснейший способ проведения атак. Выделяют грани вредоносного ПО, такие как вредоносная функция, способ распространения и внешнее представление. [2,15]

Можно ввести такое понятие как бомба вредоносной функции, т.е. назовем так часть, составляющую разрушительную функцию. Бомба, как и любая другая программа, может обладать сколь угодно сложной логикой, поэтому спектр вредоносных функций неограничен.

Но обычно бомбы используют для внедрения другого вредоносного ПО, агрессивного потребления ресурсов, получения контроля над атакуемой системой и изменения или разрушения программ и данных.

По механизму распространения бывают вирусы и черви.

Вирусом называют код, который может распространятся путем внедрения в другие программы.

Черви – так же код, но который самостоятельно, т.е. без внедрения в другие программы, может вызывать распространение своих копий по информационным компьютерным системам и выполнять их путем запуска заряженной программы.

Обычно вирусы распространяются локально в пределах узла сети, т.е. что бы передаваться по сети им нужна дополнительная помощь (пересылка зараженного файла), а черви, наоборот, в первую очередь распространяются по сети.

Черви так же могут, к примеру, «сесть» полосу пропускания сети и ресурсы почтовых систем, тем самым можно сказать что само распространение вредоносного ПО вызывает агрессивное потребление ресурсов и, следовательно, является вредоносной функцией.

Троянским называется вредоносный код, который выглядит как функционально полезная программа. Т.е. обычная программа, будучи пораженная вирусом, становится троянской, иногда их изготавливают вручную и подсовывают доверчивым пользователям имея привлекательный вид. [4]

Глава 2. Виды и состав угроз безопасности

2.1 Общие сведения

Под угрозой безопасности информации понимается множество факторов и условий, формирующих потенциальную или реально явную опасность нарушения ИБ. [7]

Фактор, который воздействует на защищенную информацию – это явление, процесс или действие, в результате которого возможна утечка, уничтожение защищенной информации, искажение, блокировка доступа к ней.

Источник угрозы ИБ - субъект (материальный объект, физическое лицо или физическое явление), которое является непосредственной причиной появления угрозы ИБ.

Уязвимость информационной системы (брешь)- свойство информационной системы, которая обусловливается возможностью выполнения угроз безопасности обрабатываемых в ней данных.

По отношению к информационным ресурсам и информации можно подчеркнуть угрозы конфиденциальности, целостности, доступности и достоверности информации, которые появляются в разных формах нарушений (рисунок 1.). [20]

За правилом, вышеупомянутые угрозы информационных ресурсов применяются такими способами:

1) Через существующие агентурные источники в органах муниципального управления и коммерческих структурах, содержащих возможность получения личной информации (суды, коммерческие банки, налоговые органы и так далее).

2) Посредством подкупа лиц, непосредственно которые работают в структурах или организации, напрямую связанных с ее работой.

2) Посредством перехвата данных, циркулирующих в средствах и системах связи и вычислительной технике с помощью технических средств съема и разведки информации.

4) Посредством про слушки индивидуальных переговоров и иными способами несанкционированного доступа к источникам личной информации.

Угрозы информационной

безопасности

Проявляются в нарушениях

ЦЕЛОСТНОСТИ

КОНФИДЕНЦИАЛЬНОСТИ

ДОСТУПНОСТИ

1. Разглашение
2. Утечка
3. НДС
4. Искажения
5. Ошибки

6. Потери
7. Фальсификации
8. Нарушение связи
9. Воспрещение получения

Рисунок 1. Воздействие угроз информации на критерии ИБ

ИБ проявляет воздействие на защищенность интересов в разных сферах жизнедеятельности государства и общества. В любой из них содержатся свои особенности обеспечения ИБ, которые связаны со спецификой объектов обеспеченья безопасности, ступенью их уязвимости по отношению угроз ИБ. [8,14]

К примеру, с позиции обеспечения ИБ в **компьютерных системах** (КС) все количество потенциальных угроз ИБ в компьютерных системах может быть поделено на два класса.

Угрозы, которые не повязаны с намеренными действиями злоумышленников и выполняются в неожиданные моменты времени, называют **непреднамеренными или случайными.**

Использование угроз данного класса приводит к большим потерям данных (по статистической информации - до 80% от ущерба, который нанесен информационным ресурсам компьютерных систем разными угрозами). Так же могут, выполняется уничтожения, нарушения целостности и доступности информации. Не часто нарушается конфиденциальность информации, но при этом формируются предпосылки для злоумышленного влияния на информацию.

Аварии и стихийные бедствия чреваты более разрушительными результатами для информации, так как носители данных подвергаются физическому разрушению, данные теряются или доступ к ним стает невозможен.

Отказы и сбои сложных систем неизбежны. В результате отказов и сбоев нарушается функциональность технических средств, искажаются и уничтожаются программы и данные, нарушается алгоритм работоспособности устройств. Нарушения алгоритмов работоспособности отдельных устройств и узлов могут также послужить причиной нарушения конфиденциальности информации. К примеру, отказы и сбои средств выдачи данных могут привести к неразрешенному доступу к данным путем несанкционированной ее передачи в канал связи, на устройство печати и тому подобное. [19]

Ошибки при разработке компьютерных систем, программные и алгоритмические ошибки сводятся к последствиям, схожим к последствиям (отказов и сбоев технических средств). Кроме этого, данные ошибки могут быть применены злоумышленниками для влияния на ресурсы компьютерных систем. Основную опасность представляют ошибки в операционных системах (ОС) и в программных средствах защиты данных.

Согласно информации Национального института стандартов и технологий США (NIST) 65% ситуаций нарушения ИБ появляется в результате **ошибок обслуживающего персонала и пользователей.** Некомпетентное, невнимательное или небрежное использование функциональных обязанностей работниками приводят к потере, нарушению конфиденциальности и целостности информации, а также компрометации механизмов защиты.

Иной класс угроз ИБ в КП составляют преднамеренно формируемые угрозы. Угрозы данного класса в согласовании с их физической сущностью и механизмами применения могут быть разбиты по пяти группам:

- универсальный или классический шпионаж и диверсии;

- несанкционированный доступ к данным;

- наводки и электромагнитные излучения;

- разновидность структур;

- вредоносное программное обеспечение.

В качестве источников ненужного воздействия на ресурсы информации по-прежнему важны средства и методы диверсий и шпионажа, которые применялись и применяются для добычи или уничтожения данных. Данные методы также эффективны и действенны в условиях использования КС. Чаще всего они применяются для получения информации о системе защиты с целью взлома системы, а также для похищения и уничтожения информационных ресурсов.

Угрозы в коммерческой деятельности также содержат личные особенности. [11,17]

По отношению к отдельной организации есть такие ключевые **типы внешних угроз:**

- Бесчестные конкуренты.

- Формирования и криминальные группы.

- Противозаконные воздействия иных организаций и лиц административного аппарата, также и налоговых служб.

- Нарушение введенного регламента сбора, передачи и обработки данных.

Основные типы внутренних угроз:

- Намеренные преступные воздействия личного персонала организации.

- Не намеренные действия и погрешности сотрудников.

- Отказ технических средств и оборудования.

- Сбои ПО средств обработки данных.

Внешние и внутренние угрозы очень тесно взаимодействуют. К примеру, общая тенденция криминализации хозяйственных деяний ведет к понижению морально-этических норм персонала всех рангов, зачастую толкает их на действия, которые наносят ущерб компании.

Соотношение внешних и внутренних угроз в соответствии с характерными показателями: 81,7% угроз выполняется или самим персоналом организаций, или при их прямом или опосредованном участии (внутренние угрозы); 17,3% угроз — преступные действия или внешние угрозы; 1,0% угроз — это угрозы со стороны случайных лиц.

Объектами разных угроз в коммерческой деятельности есть:

- Человеческие ресурсы (сотрудники, персонал, компаньоны и другие), включая кадровые и трудовые ресурсы.

- Материальные ресурсы.

- Финансовые ресурсы.

- Временные ресурсы.

Информационные ресурсы, которые включают интеллектуальные ресурсы (незавершенные проектно-конструкторские разработки, патенты, ноу-хау, программные продукты, массивы статистической и бухгалтерской информации и прочее).

Более опасным источником угроз компаниям является собственный персонал. Мотивами внутренних угроз в данном случае представляет собой безответственность, личные побуждения (корыстные интересы, самоутверждение), некомпетентность (небольшая квалификация). [9]

В обстоятельствах сохраняющейся большой степени монополизации русской экономики угрозу предпринимательству предполагает бесчестная конкуренция, которая представляет собой:

1) Все действия, которые ведут к тому, что потребитель может принять компанию, товары, коммерческую или промышленную деятельность этой организации за компанию, товары, коммерческую или промышленную деятельность конкурента.

2) Ложные заявления в ходе коммерческих деяний, дискредитирующие компании, товары, коммерческую или промышленную деятельность конкурента.

3) Применение в ходе коммерческих деяний обозначений или указаний, которые ведут потребителя в заблуждение касательно природы, характеристик, способа изготовления, пригодности для конкретных целей или числа товаров.

Применение угроз в этом случае понижает надежность и эффективность работоспособности организаций, а в иных случаях, приводят к завершению их деятельности из-за опасности социального, экономического, организационного, правового, экологического, информационного, криминального и технического характера. Объектами угроз могут являться элементы личного («человеческого»), вещественного, финансового, информационного и иного капитала, которые состоят в экономической основе деятельности предпринимательства.

Любая угроза несет за собой особый ущерб (потерю) — материальные или моральные, а способы по противодействию данной угрозе призваны уменьшить ее величину до применимого уровня.

Оценка вероятных ущербов (потерь) подразумевает знание типов потерь, которые связаны с предпринимательской деятельностью, и знание вычисления их возможной прогнозной величины. Есть такие типы вероятных потерь (ущербов):

1) Материальные типы потерь появляются в непредусмотренных предпринимательским проектом добавочных затратах или направленных потерь оборудования, продукции, имущества, сырья, энергии и так далее.

2) Трудовые потери — потери трудового времени, которые вызваны непредвиденными, случайными обстоятельствами; меряются в часах трудового времени. Перевод рабочих потерь в финансовое выражение выполняется путем умножения рабочего времени на стоимость (цену) одного часа.

3) Кадровые потери — потери требуемых компании высококвалифицированных, профессиональных работников; меряются в затратах на обучение и подбор нового кадрового персонала в денежном эквиваленте.

4) Финансовые потери — прямонаправленный денежный ущерб, который связан с непредвиденными платежами, уплатой дополнительных налогов, выплатой штрафов, потерей финансов и ценных бумаг.

5) Временные потери. Совершаются, когда процесс предпринимательской деятельности идет медленнее, чем должен. Прямая оценка данных потерь выполняется в часах, неделях, днях, месяцах запаздывания в получении указанного результата. Чтобы переделать оценку потери времени в финансовое измерение, требуется установить, к каким потерям прибыли, дохода способны привести утеря времени. В итоге оцениваются в денежном эквиваленте.

6) Информационные потери. Является одним из самых серьезных потерь в бизнесе, которые способны привести к провалу всей компании. Исчисляются в финансовом выражении.

7) Особые типы потерь появляются в виде нанесения убытка жизни и здоровью людей, престижу предпринимателя, окружающей среде, а также вследствие иных неблагоприятных морально – психологических и социальных последствий.

Информационный ущерб (потери) связан с наявностью в процессе предпринимательской деятельности информационного риска, введенный в общий предпринимательский риск.

Информационный риск - возможность (угроза) утери активов субъекта экономики (предпринимателя) в итоге потерь, порчи, разглашения и искажения информации.

Информационный риск классифицируется таким образом:

- риск прерывания информации (окончание нормальной обработки данных, к примеру, вследствие разрушения, вывода из строя вычислительных средств). Данная категория действий может нести очень серьезные последствия, даже когда информация при этом не подвергается никакому воздействию;

- риск кражи данных (копирование или считывание информации, кражи магнитных носителей данных и итогов печати с целью получения информации, которые в дальнейшем могут применить против интересов собственника (владельца) данных);

- риск модификации данных (ввод несанкционированных изменений в информацию, которая направленна на причинение убытка собственника (владельца) данных);

- риск уничтожения данных (необратимое изменение данных, которое приводит к неосуществимости ее применения);

- риск электромагнитного влияния и перехвата данных в автоматизированных и информационных системах (АИС);

- риск съема данных по акустическому каналу;

- риск прекращения питания автоматизированных и информационных систем и поддерживающей инфраструктуры);

- риск ошибки поставщиков и операторов информационных ресурсов автоматизированных и информационных систем;

- риск сбоев ПО в автоматизированных и информационных системах;

- риск неполадок аппаратных устройств в автоматизированных и информационных системах (в результате халатных действий персонала, природных катаклизмов, несоблюдения техники безопасности, сбоев программных средств и так далее).

В заключительном итоге все противоправные действия приводят к нарушению конфиденциальности, достоверности, доступности и целостности данных.

В этом случае, перечень угроз и источников их появления достаточно разнообразен и предложенная разновидность не есть исчерпывающей. Противодействие появлениям угроз выполняется по разным направлениям, с применением полного арсенала средств и методов защиты.

2.2 Наиболее распространенные угрозы доступности.

С точки зрения размера ущерба, нанесенного определенной компании с компьютерной информационной системой, самыми частыми и опасными являются непреднамеренные ошибки различных сотрудников компании, которые и обслуживают информационную систему. [12]

В большинстве случаев. Эти ошибки и являются угрозами. Не правильно ввели данные или сделали ошибку в программе, которая вызвала крах в системе, создает уязвимые места, которыми легко могут воспользоваться злоумышленники. Обычно это ошибки администрирования компьютерных информационных систем, которые составляют до 65% потерь.

Т.е., можно сделать вывод, что наилучшим способом борьбы с этими ошибками являются автоматизация информационных систем и жесткий контроль на предприятии.

Остальные угрозы доступности можно классифицировать по компонентам компьютерных информационных систем, на которые и нацелены угрозы. К ним можно отнести отказ смой информационной системы, также отказ пользователя ИС и отказ поддерживающей инфраструктуры.

Отказ пользователей обычно случается о нежелания работать в данной ИС – необходимость обучаться информационной системе и т.д. Сюда же можно отнести отсутствие подготовки для работы в компьютерной информационной системе – это отсутствие компьютерной грамотности, неумение работать с диагностическими сообщениями, отсутствие знаний при работе с документацией.

Так же проблемой отказа пользователя от работы в информационной системе может быть распространенный недостаток – отсутствие технической поддержки по данной ИС, т.е. не полная документация, отсутствие справочной информации, отсутствие горячей линии ля информационных систем глобального и сложного характера и т.д.

К внутренним отказам можно отнести отступление от установленных правил эксплуатации, которое может быть как случайное, так и умышленное. Также из-за случайных или преднамеренных действий пользователей или персонала, обслуживающего информационную компьютерную систему, может выйти система из штатного режима эксплуатации. Примерами может быть превышение числа запросов в ИС, слишком большой обьем обрабатываемой информации и т.п.

К источникам внутренних отказов ИС так же можно отнести ошибки при конфигурации или переконфигурации системы, отказ как программного, так и аппаратного обеспечения, разрушение данных информационной системы, также повреждение или вообще разрушение аппаратуры.

По отношению к поддерживаемой инфраструктуре информационных компьютерных систем можно отнести угрозы нарушение, как случайного, так и умышленного, систем связи, теплоснабжения, водоснабжения, кондиционирования, электропитания и т.д. [18]

Так же к этим угрозам рекомендуемо относить разрушение и повреждение помещений, а так же угрозы связанные с обслуживающим персоналом и/или пользователей, связанные с невозможностью или нежеланием исполнять свои же обязанности. Это террористические акты или их угроза, забастовки, революции и т.д.

К одним из самых опасных угроз можно отнести так называемые «обиженные» сотрудники как нынешние, так и бывшие. Обычно они стремятся нанести предприятию какой-либо вред – испортить оборудование, запустить вирус, удалить данные и т.п.

Обиженные сотрудники хорошо знакомы с порядками компании и способны нанести любой всевозможный вред. Т.е. важно следить, чтобы при увольнении сотрудников его права доступа к информационным ресурсам предприятия анулировались.

2.3 Некоторые примеры угроз доступности

Примерами таких угроз являются популярны и очень вредоносные угрозы как грозы, электромагнитные импульсы высоких напряжений, отказы систем кондиционирования, протечки систем водоснабжения, теплоснабжения и канализации. [12]

Агрессивное потребление ресурсов, таких как вычислительные возможности процессора или оперативной памяти, полосы пропускания сетей и т.п., является средством вывода системы из штатного режима эксплуатации. Такое потребление можно разделить по расположению источника на локальное и удаленное. К примеру, локальная программа при просчетах в конфигурации системы способна

монополизировать процессор и/или физическую память, сведя скорость выполнения других программ к нулю.

Если пропускная способность канала до цели атаки превышает пропускную способность атакующего, то традиционная атака типа «отказ в обслуживании» не будет успешной. Распределенная ж атака в свою очередь происходит уже сразу с нескольких точек Интернета, что приводит к введению атакуемого узла из строя из-за резкого возрастания трафика. Т.е. злоумышленник может со всех узлов, задействованных в атаке, послать большой объем данных. И узел не сможет обрабатывать запросы от нормальных пользователей из-за превышения трафика.

2.4 Основные угрозы целостности

На втором месте по размерам ущерба стоят **кражи** и **подлоги**. В 1992 году в результате подобных противоправных действий с использованием персональных компьютеров американским организациям был нанесен общий ущерб в размере 882 миллионов долларов. Многие организации по понятным причинам скрывают такие инциденты; не вызывает сомнений, что в наши дни ущерб от такого рода действий вырос многократно, поэтому можно предположить, что реальный ущерб был намного больше. [13]

Обычно виновниками оказывались штатные сотрудники организаций, которые хорошо знакомые с режимом работы и мерами защиты, что подтверждает опасность внутренних угроз.

Нарушение статической целостности злоумышленник (чаще всего штатный сотрудник) может ввести неверные данные или изменить данные, когда изменяются содержательные данные, когда – служебная информация.

Угрозой целостности является фальсификация или изменение данных, а также отказ от совершенных действий. Компьютерные данные не могут рассматриваться в качестве доказательства, если нет средств обеспечить "неотказуемость". Не только данные, но и программы являются потенциально уязвимы с точки зрения нарушения целостности.

2.5 Основные угрозы конфиденциальности

Саму информацию конфиденциальности можно разделить на служебную и предметную. Служебная информация (к примеру, пароли пользователей) в компьютерной информационной системе играет техническую роль, но раскрытие ее является более опасной, из-за получения с ее помощью несанкционированного доступа ко всей информации системы,в том числе и предметной, т.к. в общем она не относится к определенной предметной области. [12]

Угрозы конфиденциальности информации могут носить некомпьютерный и вообще нетехнический характер даже если информация хранится в компьютере или предназначена для компьютерного использования.

К перехвату данных можно отнести прослушивание или подслушивание разговоров, изучение рабочего места, пассивное прослушивание сети и анализ каких-либо памятных дат и последовательностей.

К подмене данных относится использование страховых копий. На основных носителях для защиты данных используют развитые системы управления доступом, но за копии, которые нередко просто лежат где-угодно никто не заботится и многие могут получить к ним доступ.

Значимой и распространенной угрозой является кража оборудования, часто возникает из-за нахождения без присмотра ноутбуков и хендлетов, резервных носителей на работе или в автомобиле, которые просто теряются.

Так же распространённой угрозой являются методы морально-психологического воздействия (маскарад) – выполнение действий под видом лица, обладающего полномочиями для доступа к данным.

Неприятными угрозами, от которых трудно защитится являются злоупотребление полномочиями. К примеру, системный администратор способен прочитать любой файл, получить доступ к почте любого пользователя и т.д., также возможно нанесение ущерба при сервисном обслуживании, т.к. сервисный инженер получает неограниченный доступ к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

2.6 Статистика угроз безопасности

На рисунках 2 и 3 приведены диаграммы средней статистики угроз безопасности информационных систем (2015). [14]

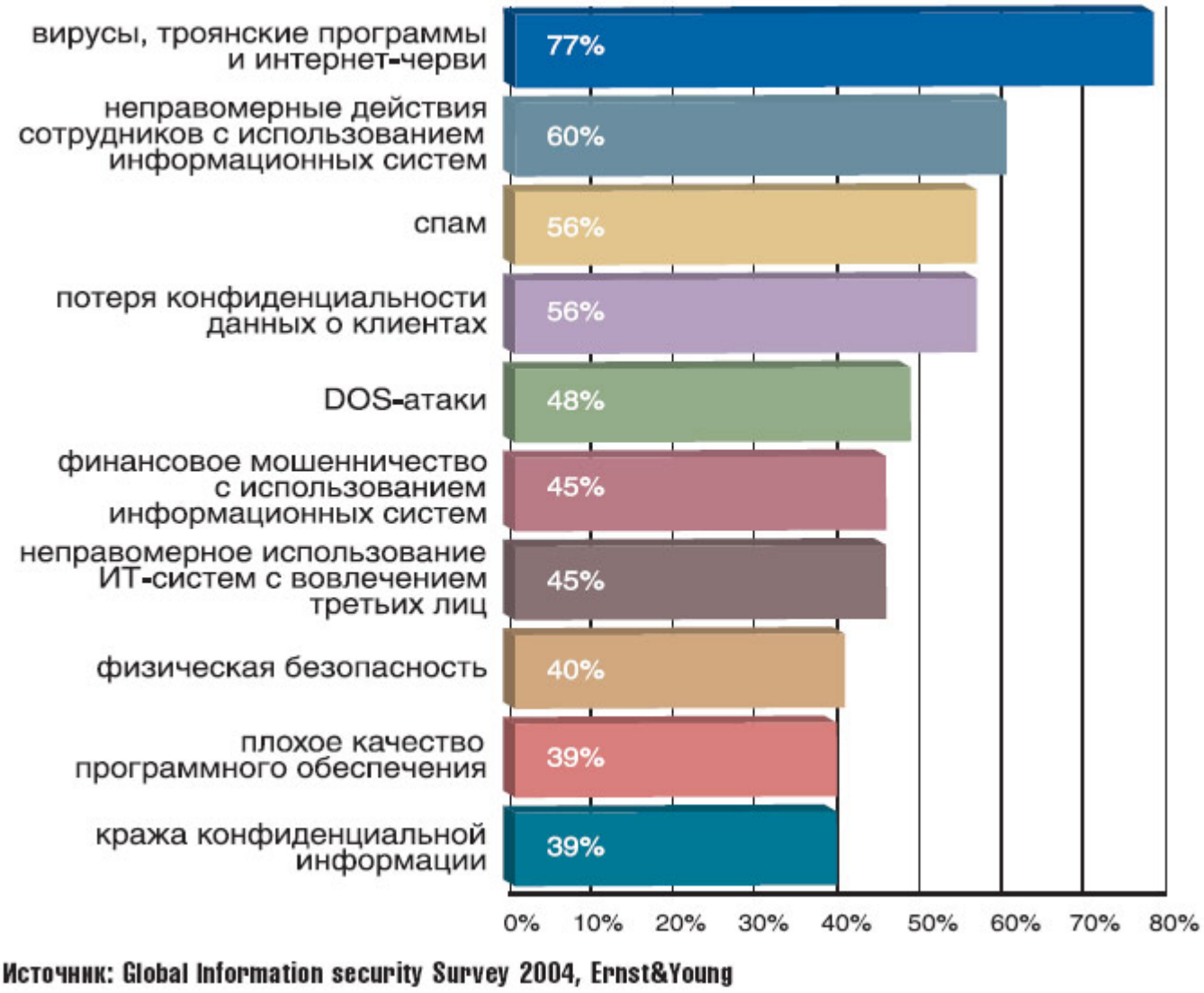

Рисунок 2. Угрозы безопасности

Рисунок 3. Угрозы безопасности

ЗАКЛЮЧЕНИЕ

В данной работе была описана значимая часть информационной безопасности – угрозы. Описаны понятия и виды угроз безопасности в компьютерных информационных системах.

ИБ относится к числу направлений деятельности, которые развиваются очень быстрыми темпами. Этому способствуют как общий прогресс информационных технологий, так и постоянное противоборство между теми, кто хочет добыть конфиденциальные данные и желающими ее сберечь.

Опыт показывает, что для достижения действующих решений по защите информации требуется сочетание правовых, технических и организационных мероприятий. То есть обеспечение защиты данных и в целом ИБ нынешних ИС нуждается в комплексном подходе. Оно невозможно без использования обширного спектра защитных средств, которые объединены в обдуманную архитектуру

В данных условиях положение по отношению к защите данных должна быть очень динамичной. Теоретические воззрения, стандарты, сложившиеся порядки требуется всегда сверять с условиями практики. От вероятных атак на

информацию не защититься без целенаправленной и систематической работы в этом направлении. Настоящее состояние безопасности нуждается в каждодневном внимании всех заинтересованных сторон.

В работе описали определения и критерия классификации угроз, проанализировали наиболее распространенные угрозы доступности с примерами, описали угрозы вредоносного ПО, рассмотрели основные угрозы целостности и конфиденциальности.

Также наведена статистика угроз безопасности в 2015 г. в России.

Вкратце угрозы можно изобразить на ниже приведенном рисунке 4.

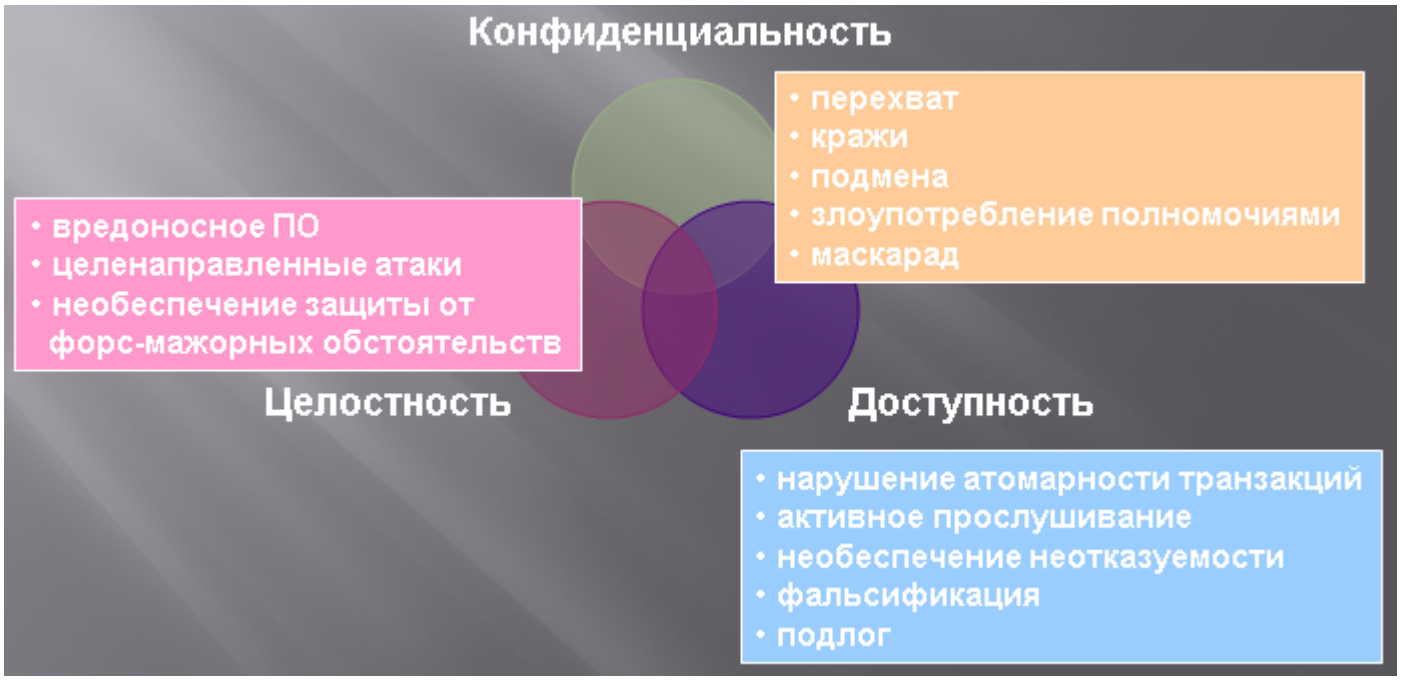

Рисунок 4. Угрозы информационной безопасности

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. Алексенцев А.И. Понятие и структура угроз защищаемой информации // Безопасность информационных технологий, № 3, 2000.
2. Бачило И.Л. Информационное право: основы практической информатики. Учебное пособие. – М: 2001. – 352 с.
3. Башлы П.Н. Информационная безопасность. Учебное пособие. Ростов н/Д: Феникс, 2006. – 253 с.

4. Вихорев С.В. Сетевые атаки и системы информационной безопасности 2001 // Cnews.ru, 2002 г.
5. Галатенко В.А. Основы информационной безопасности. Курс лекций. Учебное пособие. Третье издание.- М.: ИНТУИТ.РУ, 2006.- 208 с.
6. Герасименко В.А. Защита информации в АСОД (в двух частях). – М.: Энергоатомиздат, 1994.
7. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.
8. ГОСТ 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
9. Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии. Учебное пособие для студентов вузов. – М.: «Академия», 2009. – 416 с.
10. Девянин П.Н. и др. Теоретические основы компьютерной безопасности. Учебное пособие для студентов вузов. – М.: «Радио и связь», 2000. – 192 с.
11. Доктрина информационной безопасности Российской Федерации.
12. Журавленко Н.И., Кадулин В.Е., Борзунов К.К. Основы информационной безопасности: Учебное пособие.- Уфа: РИЦ БашГУ, 2007.-182 с.
13. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учеб. пособие. – М.: Логос, 2001. – 264 с.
14. Зегжда Д., Ивашко А. Основы безопасности информационных систем.
15. Каторин Ю.Ф. и др. Большая энциклопедия промышленного шпионажа. – СПб.: «Издательство Полигон», 2000. – 896 с.
16. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие.- М.: Горячая линия-Телеком, 2004.- 280 с.
17. Милославская Н.Г., Толстой А.И. Интрасети: обнаружение вторжений. Учеб. Пособие для вузов. – М.: ЮНИТИ-ДАНА, 2001. – 587 с.
18. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие для студентов учреждений среднего профессионального образования. – М.: ФОРУМ: ИНФРА-М, 2002. – 386с.
19. Садердинов А. А. и др. Информационная безопасность предприятия. Учеб. пособие Дашков и К, 2004.-336 с.
20. Филин С.А. Информационная безопасность. Учебное пособие. – М.:Альфа – Пресс, 2006. – 412 с.
21. Ярочкин В.И. Информационная безопасность. – М: «Гаудеамус», 2004. – 543 с.