Угрозы безопасности информации в информационно-вычислительных системах

Информационная безопасность (ИБ) в самом широком смысле – это совокупность средств защиты информации от случайного или преднамеренного воздействия. Независимо от того, что лежит в основе воздействия: естественные факторы или причины искусственного характера – владелец информации несет убытки.

Принципы информационной безопасности:

* **Целостность** информационных данных означает способность информации сохранять изначальный вид и структуру как в процессе хранения, как и после неоднократной передачи. Вносить изменения, удалять или дополнять информацию вправе только владелец или пользователь с легальным доступом к данным.
* **Конфиденциальность** – характеристика, которая указывает на необходимость ограничить доступа к информационным ресурсам для определенного круга лиц. В процессе действий и операций информация становится доступной только пользователям, который включены в информационные системы и успешно прошли идентификацию.
* **Доступность** информационных ресурсов означает, что информация, которая находится в свободном доступе, должна предоставляться полноправным пользователям ресурсов своевременно и беспрепятственно.
* **Достоверность** указывает на принадлежность информации доверенному лицу или владельцу, который одновременно выступает в роли источника информации.

Обеспечение и поддержка информационной безопасности включают комплекс разноплановых мер, которые предотвращают, отслеживают и устраняют несанкционированный доступ третьих лиц. Меры ИБ направлены также на защиту от повреждений, искажений, блокировки или копирования информации. Принципиально, чтобы все задачи решались одновременно, только тогда обеспечивается полноценная, надежная защита.

Особенно остро ставятся основные вопросы об информационном способе защите, когда взлом или хищение с искажением информации потянут за собой ряд тяжелых последствий, финансовых ущербов.

Созданная с помощью моделирования логическая цепочка трансформации информации выглядит следующим образом:

УГРОЖАЮЩИЙ ИСТОЧНИК ⇒ ФАКТОР УЯЗВИМОСТИ СИСТЕМЫ ⇒ ДЕЙСТВИЕ (**УГРОЗА БЕЗОПАСНОСТИ**) ⇒ АТАКА ⇒ ПОСЛЕДСТВИЯ

Разновидности угроз информационной безопасности

Угрозой информации называют потенциально возможное влияние или воздействие на автоматизированную систему с последующим нанесением убытка чьим-то потребностям.

На сегодня существует более 100 позиций и разновидностей угроз информационной системе. Важно проанализировать все риски с помощью разных методик диагностики. На основе проанализированных показателей с их детализацией можно грамотно выстроить систему защиты от угроз в информационном пространстве.

Классификация уязвимостей систем безопасности

Угрозы информационной безопасности проявляются не самостоятельно, а через возможное взаимодействие с наиболее слабыми звеньями системы защиты, то есть через факторы уязвимости. Угроза приводит к нарушению деятельности систем на конкретном объекте-носителе.

Основные уязвимости возникают по причине действия следующих факторов:

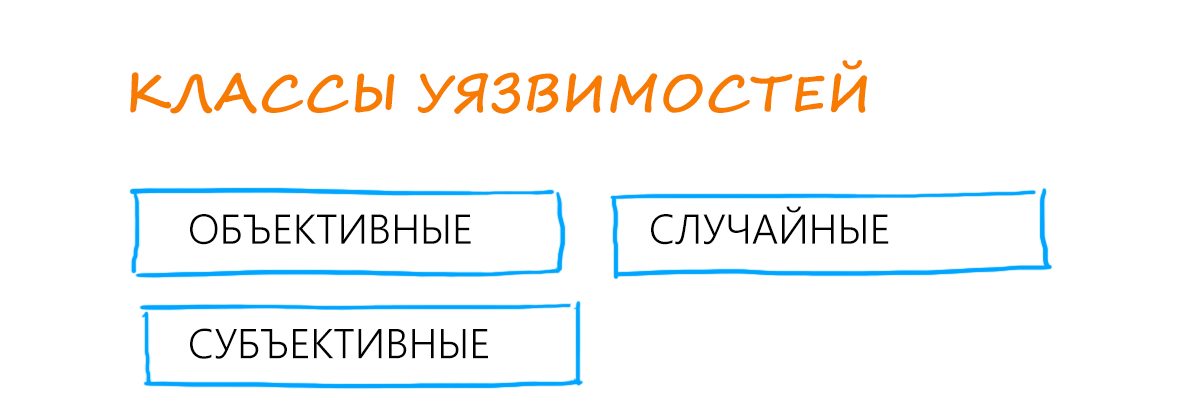
* несовершенство программного обеспечения, аппаратной платформы;
* разные характеристики строения автоматизированных систем в информационном потоке;
* часть процессов функционирования систем является неполноценной;
* неточность протоколов обмена информацией и интерфейса;
* сложные условия эксплуатации и расположения информации.

Чаще всего источники угрозы запускаются с целью получения незаконной выгоды вследствие нанесения ущерба информации. Но возможно и случайное действие угроз из-за недостаточной степени защиты и массового действия угрожающего фактора.

Существует разделение уязвимостей по классам, они могут быть:

* объективными;
* случайными;
* субъективными.

Если устранить или как минимум ослабить влияние уязвимостей, можно избежать полноценной угрозы, направленной на систему хранения информации.



Объективные уязвимости

Этот вид напрямую зависит от технического построения оборудования на объекте, требующем защиты, и его характеристик. Полноценное избавление от этих факторов невозможно, но их частичное устранение достигается с помощью инженерно-технических приемов, следующими способами:

**Связанные с техническими средствами излучения:**

* электромагнитные методики (побочные варианты излучения и сигналов от кабельных линий, элементов техсредств);
* звуковые варианты (акустические или с добавлением вибросигналов);
* электрические (проскальзывание сигналов в цепочки электрической сети, по наводкам на линии и проводники, по неравномерному распределению тока).

**Активизируемые:**

* вредоносные ПО, нелегальные программы, технологические выходы из программ, что объединяется термином «программные закладки»;
* закладки аппаратуры – факторы, которые внедряются напрямую в телефонные линии, в электрические сети или просто в помещения.

**Те, что создаются особенностями объекта, находящегося под защитой:**

* расположение объекта (видимость и отсутствие контролируемой зоны вокруг объекта информации, наличие вибро- или звукоотражающих элементов вокруг объекта, наличие удаленных элементов объекта);
* организация каналов обмена информацией (применение радиоканалов, аренда частот или использование всеобщих сетей).

**Те, что зависят от особенностей элементов-носителей:**

* детали, обладающие электроакустическими модификациями (трансформаторы, телефонные устройства, микрофоны и громкоговорители, катушки индуктивности);
* вещи, подпадающие под влияние электромагнитного поля (носители, микросхемы и другие элементы).

Случайные уязвимости

Эти факторы зависят от непредвиденных обстоятельств и особенностей окружения информационной среды. Их практически невозможно предугадать в информационном пространстве, но важно быть готовым к их быстрому устранению. Устранить такие неполадки можно с помощью проведения инженерно-технического разбирательства и ответного удара, нанесенного угрозе информационной безопасности:

**Сбои и отказы работы систем:**

* вследствие неисправности технических средств на разных уровнях обработки и хранения информации (в том числе и тех, что отвечают за работоспособность системы и за контроль доступа к ней);
* неисправности и устаревания отдельных элементов (размагничивание носителей данных, таких как дискеты, кабели, соединительные линии и микросхемы);
* сбои разного программного обеспечения, которое поддерживает все звенья в цепи хранения и обработки информации (антивирусы, прикладные и сервисные программы);
* перебои в работе вспомогательного оборудования информационных систем (неполадки на уровне электропередачи).

**Ослабляющие информационную безопасность факторы:**

* повреждение коммуникаций вроде водоснабжения или электроснабжения, а также вентиляции, канализации;
* неисправности в работе ограждающих устройств (заборы, перекрытия в здании, корпуса оборудования, где хранится информация).

Субъективные уязвимости

* Этот подвид в большинстве случаев представляет собой результат неправильных действий сотрудников на уровне разработки систем хранения и защиты информации. Поэтому устранение таких факторов возможно при помощи методик с использованием аппаратуры и ПО:

**Неточности и грубые ошибки, нарушающие информационную безопасность:**

* на этапе загрузки готового программного обеспечения или предварительной разработки алгоритмов, а также в момент его использования (возможно во время ежедневной эксплуатации, во время ввода данных);
* на этапе управления программами и информационными системами (сложности в процессе обучения работе с системой, настройки сервисов в индивидуальном порядке, во время манипуляций с потоками информации);
* во время пользования технической аппаратурой (на этапе включения или выключения, эксплуатации устройств для передачи или получения информации).

Нарушения работы систем в информационном пространстве:

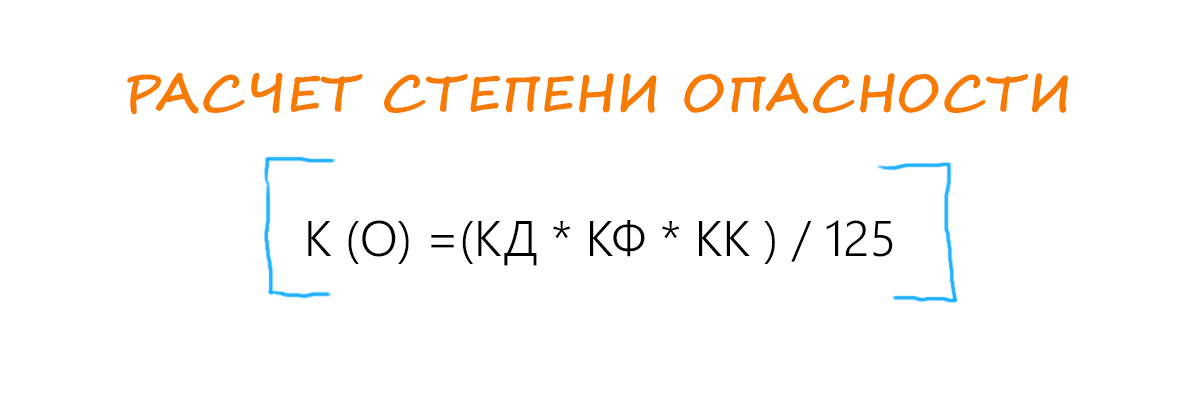
* режима защиты личных данных (проблему создают уволенные работники или действующие сотрудники в нерабочее время, они получают несанкционированный доступ к системе);
* режима сохранности и защищенности (во время получения доступа на объект или к техническим устройствам);
* во время работы с техустройствами (возможны нарушения в энергосбережении или обеспечении техники);
* во время работы с данными (преобразование информации, ее сохранение, поиск и уничтожение данных, устранение брака и неточностей).

Ранжирование уязвимостей

Каждая уязвимость должна быть учтена и оценена специалистами. Поэтому важно определить критерии оценки опасности возникновения угрозы и вероятности поломки или обхода защиты информации. Показатели подсчитываются с помощью применения ранжирования. Среди всех критериев выделяют три основных:

* **Доступность** – это критерий, который учитывает, насколько удобно источнику угроз использовать определенный вид уязвимости, чтобы нарушить информационную безопасность. В показатель входят технические данные носителя информации (вроде габаритов аппаратуры, ее сложности и стоимости, а также возможности использования для взлома информационных систем неспециализированных систем и устройств).
* **Фатальность** – характеристика, которая оценивает глубину влияния уязвимости на возможности программистов справиться с последствиями созданной угрозы для информационных систем. Если оценивать только объективные уязвимости, то определяется их информативность – способность передать в другое место полезный сигнал с конфиденциальными данными без его деформации.
* **Количество** – характеристика подсчета деталей системы хранения и реализации информации, которым присущ любой вид уязвимости в системе.

Каждый показатель можно рассчитать, как среднее арифметическое коэффициентов отдельных уязвимостей. Для оценки степени опасности используется формула. Максимальная оценка совокупности уязвимостей – 125, это число и находится в знаменателе. А в числителе фигурирует произведение из КД, КФ и КК.



Чтобы узнать информацию о степени защиты системы точно, нужно привлечь к работе аналитический отдел с экспертами. Они произведут оценку всех уязвимостей и составят информационную карту по пятибалльной системе. Единица соответствует минимальной возможности влияния на защиту информации и ее обход, а пятерка отвечает максимальному уровню влияния и, соответственно, опасности. Результаты всех анализов сводятся в одну таблицу, степень влияния разбивается по классам для удобства подсчета коэффициента уязвимости системы.

Какие источники угрожают информационной безопасности?

Если описывать классификацию угроз, которые обходят защиту информационной безопасности, то можно выделить несколько классов. Понятие классов обязательно, ведь оно упрощает и систематизирует все факторы без исключения. В основу входят такие параметры, как:

Ранг преднамеренности совершения вмешательства в информационную систему защиты:

* угроза, которую вызывает небрежность персонала в информационном измерении;
* угроза, инициатором которой являются мошенники, и делают они это с целью личной выгоды.
* Характеристики появления:
* угроза информационной безопасности, которая провоцируется руками человека и является искусственной;
* природные угрожающие факторы, неподконтрольные информационным системам защиты и вызывающиеся стихийными бедствиями.

Классификация непосредственной причины угрозы. Виновником может быть:

* человек, который разглашает конфиденциальную информацию, орудуя с помощью подкупа сотрудников компании;
* природный фактор, приходящий в виде катастрофы или локального бедствия;
* программное обеспечение с применением специализированных аппаратов или внедрение вредоносного кода в техсредства, что нарушает функционирование системы;
* случайное удаление данных, санкционированные программно-аппаратные фонды, отказ в работе операционной системы.

Степень активности действия угроз на информационные ресурсы:

* в момент обрабатывания данных в информационном пространстве (действие рассылок от вирусных утилит);
* в момент получения новой информации;
* независимо от активности работы системы хранения информации (в случае вскрытия шифров или криптозащиты информационных данных).

Существует еще одна классификация источников угроз информационной безопасности. Она основана на других параметрах и также учитывается во время анализа неисправности системы или ее взлома. Во внимание берется несколько показателей.

Классификация угроз

|  |  |
| --- | --- |
| Состояние источника угрозы | * в самой системе, что приводит к ошибкам в работе и сбоям при реализации ресурсов АС; * в пределах видимости АС, например, применение подслушивающей аппаратуры, похищение информации в распечатанном виде или кража записей с носителей данных; * мошенничество вне зоны действия АС. Случаи, когда информация захватывается во время прохождения по путям связи, побочный захват с акустических или электромагнитных излучений устройств. |
| Степень влияния | * активная угроза безопасности, которая вносит коррективы в структуру системы и ее сущность, например, использование вредоносных вирусов или троянов; * пассивная угроза – та разновидность, которая просто ворует информацию способом копирования, иногда скрытая. Она не вносит своих изменений в информационную систему. |
| Возможность доступа сотрудников к системе программ или ресурсов | * вредоносное влияние, то есть угроза информационным данным может реализоваться на шаге доступа к системе (несанкционированного); * вред наносится после согласия доступа к ресурсам системы. |
| Способ доступа к основным ресурсам системы | * применение нестандартного канала пути к ресурсам, что включает в себя несанкционированное использование возможностей операционной системы; * использование стандартного канала для открытия доступа к ресурсам, например, незаконное получение паролей и других параметров с дальнейшей маскировкой под зарегистрированного в системе пользователя. |
| Размещение информации в системе | * вид угроз доступа к информации, которая располагается на внешних устройствах памяти, вроде несанкционированного копирования информации с жесткого диска; * получение доступа к информации, которая показывается терминалу, например, запись с видеокамер терминалов; * незаконное проникание в каналы связи и подсоединение к ним с целью получения конфиденциальной информации или для подмены реально существующих фактов под видом зарегистрированного сотрудника. Возможно распространение дезинформации; * проход к системной области со стороны прикладных программ и считывание всей информации. |

При этом не стоит забывать о таких угрозах, как случайные и преднамеренные. Исследования доказали, что в системах данные регулярно подвергаются разным реакциям на всех стадиях цикла обработки и хранения информации, а также во время функционирования системы.

В качестве источника случайных реакций выступают такие факторы, как:

* сбои в работе аппаратуры;
* периодические шумы и фоны в каналах связи из-за воздействия внешних факторов (учитывается пропускная способность канала, полоса пропуска);
* неточности в программном обеспечении;
* ошибки в работе сотрудников или других служащих в системе;
* специфика функционирования среды Ethernet;
* форс-мажоры во время стихийных бедствий или частых отключений электропитания.

Погрешности в функционировании программного обеспечения встречаются чаще всего, а в результате появляется угроза. Все программы разрабатываются людьми, поэтому нельзя устранить человеческий фактор и ошибки. Рабочие станции, маршрутизаторы, серверы построены на работе людей. Чем выше сложность программы, тем больше возможность раскрытия в ней ошибок и обнаружения уязвимостей, которые приводят к угрозам информационной безопасности.

Часть этих ошибок не приводит к нежелательным результатам, например, к отключению работы сервера, несанкционированному использованию ресурсов, неработоспособности системы. Такие платформы, на которых была похищена информация, могут стать площадкой для дальнейших атак и представляют угрозу информационной безопасности.

Чтобы обеспечить безопасность информации в таком случае, требуется воспользоваться обновлениями. Установить их можно с помощью паков, выпускаемых разработчиками. Установление несанкционированных или нелицензионных программ может только ухудшить ситуацию. Также вероятны проблемы не только на уровне ПО, но и в целом связанные с защитой безопасности информации в сети.

Преднамеренная угроза безопасности информации ассоциируется с неправомерными действиями преступника. В качестве информационного преступника может выступать сотрудник компании, посетитель информационного ресурса, конкуренты или наемные лица. Причин для совершения преступления может быть несколько: денежные мотивы, недовольство работой системы и ее безопасностью, желание самоутвердиться.

Есть возможность смоделировать действия злоумышленника заранее, особенно если знать его цель и мотивы поступков:

* Человек владеет информацией о функционировании системы, ее данных и параметрах.
* Мастерство и знания мошенника позволяют ему действовать на уровне разработчика.
* Преступник способен выбрать самое уязвимое место в системе и свободно проникнуть к информации, стать угрозой для нее.
* Заинтересованным лицом может быть любой человек, как свой сотрудник, так и посторонний злоумышленник.
* Например, для работников банков можно выделить такие намеренные угрозы, которые можно реализовать во время деятельности в учреждении:
* Ознакомление сотрудников предприятия с информацией, недоступной для них.
* Личные данные людей, которые не трудятся в данном банке.
* Программные закладки с угрозами в информационную систему.
* Копирование программного обеспечения и данных без предварительного разрешения в личных целях.
* Кража распечатанной информации.
* Воровство электронных носителей информации.
* Умышленное удаление информации с целью скрытия фактов.
* Совершение локальной атаки на информационную систему.
* Отказы от возможного контроля удаленного доступа или отрицание факта получения данных.
* Удаление банковских данных самовольно из архива.
* Несанкционированная коррекция банковских отчетов лицом, не составляющим отчет.
* Изменение сообщений, которые проходят по путям связей.
* Самовольное уничтожение данных, которые повредились вследствие вирусной атаки.

Конкретные примеры нарушения защиты информации и доступа к данным

Несанкционированный доступ – один из самых «популярных» методов компьютерных правонарушений. То есть личность, совершающая несанкционированный доступ к информации человека, нарушает правила, которые зафиксированы политикой безопасности. При таком доступе открыто пользуются погрешностями в системе защиты и проникают к ядру информации. Некорректные настройки и установки методов защиты также увеличивают возможность несанкционированного доступа. Доступ и угроза информационной безопасности совершаются как локальными методами, так и специальными аппаратными установками.

С помощью доступа мошенник может не только проникнуть к информации и скопировать ее, но и внести изменения, удалить данные. Делается это с помощью:

* перехвата косвенных электромагнитных излечений от аппаратуры или ее элементов, от каналов связи, электропитания или сеток заземления;
* технологических панелей регулировки;
* локальных линий доступа к данным (терминалы администраторов системы или сотрудников);
* межсетевых экранов;
* методов обнаружения ошибок.

Из всего разнообразия методов доступа и угроз информации можно условно выделить основные преступления:

* Перехват паролей;
* «Маскарад»;
* Незаконное пользование привилегиями.

**Перехват паролей**– распространенная методика доступа, с которой сталкивалось большинство сотрудников и тех, кто занимается обеспечением информационной безопасности. Это мошенничество возможно с участием специальных программ, которые имитируют на экране монитора окошко для ввода имени и пароля. Введенные данные попадают в руки злоумышленника, и далее на дисплее появляется сообщение о неправильной работе системы. Затем возможно повторное всплывание окошка авторизации, после чего данные снова попадают в руки перехватчика информации, и так обеспечивается полноценный доступ к системе, возможно внесение собственных изменений. Есть и другие методики перехвата пароля, поэтому стоит пользоваться шифрованием паролей во время передачи, а сделать это можно с помощью специальных программ или RSA.

Способ угрозы информации**«Маскарад»** во многом является продолжением предыдущей методики. Суть заключается в действиях в информационной системе от лица другого человека в сети компании. Существуют такие возможности реализации планов злоумышленников в системе:

* Передача ложных данных в системе от имени другого человека.
* Попадание в информационную систему под данными другого сотрудника и дальнейшее совершение действий (с предварительным перехватом пароля).

Особенно опасен «Маскарад» в банковских системах, где манипуляции с платежами приводят компанию в убыток, а вина и ответственность накладываются на другого человека. Кроме того, страдают клиенты банка.

**Незаконное использование привилегий** – название разновидности хищения информации и подрыва безопасности информационной системы говорит само за себя. Именно администраторы наделены максимальным списком действий, эти люди и становятся жертвами злоумышленников. При использовании этой тактики происходит продолжение «маскарада», когда сотрудник или третье лицо получает доступ к системе от имени администратора и совершает незаконные манипуляции в обход системы защиты информации.

Но есть нюанс: в этом варианте преступления нужно перехватить список привилегий из системы предварительно. Это может случиться и по вине самого администратора. Для этого требуется найти погрешность в системе защиты и проникнуть в нее несанкционированно.

Угроза информационной безопасности может осуществляться на умышленном уровне во время транспортировки данных. Это актуально для систем телекоммуникаций и информационных сеток. Умышленное нарушение не стоит путать с санкционированными модификациями информации. Последний вариант выполняется лицами, у которых есть полномочия и обоснованные задачи, требующие внесения изменений. Нарушения приводят к разрыву системы или полному удалению данных.

Существует также угроза информационной безопасности, которая нарушает конфиденциальность данных и их секретность. Все сведения получает третье лицо, то есть посторонний человек без права доступа. Нарушение конфиденциальности информации имеет место всегда при получении несанкционированного доступа к системе.

Угроза защите безопасности информации может нарушить работоспособность компании или отдельного сотрудника. Это ситуации, в которых блокируется доступ к информации или ресурсам ее получения. Один сотрудник создает намеренно или случайно блокирующую ситуацию, а второй в это время натыкается на блокировку и получает отказ в обслуживании. Например, сбой возможен во время коммутации каналов или пакетов, а также угроза возникает в момент передачи информации по спутниковым системам. Их относят к первичным или непосредственным вариантам, поскольку создание ведет к прямому воздействию на данные, находящиеся под защитой.

Выделяют такие разновидности основных угроз безопасности информации в локальных размерах:

* **Компьютерные вирусы**, нарушающие информационную безопасность. Они оказывают воздействие на информационную систему одного компьютера или сети ПК после попадания в программу и самостоятельного размножения. Вирусы способны остановить действие системы, но в основном они действуют локально;
* **«Черви»** – модификация вирусных программ, приводящая информационную систему в состояние блокировки и перегрузки. ПО активируется и размножается самостоятельно, во время каждой загрузки компьютера. Происходит перегрузка каналов памяти и связи;
* **«Троянские кони»** – программы, которые внедряются на компьютер под видом полезного обеспечения. Но на самом деле они копируют персональные файлы, передают их злоумышленнику, разрушают полезную информацию.

Даже защитная система компьютера представляет собой ряд угроз защите безопасности. Поэтому программистам необходимо учитывать угрозу осмотра параметров системы защиты. Иногда угрозой могут стать и безобидные сетевые адаптеры. Важно предварительно установить параметры системы защиты, ее характеристики и предусмотреть возможные пути обхода. После тщательного анализа можно понять, какие системы требуют наибольшей степени защищенности (акцент на уязвимостях).

Раскрытие параметров системы защиты относят к непрямым угрозам безопасности. Дело в том, что раскрытие параметров не даст реализовать мошеннику свой план и скопировать информацию, внести в нее изменения. Злоумышленник только поймет, по какому принципу нужно действовать и как реализовать прямую угрозу защиты безопасности информации.

На крупных предприятиях методами, защищающими информационную безопасность, должна заведовать специальная служба безопасности компании. Ее сотрудники должны искать способы воздействия на информацию и устранять всевозможные прорывы злоумышленников. По локальным актам разрабатывается политика безопасности, которую важно строго соблюдать. Стоит обратить внимание и на исключение человеческого фактора, а также поддерживать в исправности все технические средства, связанные с безопасностью информации.

Наносимый ущерб

Степени и проявления ущерба могут быть разными:

* **Моральный и материальный ущерб**, нанесенный физическим лицам, чья информация была похищена.
* **Финансовый ущерб**, нанесенный мошенником в связи с затратами на восстановление систем информации.
* **Материальные затраты**, связанные с невозможностью выполнения работы из-за перемен в системе защиты информации.
* **Моральный ущерб**, связанный с деловой репутацией компании или повлекший нарушения взаимоотношений на мировом уровне.

Возможность причинения ущерба есть у лица, которое совершило правонарушение (получило несанкционированный доступ к информации, или произошел взлом систем защиты). Также ущерб может быть нанесен независимо от субъекта, обладающего информацией, а вследствие внешних факторов и воздействий (техногенных катастроф, стихийных бедствий). В первом случае вина ложится на субъекта, а также определяется состав преступления и выносится наказание посредством судебного разбирательства.

Возможно совершение деяния:

* с преступным умыслом (прямым или косвенным);
* по неосторожности (без умышленного причинения вреда).

Ответственность за правонарушение по отношению к информационным системам выбирается согласно действующему законодательству страны, в частности, по уголовному кодексу в первом случае. Если преступление совершено по неосторожности, а ущерб нанесен в малых размерах, то ситуацию рассматривает гражданское, административное или арбитражное право.

Ущербом информационного пространства считаются невыгодные для собственника (в данном случае информации) последствия, связанные с потерей материального имущества. Последствия проявляются в результате правонарушения. Выразить ущерб информационным системам можно в виде уменьшения прибыли или ее недополучения, что расценивается как упущенная выгода.

Главное, вовремя обратиться в суд и выяснить состав преступления. Ущерб нужно классифицировать согласно правовым актам и доказать его в судебном процессе, а еще важно выявить размер деяния личностей, размер их наказания на основе законодательства. Такими преступлениями и безопасностью чаще всего занимается киберполиция или служба безопасности страны в зависимости от объема и значимости вмешательства в информацию.

Этап защиты информации сегодня считается самым актуальным и требуется любому предприятию. Защищать нужно не только ПК, но и все техустройства, контактирующие с информацией. Все данные могут стать оружием в руках злоумышленников, поэтому конфиденциальность современных IT-систем должна находиться на высшем уровне.

Задержки у атакующей информационную безопасность стороны возможны только в связи с прохождением системы защиты. Абсолютных способов обезопасить себя от угроз не существует, поэтому информационную систему защиты требуется всегда усовершенствовать, поскольку мошенники тоже усовершенствуют свои методики. Пока не придуман универсальный способ, который подходит каждому и дает стопроцентную защиту. Важно остановить проникновение злоумышленников на раннем уровне.