Лекция 8:

Организация защиты информации в информационных технологиях

8.1. Угрозы безопасности информации, их виды

Автоматизированные информационные технологии позволили перейти на новый уровень в проблеме обработки и передачи информации. В частности, автоматизация решения задач и технология электронных телекоммуникаций позволили решить многие задачи повышения эффективности процессов обработки и передачи данных на предприятиях и в организациях.

Однако наряду с интенсивным развитием вычислительной техники и систем передачи информации все более актуальной становится проблема обеспечения безопасности и защиты данных в информационных технологиях.

Развитие средств, методов и форм автоматизации процессов хранения и обработки информации, массовое применение персональных компьютеров, внедрение информационных технологий на экономических объектах делают информацию гораздо более уязвимой. Информация, циркулирующая в ИТ, может быть незаконно изменена, похищена или уничтожена. Основными факторами, способствующими повышению ее уязвимости, являются следующие:

- увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации;
- сосредоточение в автоматизированных банках данных и локальных базах данных информации различного назначения и принадлежности;
- расширение круга пользователей, имеющих непосредственный доступ к ресурсам информационной технологии и информационной базы;
- усложнение режимов работы технических средств вычислительных систем;
- автоматизация коммуникационного обмена информацией, в том числе на большие расстояния.

Публикации в зарубежной печати последних лет показывают, что возможности злоупотребления информацией, передаваемой по каналам связи, развивались и совершенствовались не менее интенсивно, чем средства их предупреждения. Уже в 1974-1975 гг. в правительственных кругах США было раскрыто около 70 случаев несанкционированного проникновения в ЭВМ, которые нанесли ущерб в размере 32 млн долл. Важность решения проблемы по обеспечению защиты информации подтверждается затратами на защитные мероприятия. По опубликованным данным объем продаж средств физического контроля и регулирования в автоматизированных технологиях обработки информации в США в 1985 г. составлял более 570 млн долл; западногерманские эксперты по электронике определили, что в 1987 г. в Западной Европе промышленными фирмами, правительственными учреждениями и учебными заведениями было истрачено почти 1,7 млрд марок на обеспечение безопасности своих компьютеров.

Учитывая, что для построения надежной системы защиты данных в информационных технологиях требуются значительные материальные и финансовые затраты, необходимо

не просто разрабатывать частные механизмы защиты информации, а использовать целый комплекс мер, т. е. использовать специальные средства, методы и мероприятия с целью предотвращения потери данных. Таким образом, сегодня рождается новая современная технология - технология защиты информации в ИТ и в сетях передачи данных.

Технология защиты информации в ИТ включает в себя решение следующих проблем:

- обеспечение физической целостности информации, т. е. предотвращение искажения или уничтожения элементов информации;
- предотвращение подмены (модификации) элементов информации при сохранении ее целостности;
- предотвращение несанкционированного получения информации лицами или процессами, не имеющими на это соответствующих полномочий;
- использование передаваемых данных только в соответствии с обговоренными сторонами условиями.

Несмотря на предпринимаемые дорогостоящие меры, функционирование автоматизированных информационных технологий на различных предприятиях и в организациях выявило наличие слабых мест в защите информации. Для того, чтобы принятые меры оказались эффективными, необходимо определить:

- что такое угроза безопасности информации;
- выявить каналы утечки данных и пути несанкционированного доступа к защищаемой информации;
- определить потенциального нарушителя;
- построить эффективную систему защиты данных в информационных технологиях.

Угрозы безопасности делятся на *случайные (непреднамеренные) и умышленные.*

Источником случайных (непреднамеренных) угроз могут быть:

- отказы и сбои аппаратных средств в случае их некачественного исполнения и физического старения;
- помехи в каналах и на линиях связи от воздействия внешней среды;
- форсмажорные ситуации (пожар, выход из строя электропитания и т. д.);
- схемные системотехнические ошибки и просчеты разработчиков и производителей технических средств;
- алгоритмические и программные ошибки;
- неумышленные действия пользователей, приводящие к частичному или полному отказу технологии или разрушению аппаратных, программных, информационных ресурсов (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т. д.);
- неправомерное включение оборудования или изменение режимов работы устройств и программ;
- неумышленная порча носителей информации;
- запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в информационной технологии (форматирование или реструктуризация носителей информации, удаление данных и т. д.);
- нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим

необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях информации и т. д.);
- заражение компьютерными вирусами;
- неосторожные действия, приводящие к разглашению конфиденциальной информации или делающие ее общедоступной;
- разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т. д.);
- проектирование архитектуры технологии, разработка прикладных программ с возможностями, представляющими угрозу для работоспособности информационной технологии и безопасности информации;
- вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных носителей информации и т. д.);
- некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности экономического объекта;
- пересылка данных по ошибочному адресу абонента или устройства;
- ввод ошибочных данных;
- неумышленное повреждение каналов связи и т. д.

Меры защиты от таких угроз носят в основном организационный характер.

Злоумышленные или преднамеренные угрозы - результат активного воздействия человека на объекты и процессы с целью умышленной дезорганизации функционирования информационной технологии, вывода ее из строя, проникновения в систему и несанкционированного доступа к информации.

Умышленные угрозы, в свою очередь, делятся на следующие виды:

Пассивные угрозы направлены на несанкционированное использование информационный ресурсов, не оказывая при этом влияния на функционирование ИТ	**Активные угрозы** имеют целью нарушение нормального функционирования ИТ посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы

К пассивной угрозе относится, например, попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания.

К активным угрозам относятся, например, разрушение или радиоэлектронное подавление каналов связи, вывод из строя рабочих станций сети, искажение сведений в базах данных либо в системной информации в информационных технологиях и т. д.

Умышленные угрозы подразделяются также на следующие виды:

1.	Внутренние	возникают внутри управляемой организации. Они чаще всего сопровождаются социальной напряженностью и тяжелым моральным климатом на экономическом объекте, который провоцирует специалистов выполнять какие-либо правонарушения по отношению к информационным ресурсам
2.	Внешние	направлены на информационную технологию извне. Такие угрозы могут возникать из-за злонамеренных действий конкурентов, экономических условий и других причин (например, стихийных бедствий)

По данным зарубежных источников, в настоящее время широкое распространение получил *промышленный шпионаж*, наносящий ущерб владельцу коммерческой тайны. В процессе промышленного шпионажа выполняются незаконные сборы, присвоение и передача сведений, составляющих коммерческую тайну, лицом, не уполномоченным на это ее владельцем.

Практика функционирования информационных технологий показывает, что в настоящее время существует большое количество угроз безопасности информации. К основным угрозам безопасности информации и нормального функционирования информационной технологии относятся большое количество различных угроз, которые могут иметь *локальный* характер или *интегрированный*, т. е. совмещаться, комбинироваться или совпадать по своим действиям с другими видами угроз безопасности.

В целом можно выделить следующие умышленные угрозы безопасности данных в информационных технологиях (включая активные, пассивные, внутренние и внешние),

1. Раскрытие конфиденциальной информации - это бесконтрольный выход конфиденциальной информации за пределы информационной технологии или круга лиц, которым она была доверена по службе или стала известна в процессе работы.

Раскрытие конфиденциальной информации может быть следствием:

- разглашения конфиденциальной информации;
- утечки информации по различным, главным образом техническим, каналам (по визуально-оптическим, акустическим, электромагнитным и др.);
- несанкционированного доступа к конфиденциальной информации различными способами.

Иногда выделяют разглашение информации ее владельцем или обладателем путем умышленных или неосторожных действий должностных лиц и пользователей, которым соответствующие сведения в установленном порядке были доверены по службе или по работе, приведшие к ознакомлению с ними лиц, не допущенных к этим сведениям.

2. Несанкционированный доступ к информации выражается в противоправном преднамеренном овладении конфиденциальной информацией лицом, не имеющим права доступа к охраняемым сведениям.

Наиболее распространенными путями несанкционированного доступа к информации являются:

- перехват электронных излучений;
- принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции несущей;
- применение подслушивающих устройств (закладок);
- дистанционное фотографирование;
- перехват акустических излучений и восстановление текста принтера;
- чтение остаточной информации в памяти системы после выполнения санкционированных запросов;
- копирование носителей информации с преодолением мер защиты;
- маскировка под зарегистрированного пользователя ("маскарад");
- использование недостатков языков программирования и операционных систем;
- маскировка под запросы системы;

- использование программных ловушек;
- незаконное подключение к аппаратуре и линиям связи специально разработанных аппаратных средств, обеспечивающих доступ к информации;
- злоумышленный вывод из строя механизмов защиты;
- расшифровка специальными программами зашифрованной информации;
- информационные инфекции.

Перечисленные пути несанкционированного доступа требуют достаточно больших технических знаний и соответствующих аппаратных или программных разработок со стороны взломщика. Например, *используются технические каналы утечки* - это физические пути от источника конфиденциальной информации к злоумышленнику, посредством которых возможно получение охраняемых сведений. Причиной возникновения каналов утечки являются конструктивные и технологические несовершенства схемных решений либо эксплуатационный износ элементов. Все это позволяет взломщикам создавать действующие на определенных физических принципах преобразователи, образующие присущий этим принципам канал передачи информации - канал несанкционированного доступа.

Возможные пути утечки информации при обработке и передаче данных в автоматизированной информационной технологии

Однако есть и достаточно примитивные пути несанкционированного доступа:

- хищение носителей информации и документальных отходов;
- инициативное сотрудничество;
- склонение к сотрудничеству со стороны взломщика;
- выпытывание;
- подслушивание;
- наблюдение и другие пути.

Любые способы утечки конфиденциальной информации могут привести к значительному материальному и моральному ущербу как для организации, где функционирует информационная технология, так и для ее пользователей.

3. Компрометация информации (один из видов информационных инфекций). Реализуется, как правило, посредством несанкционированных изменений в базе данных, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений. При использовании скомпрометированной информации потребитель подвергается опасности принятия неверных решений.

4. Несанкционированное использование информационных ресурсов, с одной стороны, является последствиями ее утечки и средством ее компрометации. С другой стороны, оно имеет самостоятельное значение, так как может нанести большой ущерб управляемой системе (вплоть до полного выхода информационной технологии из строя) или ее абонентам.

5. Отказ от информации состоит в непризнании получателем или отправителем этой информации фактов ее получения или отправки. Это позволяет одной из сторон расторгать заключенные финансовые соглашения "техническим" путем, формально не отказываясь от них, нанося тем самым второй стороне значительный ущерб.

6. Нарушение информационного обслуживания представляет собой весьма существенную и распространенную угрозу, источником которой является сама автоматизированная информационная технология. Задержка с предоставлением информационных ресурсов абоненту может привести к тяжелым для него последствиям. Отсутствие у пользователя своевременных данных, необходимых для принятия решения, может вызвать его нерациональные действия.

7. Незаконное использование привилегий. Любая защищенная технология содержит средства, используемые в чрезвычайных ситуациях, или средства, которые способны функционировать с нарушением существующей политики безопасности. Например, на случай внезапной проверки пользователь должен иметь возможность доступа ко всем наборам системы. Обычно эти средства используются администраторами, операторами, системными программистами и другими пользователями, выполняющими специальные функции.

Большинство систем защиты в таких случаях используют наборы привилегий, т. е. для выполнения определенной функции требуется определенная привилегия. Обычно пользователи имеют минимальный набор привилегий, администраторы - максимальный.

Наборы привилегий охраняются системой защиты. Несанкционированный (незаконный) захват привилегий возможен при наличии ошибок в системе защиты, но чаще всего происходит в процессе управления системой защиты, в частности, при небрежном пользовании привилегиями.

Строгое соблюдение правил управления системой защиты, а также принципа минимума привилегий позволяет избежать таких нарушений.

Большинство из перечисленных технических путей утечки информации поддаются надежной блокировке при правильно разработанной и реализуемой на практике системе обеспечения безопасности.

8. "Взлом системы" - умышленное проникновение в информационную технологию, когда взломщик не имеет санкционированных параметров для входа. Способы взлома могут быть различными, и при некоторых из них происходит совпадение с ранее описанными угрозами. Например, использование пароля пользователя информационной технологии, который может быть вскрыт, например, путем перебора возможных паролей.

Следует отметить, что основную нагрузку защиты системы от взлома несет программа входа. Алгоритм ввода имени и пароля, их шифрование, правила хранения и смены паролей не должны содержать ошибок. Противостоять взлому системы поможет, например, ограничение попыток неправильного ввода пароля (т. е. исключить достаточно большой перебор) с последующей блокировкой персонального компьютера (рабочей станции) и уведомлением администратора в случае нарушения. Кроме того, администратор безопасности должен постоянно контролировать активных пользователей системы: их имена, характер работы, время входа и выхода и т. д. Такие действия помогут своевременно установить факт взлома и предпринять необходимые действия.

Реализация угроз безопасности информации в информационных технологиях приводит к различным видам прямых или косвенных потерь. Потери могут быть связаны с материальным ущербом:

- стоимость компенсации, возмещение другого косвенно утраченного имущества;

- стоимость ремонтно-восстановительных работ;
- расходы на анализ, исследование причин и величины ущерба;
- дополнительные расходы на восстановление информации, связанные с восстановлением работы и контролем данных и т. д.

Потери могут выражаться в ущемлении интересов экономического объекта, финансовых издержках или в потере клиентуры.

Специалистам информационных технологий следует помнить, что довольно большая часть причин и условий, создающих предпосылки и возможность неправомерного овладения конфиденциальной информацией, возникает из-за элементарных недоработок руководителей предприятий и организаций и их сотрудников. Например, к причинам и условиям, создающим предпосылки для утечки коммерческих секретов, могут относиться:

- недостаточное знание работниками организации правил защиты конфиденциальной информации и непонимание необходимости их тщательного соблюдения;
- использование неаттестованных технических средств обработки конфиденциальной информации;
- слабый контроль за соблюдением правил защиты информации правовыми, организационными и инженерно-техническими мерами;
- текучесть кадров, в том числе владеющих сведениями, составляющими коммерческую тайну;
- организационные недоработки, в результате которых виновниками утечки информации являются люди - сотрудники информационных технологий.

Необходимо отметить, что особую опасность в настоящее время представляет проблема компьютерных вирусов и вредоносных программ, т. к. эффективной защиты против них разработать не удалось.

Этот вид угроз может быть непосредственно связан с понятием "атака", который в настоящее время широко используется нарушителями против информационных технологий различных экономических объектов.

Например, атакой является применение любой из вредоносных программ. Среди атак на информационные технологии часто выделяют "маскарад" и "взлом системы", которые могут быть результатом реализации разнообразных угроз (или комплекса угроз).

В этой связи важно определить характеристику человека, который может реализовать угрозы безопасности информации в информационных технологиях.

Субъекты, совершившие противоправные действия по отношению к информации в информационных технологиях, называются *нарушителями*. Нарушителями в информационных технологиях экономического объекта являются, прежде всего, пользователи и работники ИТ, имеющие доступ к информации. По данным некоторых исследований, 81,7% нарушений совершается служащими организации, имеющими доступ к информационным технологиям, и только 17,3% - лицами со стороны (в том числе 1% приходится на случайных лиц).

Для определения потенциального нарушителя следует определить:

1. Предполагаемую категорию лиц, к которым может принадлежать нарушитель.

2. Мотивы действий нарушителей (цели, которые нарушители преследуют).
3. Квалификацию нарушителей и их техническую оснащенность (методы и средства, используемые для совершения нарушений).

1. Предполагаемая категория лиц. По отношению к информационной технологии нарушители могут быть *внутренними* (из числа персонала информационной технологии) или *внешними* (посторонние лица).

Внутренними нарушителями могут быть лица из следующих категорий персонала:

- специалисты (пользователи) информационной технологии;
- сотрудники-программисты, сопровождающие системное, общее и прикладное программное обеспечение;
- персонал, обслуживающий технические средства (инженерные работники информационной технологии);
- другие сотрудники, имеющие санкционированный доступ к ресурсам информационной технологии (в том числе подсобные рабочие, уборщицы, электрики, сантехники и т. д.);
- сотрудники службы безопасности информационной технологии;
- руководители различного уровня управления.

Доступ к ресурсам информационной технологии других посторонних лиц, не принадлежащих к указанным категориям, может быть ограничен организационно-режимными мерами. Однако следует также учитывать следующие категории посторонних лиц:

- посетители (лица, приглашенные по какому-либо поводу);
- клиенты (представители сторонних организаций или граждане, с которыми работают специалисты организации);
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности экономического объекта (энерго-, водо-, теплоснабжения и т. д.);
- представители конкурирующих организаций, иностранных спецслужб, лиц, действующих по их заданию и т. д. ;
- лица, случайно или умышленно нарушившие пропускной режим (даже без цели нарушения безопасности ИТ);
- любые лица за пределами контролируемой территории.

2. Мотивы действий нарушителей. Можно выделить три основных мотива нарушений:

Безответственность	Пользователь целенаправленно или случайно производит какие-либо разрушающие действия, не связанные со злым умыслом, которые, однако, могут привести к достаточно серьезным последствиям. В большинстве случаев такие действия являются следствием некомпетентности или небрежности
Самоутверждение	Специалист ИТ или пользователь хочет самоутвердиться в своих глазах или в глазах коллег, выполнив какие-либо действия, связанные с функционированием информационной технологии, доказывая свою высокую компетентность
Корыстный интерес	В этом случае пользователь будет целенаправленно пытаться преодолеть систему защиты для доступа к хранимой, передаваемой и

	обрабатываемой информации в ИТ. Даже если информационная технология имеет средства, делающие такое проникновение чрезвычайно сложным, полностью защитить ее от проникновения нарушителя практически невозможно

3. Квалификация нарушителей и их уровень технической оснащенности. По уровню квалификации всех нарушителей можно классифицировать по четырем классификационным признакам:

1. **По уровню знаний об информационной технологии** различают нарушителей:
   - знающих функциональные особенности информационной технологии, умеющих пользоваться штатными средствами;
   - обладающих высоким уровнем знаний и опытом работы с техническими средствами информационной технологии и их обслуживания;
   - обладающих высоким уровнем знаний в области программирования и вычислительной техники, проектирования и эксплуатации информационных технологий;
   - знающих структуру, функции и механизм действия средств защиты, их сильные и слабые стороны.
2. **По уровню возможностей** нарушителями могут быть:
   - применяющие агентурные методы получения сведений;
   - применяющие пассивные средства (технические средства перехвата без модификации компонентов информационной технологии);
   - использующие только штатные средства и недостатки систем защиты для ее преодоления (несанкционированные действия с использованием разрешенных средств), а также компактные машинные носители информации, которые могут быть скрытно пронесены через посты охраны;
   - применяющие методы и средства активного воздействия (модификация и подключение дополнительных устройств, внедрение программных "закладок" и т. д.).
3. **По времени действия** различают нарушителей действующих:
   - в процессе функционирования информационной технологии (во время работы компонентов системы);
   - в нерабочее время, во время плановых перерывов в работе информационной технологии, перерывов для обслуживания и ремонта и т. д. ;
   - как в процессе функционирования информационной технологии, так и в нерабочее время.
4. **По месту действия** нарушители могут быть:
   - имеющие доступ в зону управления средствами обеспечения безопасности ИТ;
   - имеющие доступ в зону данных;
   - действующие с автоматизированных рабочих мест (рабочих станций);
   - действующие внутри помещений, но не имеющие доступа к техническим средствам информационной технологии;
   - действующие с контролируемой территории без доступа в здания и сооружения;
   - не имеющие доступа на контролируемую территорию организации.

Определение конкретных значений характеристик потенциальных нарушителей в значительной степени субъективно. Поэтому все выше указанные характеристики рассматриваются в комплексе с учетом тщательной проверки каждой.