Тема 14. Обеспечение достоверности и защиты информации в ИОУ. 2 часа

Компьютеры стали привычным атрибутом нашей жизни и деятельности, однако расширение сфер их использования принесло не только известные удобства, но и множество проблем, наиболее серьезной из которых является проблема информационной безопасности.

Информационной безопасностью называют меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Под **безопасностью информации** понимается состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы от внутренних или внешних угроз. Другими словами – это состояние устойчивости информации к случайным или преднамеренным воздействиям, исключающее недопустимые риски ее уничтожения, искажения и раскрытия, которые приводят к материальному ущербу владельца или пользователя информации.

Обращает на себя внимание, что в определении термина информационная безопасность упоминаются внутренние угрозы. Существует статистика, по которой около 80% злоумышленников – штатные сотрудники компании

1. Классификация информации по уровню защиты

Применительно к уровню защиты информацию можно разделить на три категории:

- информация, составляющая государственную тайну;
- сведения, содержащие коммерческую тайну;
- персональные данные.

Владельцем информации, составляющей *государственную тайну*, является государство. Оно само выдвигает требования по ее защите и контролирует их исполнение Законом РФ «О государственной тайне» с изменениями на 22 августа 2004 г. Нарушение этих требований влечет за собой применение санкций, предусмотренных Уголовным кодексом РФ.

Сведения, содержащие коммерческую тайну. Информацией этой категории владеют предприятия, и поэтому они вправе ею распоряжаться и самостоятельно определять степень защиты. Вопросы законодательной защиты коммерческой тайны рассматриваются в Федеральном законе «О коммерческой тайне» от 29 июля 2004 г. №98-ФЗ

Персональные данные. Собственниками информации данной категории являемся мы сами. Осознавая степень важности этой информации и ее роль в обеспечении безопасности каждой отдельно взятой личности, государство рассматривает ее защиту как одну из своих важных задач.

Любая организация вне зависимости от размеров и формы собственности имеет достаточные объемы информации, которую необходимо защищать. К такой информации обычно относятся:

- вся информация, имеющая коммерческую значимость, а именно сведения о клиентах, поставщиках, новых разработках и ноу-хау, факты и содержание заключенных договоров с партнерами;
- данные о себестоимости продукции и услуг предприятия;
- результаты аналитических и маркетинговых исследований и вытекающие из них практические выводы;
- планы организации, тактика и стратегия действий на рынке;
- данные о финансовом состоянии организации, размерах окладов, премий, денежном наличном обороте.

2. Цели и задачи защиты информации

Основными *целями* защиты информации являются:

- предотвращение утечки, хищения, искажения, подделки;
- обеспечение безопасности личности, общества, государства;
- предотвращение несанкционированного ознакомления, уничтожения, искажения, копирования, блокирования информации в информационных системах;

- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных;
- сохранение государственной тайны, конфиденциальности документированной информации;
- соблюдение правового режима использования массивов, программ обработки информации, обеспечение полноты, целостности, достоверности информации в системах обработки;
- сохранение возможности управления процессом обработки и пользования информацией.

Основными *задачами* защиты информации традиционно считаются обеспечение:

- доступности (возможность за приемлемое время получить требуемую информационную услугу);
- конфиденциальности (защищенность информации от несанкционированного ознакомления);
- целостности (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- юридической значимости.

Наиболее подробно эти задачи рассматриваются при проведении мероприятий по сохранению государственной тайны. Формирование и развитие отечественного рынка, стремящегося к полноценной интеграции с мировой торговой системой, стимулируют интенсивное развитие индустрии информационной защиты.

Юридическая значимость информации приобретает важность в последнее время. Одной из причин этого является создание и развитие нормативно-правовой базы безопасности информации в нашей стране. Например, юридическая значимость актуальна при необходимости обеспечения строгого учета платежных документов и любых информационных услуг. Это экономическая основа работы информационных систем, она служит для соблюдения жесткой рег-

ламентации и регистрации доступа к информации при пользовании информационными ресурсами.

Развитие информационных технологий и клиентоориентированная деятельность организаций (особенно коммерческих) привели к возникновению новой задачи – *нотаризации*. Решение этой задачи обеспечивает юридически значимую регистрацию информации, что является очень важным при разборе возникающих конфликтов между заказчиками и исполнителями работ по информационному обслуживанию.

Проблемы информационной безопасности решаются, как правило, посредством создания специализированных систем защиты информации, которые должны обеспечивать безопасность информационной системы от несанкционированного доступа к информации и ресурсам, несанкционированных и непреднамеренных вредоносных воздействий. Система защиты информации является инструментом администраторов информационной безопасности, выполняющих функции по обеспечению защиты информационной системы и контролю ее защищенности.

Система защиты информации должна выполнять следующие *функции*:

- регистрация и учет пользователей, носителей информации, информационных массивов;
- обеспечение целостности системного и прикладного программного обеспечения и обрабатываемой информации;
- защита коммерческой тайны, в том числе с использованием сертифицированных средств криптозащиты;
- создание защищенного электронного документооборота с использованием сертифицированных средств криптопреобразования и электронной цифровой подписи;
- централизованное управление системой защиты информации, реализованное на рабочем месте администратора информационной безопасности;
- защищенный удаленный доступ мобильных пользователей на основе использования технологий виртуальных частных сетей (VPN);

- управление доступом;
- обеспечение эффективной антивирусной защиты.

Комплекс требований, которые предъявляются к системе информационной безопасности, предусматривает функциональную нагрузку на каждый из приведенных на рис. 6.1 уровней.

Рис. 1. Уровни защиты информационной системы

Организация защиты на *физическом уровне* должна уменьшить возможность несанкционированных действий посторонних лиц и персонала предприятия, а также снизить влияние техногенных источников.

Защита на *технологическом уровне* направлена на уменьшение возможных проявлений угроз безопасности информации, связанных с использованием некачественного программного продукта и технических средств обработки информации и некорректных действий разработчиков программного обеспечения. Система защиты на этом уровне должна быть автономной, но обеспечивать реализацию единой политики безопасности и строиться на основе использования совокупности защитных функций встроенных систем защиты операционной системы и систем управления базами данных и знаний.

На *локальном уровне* организуется разделение информационных ресурсов информационной системы на сегменты по степени конфиденциальности, территориальному и функциональному принципу, а также выделение в обособленный сегмент средств работы с конфиденциальной информацией. Повышению уровня защищенности способствуют ограничение и минимизация количества

точек входа/выхода (точек взаимодействия) между сегментами, создание надежной оболочки по периметру сегментов и информационной системы в целом, организация защищенного обмена информацией.

На *сетевом уровне* требуется организовать защищенный информационный обмен между автоматизированными рабочими местами, в том числе удаленными и мобильными, и создать надежную оболочку по периметру информационной системы в целом. Система защиты информации на этом уровне должна строиться с учетом реализации защиты предыдущих уровней. Основой организации защиты может служить применение программно-аппаратных средств аутентификации и защиты от несанкционированного доступа к информации.

На *пользовательском уровне* требуется обеспечить допуск только авторизованных пользователей к работе в информационной системе, создать защитную оболочку вокруг ее элементов, а также организовать индивидуальную среду деятельности каждого пользователя.

3. Классификация угроз информационной безопасности

Угрозами информационной безопасности называются потенциальные источники нежелательных событий, которые могут нанести ущерб ресурсам информационной системы.

По способу реализации выделяют следующие основные классы угроз безопасности, направленных против информационных ресурсов:

- угрозы, реализуемые либо воздействием на *программное обеспечение* и конфигурационную информацию системы, либо посредством некорректного использования системного и прикладного программного обеспечения;
- угрозы, связанные с выходом из строя *технических средств* системы, приводящим к полному или частичному разрушению информации, хранящейся и обрабатываемой в системе;
- угрозы, обусловленные *человеческим фактором* и связанные с некорректным использованием сотрудниками программного обеспечения или с воз-

действием на технические средства, в большей степени зависят от действий и «особенностей» морального поведения сотрудников;

- угрозы, вызванные *перехватом побочных электромагнитных излучений и наводок*, возникающих при работе технических средств системы, с использованием специализированных средств технической разведки.

Угрозы с использованием программных средств. Наиболее многочисленный класс угроз конфиденциальности, целостности и доступности информационных ресурсов связан с получением внутренними и внешними нарушителями логического доступа к информации с использованием возможностей, предоставляемых общесистемным и прикладным программным обеспечением.

Большинство рассматриваемых в этом классе угроз реализуется путем локальных или удаленных атак на информационные ресурсы системы внутренними и внешними нарушителями. Результатом осуществления этих угроз становится несанкционированный доступ к данным, управляющей информации, хранящейся на рабочем месте администратора системы, конфигурационной информации технических средств, а также к сведениям, передаваемым по каналам связи.

В этом классе выделяются следующие основные угрозы:

- использование сотрудниками чужого идентификатора;
- использование чужого идентификатора поставщиками услуг;
- использование чужого идентификатора посторонними;
- несанкционированный доступ к приложению;
- внедрение вредоносного программного обеспечения;
- злоупотребление системными ресурсами;
- отказ от подтверждения авторства передаваемой информации;
- ошибки при маршрутизации;
- использование телекоммуникаций для несанкционированного доступа сотрудниками организации, поставщиком услуг, посторонними лицами;
- неисправность средств сетевого управления, управляющих или сетевых серверов;

- сбои системного и сетевого программного обеспечения;
- сбои прикладного программного обеспечения.

Угрозы техническим средствам. Угрозы доступности и целостности информации (хранимой, обрабатываемой и передаваемой по каналам связи) связаны с физическими повреждениями и отказами технических средств системы и вспомогательных коммуникаций. Последствия реализации этого класса угроз могут привести к полному или частичному разрушению информации, отказу в обслуживании пользователей и их запросов к системе, невозможности вывода или передачи информации.

В этом классе выделяются следующие основные угрозы:

- пожар;
- затопление;
- природные катаклизмы;
- неисправности сетевого сервера, накопительного устройства, печатающих устройств, сетевых распределяющих компонентов, сетевых шлюзов, сетевых интерфейсов, электропитания, кондиционеров.

Угрозы, обусловленные человеческим фактором. Угрозы возникают вследствие умышленных или неумышленных действий персонала или посторонних лиц, приводящих к выходу из строя либо нештатной работе программных или технических средств информационной системы.

В этом классе выделяются следующие основные угрозы:

- ошибки операторов (ошибки администраторов при конфигурировании системы);
- ошибки пользователей при работе с системой;
- ошибки при работах с программным обеспечением (ошибки администраторов при проведении профилактических работ);
- ошибки при работах с оборудованием (ошибки сотрудников службы технической поддержки при проведении профилактических работ);
- кражи со стороны сотрудников.