Базовая информационная технология: технология защиты информации

1. Основные понятия и определения

Широкое внедрение различных информационных технологий, кроме позитивного влияния на все стороны деятельности человека, привело к появлению угроз безопасности. Возросли возможности нанесения ущербов, связанных с хищением информации, поскольку воздействовать на любые системы (социальные, биологические или технические) с целью их уничтожения, воровства ресурсов, снижения эффективности функционирования возможно, когда известна информация относительно их структуры и принципов функционирования. В связи с этим развивается и совершенствуется *технология защиты информации.*

Угроза – это потенциальная возможность определенным образом нарушить информационную безопасность.

Попытка реализации угрозы называется *атакой*, а тот, кто предпринимает такую попытку, – *злоумышленником*. Потенциальные злоумышленники называются источниками угрозы.

Защита информации – это деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Технологии защиты информации основываются на применении современных методов и средств, которые предотвращают утечку информации и ее потерю.

Методами защиты информации в ИС являются: препятствие; управление доступом; механизмы шифрования; противодействие атакам вредоносных программ; регламентация; принуждение; побуждение.

Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).

Управление доступом – методы защиты информации регулированием использования всех ресурсов ИС и ИТ. Эти методы должны противостоять всем возможным путям несанкционированного доступа к информации.

Управление доступом включает следующие функции зашиты:

- идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);
- опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;
- проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
- разрешение и создание условий работы в пределах установленного регламента;
- регистрацию (протоколирование) обращений к защищаемым ресурсам;

• реагирование (сигнализация, отключение, задержка работ, отказ в запросе и т.п.) при попытках несанкционированных действий.

Механизмы шифрования – криптографическое закрытие информации. Эти методы защиты все шире применяются как при обработке, так и при хранении информации на магнитных носителях. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.

Противодействие атакам вредоносных программ предполагает комплекс разнообразных мер организационного характера и использование антивирусных программ. Цели принимаемых мер – это уменьшение вероятности инфицирования АИС, выявление фактов заражения системы; уменьшение последствий информационных инфекций, локализация или уничтожение вирусов; восстановление информации в ИС. Овладение этим комплексом мер и средств требует знакомства со специальной литературой.

Регламентация – создание таких условий автоматизированной обработки, хранения и передачи защищаемой информации, при которых нормы и стандарты по защите выполняются в наибольшей степени.

Принуждение – метод защиты, при котором пользователи и персонал ИС вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Побуждение – метод защиты, побуждающий пользователей и персонал ИС не нарушать установленные порядки за счет соблюдения сложившихся моральных и этических норм.

Средствами защиты информации являются: физические; аппаратные; программные; организационные; законодательные; психологические.

Физические средства защиты информации предотвращают доступ посторонних лиц на охраняемую территорию. Основным и наиболее старым средством физического препятствия является установка прочных дверей, надежных замков, решеток на окна. Для усиления защиты информации используются пропускные пункты, на которых контроль доступа осуществляют люди (охранники) или специальные системы. С целью предотвращения потерь информации также целесообразна установка электронной противопожарной и охранной систем. Физические средства используются для охраны данных как на бумажных, так и на электронных носителях.

Аппаратные средства представлены устройствами, которые встраиваются в аппаратуру для обработки информации.

Программные средства – программы, отражающие хакерские атаки. Также к программным средствам можно отнести программные комплексы, выполняющие восстановление утраченных сведений. При помощи комплекса аппаратуры и программ обеспечивается резервное копирование информации – для предотвращения потерь.

Организационные средства сопряжены с несколькими методами защиты: регламентацией, управлением, принуждением. К организационным

средствам относится разработка должностных инструкций, беседы с работниками, комплекс мер наказания и поощрения. При эффективном использовании организационных средств работники предприятия хорошо осведомлены о технологии работы с охраняемыми сведениями, четко выполняют свои обязанности и несут ответственность за предоставление недостоверной информации, утечку или потерю данных.

Законодательные средства – комплекс нормативно-правовых актов, регулирующих деятельность людей, имеющих доступ к охраняемым сведениям и определяющих меру ответственности за утрату или кражу секретной информации.

Психологические средства – комплекс мер для создания личной заинтересованности работников в сохранности и подлинности информации. Для создания личной заинтересованности персонала руководители используют разные виды поощрений. К психологическим средствам относится и построение корпоративной культуры, при которой каждый работник чувствует себя важной частью системы и заинтересован в успехе предприятия.

2. Виды информационных угроз и способы защиты информации

Все виды информационных угроз можно разделить на две большие группы:

1) отказы и нарушения работоспособности программных и технических средств;

2) преднамеренные угрозы, заранее планируемые злоумышленниками для нанесения вреда. Этот вид информационных угроз можно разделить на две подгруппы:

• угрозы, реализация которых выполняется при постоянном участии человека;

• угрозы, реализация которых после разработки злоумышленником соответствующих компьютерных программ выполняется этими программами без непосредственного участия человека.

При информационных угрозах первого типа возникает опасность нарушения физической и логической целостности хранящихся в оперативной и внешней памяти структур данных из-за старения или износа ее носителей либо из-за некорректного использования возможностей компьютера; возможна потеря данных и другой важной для пользователя информации из-за неправильного использования программного обеспечения; разрушающего воздействия разного рода ошибок в программных средствах, не выявленных в процессе отладки и испытаний программ, а также ошибок, оставшихся в аппаратных средствах после их разработки, и т.п.

Помимо естественных способов выявления и своевременного устранения, указанных выше причин используют следующие специальные способы защиты информации от нарушений работоспособности компьютерных систем:

1) внесение структурной, временной, информационной и функциональной избыточности компьютерных ресурсов;

Структурная избыточность компьютерных ресурсов достигается за счет резервирования аппаратных компонентов и машинных носителей данных, организации замены отказавших и своевременного пополнения резервных компонентов. Структурная избыточность составляет основу остальных видов избыточности.

Временная избыточность или резерв времени используется на контроль и обнаружение искажений, на их диагностику и выработку решений по восстановлению информации, а также на реализацию операций восстановления.

Внесение информационной избыточности выполняется путем периодического или постоянного (фонового) резервирования данных на основных и резервных носителях. Зарезервированные данные обеспечивают восстановление случайно или преднамеренно уничтоженной и искаженной информации. Для восстановления работоспособности компьютерной системы после появления устойчивого отказа кроме резервирования обычных данных следует заблаговременно резервировать и системную информацию, а также подготавливать программные средства восстановления.

Функциональная избыточность компьютерных ресурсов достигается дублированием функций или внесением дополнительных функций в программно-аппаратные ресурсы вычислительной системы для повышения ее защищенности от сбоев и отказов, например периодическое тестирование и восстановление, а также самотестирование и самовосстановление компонентов компьютерной системы.

2) защита от некорректного использования ресурсов компьютерной системы;

Этот способ защиты заключается в корректном функционировании программного обеспечения с позиции использования ресурсов вычислительной системы. Программа может четко и своевременно выполнять свои функции, но некорректно использовать компьютерные ресурсы из-за отсутствия всех необходимых функций (например, изолирование участков оперативной памяти для операционной системы и прикладных программ, защита системных областей на внешних носителях, поддержка целостности и непротиворечивости данных).

3) выявление и своевременное устранение ошибок на этапах разработки программно-аппаратных средств.

Это достигается путем качественного выполнения базовых стадий разработки на основе системного анализа концепции, проектирования и реализации проекта.

Преднамеренные угрозы связаны с целенаправленными действиями нарушителя. В качестве нарушителя может быть служащий, посетитель, конкурент и т. д. Действия нарушителя могут быть обусловлены разными мотивами: недовольством служащего своей карьерой, сугубо материальным

интересом (взятка), любопытством, конкурентной борьбой, стремлением самоутвердиться любой ценой и т. п.

Вид преднамеренных информационных угроз можно разделить на две подгруппы:

• угрозы, реализация которых выполняется при постоянном участии человека;

• угрозы, реализация которых после разработки злоумышленником соответствующих компьютерных программ выполняется этими программами без непосредственного участия человека.

2.1. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности

Несанкционированный доступ к информации (НСД) – нарушение установленных правил разграничения доступа. Лицо или процесс, осуществляющие НСД к информации, являются нарушителями правил разграничения доступа.

Для достижения требуемого уровня информационной безопасности АС необходимо обеспечить противодействие этим угрозам и минимизировать возможное влияние «человеческого фактора». При этом ставятся задачи по защите информации:

• запрещение несанкционированного доступа к ресурсам вычислительных систем;

• невозможность несанкционированного использования компьютерных ресурсов при осуществлении доступа;

• своевременное обнаружение факта несанкционированных действий, устранение их причин и последствий.

Основным способом запрещения несанкционированного доступа к ресурсам вычислительных систем является подтверждение подлинности пользователей и разграничение их доступа к информационным ресурсам, включающего следующие этапы:

• идентификация;

• установление подлинности (аутентификация);

• авторизация.

Идентификация необходима для указания компьютерной системе уникального идентификатора обращающегося к ней пользователя. Идентификатор может представлять собой любую последовательность символов и должен быть заранее зарегистрирован в системе администратора службы безопасности. В процессе регистрации заносится следующая информация:

• фамилия, имя, отчество (при необходимости другие характеристики пользователя);

• уникальный идентификатор пользователя;

• имя процедуры установления подлинности;

• эталонная информация для подтверждения подлинности (например пароль);

• ограничения на используемую эталонную информацию (например время действия пароля);

• полномочия пользователя по доступу к компьютерным ресурсам.

Установление подлинности (аутентификация) заключается в проверке истинности полномочий пользователя.

Для особо надежного опознания при идентификации используются технические средства, определяющие индивидуальные характеристики человека (голос, отпечатки пальцев, структура зрачка). Наиболее массово используемыми являются парольные методы проверки подлинности пользователей. Пароли можно разделить на две группы: простые и динамически изменяющиеся.

Простой пароль не изменяется от сеанса к сеансу в течение установленного периода его существования.

Во втором случае пароль изменяется по правилам, определяемым используемым методом. Выделяют следующие методы реализации динамически изменяющихся паролей:

• методы модификации простых паролей. Например, случайная выборка символов пароля и одноразовое использование паролей;

• метод «запрос – ответ», основанный на предъявлении пользователю случайно выбираемых запросов из имеющегося массива;

• функциональные методы, основанные на использовании некоторой функции F с динамически изменяющимися параметрами (дата, время, день недели и др.), с помощью которой определяется пароль.

Для защиты от несанкционированного входа в компьютерную систему используются как общесистемные, так и специализированные программные средства защиты. После идентификации и аутентификации пользователя система защиты должна выполнить процедуру авторизации. Авторизация – это процедура предоставления законному субъекту, успешно прошедшему идентификацию и аутентификацию, соответствующих полномочий и доступных ресурсов системы (сети).

В качестве компьютерных ресурсов рассматриваются:

• программы;

• внешняя память (файлы, каталоги, логические диски);

• информация, разграниченная по категориям в базах данных;

• оперативная память;

• время (приоритет) использования процессора;

• порты ввода-вывода;

• внешние устройства.

Различают следующие виды прав пользователей по доступу к ресурсам:

• всеобщее (полное предоставление ресурса);

• функциональное или частичное;

• временное.

Наиболее распространенными способами разграничения доступа являются:

• разграничение по спискам (пользователей или ресурсов);

• использование матрицы установления полномочий (строки матрицы – идентификаторы пользователей, столбцы – ресурсы компьютерной системы);

• разграничение по уровням секретности и категориям (например, общий доступ, конфиденциально, секретно);

• парольное разграничение.

Одной из основных угроз хищения информации является угроза доступа к остаточным данным в оперативной и внешней памяти компьютера. Под остаточной информацией понимают данные, оставшиеся в освободившихся участках оперативной и внешней памяти после удаления файлов пользователя, удаления временных файлов без ведома пользователя, находящиеся в неиспользуемых хвостовых частях последних кластеров, занимаемых файлами, а также в кластерах, освобожденных после уменьшения размеров файлов и после форматирования дисков.

Примеры вспомогательных программных средств защиты информации:

• программы уничтожения остаточной информации (в блоках оперативной памяти, временных файлах и т. п.);

• программы аудита (ведения регистрационных журналов) событий, связанных с безопасностью КС, для обеспечения возможности восстановления и доказательства факта происшествия этих событий;

• программы имитации работы с нарушителем (отвлечения его на получение якобы конфиденциальной информации);

• программы тестового контроля защищенности КС и др.

2.2. Криптографические методы защиты и шифрование

Шифрование является основным средством обеспечения конфиденциальности. Так, в случае обеспечения конфиденциальности данных на локальном компьютере применяют шифрование этих данных, а в случае сетевого взаимодействия – шифрованные каналы передачи данных.

Науку о защите информации с помощью шифрования называют криптографией (криптография в переводе означает загадочное письмо или тайнопись).

Криптография применяется:

для защиты конфиденциальности информации, передаваемой по открытым каналам связи;

для аутентификации (подтверждении подлинности) передаваемой информации;

для защиты конфиденциальной информации при ее хранении на открытых носителях;

для обеспечения целостности информации (защите информации от внесения несанкционированных изменений) при ее передаче по открытым каналам связи или хранении на открытых носителях;

для обеспечения неоспоримости передаваемой по сети информации (предотвращения возможного отрицания факта отправки сообщения);

для защиты программного обеспечения и других информационных ресурсов от несанкционированного использования и копирования.

Задачей криптографии является обратимое преобразование некоторого понятного исходного текста (открытого текста) в кажущуюся случайной последовательность некоторых знаков, часто называемых шифротекстом, или криптограммой. В шифре выделяют два основных элемента – алгоритм и ключ. Алгоритм шифрования представляет собой последовательность преобразований обрабатываемых данных, зависящих от ключа шифрования. Ключ задает значения некоторых параметров алгоритма шифрования, обеспечивающих шифрование и дешифрование информации. В криптографической системе информация I и ключ K являются входными данными для шифрования и дешифрования информации. При похищении информации необходимо знать ключ и алгоритм шифрования.

По способу использования ключей различают два типа криптографических систем: симметрические и асимметрические.

В симметрических (одноключевых) криптографических системах ключи шифрования и дешифрования либо одинаковы, либо легко выводятся один из другого.

В асимметрических (двухключевых или системах с открытым ключом) криптографических системах ключи шифрования и дешифрования различаются таким образом, что с помощью вычислений нельзя вывести один ключ из другого.

Скорость шифрования в двухключевых криптографических системах намного ниже, чем в одноключевых. Поэтому асимметрические системы используют в двух случаях:

- для шифрования секретных ключей, распределенных между пользователями вычислительной сети;
- для формирования цифровой подписи.

Одним из сдерживающих факторов массового применения методов шифрования является потребление значительных временных ресурсов при программной реализации большинства хорошо известных шифров (DES, FEAL, REDOC, IDEA, ГОСТ).

2.3. Методы и средства противодействия атакам вредоносных программ

Подсистема защиты от компьютерных вирусов (специально разработанных программ для выполнения несанкционированных действий) является одним из основных компонентов системы защиты информации и процесса ее обработки в вычислительных системах.

Выделяют три уровня защиты от компьютерных вирусов:

- защита от проникновения в вычислительную систему вирусов известных типов;
- углубленный анализ на наличие вирусов известных и неизвестных типов, преодолевших первый уровень защиты;

• защита от деструктивных действий и размножения вирусов, преодолевших первые два уровня.

Поиск и обезвреживание вирусов осуществляются как автономными антивирусными программными средствами (сканеры), так и в рамках комплексных систем защиты информации.

Среди транзитных сканеров, которые загружаются в оперативную память, наибольшей популярностью в нашей стране пользуются антивирусные программы Aidstest Дмитрия Лозинского и DrWeb Игоря Данилова. Эти программы просты в использовании и для детального ознакомления с руководством по каждой из них следует прочитать файл, поставляемый вместе с антивирусным средством.

Широкое внедрение в повседневную практику компьютерных сетей, их открытость, масштабность делают проблему защиты информации исключительно сложной. Выделяют две базовые подзадачи:

• обеспечение безопасности обработки и хранения информации в каждом из компьютеров, входящих в сеть;

• защита информации, передаваемой между компьютерами сети.

Решение первой задачи основано на многоуровневой защите автономных компьютерных ресурсов от несанкционированных и некорректных действий пользователей и программ, рассмотренных выше.

Безопасность информации при сетевом обмене данными требует также обеспечения их конфиденциальности и подлинности. Защита информации в процессе передачи достигается на основе защиты каналов передачи данных, а также криптографического закрытия передаваемых сообщений. В идеальном случае защита каналов передачи данных должна обеспечивать их защиту как от нарушений работоспособности, так и несанкционированных действий (например подключения к линиям связи). По причине большой протяженности каналов связи, а также возможной доступности их отдельных участков (например при беспроводной связи) защита каналов передачи данных от несанкционированных действий экономически неэффективна, а в ряде случаев невозможна. Поэтому реально защита каналов передачи данных строится на основе защиты нарушений их работоспособности.

2.4. Методы и средства организационно-правовой защиты информации

К методам и средствам организационной защиты информации относятся организационно-технические и организационно-правовые мероприятия, проводимые в процессе создания и эксплуатации КС для обеспечения защиты информации. Эти мероприятия должны проводиться при строительстве или ремонте помещений, в которых будет размещаться КС; проектировании системы, монтаже и наладке ее технических и программных средств; испытаниях и проверке работоспособности КС.

На этом уровне защиты информации рассматриваются международные договоры, подзаконные акты государства, государственные стандарты и локальные нормативные акты конкретной организации. Рассмотрим примеры правовой охраны информации.

1) Правовая охрана программ и баз данных. Охрана интеллектуальных прав, а также прав собственности распространяется на все виды программ для компьютера, которые могут быть выражены на любом языке и в любой форме, включая исходный текст на языке программирования и машинный код. Однако правовая охрана не распространяется на идеи и принципы, лежащие в основе программы, в том числе на идеи и принципы организации интерфейса и алгоритма.

Правовая охрана программ для ЭВМ и баз данных впервые в полном объеме введена в Российской Федерации Законом «О правовой охране программ для электронных вычислительных машин и баз данных», который вступил в силу в 1992 году.

Для признания авторского права на программу для компьютера не требуется ее регистрации в какой-либо организации. Авторское право на программу возникает автоматически при ее создании. Для оповещения о своих правах разработчик программы может, начиная с первого выпуска в свет программы, использовать знак охраны авторского права, состоящий из трех элементов:

- буквы С в окружности или круглых скобках ©;
- наименования (имени) правообладателя;
- года первого выпуска программы в свет.

Например, знак охраны авторских прав на текстовый редактор Word выглядит следующим образом: © Корпорация Microsoft, 1983-2007.

Автору программы принадлежит исключительное право осуществлять воспроизведение и распространение программы любыми способами, а также модифицировать программу. Организация или пользователь, правомерно владеющие экземпляром программы (купившие лицензию на ее использование), могут осуществлять любые действия, связанные с функционированием программы, в том числе ее запись и хранение в памяти компьютера.

Необходимо знать и выполнять существующие законы, запрещающие нелегальное копирование и использование лицензионного программного обеспечения. В отношении организаций или пользователей, которые нарушают авторские права, разработчик может потребовать через суд возмещения причиненных убытков и выплаты нарушителем компенсации.

2) Электронная подпись. Электронная цифровая подпись в электронном документе признается юридически равнозначной подписи в документе на бумажном носителе.

В 2002 году был принят закон «Об электронно-цифровой подписи», который стал законодательной основой электронного документооборота в России.

При регистрации электронно-цифровой подписи в специализированных центрах корреспондент получает два ключа: *секретный* и *открытый.* Секретный ключ хранится на дискете или смарткарте и должен быть известен только самому корреспонденту. Открытый ключ должен быть у всех потенциальных получателей документов и обычно рассылается по

электронной почте.

Процесс электронного подписания документа состоит в обработке с помощью секретного ключа текста сообщения. Далее зашифрованное сообщение посылается по электронной почте абоненту. Для проверки подлинности сообщения и электронной подписи абонент использует открытый ключ.

3. Лицензионные, условно бесплатные и свободно распространяемые программы

Программы по их правому статусу можно разделить на три большие группы: лицензионные, условно бесплатные и свободно распространяемые.

Лицензионные программы. В соответствии с лицензионным соглашением разработчики программы гарантируют ее нормальное функционирование в определенной операционной системе и несут за это ответственность.

Лицензионные программы разработчики продают пользователям обычно в форме коробочных дистрибутивов.

В коробке находятся CD-диски, с которых производится установка программы на компьютеры пользователей, и руководство пользователя по работе с программой.

Довольно часто разработчики предоставляют существенные скидки при покупке лицензий на использование программы на большом количестве компьютеров или на использование программы в учебных заведениях.

Условно бесплатные программы. Некоторые фирмы-разработчики программного обеспечения предлагают пользователям условно бесплатные программы в целях их рекламы и продвижения на рынок. Пользователю предоставляется версия программы с ограниченным сроком действия (после истечения указанного срока программа перестает работать, если за нее не была произведена оплата) или версия программы с ограниченными функциональными возможностями (в случае оплаты пользователю сообщается код, включающий все функции).

Свободно распространяемые программы. Многие производители программного обеспечения и компьютерного оборудования заинтересованы в широком бесплатном распространении программного обеспечения. К таким программным средствам можно отнести:

- новые недоработанные (бета) версии программных продуктов (это позволяет провести их широкое тестирование);
- программные продукты, являющиеся частью принципиально новых технологий (это позволяет завоевать рынок);
- дополнения к ранее выпущенным программам, исправляющие найденные ошибки или расширяющие возможности;
- драйверы к новым или улучшенные драйверы к уже существующим устройствам.

Задание для самостоятельной работы

1. Ознакомиться с законами «О правовой охране программ для электронных вычислительных машин и баз данных», «Об электронно-цифровой подписи» и «О защите персональных данных» в информационно-правовой системе.

2. Рассмотреть современные концепции обеспечения информационной безопасности (квантовая криптография).