**2.1.** **Преднамеренные угрозы безопасности систем обработки информации (СОИ)**

**и направления защиты**

**Угрозы безопасности СОИ**

Реализация угрозы будет называться атакой. Классификацию угроз безопасности можно проводить по различным признакам.

**Цели реализации угрозы:**

• нарушение конфиденциальности информации (информация в СОИ имеет большую ценность для ее владельца). Ее несанкционированное использование другими лицами наносит значительный ущерб интересам владельца;

• нарушение целостности информации (полная или частичная дезинформация — ценная информация может быть утрачена или обесценена путем ее несанкционированного удаления или модификации). Ущерб может быть намного больше, чем при нарушении конфиденциальности;

• частичное или полное нарушение работоспособности СОИ (нарушение доступности, так как диапазон услуг, предоставляемых современными СОИ, весьма широк, отказ в обслуживании может существенно повлиять на работу пользователя).

**Принципы воздействия на СОИ:**

• атака с использованием стандартных каналов доступа субъекта системы (пользователя, процесса) к объекту (файлу данных, каналу связи и т. д.). Под доступом понимается воздействие субъекта (выполнение некоторой операции) на объект, приводящее к возникновению информационного потока от объекта к субъекту. При этом происходит взаимодействие субъекта и объекта и, следовательно, изменяется состояние объекта. Воздействие, основанное на этом принципе, проще, более информативнее и от него легче защититься;

• атака с использованием скрытых каналов. Под скрытым каналом понимается путь передачи информации, позволяющий двум взаимодействующим процессам обмениваться информацией таким образом, который нарушает системную политику безопасности. При этом используются лишь побочные эффекты от взаимодействия двух субъектов, что не оказывает влияние на состояние системы. Здесь воздействие организовывать относительно трудно, принцип отличается меньшей информативностью и сложностью обнаружения и устранения. Эти каналы бывают двух типов:

— скрытые каналы с памятью (позволяющие произвести чтение или запись информации другого процесса

непосредственно или с помощью промежуточных объектов для хранения информации — временная память);

— скрытые временные каналы (один процесс может получать информацию о действиях другого процесса, используя интервалы между какими-либо событиями — например, интервал времени между началом и концом процесса ввода-вывода дает информацию о размере вводимой или выводимой информации).

**Характер воздействия на СОИ:**

• активное воздействие (всегда связано с выполнением пользователем каких-либо действий, выходящих за рамки его обязанностей и нарушающих существующую политику безопасности — доступ к определенным наборам данных, программам, вскрытие пароля и т. д.). В результате изменяется состояние системы (осуществляется с использованием доступа и/или с использованием доступа и скрытых каналов);

• пассивное воздействие (осуществляется путем наблюдения каких-либо побочных эффектов и их анализа — например, прослушивание линии связи между двумя узлами сети). При этом нарушается только конфиденциальность информации (так как при нем никаких действий с объектами и субъектами не производится), а состояние системы не изменяется.

**Причины появления используемой ошибки защиты.** Реализация какой-либо угрозы становится возможной, если в системе имеется ошибка или брешь в защите. Ошибка может быть обусловлена одной из следующих причин:

• неадекватность политики безопасности реальной СОИ (разработанная для данной системы политика безопасности настолько не отражает реальные аспекты обработки информации, что становится возможным использование этого несоответствия для выполнения несанкционированных действий);

• ошибки административного управления, под которыми понимается некорректная реализация или поддержка принятой политики безопасности в данной системе (например, неправильное определение прав доступа к определенным наборам данных);

• ошибки в алгоритмах программ, в связях между ними и т. д., которые возникают на этапе проектирования

программных продуктов и благодаря которым их можно использовать совсем не так, как описано в документации (например, ошибка в программе аутентификации пользователя системой дает возможность с помощью определенных действий пользователю войти в систему без пароля);

• ошибки реализации программ (ошибки кодирования), связей между ними и т. д., которые возникают на этапе реализации или отладки. Они могут служить источником недокументированных свойств (например, люки, которые обнаружить труднее всего).

**Способы активного воздействия на объект атаки:**

• непосредственное воздействие на объект атаки, в том числе с использованием привилегий (например, непосредственный доступ к набору данных, программе, службе, каналу связи и т. д.), воспользовавшись какой-либо ошибкой (нужно применить контроль доступа);

• воздействие на систему разрешений, в том числе с захватом привилегий (здесь несанкционированные действия выполняются относительно прав пользователей, а сам доступ к объекту потом осуществляется законным образом — например, захват привилегий);

• опосредованное воздействие через других пользователей, в том числе:

— «маскарад», когда пользователь присваивает себе каким-либо образом полномочия другого, выдавая себя за него;

— «использование вслепую» (один пользователь заставляет другого выполнить необходимые действия, которые для системы защиты не выглядят несанкционированными — для этой угрозы может использоваться вирус, который выполняет необходимые действия и сообщает тому, кто его внедрил о результате). Для предотвращения подобных действий требуется постоянный контроль за работой

СОИ в целом и со стороны пользователей за своими наборами данных.

**Способы воздействия на СОИ:**

• в интерактивном (on-line) режиме (например, атака на систему с помощью интерпретатора команд). Атака оказывается более длительной по времени и, может быть обнаружена, но воздействие является более гибким;

• в пакетном (off-line) режиме (например, с помощью вирусов). Атака является кратковременной, трудно диагностируемой и более опасной, но требует большой предварительной подготовки, так как необходимо предусмотреть все возможные последствия вмешательства.

**Объекты атаки:**

• СОИ в целом (для этого используются «маскарад», перехват или подделка пароля, взлом или доступ к СОИ через сеть);

• объекты СОИ (программы в оперативной памяти или на внешних носителях, сами устройства системы, каналы передачи данных и т. д., с целью получения доступа к содержимому носителей информации или нарушения их функциональности);

• субъекты СОИ — процессы и подпроцессы пользователей (цели: приостановка; изменение привилегий или характеристик; использование злоумышленником привилегий или характеристик и т. д.);

• каналы передачи данных — передаваемые по каналу связи пакеты данных и сами каналы (цели: нарушение конфиденциальности, подмена или модификация сообщений, нарушение целостности информации, изменение топологии и характеристик сети, нарушение доступности сети и т. д.).

**Состояние объекта атаки:**

• хранение (диск или другой вид носителя информации находится в пассивном состоянии) и воздействие осуществляется с использованием доступа;

• передача по линиям связи между узлами сети или внутри узла;

• обработка (объектом атаки является процесс пользователя).

**Используемые средства атаки:**

• использование стандартного программного обеспечения (ПО);

• использование специально разработанных программ (поэтому в защищенных системах рекомендуется не допускать добавление программ в СОИ без разрешения администратора безопасности системы).

**Каналы несанкционированного получения информации в СОИ (КНПИ)**

Под КНПИ понимаются такие дестабилизирующие факторы, следствием проявления которых может быть получение (или опасность получения) защищаемой информации лицами или процессами, не имеющими на это законных полномочий.

Перечни основных типов каналов несанкционированного доступа к информации выглядят следующим образом.

**Каналы, проявляющиеся безотносительно к обработке** информации и без доступа злоумышленника к элементам ЭВТ:

• хищение носителей информации на заводах, где производится ремонт ЭВТ;

• подслушивание разговоров лиц, имеющих отношение к СОИ;

• провоцирование на разговоры лиц, имеющих отношение к СОИ;

• использование злоумышленником визуальных средств;

• использование злоумышленником оптических средств;

• использование злоумышленником акустических средств.

**Каналы, проявляющиеся в процессе обработки информации** без доступа злоумышленника к элементам СОИ (в основном — побочные электромагнитные излучения и наводки, ПЭМИН):

• электромагнитные излучения устройств отображения информации;

• электромагнитные излучения процессоров;

• электромагнитные излучения внешних запоминающих устройств;

• электромагнитные излучения аппаратуры связи;

• электромагнитные излучения линий связи;

• электромагнитные излучения вспомогательной аппаратуры;

• паразитные наводки в коммуникациях водоснабжения;

• паразитные наводки в системах канализации;

• паразитные наводки в сетях теплоснабжения;

• паразитные наводки в системах вентиляции;

• паразитные наводки в шинах заземления;

• паразитные наводки в цепях радиофикации;

• паразитные наводки в цепях телефонизации и диспетчерской связи;

• паразитные наводки в сетях питания по цепи 50 Гц;

• подключение генераторов помех;

• подключение регистрирующей аппаратуры;

• осмотр отходов производства, попадающих за пределы контролируемой зоны.

**Каналы, проявляющиеся безотносительно к обработке информации** с доступом злоумышленника к элементам СОИ, но без изменения последних:

• копирование бланков с исходными данными;

• копирование магнитных носителей;

• копирование с устройств отображения;

• копирование выходных документов;

• копирование других документов;

• хищение производственных отходов.

**Каналы, проявляющиеся в процессе обработки информации с доступом злоумышленника к элементам СОИ, но без изменения последних:**

• запоминание информации на бланках с исходными данными;

• запоминание информации с устройств наглядного отображения;

• запоминание информации на выходных документах;

• запоминание служебных данных;

• копирование (фотографирование) информации в процессе обработки;

• изготовление дубликатов массивов и выходных документов;

• копирование распечатки массивов;

• использование программных ловушек;

• маскировка под зарегистрированного пользователя; использование недостатков систем программирования;

• использование недостатков операционных систем;

• использование зараженности программного обеспечения вирусом.

**Каналы, проявляющиеся безотносительно к обработке информации с доступом злоумышленника к элементам СОИ с изменением последних:**

• подмена/хищение бланков;

• подмена/хищение магнитных носителей;

• подмена/хищение выходных документов;

• подмена/хищение аппаратуры;

• подмена элементов программ;

• подмена элементов баз данных;

• хищение других документов;

• внедрение в программы блоков типа «троянский конь», «бомба» и т. п.;

• чтение остаточной информации в ЗУ после выполнения санкционированных запросов.

**Каналы, проявляющиеся в процессе обработки информации с доступом злоумышленника к объектам СОИ с их изменением:**

• незаконное подключение к аппаратуре;

• незаконное подключение к линиям связи;

• снятие информации на шинах питания устройств отображения;

• снятие информации на шинах питания процессоров;

• снятие информации на шинах питания аппаратуры связи;

• снятие информации на шинах питания линий связи;

• снятие информации на шинах питания печатающих устройств;

• снятие информации на шинах питания внешних запоминающих устройств;

• снятие информации на шинах питания вспомогательной аппаратуры.

**Основные направления борьбы с угрозами безопасности СОИ**

**«Оранжевая книга»**. Наиболее известным стандартом безопасности компьютерных систем является упоминавшийся выше документ под названием «Критерии безопасности доверенных/надежных компьютерных систем» («Оранжевая книга»). Согласно «Оранжевой книге» все защищенные компьютерные системы делятся на семь классов (А1 — гарантированная защита, В1, В2, ВЗ — полное управление доступом, С 1, С2 — избирательное управление доступом, D — минимальная безопасность).Согласно «Оранжевой книге» политика безопасности должна включать в себя по крайней мере следующие элементы:

• произвольное управление доступом;

• безопасность повторного использования объектов;

• метки безопасности;

• принудительное управление доступом;

• идентификация и аутентификация;

• безопасность повторного использования объектов.

**Руководящие документы Гостехкомиссии.** В 1992 г. Гостехкомиссия при Президенте Российской Федерации опубликовала пять руководящих документов, посвященных вопросам защиты компьютерных систем. В документе «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» установлено семь классов защищенности средств вычислительной техники. Самые низкие требования предъявляются к классу 7, самые высокие — к классу 1. Требования этих классов в основном соответствуют аналогичным требованиям «Оранжевой книги».

Идейной основой набора Руководящих документов является «Концепция защиты СВТ и АС от НСД к информации». В Концепции различаются понятия средств вычислительной техники (СВТ) и автоматизированной

системы (АС). Различие двух направлений порождено тем, что СВТ разрабатываются и поставляются на рынок лишь как элементы, из которых в дальнейшем строятся функционально ориентированные АС, и поэтому, не решая прикладных задач, СВТ не содержат пользовательской информации. В Концепции

формулируются следующие основные принципы защиты от НСД к информации:

• защита СВТ обеспечивается комплексом программно-технических средств;

• защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер;

• защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функ­ционирования, в том числе при проведении ремонтных и регламентных работ;

• программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС).

Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ. Выделяется четыре уровня этих возможностей, причем в рамках «своего» уровня считается, что нарушитель является специалистом высшей квалификации, знает все о АС и, в частности, о системе

и средствах ее защиты. Классификация является иерархической, т. е. каждый следующий уровень включает в себя функциональные возможности предыдущего:

• первый — самый низкий уровень возможностей ведения диалога в АС — запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации;

• второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации;

• третий определяется возможностью управления функционированием АС, т. е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования;

• четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

В качестве главного средства защиты от НСД к информации в Концепции рассматривается система разграничения доступа (СРД) субъектов к объектам доступа. Основными функциями СРД являются:

• реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным и устройствам создания твердых копий;

• изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;

• управление потоками данных с целью предотвращения записи данных на носители несоответствующего грифа;

• реализация правил обмена данными между субъектами для АС и СВТ, построенных по сетевым принципам.

Кроме того, Концепция предусматривает наличие обеспечивающих средств для СРД, которые выполняют следующие функции:

• идентификацию и опознание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;

• регистрацию действий субъекта и его процесса;

• предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;

• реакцию на попытки НСД, например, сигнализацию, блокировку, восстановление после НСД;

• тестирование;

• очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;

• учет выходных печатных и графических форм и твердых копий в АС;

• контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств.

**Сервисы безопасности.** Кроме перечисленных понятий, связанных с политикой безопасности, при рассмотрении защиты информации в распределенных системах и сетях часто используется представление о сервисах безопасности, обычно включающих такие, как:

• идентификация/аутентификация;

• разграничение доступа;

• шифрование;

• протоколирование/аудит;

• контроль целостности и защищенности;

• обнаружение отказов и оперативное восстановление;

• экранирование и туннелирование.