2. БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ. ТРАДИЦИОННЫЙ ПОДХОД К АНАЛИЗУ ПРОБЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1 Актуальность задач компьютерной безопасности

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации повышается зависимость общества от степени безопасности используемых им информационных технологий, от которых порой зависит благополучие, а иногда и жизнь многих людей.

Актуальность и важность проблемы обеспечения безопасности информационных технологий обусловлены следующими причинами:

- *резкое увеличение вычислительной мощности современных компьютеров при одновременном упрощении их эксплуатации;*
- *резкое увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации;*
- *сосредоточение в единых базах данных информации различного назначения и различной принадлежности;*
- *высокие темпы роста парка персональных компьютеров, находящихся в эксплуатации в самых разных сферах деятельности;*
- *резкое расширение круга пользователей, имеющих непосредственный доступ к вычислительным ресурсам и массивам данных;*
- *бурное развитие программных средств, не удовлетворяющих даже минимальным требованиям безопасности;*
- *повсеместное распространение сетевых технологий и объединение локальных сетей в глобальные;*
- *развитие глобальной сети Internet, практически не препятствующей нарушениям безопасности систем обработки информации во всем мире.*

2.2 Основные понятия информационной безопасности автоматизированных систем обработки информации

Безопасность автоматизированной системы обработки информации (АСОИ) *– свойство защищенности системы от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, изменения или разрушения ее компонентов.*

Природа воздействий на АСОИ может быть самой разнообразной. Это и стихийные бедствия (землетрясение, ураган, пожар), и выход из строя

составных элементов АСОИ, и ошибки персонала, и попытка проникновения злоумышленника.

Безопасность АСОИ достигается *принятием мер по обеспечению конфиденциальности и целостности обрабатываемой ею информации, а также доступности и целостности компонентов и ресурсов системы.*

Под доступом к информации понимается *ознакомление с информацией, ее обработка, в частности копирование, модификация или уничтожение информации.*

Различают следующие виды доступа к информации:

- ***санкционированный доступ*** - *доступ к информации, не нарушающий установленные правила разграничения доступа;*
- ***несанкционированный доступ*** **(*НСД*)** - *характеризуется нарушением установленных правил разграничения доступа*. Лицо или процесс, осуществляющие несанкционированный доступ к информации, являются нарушителями правил разграничения доступа. Несанкционированный доступ является наиболее распространенным видом компьютерных нарушений.

Правила разграничения доступа *служат для регламентации права доступа субъектов доступа к объектам доступа.*

Конфиденциальность данных - *это статус, предоставленный данным и определяющий требуемую степень их защиты. По существу - это свойство информации быть известной только допущенным и прошедшим проверку* (авторизированным) субъектам системы (пользователям, процессам, программам). Для остальных субъектов системы эта информация должна быть неизвестной.

Субъект - *это активный компонент системы, который может стать причиной потока информации от объекта к субъекту или изменения состояния системы.*

Объект - *пассивный компонент системы, хранящий, принимающий или передающий информацию. Доступ к объекту означает доступ к содержащейся в нем информации.*

Целостность информации обеспечивается в том случае, если данные в системе не отличаются в семантическом отношении отданных в исходных документах, т.е. если не произошло их случайного или преднамеренного искажения или разрушения.

Целостность компонента или ресурса системы *— это свойство компонента или ресурса быть неизменными в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений или разрушающих воздействий.*

Доступность компонента или ресурса системы - *это свойство компонента или ресурса быть доступным для авторизованных законных субъектов системы.*

Под угрозой безопасности АСОИ понимаются *возможные воздействия на АСОИ, которые прямо или косвенно могут нанести ущерб ее безопасности.*

Ущерб безопасности *подразумевает нарушение состояния защищенности информации, содержащейся и обрабатывающейся в АСОИ.* С понятием угрозы безопасности тесно связано понятие уязвимости АСОИ.

Уязвимость АСОИ *- это некоторое неудачное свойство системы, которое делает возможным возникновение и реализацию угрозы.*

Атака на компьютерную систему *— это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы*. Таким образом. атака — это одна из реализаций угрозы безопасности.

Противодействие угрозам безопасности является целью защиты систем обработки информации.

Безопасная или защищенная система *- это система со средствами защиты, которые успешно и эффективно противостоят угрозам безопасности.*

Комплекс средств защиты *- программных и технических средств, создаваемых и поддерживаемых для обеспечения информационной безопасности АСОИ. Комплекс создается и поддерживается в соответствии с принятой в данной организации политикой безопасности.*

Политика безопасности *- это совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АСОИ от заданного множества угроз безопасности.*

2.3 Понятие «угрозы». Основные угрозы безопасности систем обработки информации

По цели воздействия различают три основных типа угроз безопасности АСОИ:

- *угрозы нарушения конфиденциальности информации;*
- *угрозы нарушения целостности информации;*
- *угрозы нарушения работоспособности системы (отказы в обслуживании).*

Угрозы нарушения конфиденциальности *направлены на разглашение конфиденциальной или секретной информации. При реализации этих угроз информация становится известной лицам, которые не должны иметь к ней доступ.* В терминах компьютерной безопасности угроза нарушения конфиденциальности имеет место всякий раз, когда получен несанкционированный доступ к некоторой закрытой информации, хранящейся в компьютерной системе или передаваемой от одной системы к другой.

***Угрозы нарушения целостности информации**, хранящейся в компьютерной системе или передаваемой по каналу связи, направлены на ее изменение или искажение, приводящее к нарушению ее качества или полному уничтожению.* Целостность информации может быть нарушена умышленно злоумышленником, а также в результате объективных воздействий со стороны среды, окружающей систему. Эта угроза особенно актуальна для систем передачи информации - компьютерных сетей и систем телекоммуникаций. Умышленные нарушения целостности информации не следует путать с ее санкционированным изменением, которое выполняется полномочными лицами с обоснованной целью (например, таким изменением является периодическая коррекция некоторой базы данных).

***Угрозы нарушения работоспособности** (отказ в обслуживании) направлены на создание таких ситуаций, когда определенные преднамеренные действия либо снижают работоспособность АСОИ, либо блокируют доступ к некоторым ее ресурсам.* Например, если один пользователь системы запрашивает доступ к некоторой службе, а другой предпринимает действия по блокированию этого доступа, то первый пользователь получает отказ в обслуживании. Блокирование доступа к ресурсу может быть постоянным или временным.

Современная автоматизированная система обработки информации представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными.

АСОИ состоит из следующих компонент:

- *аппаратные средства* — ЭВМ и их составные части (процессоры, мониторы, терминалы, периферийные устройства-дисководы, принтеры, контроллеры, кабели, линии связи) и т.д.;
- *программное обеспечение* — приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т.д.;
- *данные* — хранимые временно и постоянно, на магнитных носителях, печатные, архивы, системные журналы и т.д.;
- *персонал* — обслуживающий персонал и пользователи.

Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя.

Опасные воздействия на АСОИ можно подразделить на:

- *случайные;*
- *преднамеренные.*

Случайные воздействия. Анализ опыта проектирований, изготовления и эксплуатации АСОИ показывает, что информация подвергается различным

случайным воздействиям на всех этапах цикла жизни и функционирования АСОИ.

Причинами случайных воздействий при эксплуатации АСОИ могут быть:

- *аварийные ситуации из-за стихийных бедствий и отключений электропитания;*
- *отказы и сбои аппаратуры;*
- *ошибки в программном обеспечении;*
- *ошибки в работе обслуживающего персонала и пользователей;*
- *помехи в линиях связи из-за воздействий внешней среды.*

Преднамеренные угрозы *связаны с целенаправленными действиями нарушителя.* В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник 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.

Исходя из возможности возникновения наиболее опасной ситуации, обусловленной действиями нарушителя, можно составить ***гипотетическую модель потенциального нарушителя:***

1. *квалификация нарушителя может быть на уровне разработчика данной системы;*
2. *нарушителем может быть как постороннее лицо, так и законный пользователь системы;*
3. *нарушителю известна информация о принципах работы системы;*
4. *нарушитель выберет наиболее слабое звено в защите.*

В частности, для банковских АСОИ можно выделить следующие преднамеренные угрозы:

1. несанкционированный доступ посторонних лиц, не принадлежащих к числу банковских служащих, и ознакомление с хранимой конфиденциальной информацией;
2. ознакомление банковских служащих с информацией, к которой они не должны иметь доступ;
3. несанкционированное копирование программ и данных;
4. кража магнитных носителей, содержащих конфиденциальную информацию;
5. кража распечатанных банковских документов;
6. умышленное уничтожение информации;
7. несанкционированная модификация банковскими служащими финансовых документов, отчетности и баз данных;
8. фальсификация сообщений, передаваемых по каналам связи;
9. отказ от авторства сообщения, переданного по каналам связи;
10. отказ от факта получения информации;
11. навязывание ранее переданного сообщения;
12. разрушение информации, вызванное вирусными воздействиями;

13. разрушение архивной банковской информации, хранящейся на магнитных носителях;
14. кража оборудования.

В таблице 2.1 показаны основные пути реализации угроз безопасности АСОИ при воздействии на ее компоненты. Конечно, таблица 2.1 дает самую общую картину того, что может произойти с системой. Конкретные обстоятельства и особенности должны рассматриваться отдельно.

Таблица 2.1 - Основные пути реализации угроз безопасности АСОИ при воздействии на ее компоненты

Объекты воздействия	***Нарушение конфиденциальност и информации***	***Нерушение целостности информации***	***Нарушение работоспособност и системы***
Аппаратные средства	*НСД-подключение; использование ресурсов; хищение носителей.*	*НСД-подключение; использование ресурсов; модификация, изменение режимов*	*НСД-изменение режимов; вывод из строя; разрушение*
Программное обеспечение	*НСД-копирование; хищение; перехват.*	*НСД, внедрение «троянского коня», «вирусов». «червей»*	*НСД-искажение; удаление; подмена*
Данные	*НСД-копирование; хищение; перехват*	*НСД- искажение; модификация*	*НСД - искажение; удаление: подмена*
Персонал	*Разглашение: передача сведений о защите; халатность.*	*«Маскарад»; вербовка; подкуп персонала*	*Уход с рабочего места; физическое устранение*

Термин «вирус» в применении к компьютерам был предложен Фредом Коэном из Университета Южной Калифорнии. Исторически первое определение, котрое дал Ф. Коэн: «***Компьютерный вирус*** - *это программа, которая может заражать другие программы, модифицируя их посредством включения в них своей, возможно, измененной копии, причем последняя сохраняет способность к дальнейшему размножению»*. Ключевыми понятиями в определении компьютерного вируса являются способность вируса к саморазмножению и способность к модификации вычислительного процесса. Указанные свойства компьютерного вируса аналогичны паразитиованию в живой природе биологического вируса.

Компьютерный вирус пытается тайно записать себя на компьютерные диски. Способ функционирования большинства вирусов заключается в таком изменении системных файлов компьютера, чтобы вирус начинал свою деятельность при каждой загрузке. Например, вирусы, поражающие загрузочный сектор, пытаются инфицировать часть дискеты или жесткого диска, зарезервированную. только для операционной системы и хранения файлов запуска. Эти вирусы особенно коварны, так как они загружаются в память при каждом включении компьютера. Такие вирусы обладают

наибольшей способностью к размножению и могут постоянно распространяться на новые диски.

Сетевой «червь» *представляет собой разновидность программы-вируса, которая распространяется по глобальной сети и не оставляет своей копии на магнитном носителе.* Термин «червь» пришел из научно-фантастического романа Джона Бруннера «По бурным волнам». Этот термин используется для именования программ, которые подобно ленточным червям перемещаются по компьютерной сети от одной системы к другой.

Первоначально «черви» были разработаны для поиска в сети других компьютеров со свободными ресурсами, чтобы получить возможность выполнить распределенные вычисления. При правильном использовании технология «червей» может быть весьма полезной. Например, «червь» World Wide Web Worm формирует индекс поиска участков Web. Однако «червь» легко превращается во вредоносную программу. «Червь» использует механизмы поддержки сети для определения узла, который может быть поражен. Затем с помощью этих же механизмов передает свое тело в этот узел и либо активизируется, либо ждет походящих условий для активизации.

2.4. Понятие несанкционированного доступа

Несанкционированный доступ (НСД) *состоит в получении пользователем (нарушителем) доступа к объекту в нарушение правил разграничения доступа, установленных в соответствии с принятой в организации политикой безопасности.* НСД является наиболее распространенным и многообразным видом компьютерных нарушений. НСД использует любую ошибку в системе зашиты и возможен при нерациональном выборе средств зашиты, их некорректной установке и настройке. НСД может быть осуществлен как штатными средствами АСОИ. так и специально созданными аппаратными и программными средствами.

Перечислим основные каналы несанкционированного доступа, через которые нарушитель может получить доступ к компонентам АСОИ и осуществить хищение, модификацию и/или разрушение информации:

- *все штатные каналы доступа к информации (терминалы пользователей, оператора, администратора системы; средства отображения и документирования информации; каналы связи) при их использовании нарушителями, а также законными пользователями вне пределов их полномочий;*
- *технологические пульты управления;*
- *линии связи между аппаратными средствами АСОИ;*
- *побочные электромагнитные излучения от аппаратуры, линий связи, сетей электропитания и заземления и др.*

Из всего разнообразия способов и приемов несанкционированного доступа ***наиболее распространенными нарушениями являются:***

- *перехват паролей;*
- *«маскарад»;*
- *незаконное использование привилегий.*

Перехват паролей осуществляется специально разработанными программами. При попытке законного пользователя войти в систему программа-перехватчик имитирует на экране дисплея ввод имени и пароля пользователя, которые сразу пересылаются владельцу программы-перехватчика, после чего на экран выводится сообщение об ошибке и управление возвращается операционной системе. Пользователь предполагает, что допустил ошибку при вводе пароля. Он повторяет ввод и получает доступ в систему. Владелец программы-перехватчика, получивший имя и пароль законного пользователя, может теперь использовать их в своих целях. Существуют и другие способы перехвата паролей.

«Маскарад» - *это выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями.* Целью «маскарада» является приписывание каких-либо действий другому пользователю либо присвоение полномочий или привилегий другого пользователя.

Примерами реализации «маскарада» являются:

- *вход в систему под именем и паролем другого пользователя (этому «маскараду» предшествует перехват пароля);*
- *передача сообщений в сети от имени другого пользователя.*

Незаконное использование привилегий. Большинство систем защиты устанавливают определенные наборы привилегий для выполнения заданных функций. Каждый пользователь получает свой набор привилегий: обычные пользователи — минимальный, администраторы — максимальный. Несанкционированный захват привилегий, например посредством «маскарада», приводит к возможности выполнения нарушителем определенных действий в обход системы защиты. Следует отметить, что незаконный захват привилегий возможен либо при наличии ошибок в системе защиты, либо из-за халатности администратора при управлении системой и назначении привилегий

Угрозы, компьютерных сетей.

Особо следует остановиться на угрозах, которым могут подвергаться компьютерные сети. Основная особенность любой компьютерной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами (объектами) сети осуществляется физически с помощью сетевых линий связи и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между объектами сети, передаются в виде пакетов обмена.

При вторжении в компьютерную сеть злоумышленник может использовать как пассивные, так и активные методы вторжения.

Пассивное вторжение (перехват информации) *- нарушитель только наблюдает за прохождением информации по каналу связи, не вторгаясь ни в информационный поток, ни в содержание передаваемой информации.* Как правило, злоумышленник может определить пункты назначения и идентификаторы либо только факт прохождения сообщения, его длину и частоту обмена, если содержимое сообщения не распознаваемо, т.е. выполнить анализ трафика (потока сообщений) в данном канале.

Активное вторжение *- нарушитель стремится подменить информацию, передаваемую в сообщении. Он может выборочно модифицировать, изменить или добавить правильное или ложное сообщение, удалить, задержать или изменить порядок следования сообщений.* Злоумышленник может также аннулировать и задержать все сообщения, передаваемые по каналу. Подобные действия можно квалифицировать как отказ в передаче сообщений.