ТЕМА 1. Информационная безопасность компьютерных систем

1.1. Основные понятия и определения

Рассмотрим основные понятия ЗИ и информационной безопасности КсиС с учетом определений стандарта ГОСТ Р 50922-96.

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

Объект защиты – информация, или носитель информации, или информационный процесс, в отношении которого необходимо обеспечивать защитту в соответствии с поставленной целью ЗИ.

Цель ЗИ – это желаемый результат ЗИ. Целью ЗТ может быть предотвращение ущерба собственнику, влалельцу, пользователю инофрмации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

Эффективность ЗИ – степень воздействия результатов ЗИ поставленной цели.

Система ЗИ – совокупность органов и/или исполнителей, используемая ими техника ЗИ, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по ЗИ.

Под *информационной безопасностью* понимают защищенность информации от незаконного ознакомления, преобразования и уничтожения, а также защищенность информационных ресурсов от воздействий, направленных на нарушение их работоспособности.

Компоненты Автоматизированных систем обработки информации (далее – АСОИ) можно разбить на следующие группы:

- Аппаратные средства;
- Программное обеспечение;
- Данные;
- Персонал.

Информационаая безопасность компьютерных систем достигается обеспечением *конфиденциальности, целостности и достоверности* обрабатываемых данных, а также доступности и целостности информационных компонентов и ресурсов системы.

Конфиденциальность данных – этот статус, предоставленный данным и определяющий требуемую степень их защиты. К конфиденциальным данным можено отнести, например, следующие: личная информация пользователей; учетные записи; данные о кредитных картах; бухгалтерские сведения.

Под *целостностью информации* понимается свойство информации сохранять свою структуру и/или содержание в процессе передачи и хранения. Целостность информации обеспечивается в том случае, если данные не в

системе не отличаются в семантическом отношении от исходных документов, то есть если не произошло их случайного или преднамеренного разрушения.

Достоверность информации – свойство информации, выражающееся в строгой принадлежности субъекту, который является ее источником, либо тому субъекту, от которого эта информация принята.

Собственник информации – субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами.

Доступность данных. Работа пользователя с данными возможна только в том случае, если он имеет к ним доступ.

Доступ к информации – получение субъектом овзможности ознакомления с информацией, в том числе при помощи технических средств.

Различают санкционированный и несанкционированный доступ к информации.

Санкционированный доступ к информации – это доступ к информации, не нарушающий установленные правила разграничения доступа. Правила разграничения доступа служат для регламентации права доступа к компонентам системы.

Несанкционированный доступ (НСД) характеризуется нарушением установленных правил разграничения доступа. Лицо или процесс, осуществляющие НСД к информации, являются нарушителями правил разграничения доступа. НСД является наиболее распространенным видом компьютерных нарушений.

С допуском к информации и ресурсам системы связана группа таких важных понятий, как идентификация, аутентификация, авторизация.

Идентификация субъекта – это процедура распознавания субъекта по его идентификатору. Идентификация выполняется при попытке субъекта войти в систему (сеть).

Аутентификация субъекта – это проверка подлинности субъекта с данным идентификатором. Процедура аутентификации устанавливает, является ли субъект именно тем, кем он себя объявил.

Авторизация субъекта – это процедура предоставления законному субъекту, успешно прошедшему идентификацию и аутентификацию, соответствующих полномочий и доступных ресурсов системы (сети).

Под *угрозой безопасности* АСОИ понимаются возможные действия, способные прямо или косвенно нанести ущерб ее безопасности. *Ущерб безопасности* подразумевает нарушение состояния защищенности информации, содержащейся и обрабатываемой в системе.

Уязвимость компьютерной системы – это присущее системе неудачное свойство, которое может привести к реализации угрозы.

Атака на компьютерную систему – это поиск и / или использование злоумышленником той или иной уязвимости системы.*Атака* – любое действие, нарушающее политику безопасности информационной системы. Иными словами, атака – это реализация угрозы безопасности.

Противодействие угрозам безопасности является целью средств защиты компьютерных систем и сетей.

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

Комплекс средств защиты представляет собой совокупность программных и технических средств, создаваемых и поддерживаемых для обеспечения информационной безопасности АСОИ.

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