Военная кафедра
КазНТУ им. К.Сатпаева

Цикл автоматизированных систем управления войсками и информационной защиты

Тема № 2:

- **«Основы комплексной системы защиты информации»**

ЗАНЯТИЕ 1.

«Основы комплексной системы защиты информации»

Учебные вопросы.

1. **Методологические основы комплексной системы защиты информации.**
2. **Основные положения теории систем.**

3. **Общие законы кибернетики.**

В руководящих документах приведены следующие основные способы несанкционированного доступа к информации в КС:

- **непосредственное обращение к объекту с конфиденциальной информацией (например, с помощью управляемой пользователем программы, читающей данные из файла или записывающей их в него);**

- создание программных и технических средств, выполняющих обращение к объекту в обход средств защиты (например, с использованием случайно или намеренно оставленных разработчиком этих средств, так называемых люков);
- модификация средств защиты для осуществления несанкционированного доступа (например, внедрение программных закладок);

- внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих структуру и функции этих средств для осуществления несанкционированного доступа (например, путем загрузки на компьютере иной, незащищенной операционной системы).

Модель нарушителя в руководящих документах определяется исходя из следующих предположений:

- **нарушитель имеет доступ к работе со штатными средствами КС;**
- **нарушитель является специалистом высшей квалификации**

Можно выделить следующие уровни возможностей нарушителя, предоставляемые ему штатными средствами КС (каждый следующий уровень включает в себя предыдущий):

1) запуск программ из фиксированного набора (например,подготовка документов или получение почтовых сообщений);

2) **создание и запуск собственных программ** (возможности опытного пользователя или пользователя с полномочиями отладки программ);

3)**управление функционированием КС** — воздействие на ее базовое программное обеспечение, состав и конфигурацию КС (например, внедрение программной закладки);

4) весь объем возможностей лиц, осуществляющих проектирование, реализацию и ремонт средств КС, вплоть до включения в состав КС собственных СВТ с новыми функциями.

С учетом различных уровней возможностей нарушителя выделяют следующие вспомогательные способы несанкционированного доступа к информации в КС, позволяющие нарушителю использовать перечисленные ранее основные способы:

- ручной или программный подбор паролей путем их полного перебора или при помощи специального словаря (взлом КС);
- подключение к КС в момент кратковременного прекращения работы легального пользователя, работающего в интерактивном режиме и не заблокировавшего свой терминал;

- **подключение к линии связи и перехват доступа к КС после отправки пакета завершения сеанса легального пользователя, работающего в удаленном режиме;**
- **выдача себя за легального пользователя с применением похищенной у него или полученной обманным путем (с помощью так называемой социальной инженерии) идентифицирующей информации — «маскарад»;**

- **создание условий для связи по компьютерной сети легального пользователя с терминалом нарушителя, выдающего себя за легального объекта КС (например, одного из ее серверов), — «мистификация»;**
- **создание условий для возникновения в работе КС сбоев, которые могут повлечь за собой отключение средств защиты информации или нарушение правил политики безопасности;**

- **тщательное изучение подсистемы защиты КС и используемой в ней политики безопасности, выявление ошибочных участков в программных средствах защиты информации в КС, введение программных закладок, разрешающих доступ нарушителю.**

Если к регистрационной базе данных КС разрешен доступ по чтению, то пользователь нарушитель сможет скопировать ее на собственный носитель или просто в другой файл и осуществить попытку подбора идентифицирующей информации (например, пароля) привилегированного пользователя для осуществления несанкционированного доступа с помощью «маскарада».

Для удобства назначения полномочий пользователям КС они могут объединяться в группы в соответствии с должностным положением пользователей в организации и (или) их принадлежностью одному из ее структурных подразделений. Информация о группах пользователей также может размещаться в регистрационной базе данных КС.

При выборе паролей пользователи КС должны руководствоваться двумя, по сути взаимоисключающими, правилами — пароли должны трудно подбираться и легко запоминаться (поскольку пароль ни при каких условиях не должен нигде записываться, так как в этом случае необходимо будет дополнительно решать задачу защиты носителя пароля).

Требование не повторяемости паролей может быть реализовано двумя способами. Во-первых, можно установить минимальный срок действия пароля (в противном случае пользователь, вынужденный после истечения срока действия своего пароля поменять его, сможет тут же сменить пароль на старый). Во-вторых, можно вести список уже использовавшихся данным пользователем паролей (максимальная длина, списка при этом может устанавливаться администратором).

Постоянная блокировка учетной записи при обнаружении по-1 пытки подбора пароля (до снятия блокировки администратором) менее целесообразна, поскольку она позволит нарушителю намеренно заблокировать работу в КС легального пользователя (реализовать угрозу нарушения доступности информации).

При любой реакции системы на попытку подбора пароля необходимо в настройках параметров политики учетных записей обеспечить сброс значения счетчика попыток входа в систему под конкретной учетной записью через заданный промежуток времени, иначе значения счетчика будут суммироваться для разных сеансов работы пользователя.

Вопрос№2.Основные положения теории систем.