Лекция 15. Основные механизмы защиты, используемые в системах защиты информации (СЗИ) информационных систем (ИС)

1. Перечень защитных механизмов, используемых в СЗИ ИС.
2. Аутентификация и идентификация пользователей.
3. Разграничение доступа субъектов к ресурсам ИС.
4. Защита периметра компьютерной сети.

1.Перечень защитных механизмов, используемых в СЗИ ИС.

Я знаю, что ты можешь напакостить, но я тебя вычислю и ноги тебе переломаю …..

Перечень основных задач, которые должны решаться системой компьютерной безопасности:

•управление доступом пользователей к ресурсам АС с целью ее защиты от неправо-мерного случайного или умышленного вмешательства в работу системы и НСД; •защита данных, передаваемых по каналам связи;

• регистрация, сбор, хранение, обработка и выдача сведений обо всех событиях, происходящих в системе и имеющих отношение к ее безопасности;

•контроль работы пользователей системы со стороны администрации и оперативное оповещение администратора безопасности о попытках НСД к ресурсам системы;

•контроль и поддержание целостности критичных ресурсов системы защиты и среды исполнения прикладных программ;

• обеспечение замкнутой среды проверенного программного обеспечения с целью защиты от бесконтрольного внедрения в систему потенциально опасных программ (закладки или опасные ошибки) и средств преодоления системы защиты, а также от внедрения и распространения компьютерных вирусов;

•управление средствами системы защиты.

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
1. Подсистема управления доступом									
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:									
в систему;	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ;	-	-	-	+	-	+	+	+	+
к программам;	-	-	-	+	-	+	+	+	+
к томам, каталогам, файлам, записям, полям записей.	-	-	-	+	-	+	+	+	+
1.2. Управление потоками информации.	-	-	-	+	-	-	+	+	+
2. Подсистема регистрации и учета									
2.1. Регистрация и учет:									
входа/выхода субъектов доступа в/из системы (узла сети);	+	+	+	+	+	+	+	+	+
выдачи печатных (графических) выходных документов;	-	+	-	+	-	+	+	+	+
запуска/завершения программ и процессов (заданий, задач);	-	-	-	+	-	+	+	+	+
доступа программ субъектов доступа к защищаемым файлам, включая их создания и удаления, передачу по линиям и каналам связи;	-	-	-	+	-	+	+	+	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;	-	-	-	+	-	+	+	+	+
изменения полномочий субъектов доступа;	-	-	-	-	-	-	+	+	+
создаваемых защищаемых объектов доступа.	-	-	-	+	-	-	+	+	+
2.2. Учет носителей информации.	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей.	-	+	-	+	-	+	+	+	+
2.4. Сигнализация попыток нарушения защиты.	-	-	-	-	-	-	+	+	+
3. Криптографическая подсистема									
3.1. Шифрование конфиденциальной информации.	-	-	-	+	-	-	-	+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах.	-	-	-	-	-	-	-	-	+
3.3. Использование аттестованных (сертифицированных) криптографических средств.	-	-	-	+	-	-	-	+	+
4. Подсистема обеспечения целостности									
4.1. Обеспечения целостности программных средств и обрабатываемой информации.	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации.	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в АС.	-	-	-	+	-	-	+	+	+
4.4. Периодическое тестирование СЗИ ***НСД***.	+	+	+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ ***НСД***.	+	+	+	+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты.	-	+	-	+	-	-	+	+	+

2. Аутентификация и идентификация пользователей

Идентификация - Сопоставление пользователя и его данных (в частности, его идентификатора) (грубо говоря, отделение одного пользователя от другого). Идентификатор – имя пользователя.

Аутентификация - Сопоставление пользователя (уже идентифицированного, можно сказать, что сопоставление идентификатора) и его атрибутов безопасности (на основе секрета: пароль, биометрические данные, …..).

Авторизация - проверка атрибутов безопасности пользователя на наличие полномочий на выпол-нение определенного

3. Разграничение доступа субъектов к ресурсам ИС

Отношение "субъекты-объекты" можно представить в виде **матрицы доступа**, в строках которой перечислены субъекты, в столбцах – объекты, а в клетках, расположенных на пересечении строк и столбцов, записаны дополнительные условия (например, время и место действия) и разрешенные виды доступа. Фрагмент матрицы может выглядеть, например, так:

Таблица 1 - Фрагмент матрицы доступа

"o" – обозначает разрешение на передачу прав доступа другим пользователям,
"r" – чтение,
"w" – запись,
"e" – выполнение,
"a" – добавление информации

Пользователи	**Файл**	**Программа**	**Линия связи**	Реляционная таблица
Пользователь 1	orw С системной консоли	e	rw с 8:00 до 18:00	
Пользователь 2				a

1. **Мандатный доступ** (лицо, имеющее право доступа к информации с грифом “совершенно-секретно” допущен ко всей информации с “нижними грифами”).
2. **Ролевой доступ** (лицо имеет доступ к информации в соответствии с его ролью в учреждении).

4. Защита периметра компьютерной сети

Основные угрозы, исходящие из внешних сетей:

- Сканирование портов и сбор сведений о работающих сервисах, в том числе через сбор «баннеров» (service banners) — приглашений, выдаваемых службой при соединении с ней.
- Атаки переполнения буфера с целью получения контроля над системой.
- DoS-атаки.
- Проникновение вирусов и червей.

Основным методом защиты периметра является применение межсетевых экранов (фильтров) (firewall), также называемых брандмауэрами.

Межсетевой экран (firewall) — программа или аппаратно-прог-раммный комплекс, который располагается между сетями с различными уровнями доверия и фильтрует (блокирует или разрешает) пакеты согласно правилам фильтрации, заложен-ным администратором сети.