ДОКЛАД НА ТЕМУ

КЛАССИФИКАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ (АС) ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА (НСД). ТРЕБОВАНИЯ ПО ЗАЩИТЕ АС

НЕСАНЦИОНИРОВАННЫЙ ДОСТУП

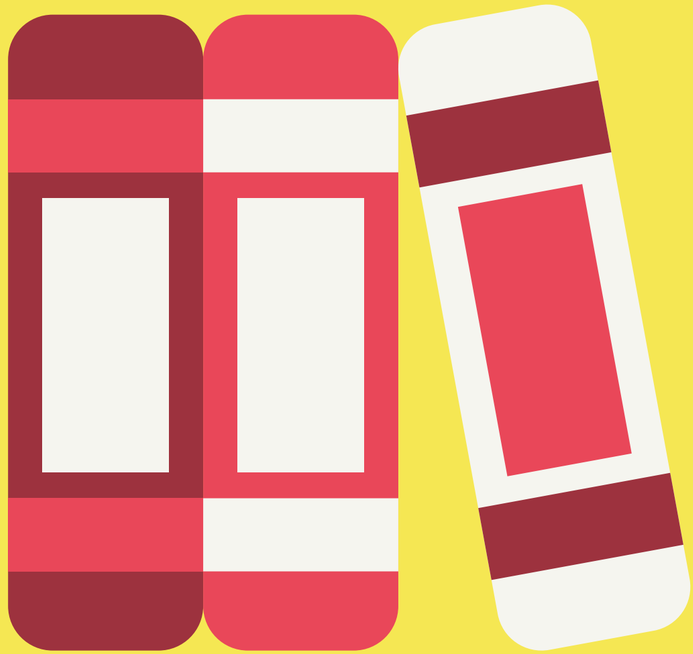
- НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ - ДОСТУП К ИНФОРМАЦИИ ОСУЩЕСТВЛЯЕМЫЙ С НАРУШЕНИЕМ УСТАНОВЛЕННЫХ ПРАВ И (ИЛИ) ПРАВИЛ ДОСТУПА К ИНФОРМАЦИИ С ПРИМЕНЕНИЕМ ШТАТНЫХ СРЕДСТВ ПРЕДОСТАВЛЯЕМЫХ СРЕДСТВАМИ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ (СВТ) ИЛИ АВТОМАТИЗИРОВАННЫМИ СИСТЕМАМИ (АС), ИЛИ СРЕДСТВ АНАЛОГИЧНЫХ ИМ ПО СВОИМ ФУНКЦИОНАЛЬНОМУ ПРЕДНАЗНАЧЕНИЮ И ТЕХНИЧЕСКИМ ХАРАКТЕРИСТИКАМ.

ОСНОВНЫМИ ЭТАПАМИ КЛАССИФИКАЦИИ АС ЯВЛЯЮТСЯ:

- РАЗРАБОТКА И АНАЛИЗ ИСХОДНЫХ ДАННЫХ;
- ВЫЯВЛЕНИЕ ОСНОВНЫХ ПРИЗНАКОВ АС, НЕОБХОДИМЫХ ДЛЯ КЛАССИФИКАЦИИ;
- СРАВНЕНИЕ ВЫЯВЛЕННЫХ ПРИЗНАКОВ АС С КЛАССИФИЦИРУЕМЫМИ;
- ПРИСВОЕНИЕ АС СООТВЕТСТВУЮЩЕГО КЛАССА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД.

УГРОЗЫ НСД К ИНФОРМАЦИИ С ПРИМЕНЕНИЕМ ПРОГРАММНЫХ СРЕДСТВ ВКЛЮЧАЮТ В СЕБЯ:

-УГРОЗЫ ДОСТУПА (ПРОНИКНОВЕНИЯ) В ОПЕРАЦИОННУЮ СРЕДУ КОМПЬЮТЕРА С ИСПОЛЬЗОВАНИЕМ ШТАТНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (СРЕДСТВ
ОПЕРАЦИОННОЙ СИСТЕМЫ ИЛИ ПРИКЛАДНЫХ ПРОГРАММ ОБЩЕГО ПРИМЕНЕНИЯ);
-УГРОЗЫ СОЗДАНИЯ НЕШТАТНЫХ РЕЖИМОВ РАБОТЫ ПРОГРАММНЫХ СРЕДСТВ ЗА СЧЕТ ПРЕДНАМЕРЕННЫХ ИЗМЕНЕНИЙ СЛУЖЕБНЫХ ДАННЫХ, ИГНОРИРОВАНИЯ
ПРЕДУСМОТРЕННЫХ В ШТАТНЫХ УСЛОВИЯХ ОГРАНИЧЕНИЙ НА СОСТАВ И ХАРАКТЕРИСТИКИ
ОБРАБАТЫВАЕМОЙ ИНФОРМАЦИИ, ИСКАЖЕНИЯ (МОДИФИКАЦИИ) САМИХ ДАННЫХ И Т.П.;
-УГРОЗЫ ВНЕДРЕНИЯ ВРЕДОНОСНЫХ ПРОГРАММ (ПРОГРАММНО-МАТЕМАТИЧЕСКОГО
ВОЗДЕЙСТВИЯ).



Третья группа

АС, в которых работает ***один пользователь***, допущенный ***ко всей информации*** АС, размещенной на носителях одного уровня конфиденциальности

3 А — информация, составляющая гостайну

3 Б — служебная тайна или персональные данные

Вторая группа

АС, в которых ***пользователи имеют одинаковые права доступа*** (полномочия) ***ко всей информации*** АС, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности

2 А — информация, составляющая гостайну

2 Б — служебная тайна или персональные данные

Первая группа

многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация ***разных уровней конфиденциальности*** и ***не все*** пользователи ***имеют право доступа ко всей информации*** АС

1 А | **1 Б** | **1 В** | **1 Г** | **1 Д**

АС, в которых циркулирует информация, составляющая гостайну: 1А, 1Б и 1В.

1 В - в случае обработки секретной информации с грифом не выше «секретно»

1 Б - в случае обработки секретной информации с грифом не выше «совершенно секретно»

1 А - в случае обработки секретной информации с грифом «особая важность»

1 Г - АС, в которых циркулирует служебная тайна

1 Д - АС, в которых циркулируют персональные данные

ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ НСД ДЛЯ АС.

. ЗАЩИТА ИНФОРМАЦИИ ОТ НСД ЯВЛЯЕТСЯ СОСТАВНОЙ ЧАСТЬЮ ОБЩЕЙ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ. МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ НСД ДОЛЖНЫ ОСУЩЕСТВЛЯТЬСЯ ВЗАИМОСВЯЗАНО С МЕРОПРИЯТИЯМИ ПО СПЕЦИАЛЬНОЙ ЗАЩИТЕ ОСНОВНЫХ И ВСПОМОГАТЕЛЬНЫХ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ, СРЕДСТВ И СИСТЕМ СВЯЗИ ОТ ТЕХНИЧЕСКИХ СРЕДСТВ РАЗВЕДКИ И ПРОМЫШЛЕННОГО ШПИОНАЖА.

. В ОБЩЕМ СЛУЧАЕ, КОМПЛЕКС ПРОГРАММНО-ТЕХНИЧЕСКИХ СРЕДСТВ И ОРГАНИЗАЦИОННЫХ (ПРОЦЕДУРНЫХ) РЕШЕНИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ НСД РЕАЛИЗУЕТСЯ В РАМКАХ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД (СЗИ НСД), УСЛОВНО СОСТОЯЩЕЙ ИЗ СЛЕДУЮЩИХ ЧЕТЫРЕХ ПОДСИСТЕМ:
- УПРАВЛЕНИЯ ДОСТУПОМ;
- РЕГИСТРАЦИИ И УЧЕТА;
- КРИПТОГРАФИЧЕСКОЙ;
- ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ.

. В ЗАВИСИМОСТИ ОТ КЛАССА АС В РАМКАХ ЭТИХ ПОДСИСТЕМ ДОЛЖНЫ БЫТЬ РЕАЛИЗОВАНЫ ТРЕБОВАНИЯ В СООТВЕТСТВИИ С ПП. 2.4, 2.7 И 2.10. ПОДРОБНО ЭТИ ТРЕБОВАНИЯ СФОРМУЛИРОВАНЫ В ПП. 2.5, 2.6, 2.8, 2.9 И 2.11-2.15.

ТРЕБОВАНИЯ К АС ТРЕТЬЕЙ ГРУППЫ

Подсистемы и требования	Классы	
	3Б	3А
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) систему(ы) (узел сети)	+	+
выдачи печатных (графических) выходных документов	-	+
запуска (завершения) программ и процессов (заданий, задач)	-	-
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, 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	-	-
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. Обеспечение 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	-	+

ТРЕБОВАНИЯ К АС ВТОРОЙ ГРУППЫ

Подсистемы и требования	Классы	
	2Б	2А
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) систему (узел сети)	+	+
выдачи печатных (графических) выходных документов	-	+
запуска (завершения) программ и процессов (заданий, задач)	-	+
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, 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. Обеспечение 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	-	+

ТРЕБОВАНИЯ К АС ПЕРВОЙ ГРУППЫ

Подсистемы и требования	Классы				
	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) систему (узел сети)	+	+	+	+	+
выдачи печатных (графических) выходных документов	-	+	+	+	+
запуска (завершения) программ и процессов (заданий, задач)	-	+	+	+	+
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, 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. Обеспечение 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	-	-	+	+	+

СПАСИБО ЗА ВНИМАНИЕ!