Курс: **основы информационной безопасности**

Тема: **Категории нарушителей ИБ**

Преподаватель: Пятков
Антон Геннадьевич

Красноярск

Модель нарушителя

Модель нарушителя – абстрактное (формализованное/неформализованное) описание нарушителя правил разграничения доступа.

Модель нарушителя может иметь разную степень детализации. Определяет:

- ✔ категории (типы) нарушителей, которые могут воздействовать на объект;
- ✔ цели, которые могут преследовать нарушители каждой категории, количественный состав, используемые инструменты;
- ✔ типовые сценарии возможных действий нарушителей, описывающие последовательность (алгоритм) действий групп и отдельных нарушителей, способы их действий на каждом этапе.

С точки зрения права доступа в контролируемую зону в КЗ нарушители бывают:

- ✔ внешние (не имеющие права доступа в КЗ территории/помещения);
- ✔ внутренние (имеющие право доступа в КЗ территории/помещения).

Варианты моделей нарушителя

Содержательная модель нарушителей отражает систему принятых руководством объекта, ведомства взглядов на контингент потенциальных нарушителей, причины и мотивацию их действий, преследуемые цели и общий характер действий в процессе подготовки и совершения акций воздействия.

Сценарии воздействия нарушителей определяют классифицированные типы совершаемых нарушителями акций с конкретизацией алгоритмов и этапов, а также способов действия на каждом этапе.

Математическая модель воздействия нарушителей представляет собой формализованное описание сценариев в виде логико-алгоритмической последовательности действий нарушителей, количественных значений, параметрически характеризующих результаты действий, и функциональных (аналитических, численных или алгоритмических) зависимостей, описывающих протекающие процессы взаимодействия нарушителей с элементами объекта и системы охраны. Именно этот вид модели используется для количественных оценок уязвимости объекта и эффективности охраны.

Модель нарушителя по РД (ФСТЭК)

Согласно РД ГТК по защите АС от НСД к информации в качестве нарушителя рассматривается субъект, имеющий доступ к работе со штатными средствами АС и СВТ как части АС. Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ.
Выделяется 4 уровня этих возможностей (классификация иерархическая, т.е. каждый следующий уровень включает в себя предыдущий):
1 уровень определяет самый низкий уровень возможностей ведения диалога в АС (запуск задач/программ из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации);
2 уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации;
3 уровень определяется возможностью управления функционированием АС, т.е. воздействием на базовое ПО системы, состав и конфигурацию оборудования;
4 уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

! в своем уровне нарушитель является специалистом высшей квалификации, знает всё об АС и, в частности, о системе и средствах её защиты.

Модель вероятного нарушителя ИБ

Под нарушителем понимается физическое лицо, случайно или преднамеренно совершающее действия, результатом которых является нарушение безопасности защищаемой информации при её обработке в АС. Для построения формируем категории нарушителей для каждого типа нарушителя (внутренние и внешние) распределяем типы угроз между ними в виде матрицы (таблицы).

Тип угрозы	Нарушитель				
	Оператор	Сотрудник из управления	Программист	Инженер по техническому обслуживанию	Пользователь
Изменение кодов	+		+		
Копирование файлов	+		+		
Уничтожение файлов	+	+	+		+
Присвоение программ			+		
Шпионаж	+	+	+	+	
Установка подслушивания			+	+	
Саботаж	+		+		
Продажа данных	+	+	+		+
Воровство			+	+	+

Пример простой модели нарушителя ИБ

Наименование	Тип нарушителя	Описание возможностей
Основной/вспомогательный персонал	Внутренний	Обладают хорошими знаниями в области эксплуатации ПО и технических средств, знакомы со спецификой
Представители служб безопасности, технический персонал	Внутренний	Хорошо знакомы со структурой, основными функциями и принципами работы программно-аппаратных средств ЗИ
Лица, распространяющие вирусы/вредоносные программы, другие лица, осуществляющие НСД	Внешний	Обладают достаточными знаниями в области осуществления НСД к ресурсам ИС
Представители менеджмента организации	Внутренний	Являются наиболее актуальными источниками угроз на уровне бизнес-процессов
Поставщики различных услуг, персонал надзорных организаций и аварийных служб	Внешний	Возможные реализуемые угрозы: уничтожение, блокирование, искажение информации. Действия совершаются по незнанию, невнимательности или халатности, но без злого умысла.
Недобросовестные партнеры, хакеры	Внешний	Способны умышленно дезорганизовать работу, вывести системы из строя, разгласить и исказить конф. инфорации за счет НСД к информации и утечки по ТКУИ
Клиенты	Внешний	Могут нанести ущерб намеренно или по незнанию

Пример модели нарушителя ИБ

Модель угроз внутренних нарушителей

№ п/п	Тип угроз безопасности АС	Внутренние нарушители			
		1 Кат.	2 Кат.	3 Кат.	4 Кат.
1	Угрозы утечки информации по техническим каналам.				
1.1	Угрозы утечки акустической (речевой) информации.	+	+	+	+
1.2	Угрозы утечки видовой информации	+	+	+	+
1.3	Угрозы утечки информации по каналу ПЭМИН	-	-	-	-
2	Угрозы несанкционированного доступа				
2.1	Кража ПЭВМ	+	+	+	+
2.2	Кража носителей информации	+	+	+	+
2.3	Кража ключей и атрибутов доступа	+	+	-	+
2.4	Кража, модификация, уничтожение информации	-	+	+	-
2.5	Несанкционированный доступ к информации при техническом обслуживании (ремонте, замене) узлов ПЭВМ	-	-	+	+
3	Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств				
3.1	Действия вредоносных программ (вирусов)	-	+	+	+
3.2	Не декларированные возможности системного ПО	-	-	+	+
3.3	Установка ПО, не связанного с исполнением служебных обязанностей	-	+	+	+
4	Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования АС из-за сбоев в программном обеспечении, а также от угроз неантропогенного и характера				
4.1	Утрата ключей и атрибутов доступа	-	+	+	-
4.2	Непреднамеренная модификация (уничтожение) информации сотрудниками	-	+	+	-
4.3	Непреднамеренное изменение настроек средств защиты	-	+	+	+
4.4	Выход из строя аппаратно-программных средств	+	+	+	+
4.5	Сбой системы электроснабжения	-	-	-	-
4.6	Стихийное бедствие	-	-	-	-
5	Угрозы преднамеренных действий пользователей				
5.1	Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	+	-	-	+
5.2	Разглашение, модификация, уничтожение информации сотрудниками, допущенными к ее обработке	-	+	+	-
6	Угрозы несанкционированного доступа по каналам связи				
6.1	Анализ сетевого трафика	+	+	+	+
6.2	Сканирование сети	+	+	+	+
6.3	Отказ в обслуживании	+	+	+	+

Пример модели нарушителя ИБ

Модель угроз внешних нарушителей

№ п/п	Тип угроз безопасности АС	Внешние нарушители		
		1 Кат.	2 Кат.	3 Кат.
1	Угрозы утечки информации по техническим каналам.			
1.1	Угрозы утечки акустической (речевой) информации.	-	+	+
1.2	Угрозы утечки видовой информации	-	+	+
1.3	Угрозы утечки информации по каналу ПЭМИН	-	-	-
2	Угрозы несанкционированного доступа			
2.1	Кража ПЭВМ	-	+	+
2.2	Кража носителей информации	+	+	+
2.3	Кража ключей и атрибутов доступа	+	+	+
2.4	Кража, модификация, уничтожение информации	-	+	+
2.5	Несанкционированный доступ к информации при техническом обслуживании (ремонте, замене) узлов ПЭВМ	-	-	+
3	Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств			
3.1	Действия вредоносных программ (вирусов)	+	+	+
3.2	Недекларированные возможности системного ПО	-	-	+
3.3	Установка ПО, не связанного с исполнением служебных обязанностей	-	+	+
4	Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования АС из-за сбоев в программном обеспечении, а также от угроз неантропогенного и стихийного характера			
4.1	Утрата ключей и атрибутов доступа	-	+	+
4.2	Непреднамеренная модификация (уничтожение) информации сотрудниками	-	+	+
4.3	Непреднамеренное изменение настроек средств защиты	-	+	+
4.4	Выход из строя аппаратно-программных средств	-	+	+
4.5	Сбой системы электроснабжения	+	+	+
4.6	Стихийное бедствие	-	-	-
5	Угрозы преднамеренных действий пользователей			
5.1	Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	-	+	+
5.2	Разглашение, модификация, уничтожение информации сотрудниками, допущенными к ее обработке	-	+	+
6	Угрозы несанкционированного доступа по каналам связи			
6.1	Анализ сетевого трафика	+	+	+
6.2	Сканирование сети	+	+	+
6.3	Отказ в обслуживании	+	+	+

Модели нарушителя от ФСБ

Модель нарушителя – предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

Различают 6 основных типов нарушителей: H_1, H_2, ... , H_6.

H_1: одиночный нарушитель, располагает только доступной в свободной продаже документацией и компонентами СКЗИ, может использовать штатные средства только если они расположены за пределами КЗ;

H_2: H_1 + обладает возможностями по созданию способов подготовки атак, возможности по использованию штатных средств зависят от реализованных в ИС организационных мер ЗИ;

H_3: H_2 + известны все сети связи, работающие на едином ключе, могут иметь дополнительные возможности по получению компонент СКЗИ;

H_4: H_3 + могут вступать в сговор;

H_5: H_4 + имеющие доступ к исходным текстам прикладного ПО;

H_6: H_5 + располагают всей документацией на СКЗИ, любыми компонентами СКЗИ

Предполагается, что нарушители типа H_5 и H_6 могут ставить работы по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа криптосредств.