**Лабораторная работа №3**

**Определение актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности**

В данной работе предполагается продолжение знакомства с документом «Методика оценки угроз безопасности информации», а также подготовка к созданию модели нарушителя персональной информационной системы.

**Теоретические сведения**

Согласно методическому документу, определение источников угроз безопасности информации является частью моделирования угроз, хотя кажется более логичным определять их до моделирования, сразу же после определения возможных негативных последствий.

Методика определяет основные виды нарушителей (спецслужба иностранного государства, террористическая группировка, криминальная группа, авторизованные пользователи информационной системы и сети). Этот перечень не является исчерпывающим и при необходимости может дополняться. Также перечень не является классификацией: так, авторизованный пользователь может быть членом преступной группы, которая, в свою очередь, может действовать в интересах иностранной спецслужбы.

Основная задача, которая решается определением видов нарушителя – сформулировать цель (т. е. мотив) действий нарушителя и решить, признается ли нарушитель данного вида актуальным для информационной системы или информационно-телекоммуникационной сети, если одно или несколько рассматриваемых в процессе моделирования негативных последствий, соответствуют целям, определенным для данного вида нарушителей в Приложении 6 методического документа.

Вид нарушителя, в свою очередь, определяет уровень его возможностей. Методика определяет четыре уровня возможностей нарушителя: базовый (Н1), базовый повышенный (Н2), средний (Н3) и высокий (Н4). Подробное описание возможностей нарушителей разных уровней приведено в Приложении 8 методического документа. Вкратце их можно охарактеризовать следующим образом.

Нарушитель уровня Н1 не является специалистом, он использует только известные уязвимости и бесплатные инструменты.

Нарушитель уровня Н2 также использует только свободно распространяемые инструменты, но является специалистом. Он способен находить и использовать уязвимости нулевого дня на атакуемых объектах.

Нарушитель уровня Н3 дополнительно к этому способен приобретать дорогостоящие инструменты и проводить лабораторные исследования по поиску уязвимостей нулевого дня в оборудовании и программных средствах, аналогичных используемым на атакуемых объектах.

Нарушитель уровня Н4 способен внедрять программные и аппаратные закладки в серийно изготавливаемое оборудование и программное обеспечение, может использовать побочное электромагнитное излучение, наводки и скрытые каналы, умеет проводить долгосрочные APT-атаки и обладает неограниченными ресурсами.

Таким образом, методика задает прямое соответствие между негативными последствиями, целями нарушителей различных видов и их возможностями. При этом принятие решения о соответствии возможных негативных последствий целям нарушителей оставлено на усмотрение экспертов, проводящих анализ угроз. Так, для информационной системы персональных данных, используемой предприятием розничной торговли для учета заказов покупателей, допустимо признать неактуальными угрозы со стороны спецслужб. Здравый смысл подсказывает, что атака на подобный информационный ресурс не приведет к «нанесению ущерба государству в области обеспечения обороны, безопасности и правопорядка…», и при этом нет нормативных требований, обязывающих оператора информационной системы считать подобного нарушителя актуальным.

Кроме того, методика подразделяет нарушителей на внешних и внутренних. Нарушитель считается внешним, если он не имеет ни санкционированного физического доступа в контролируемую зону, ни санкционированного удаленного доступа к интерфейсам информационной системы. Подобное разделение является чистой условностью: единственное, что отличает моделирование угроз со стороны внешнего нарушителя, это необходимость рассмотрения в сценариях реализации угроз техник первичного проникновения в ИТ-инфраструктуру атакуемой организации.

Наряду с нарушителями, в качестве источников угроз безопасности информации рассматриваются и техногенные источники – исходя из контекста, речь идет об источниках угроз, не

являющихся непосредственным результатом целенаправленного или ошибочного действия человека. На практике рассматривать такие источники угроз целесообразно только в тех случаях, когда связанные с ними негативные последствия не соответствуют целям ни одного из нарушителей: практически все, что может произойти спонтанно, может произойти и в результате целенаправленного вредительства, а значит будет учтено при моделировании угроз со стороны нарушителя.

**Задания:**

**1. Определить виды нарушителей, актуальные для персональной ИС.**

1.1. Используя таблицу «Возможные цели реализации угроз безопасности информации нарушителями», полученную в лабораторной работе №2, оценить цели реализации данных угроз. Для этого необходимо составить таблицу по примеру из Приложения 7 «Методики оценки угроз безопасности» (Учесть, что в нашем частном случае актуально только «нанесение ущерба физическому лицу»).

1.2. Используя таблицу «Уровни возможностей нарушителей по реализации угроз безопасности информации» (с.56-59), составить таблицу по примеру на с. 60.

**2. Определить актуальные способы реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности.**

2.1. Объединить ранее составленные таблицы и получить новую по примеру на с.62.

Содержание отчёта:

1. Титульный лист.
2. Таблица «Оценка целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации».
3. Таблица «Результат определения актуальных нарушителей при реализации угроз безопасности информации и соответствующие им возможности»
4. Таблица «Определение актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности».
5. Вывод.
6. Ответ на контрольные вопросы:
    a. С какими видами нарушителей вы встречались в своей практике пользования ИС?
    b. Опишите три любых сценария утечки данных из вашей ИС (количество слов в каждом сценарии не менее 50).