**Лабораторная работа №4**

**Оценка сценариев реализации угроз и актуальности угроз. Модель угроз персональной ИС.**

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**

В ходе оценки угроз безопасности информации должны быть определены возможные способы реализации (возникновения) угроз безопасности информации, за счет использования которых актуальными нарушителями могут быть реализованы угрозы безопасности информации в системах и сетях, – актуальные способы реализации (возникновения) угроз безопасности информации.

Исходными данными для определения актуальных способов реализации (возникновения) угроз безопасности информации являются:

а) общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

б) описания векторов компьютерных атак, содержащихся в базах данных и иных источниках, опубликованных в сети «Интернет» (CAPEC, ATT&CK, OWASP, STIX, WASC и др.);

в) документация на системы и сети (в части сведений о составе и архитектуре, о группах пользователей и их типах доступа и уровней полномочий, о внешних и внутренних интерфейсах);

г) негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в соответствии с Методикой оценки угроз безопасности информации;

д) объекты воздействия угроз безопасности информации и соответствующие им виды воздействия, определенные в соответствии с Методикой оценки угроз безопасности информации;

е) виды и категории актуальных нарушителей, которые могут реализовывать угрозы безопасности информации, в том числе непреднамеренные угрозы, и их возможности, определенные в соответствии с Методикой оценки угроз безопасности информации.

На основе анализа исходных данных, а также возможностей нарушителей определяются способы реализации (возникновения) угроз безопасности информации, актуальные для систем и сетей.

Основными способами реализации (возникновения) угроз безопасности информации являются:

1) использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей);

2) внедрение вредоносного программного обеспечения;

3) использование недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств;

4) установка программных и (или) программно-аппаратных закладок в программное обеспечение и (или) программно-аппаратные средства;

5) формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных;

6) перехват (измерение) побочных электромагнитных излучений и наводок (других физических полей) для доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации;

7) инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации;

8) нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию);

9) ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств.

Способы реализации (возникновения) угроз безопасности информации определяются применительно к объектам воздействия, определенным в соответствии с Методикой оценки угроз безопасности информации. Способы являются актуальными, когда возможности нарушителя позволяют их использовать для реализации угроз безопасности и имеются или созданы условия, при которых такая возможность может быть реализована в отношении объектов воздействия. Одна угроза безопасности информации может быть реализована несколькими способами.

Условием, позволяющим нарушителям использовать способы реализации угроз безопасности информации, является наличие у них возможности доступа к следующим типам интерфейсов объектов воздействия:

* внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными (взаимодействующими) системами или сетями (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);
* внутренние сетевые интерфейсы, обеспечивающие взаимодействие (в том числе через промежуточные компоненты) с компонентами систем и сетей, имеющими внешние сетевые интерфейсы (проводные, беспроводные);
* интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);
* интерфейсы для использования съемных машинных носителей информации и периферийного оборудования;
* интерфейсы для установки, настройки, испытаний, пусконаладочных работ (в том числе администрирования, управления, обслуживания) обеспечения функционирования компонентов систем и сетей;
* возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей.

Наличие указанных интерфейсов определяется архитектурой, составом и условиями функционирования систем и сетей, группами пользователей, их типами доступа и уровнями полномочий. В ходе анализа должны быть определены как логические, так и физические интерфейсы объектов воздействия, в том числе требующие физического доступа к ним.

Интерфейсы определяются на аппаратном, системном и прикладном уровнях систем и сетей, а также для телекоммуникационного оборудования. Возможность их использования на указанных уровнях определяется возможностями актуальных нарушителей.

На этапе создания систем и сетей определение интерфейсов объектов воздействия, которые могут использоваться для реализации угроз безопасности, проводится на основе предполагаемой архитектуры и условий функционирования систем и сетей, определенных на основе изучения и анализа исходных данных о них.

На этапе эксплуатации систем и сетей для определения интерфейсов объектов воздействия, которые могут использоваться для реализации угроз безопасности, дополнительно к документации на сети и системы используются результаты инвентаризации систем и сетей, проведенной с использованием автоматизированных средств.

Угроза признается возможной, если определяется нарушитель, целям которого соответствуют негативные последствия реализации угрозы, и возможности которого позволяют выполнить соответствующее воздействие. Если угроза признается возможной, остается оценить может ли выбранный нарушитель практически реализовать угрозу, рассмотрев возможные сценарии реализации угрозы – последовательности тактик и техник действий нарушителя, посредством которой он мог бы из некоторого начального состояния получить возможности, необходимые для реализации угрозы. На практике это означает оценку того, может ли нарушитель из заданных стартовых условий “пройти” по ИТ-инфраструктуре организации и получить практическую возможность реализовать угрозу.

Угроза признается актуальной, если есть хотя бы один сценарий ее реализации. На стадии создания информационной системы актуальность угрозы означает необходимость усиления и дополнения базового набора мер защиты с тем, чтобы нейтрализовать угрозу. На стадии эксплуатации актуальность угрозы означает необходимость модернизации системы защиты, направленную на усиление и дополнение уже реализованных мер защиты.

**Задания:**

1. **Дополнить перечень угроз.**
   1. Используя банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), выбрать актуальные для своей персональной информационной системы угрозы. Таких угроз должно быть выбрано **не менее 5**.
   2. Внести информацию об угрозах в таблицу, полученную в Лабораторной работе №3 «Определение актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности» (последняя результирующая таблица работы) // *«Описание угрозы» внести в столбец «Способ реализации».*
2. **Предположить возможные сценарии реализации угроз.**
   1. Выбрать из Приложения 11 к Методике оценки угроз безопасности информации **все** актуальные тактики и основные техники реализации угроз (данные внести в таблицу с соответствующим названием.
   2. Подробно описать один из возможных вариантов реализации угроз, для описания использовать простую блок-схему или язык uml.
3. **Разработка Модели угроз персональной ИС.**
   1. Собрать в единый документ с названием «Модель угроз «Название вашей ИС»» все ранее полученные результаты (Лабораторных работ 1-4) по примеру, приведенному на страницах 39-41 Методики оценки угроз безопасности.

Содержание отчёта:

1. Титульный лист.
2. Модель угроз персональной ИС.
3. Вывод.
4. Ответ на контрольные вопросы:
   1. Зачем необходимо создавать Модель угроз в организации? Дать обоснованный ответ (не менее 100 слов).
   2. Что такое политика информационной безопасности?