Практическая работа №4

МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМЫ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

Цель работы. Изучить методику построения модели нарушителя информационной безопасности. Произвести классификацию определенного нарушителя и построить его модель.

Краткие сведения из теории

Модель нарушителя информационной безопасности – это набор предположений об одном или нескольких возможных нарушителях информационной безопасности, их квалификации, технических и материальных средствах и т. д.

Правильно разработанная модель нарушителя является гарантией построения адекватной системы обеспечения информационной безопасности. Опираясь на построенную модель, уже можно строить адекватную систему информационной защиты.

Чаще всего строится неформальная модель нарушителя, отражающая причины и мотивы действий, его возможности, априорные знания, преследуемые цели, их приоритетность для нарушителя, основные пути достижения поставленных целей: способы реализации исходящих от него угроз, место и характер действия, возможная тактика и т. п. Для достижения поставленных целей нарушитель должен приложить определенные усилия и затратить некоторые ресурсы. Например, модель нарушителя может быть представлена в форме таблицы, которая описывает характеристики некоторого нарушителя (таблица 1).

Таблица 1 – **Форма представления модели нарушителя информационной безопасности**

Характеристика	Нарушитель
Вычислительная мощность технических средств	
Доступ к интернету, тип каналов доступа	
Финансовые возможности	
Уровень знаний в области IT	
Используемые технологии	
Знания о построении системы защиты объекта	
Преследуемые цели	
Характер действий	
Глубина проникновения	

Определив основные причины нарушений, представляется возможным оказать на них влияние или необходимым образом скорректировать требования к системе защиты от данного типа угроз. При анализе нарушений за-

щиты необходимо уделять внимание субъекту (личности) нарушителя. Устранение причин или мотивов, побудивших к нарушению, в дальнейшем может помочь избежать повторения подобного случая.

Модель может быть не одна, целесообразно построить несколько отличающихся моделей разных типов нарушителей информационной безопасности объекта защиты.

Для построения модели нарушителя используется информация, полученная от служб безопасности и аналитических групп, данные о существующих средствах доступа к информации и ее обработки, о возможных способах перехвата данных на стадиях их передачи, обработки и хранении, об обстановке в коллективе и на объекте защиты, сведения о конкурентах и ситуации на рынке, об имевших место свершившихся случаях нарушения информационной безопасности и т. п.

Кроме этого оцениваются реальные оперативные технические возможности злоумышленника для воздействия на систему защиты или на защищаемый объект. Под техническими возможностями подразумевается перечень различных технических средств, которыми может располагать нарушитель в процессе совершения действий, направленных против системы информационной защиты.

В последнее время модель нарушителя информационной безопасности перестает быть простой формальностью и начинает оказывать большое влияние на перечень актуальных угроз для информационной системы. В перечне угроз для информационной системы для каждой угрозы задан тип и потенциал нарушителя, который может ее реализовать. За счет этого устанавливается взаимосвязь между перечнями угроз и нарушителями информационной безопасности.

Потенциал нарушителя может быть высоким, средним или низким. Для каждого из вариантов задан свой набор возможностей.

Так, нарушители с низким потенциалом могут для реализации атак использовать информацию только из общедоступных источников. К нарушителям с низким потенциалом можно отнести любых внешних лиц, а также внутренний персонал и пользователей информационной системы.

Внешние нарушители, к которым могут относиться и бывшие сотрудники, имеют возможность самостоятельно создавать способы атак, проводить их подготовку и реализацию только за пределами контролируемой зоны. Внутренний персонал имеет возможность проводить атаки в пределах контролируемой зоны с возможным физическим доступом к аппаратным средствам, на которых реализована ИС, в зависимости от величины штатных полномочий.

Нарушители со средним потенциалом имеют возможность проводить анализ кода прикладного программного обеспечения, самостоятельно находить в нем уязвимости и использовать их. К таким нарушителям можно от-

носить террористические и криминальные группы, конкурирующие организации, администраторов системы и разработчиков ПО. Эти нарушители имеют возможность привлекать специалистов с опытом разработки и анализа систем комплексной защиты информации (СКЗИ) (включая специалистов в области использования для реализации атак анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок, а также недокументированных возможностей прикладного программного обеспечения).

Нарушители с высоким потенциалом имеют возможность вносить закладки в программно-техническое обеспечение системы, проводить специальные исследования и применять специальные средства проникновения и добывания информации. К таким нарушителям следует относить только иностранные и отечественные спецслужбы. Они имеют возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования ИС).

Классификация нарушителей информационной безопасности. Нарушители бывают внутренними и внешними.

Среди внутренних нарушителей в первую очередь можно выделить:

– непосредственных пользователей и операторов информационной системы, в том числе руководителей различных уровней;

– администраторов вычислительных сетей и информационной безопасности;

– прикладных и системных программистов;

– сотрудников службы безопасности;

– технический персонал по обслуживанию зданий и вычислительной техники, от уборщицы до сервисного инженера;

– вспомогательный персонал и временных работников.

Среди причин, побуждающих сотрудников к неправомерным действиям, можно указать:

– безответственность;

– ошибки пользователей и администраторов;

– демонстрацию своего превосходства (самоутверждение);

– «борьбу с системой»;

– корыстные интересы пользователей системы;

– недостатки используемых информационных технологий.

Группу внешних нарушителей могут составлять:

– клиенты;

– приглашенные посетители;

– представители конкурирующих организаций;

– сотрудники органов ведомственного надзора и управления;

– нарушители пропускного режима;

– наблюдатели за пределами охраняемой территории.

Помимо этого классификацию можно проводить по следующим параметрам.

Используемые методы и средства:

– сбор информации и данных;

– пассивные средства перехвата;

– использование средств, входящих в информационную систему или систему ее защиты, и их недостатков;

– активное отслеживание модификаций существующих средств обработки информации, подключение новых средств, использование специализированных утилит, внедрение программных закладок и «черных ходов» в систему, подключение к каналам передачи данных.

Уровень знаний нарушителя относительно организации информационной структуры:

– типовые знания о методах построения вычислительных систем, сетевых протоколов, использование стандартного набора программ;

– высокий уровень знаний сетевых технологий, опыт работы со специализированными программными продуктами и утилитами;

– высокие знания в области программирования, системного проектирования и эксплуатации вычислительных систем;

– обладание сведениями о средствах и механизмах защиты атакуемой системы;

– нарушитель являлся разработчиком или принимал участие в реализации системы обеспечения информационной безопасности.

Время информационного воздействия:

– в момент обработки информации;

– в момент передачи данных;

– в процессе хранения данных (учитывая рабочее и нерабочее состояния системы).

По месту осуществления воздействия:

– удаленно с использованием перехвата информации, передающейся по каналам передачи данных, или без ее использования;

– доступ на охраняемую территорию;

– непосредственный физический контакт с вычислительной техникой, при этом можно выделить: доступ к рабочим станциям, серверам предприятия, системам администрирования, контроля и управления информационной системой, программам управления системы обеспечения информационной безопасности.

Порядок выполнения работы

1 В соответствии с последней цифрой шифра из таблицы 2 выбрать нарушителя информационной безопасности.

2 Определить потенциал нарушитель информационной безопасности.

3 Определить, к каким классам относится нарушитель информационной безопасности в соответствии с классификацией, представленной в кратких сведениях из теории.

Таблица 2 – **Нарушители информационной безопасности**

Цифра шифра	Нарушитель информационной безопасности	Цифра шифра	Нарушитель информационной безопасности
0	Несовершеннолетний хакер	5	Опытный хакер одиночка
1	Работник предприятия, не относящийся к службе ЗИ	6	Уволенный работник
2	Группа хакеров	7	Работник службы ЗИ предприятия
3	Спецподразделение конкурирующей компании	8	Разведка своего государства
4	Разведка другого государства	9	Террористическая группировка

4 Для выбранного нарушителя информационной безопасности построить модель в соответствии с указанной выше формой представления (см. таблицу 1), используя в качестве объекта защиты информационную систему, исследованную в практической работе № 1.

Содержание отчета

1 Цель работы.
2 Классификация и потенциал нарушителя информационной безопасности.
3 Модель нарушителя информационной безопасности.
4 Вывод по работе.

Контрольные вопросы

1 Что такое модель нарушителя информационной безопасности?
2 С какой целью строится модель нарушителя информационной безопасности?
3 Какова методика построения модели нарушителя информационной безопасности?
4 Что такое потенциал нарушителя информационной безопасности?
5 По каким основным критериям производится классификация нарушителей информационной безопасности?
6 Какие классы нарушителей информационной безопасности являются наиболее опасными для определенной информационной системы?