УДК 004.056.53

Ерышов Вадим Георгиевич, к.т.н., доцент,
Санкт-Петербургский государственный университет
аэрокосмического приборостроения, Санкт-Петербург

ИМИТАЦИОННАЯ МОДЕЛЬ СИСТЕМЫ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ОРГАНИЗАЦИИ ОТ КОМПЬЮТЕРНЫХ АТАК

Аннотация: в статье рассматривается модель системы комплексной защиты информационной системы организации от компьютерных атак. Данная модель может быть использована для оценки эффективности существующих, а также вновь создаваемых систем комплексной защиты информационных систем.

Ключевые слова: модель, информационная безопасность, защита информации, система защиты, компьютерные атаки, нарушения безопасности информации, конфиденциальная информация.

На современном этапе развития новых информационных систем (ИС), внедрения новейших информационных технологий, глобальной цифровизации экономики, в организациях резко возросла актуальность обеспечения информационной безопасности (ИБ), в частности, защиты информации (ЗИ) от компьютерных атак (КА), осуществляемых как иностранными государствами, так и организациями – конкурентами, ведущими промышленный шпионаж [1].

Компьютерные атаки происходят после проведения предварительной компьютерной разведки (КР), которая направлена на добывание разведывательной информации в ИС. После чего начинаются активные действия, направленные на получение несанкционированного доступа (НСД), осуществление несанкционированных воздействий (НСВ) на защищаемую информацию (ЗИ), нарушение функционирования ИС [2].

В связи с этим защита от КА (КР) является составной частью общего процесса обеспечения ИБ ИС в целом. В связи с этим для служб информационной безопасности (СИБ) любой современной организации актуальной становится задача обеспечения защиты от КА и КР, создания современных систем комплексной защиты информационных систем (СКЗ ИС) организации от КА. Для решения данной задачи необходимо проведение исследований в этой области, в том числе - разработка имитационной модели СКЗ ИС с целью определения вероятностно-временных характеристик, зависимостей, показателей, происходящих в них событий и состояний [3].

В связи с этим необходимо разработать имитационную модель, которая позволит в результате моделирования получить характеристики системы КА и СКЗ ИС.

Обобщенная модель СКЗ ИС от КА включает в себя [4]:

1) систему КА и подсистемы, реализующие добывание, сбор, анализ, управления и принятия решений, осуществления НСД, КА;

2) СКЗ ИС и ее подсистемы: сбора и обработки информации; анализа и управления, ЗИ;

3) защищаемые объекты, такие как: ИС, автоматизированные системы (АС). В современных организациях могут функционировать: АС, ИС объектов организаций, а также автоматизированные системы управления (АСУ).

Защищаемый объект может включать в себя следующие основные элементы: коммутационное оборудование; сегмент, состоящий из внешних серверов; сегмент, состоящий из внутренних серверов и сегмент ИС, состоящий из автоматизированных рабочих мест (АРМ).

СКЗ ИС должна включать в себя следующие основные подсистемы: систему криптографической защиты (СКЗИ), систему обнаружения вторжений (СОВ), межсетевой экран (МЭ), систему антивирусной защиты (САВЗ), систему анализа защищенности (САЗ), систему защиты от утечки КИ (DLP), СЗИ от НСД, систему управления ИБ (СУИБ, SIEM),

АРМ (сервер) администратора ИБ, который осуществляет управление процессом ЗИ и ряд других вспомогательных систем (резервирования и т.д.).

Первостепенная задача системы КА состоит в том, чтобы методом пассивного и активного сканирования IP адресов элементов ИС, перехвата, обработки и анализа сетевого трафика выявить структуру ИС и ее технические параметры, вскрыть ее (этап КР), после чего принять решение на осуществление того или иного вида действия, в том числе посредством КА.

Основными задачами СКЗ ИС являются своевременное и достоверное обнаружение и устранение уязвимостей, угроз ИБ, обнаружение и предотвращение нарушений безопасности информации – НБИ (НСД, НСВ, КА), расследование инцидентов ИБ и минимизация последствий от реализации КА.

Одной из известных систем, предназначенных для создания имитационных моделей, является система имитационного моделирования «AnyLogic», как одна из эффективных систем, позволяющих моделировать процессы в ИС. В связи с этим и был выбран данный инструмент для построения исследуемой модели и процесса [3].

Исходными данными для имитации действий системы КА, нарушителя ИБ, процесса защиты объекта являются:

количество: органов системы КА (нарушителей ИБ);

требуемые вероятности и времена: обнаружения, идентификации, анализа, принятия решения на вскрытие ИС, осуществление НБИ (КА);

количество и типы средств ЗИ объектов (защищаемых АС);

требуемые вероятности и времена: обнаружения, идентификации и предотвращения НБИ (КА).

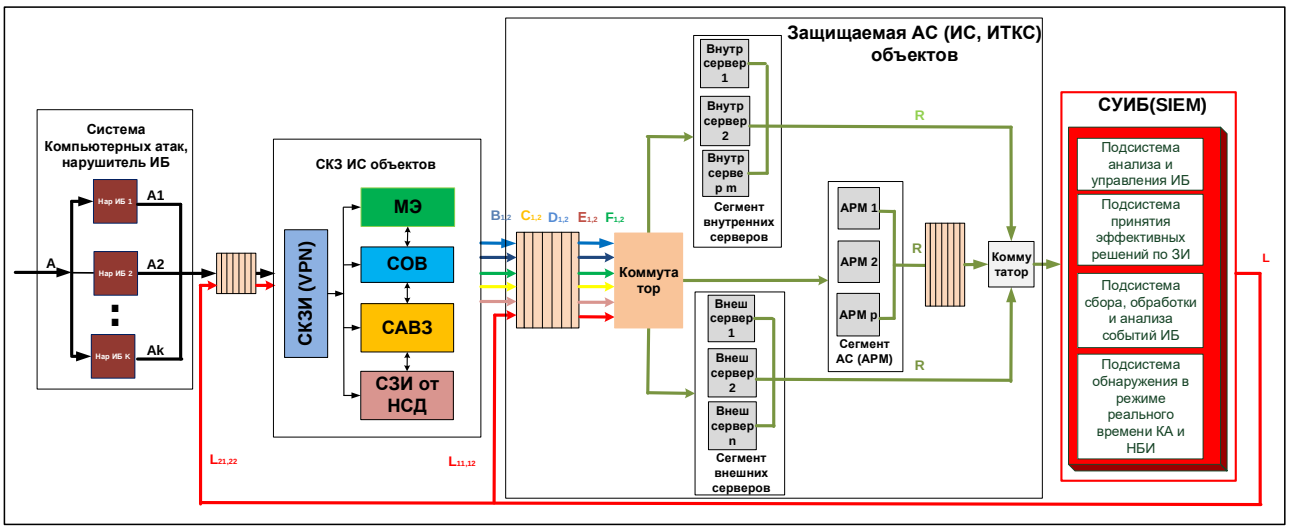
Модель представляет собой имитационную модель, реализованную в системе имитационного моделирования: «AnyLogic».

На рисунке 1 показана обобщенная структурная схема имитационной модели СКЗ ИС от КА.

В разработанной имитационной модели последовательность действий системы КА и последовательность функционирования СКЗ ИС с целью обнаружения КА и защиты от них моделируется следующими основными модулями:

Модуль № 1. В нем происходит имитация органов системы КА (нарушителя ИБ).

Модуль № 2. В нем происходит имитация процесса функционирования элементов ИС.



A - Поток заявок по созданию НБИ

B - Поток заявок, прошедших через СКЗИ

C - Поток заявок, прошедших через САВЗ

D - Поток заявок, прошедших через СОВ

E - Поток заявок, прошедших через СЗИ от НСД

F - Поток заявок, прошедших через МЭ

R - Поток заявок, прошедших через АРМы, внутренние и внешние серверы

L - Поток заявок, прошедших через СУИБ

Рисунок 1 – Структурная схема имитационной модели СКЗ ИС от КА

Модуль № 3. В нем происходит имитация процесса функционирования СКЗ ИС.

В разработанной модели система КА представляет сбой сеть СМО. Моделируется общий поток заявок от системы КА – «А» на осуществление процессов обнаружения, анализа и принятия решения на вскрытие защищаемой ИС, принятие решения о методе воздействия и осуществления НБИ (КА). СКЗ ИС в разработанной модели представлена совокупностью последовательно включенных друг за другом подсистем ЗИ: СКЗИ, СОВ, САВЗ, МЭ, СЗИ от НСД, каждая из которых также представляет собой многоканальную СМО.

Поток заявок от системы КА по осуществлению НБИ, обнаруженных и предотвращенных подсистемами ЗИ завершается на данных подсистемах ЗИ.

Поток заявок системы КА – «А» последовательно проходит через подсистемы ЗИ, в которых имитируются процессы обнаружения и предотвращения НБИ.

Весь оставшийся поток заявок от системы КА по осуществлению НБИ, необнаруженных и непредотвращенных, подсистемами ЗИ («B_1», «C_1», «D_1», «E_1», «F_1») направляется на внешние, внутренние серверы и АРМы пользователей. Далее поток заявок – «R» подается на СУИБ, которая на основе сбора, обобщения, анализа всех данных от подсистем ЗИ может обнаружить и предотвратить ранее не обнаруженные НБИ.

В случае обнаружения и предотвращения в SIEM таких НБИ, формируется поток с управляющими воздействиями на соответствующие подсистемы ЗИ – «L_{21}» с целью предотвращения НБИ, а также поток заявок – «L_{11}» агентам СЗИ от НСД, установленным на все АРМы ИС на их блокировку.

В этом случае НБИ считаются предотвращенными, их поток считается завершенным. В противном случае фиксируется количество осуществленных НБИ. Рассчитываются вероятности осуществления КР, обнаружения, предотвращения подсистемами ЗИ НБИ и интегральный показатель: вероятность ЗИ от КР.

СУИБ также формирует потоки заявок – «L_{22}» на подсистемы СКЗ ИС и – «L_{12}» на элементы ИС для проведения периодических проверок на наличие НПВ с целью обнаружения и реагирования на них.

Защищаемая ИС в модели представлена совокупностью 3-х подсистем: АРМов сотрудников, серверов, каждая из которых также представляет собой многоканальную СМО. Для всех элементов ИС имитируется поток заявок на возникновение НПВ. Из элементов ИС, где установлены клиентские агенты СЗИ от НСД на СУИБ посылается поток заявок – «R_1 от подсистем ЗИ, «R_2» поток заявок с НПВ и «R_3» - без НПВ.

Выходными данными в разработанной имитационной модели являются:

смоделированное количество систем ЗИ ИС;

смоделированное количество событий: НСД, НСВ, НПВ, НБИ (КА);

смоделированные и расчетные вероятности и времена обнаружения, идентификации, анализа и вскрытия системой КА элементов защищаемых ИС;

смоделированное и расчетные вероятности и времена обнаружения и предотвращения НСД, НСВ, НПВ, НБИ, обеспечения ЗИ от КА;

смоделированное время осуществления КА и функционирования ИС.

В заключении можно отметить, что разработанная имитационная модель СКЗ ИС от КА обладает новизной и позволяет оценивать эффективность существующих СКЗ ИС от КА в зависимости от варьируемых исходных данных, а также разрабатывать требования для новых СКЗ ИС организации.

Список литературы:

1. Меньшаков Ю.К. Теоретические основы технических разведок. М.: ИПЦ «Маска», 2017, 640 с.

2. Корабельников, С. М. Преступления в сфере информационной безопасности: учебное пособие для вузов. - Москва: Издательство Юрайт, 2020. - 111 с.

3. Ерышов В.Г., Ерышов Н.В. «Модель процесса защиты информации от компьютерной разведки в информационных системах организаций». «Высокие технологии и инновации в науке: сборник избранных статей Международной научной конференции (Санкт-Петербург, Июль 2020). – СПб.: ГНИИ «Нацразвитие», 2020, 306 с. Стр. 135-143.
4. Бирюков А. А. Информационная безопасность: защита и нападение. - 2-е изд., перераб. и доп. - М.: ДМК Пресс, 2017. - 434 с.