УДК-004.056

РАСЧЕТ ОЖИДАЕМОГО УЩЕРБА ОТ УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ КОМПАНИИ НА ОСНОВЕ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ

Эндриш А.С. (Государственный университет управления)
Научный руководитель – доцент, кандидат технических наук, Тимофеева Т.Б.
(Государственный университет управления)

Введение. В настоящее время проблема оценки и снижения рисков информационной безопасности является особенно актуальной. Наиболее распространенным видом угроз информационной безопасности является утечка конфиденциальных данных, как частных компаний, так и государства в целом. Анализ показал, что 2022 год стал в России рекордным по количеству зафиксированных инцидентов, связанных с утечкой информации [1]. Для создания эффективной системы снижения рисков информационной безопасности необходимо разработать и реализовать модели для их оценки [2]. Одним из наиболее эффективных методов оценки ожидаемого ущерба от утечки конфиденциальной информации компании является имитационный подход. На основе данного подхода была разработана и программно реализована имитационная модель, применение которой позволяет оценить ожидаемый ущерб от утечки конфиденциальной информации компании с учетом случайных факторов.

Основная часть. Для создания имитационной модели была построена математическая модель результирующего показателя (ущерба, связанного с утечкой конфиденциальных данных компании) как функции случайных переменных и детерминированных параметров. В качестве случайных переменных выступает индикатор попадания в уязвимость информационной системы компании, доля украденной информации и индикатор реализации угрозы информационной безопасности. Детерминированными параметрами являются стоимость данных компании, коэффициент конфиденциальности информации, вероятность кражи информации.

Алгоритм работы имитационной модели включает в себя следующие этапы:

1) Ввод данных: виды угроз информационной безопасности компании; частота реализации угроз информационной безопасности каждого вида, зафиксированная в компании; виды уязвимостей, в которые может попасть угроза информационной безопасности компании; вероятности попадания в уязвимость каждого вида; для каждого вида информации закон распределения доли украденной информации необходимое количество имитационных экспериментов.
2) Генерация случайной величины и определение реализована ли угроза в данный момент времени или нет (применяется нормальный закон распределения).
3) Установка попала ли угроза в уязвимость, если да, то переходим к шагу №4, если нет, то переходим к следующему промежутку времени.
4) Генерация случайной величины и определение информации, в которую попала угроза (дискретный закон).
5) Определение, данная информация является конфиденциальной, если да, переходим к шагу №6, если нет, то к следующему промежутку времени.
6) Расчет коэффициента конфиденциальности информации.
7) Генерация случайной величины и расчет доли украденной информации (равномерное распределение).
8) Расчет величины затрат на восстановление информации как произведения коэффициента конфиденциальности данных, доли украденной информации и стоимости данных компании для данного вида конфиденциальной информации.
9) Расчет величины ущерба компании от утечки конфиденциальный информации в заданный момент времени. Величина ущерба представляет собой произведение следующих

показателей: коэффициента конфиденциальности украденной информации, затрат на восстановление информации, доли кражи информации и индикатора реализации угроз.

10) Определение, достиг ли конца интервала планирования, если да, то переходим в шагу №11, если нет, то к новому промежутку времени.
11) Расчет суммарной величины ущерба от утечки конфиденциальной информации.
12) Если счетчик испытаний достиг предела, то переходим к следующему шагу, если нет, то возвращаемся к первому эксперименту.
13) Расчет по методу Монте-Карло ожидаемого ущерба от утечки конфиденциальных данных компании. Суть данного метода состоит в следующем: например, необходимо найти оценку некоторой случайной величины, в данном случае ожидаемый ущерб компании от утечки конфиденциальной информации [3]. Для этого моделируют n возможных значений величины ущерба и находят их среднее за рассматриваемый период.
14) Расчет доли ожидаемого ущерба компании от утечки конфиденциальной информации компании, а также его доля в общем объеме прибыли.
15) Исходя из полученных данных, делается вывод об уровне данного ожидаемого ущерба. В зависимости от доли ущерба в общем объеме прибыли выделяют 4 уровня: незначительный (0-5% от прибыли); существенный (от 5% до 50% от прибыли); высокий (от 50% до 75%) и критический (от 75 до 100%).

В дальнейшем именно от уровня ожидаемого ущерба будут зависеть меры, разрабатываемые для снижения или предотвращения потерь от утечки конфиденциальных данных компании.

Применение разработанной имитационной модели позволяет: выявить вид канала связи, по которому вероятнее всего произойдет утечка данных; определить ожидаемый объем финансовых потерь компании от утечки конфиденциальных данных и оценить объем вложений, необходимый для обеспечения информационной безопасности в компании.

Выводы. Разработана и подробно описана имитационная модель для оценки ожидаемого ущерба компании вследствие утечки конфиденциальной информации. Реализация алгоритма работы описанной модели позволит эффективно анализировать риски информационной безопасности компании и принимать оперативные решения по их минимизации.

Список использованных источников:

1. Аналитические отчеты по направлениям «Утечки информации», «Безопасность цифровой экономики» и «Кибербезопасность» в РФ и мире [Электронный ресурс] Раздел аналитики экспертно-аналитического центра InfoWatch. URL: https://www.infowatch.ru/analytics/analitika (дата обращения 11.02.2023)
2. Даев К. Опасности и риски утечки персональных данных // Общество и экономика. – 2022. - №6. – С. 86-90
3. Галиуллин Н.А. Имитационное моделирование в обеспечении информационной безопасности предприятия // Сборник трудов X Международной научно-практической конференции студентов, аспирантов и молодых ученых. – 2018. – С. 22-24