УДК 004.89, 004.942 **DOI: 10.31799/978-5-8088-1446-2-2020-15-317-320**

Т. Н. Елина*
кандидат экономических наук, доцент
В. А. Мыльников*
кандидат технических наук, доцент
**Санкт-Петербургский государственный университет аэрокосмического приборостроения*

МОДЕЛИРОВАНИЕ ДЕЙСТВИЙ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ С ИСПОЛЬЗОВАНИЕМ СЕТЕЙ ПЕТРИ

Рассмотрен анализ угроз информационной безопасности на примере утечек конфиденциальной информации, предложена математическая модель оценки сценариев действий нарушителей с помощью вероятностных сетей Петри. Рассчитанный размер ущерба поможет оценить потенциально возможный объем затрат на мероприятия по защите большинства объектов системы. Полученные результаты возможно использовать при оценке затрат и контроля системы безопасности, что позволяет выявить слабые места и уязвимости в рассматриваемых корпоративных информационных системах.
Ключевые слова: *корпоративные информационные системы, математическое моделирование, сети Петри, защита информации.*

T. N. Yelina*
PhD Sc. Economic, Associate Professor
V. A. Mylnikov*
PhD Sc. Tech., Associate Professor
**St. Petersburg State University of Aerospace Instrumentation*

MODELING OF ACTIONS OF THE VIOLATOR OF INFORMATION SECURITY OF THE ENTERPRISE WITH THE USE OF PETRI NETS

The article deals with the analysis of information security threats on the example of confidential information leaks, and offers a mathematical model for evaluating scenarios of violators ' actions using probabilistic Petri nets. The calculated amount of damage will help to estimate the potential cost of measures to protect most of the system objects. The obtained results can be used in assessing the costs and control of the security system, which allows you to identify weaknesses and vulnerabilities in the considered corporate information systems.
Keywords: *corporate information systems, mathematical modeling, Petri nets, information security.*

Ежегодно в мире растет количество инцидентов информационной безопасности. Согласно исследованиям аналитического центра InfoWatch [1] в первом полугодии 2019 года зарегистрировано 1276 случаев утечки конфиденциальной информации, что на 22 % больше аналогичного периода 2018 года (1039 утечек). На рис. 1 представлена динамика количества утечек в период 2006–2019 годов.

Более 55 % от зарегистрированных утечек (695 шт.) составили утечки информации из-за внутренних нарушителей, а в 555 случаях (44 %) утечка информации произошла из-за внешнего воздействия, причем доля последних ежегодно увеличивается.

В ходе внешних утечек информации, как правило, компрометируются однородные дан-

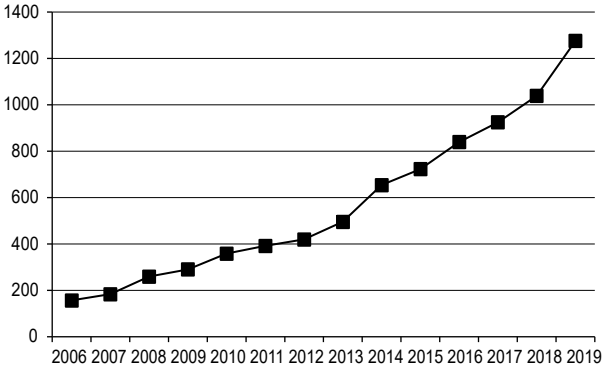

Рис. 1. Динамика количество зарегистрированных утечек информации за период с I полугодия 2006 по I полугодие 2019 года

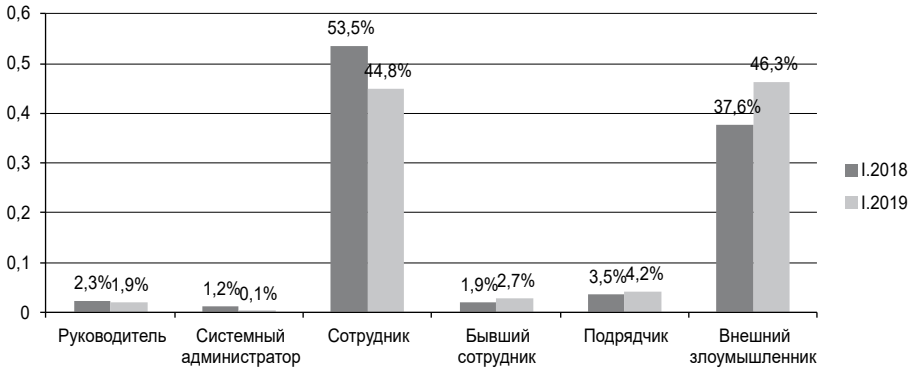

Рис. 2. Распределение утечек по источнику (виновнику) за период с I полугодия 2006 по I полугодие 2019 года

ные, ограниченные функционалом одной системы, на которую было осуществлено нападение. Внутренние же утечки являются более сложными по своим последствиям, так как их сложнее предупредить, и они могут охватывать любую информацию, включая наиболее чувствительные и разнородные данные. Распределение утечек информации в первом полугодии 2018 и 2019 года по виновнику инцидента представлено на рис. 2.

По виду информации наибольшая доля утечек приходится на персональные данные, второе место занимает платежная информация. Распределение утечек по виду информации приведено на рис. 3.

Представленные статистические данные определяют необходимость внедрения на предприятиях комплексной системы защиты информации. Для ее реализации требуется проведение всестороннего анализа угроз информационной безопасности и моделирование различных сценариев действий нарушителей. Один из видов моделей, реализующих данный функционал, строится на основе модели вероятностных сетей Петри [2], учитывающих возможную вероятность возникновения и действия угрозы в определенном временном интервале, а также позволяющих моделировать одновременное возникновение угроз, попыток несанкционированного доступа в целях определения политики безопасности.

Для создания модели необходимо реализовать следующие подзадачи [3]:

1. Определение множества методов защиты конкретных объектов от отдельных угроз информационной безопасности системы (возможно использование модели с полным перекрытием угроз).

2. Для каждого выделенного воздействия определение размера вероятности его возникновения.

3. Расчет суммарной вероятности осуществления угрозы информационной безопасности всей системы.

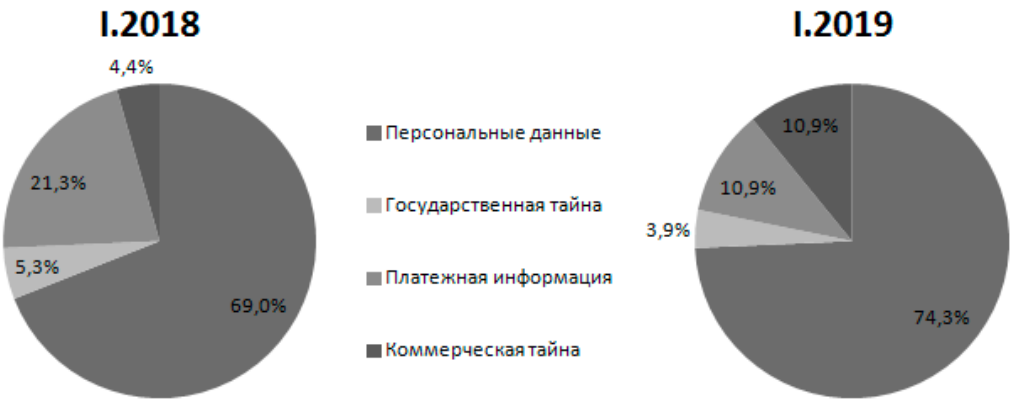

Рис. 3. Распределение утечек по виду информации за период с I полугодия 2006 года по I полугодие 2019 года

Таблица 1

Действия нарушителя информационной безопасности

	Система электроснабжения	Серверы	ЛВС	Персональные машины	Программное обеспечение	Методы защиты
Несанкционированное проникновение	+	+		+		СКУД
Вредоносное программное обеспечение			+		+	Антивирус
Атаки DoS и DDoS			+			Межсетевые экраны. Пакетные фильтры
Подбор пароля			+	+		Система обнаружения и предотвращения вторжений
Атаки, ориентированные на клиента			+		+	Использование зашифрованных соединений. VPN, VLAN и VPLS
Сетевая разведка		+	+	+		Использование зашифрованных соединений. VPN, VLAN и VPLS
SQL-инъекции					+	Защита от SQL-инъекций

4. Ранжирование объектов защиты и на основе определенной вероятности проведение расчета показателей доверия всей политике информационной безопасности системы.

Список действий злоумышленников представляет собой конечное множество, которое можно разбить на отдельные группы в зависимости от их принадлежности к конкретным целям атак. Примерный набор действий представлен в табл. 1.

В табл. 1 плюсами отмечены наиболее вероятные угрозы (Y) на отдельных объектах (O) корпоративной информационной системы. Идеальная модель предполагает рассмотрение всех сочетаний $Y \times O$, однако учет реальных условий эксплуатации системы значительно сократит это множество.

Рассмотрим угрозу несанкционированного проникновения, которая может быть реализована на системе электроснабжения, на серверах или персональных машинах. Смоделировать работу системы в этом случае можно, используя вероятностные сети Петри [3] (рис. 4). В позиции P_0 отражена вся совокупность угроз несанкционированного проникновения, конкретный тип которых определяется срабатыванием переходов T_0, T_1 или T_2 в позиции P_1, P_2 и P_3 соответственно. В зависимости от успешности работы системы защиты переходы T_3, T_4 и T_5 могут привести систему к проникновению злоумышленника (позиция P_4) или отраженной атаке (позиция P_5). Позиция P_6 с маркером отвечает за безопасное функционирование СКУД. Если срабатывает переход T_7, то маркер перемещается в P_7, что говорит о действиях злоумышленника в системе, против которых существующая система контроля и управления доступом не эффективна. Реализация угрозы переносит маркер системы в позицию P_8.

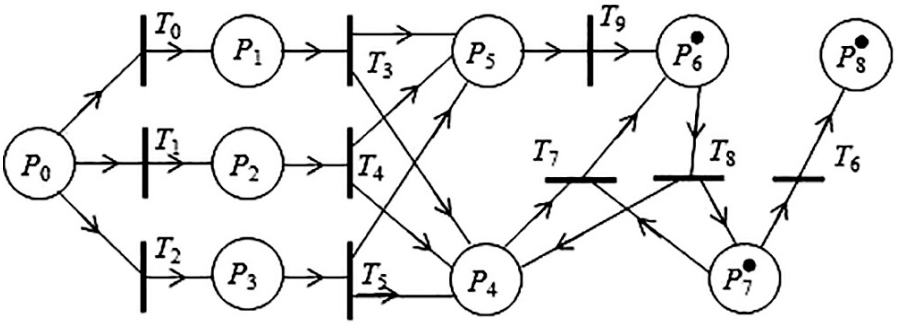

Рис. 4. Сеть Петри на примере работы СКУД

Далее для каждого ребра сети Петри P_iP_j определяется вероятность его появления q_{ij}, а также его стоимость c_{ij} (размер ущерба, ден. ед.). Общую стоимость реализации угрозы на данном объекте можно рассчитать как .

Очевидно, что рассчитанный размер ущерба поможет оценить потенциально возможный объем затрат на мероприятия по защите всех объектов системы [4].

Полученные в результате расчетов с помощью вероятностных сетей Петри результаты можно использовать как при оценке инвестиционных затрат на систему информационной безопасности, так и для контроля существующих систем [5]. Анализ промежуточных значений поможет выявить слабые места и уязвимости в рассматриваемых корпоративных информационных системах.

Библиографический список

1. Глобальное исследование утечек конфиденциальной информации в первом полугодии 2019 года. Аналитический центр InfoWatch. 2019. 30 с. URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/Global_Data_Leaks_Report_2019_half_year.pdf?rel=1 (дата обращения: 18.12.2019).

2. *Котов В. Е.* Сети Петри. М.: Наука, 1984. 160 с.

3. *Бейбутов Э. Р.* Анализ защищенности корпоративных систем на основе вероятностных сетей Петри // Сб. мат. II междунар. науч.-практ. конф. «Актуальные проблемы безопасности информационных технологий» / Сиб. гос. аэрокосмич. ун-т. Красноярск, 2008. С. 53–56.

4. *Мыльников В. А., Елина Т. Н.* Анализ причин нарушения устойчивости облачных систем с учетом требований надежности и оперативности // Завалишинские чтения'18. СПб.: ГУАП, 2018. С. 258–261.

5. *Беззатеев С. В., Елина Т. Н., Мыльников В. А.* Моделирование процессов подбора параметров облачных систем для обеспечения их устойчивости с учетом надежности и безопасности // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 4. С. 654–662.