DOI 10.37882/2223–2966.2021.04.27

СОПОСТАВЛЕНИЕ МЕТОДОВ ОЦЕНКИ ЗАЩИЩЕННОСТИ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

COMPARISON OF METHODS FOR ASSESSING THE SECURITY OF CORPORATE INFORMATION SYSTEMS

K. Makovsky

Summary. The article is devoted to the critical analysis of methods for assessing the security of corporate information systems. In the course of the research, quantitative and qualitative methods were considered, as well as software tools, their features, advantages and disadvantages were highlighted. Special attention is paid to the method of expert assessment, fuzzy sets, and the peculiarities of calculating the integral indicator of security.

Keywords: expert assessment, fuzzy sets, integral security indicator.

Маковский Константин Евгеньевич
Аспирант, Дальневосточный федеральный университет, г. Владивосток
makovskii_ke@dvfu.ru

Аннотация. Статья посвящена проведению критического анализа методов оценки защищенности корпоративных информационных систем. В процессе исследования были рассмотрены количественные и качественные методы, выделены их особенности, достоинства и недостатки. Отдельное внимание уделено методу экспертного оценивания, нечетким множествам, особенностям расчета интегрального показателя защищенности.

Ключевые слова: экспертное оценивание, нечеткие множества, интегральный показатель защищенности.

Интенсивное развитие информационных технологий и их интеграция практически во все сферы жизни общества и хозяйственных отношений открывает возможности массового доступа пользователей к информации. Это способствует увеличению количества критически важного информационного ресурса (ИР), который циркулирует, накапливается и обрабатывается в информационных системах (ИС), что, в свою очередь, приводит к повышению степени зависимости большинства важных решений, принимаемых на разных уровнях, от качества информации и оперативности ее обработки.

Очевидно, что в таких условиях современная организация защиты информации является критически важным стратегическим фактором для учреждений и предприятий любого типа и формы собственности.

На сегодняшний день ключевыми и определяющими международными нормативно-правовыми актами в области управления информационной безопасности (ИБ) корпоративных систем и обеспечения защиты информации является серия стандартов ISO 27k. Также широко используется менеджмент инцидентов, зафиксированный в международном стандарте ISO/IEC27035:2011, который позволяет своевременно и эффективно выявлять, анализировать и расследовать инциденты ИБ с целью минимизации негативных последствий для ИС и организаций в целом [1]. Менеджмент инцидентов используется службой технической поддержки (Service Desk), которая отвечает за мониторинг процесса устранения всех зарегистрированных инцидентов. Этот процесс должен быть очень быстрым, поэтому для эффективного реагирования на инциденты необходимо определить формальный метод действий обученных сотрудников, который предусматривал бы использование специального ПО.

Однако, несмотря на принятые международные положения и нормы, в настоящее время не существует стандартизированных методик анализа защищенности корпоративных ИС, которые можно подразделить на количественные, качественные и комбинированные. Каждый из разработанных подходов имеет свои особенности, основанные на свойствах и характеристиках объектов корпоративной ИС. При этом на различных уровнях детализации используются методики, начиная от наиболее тривиальных и простых для оценки метрик, таких как, например, количество инцидентов нарушения ИБ за период времени или доля компьюте-

Таблица 1. Сравнение количественных методов оценки защищенности корпоративных ИС

Название	Входящие данные	Исходящие данные	Основные операции	Преимущества	Недостатки
Модель Мухина-Волокиты	Статистическая выборка данных	Счетчик угроз воздействия на информацию	Экспертные оценки, теория графов	Высокая точность обнаружения влияния	Потребность в статистических данных, зависимость от компетенции эксперта
Модель Хартсона	Ресурсы системы и их состояния; пользователи и их полномочия	Область безопасности системы	Прямое произведение	Возможность получения количественных оценок	Абстрактная формализация процесса нападения
Модель на основе нейронных сетей и цепей Маркова	Статистические данные для обучения нейронных сетей	Обнаружение вирусов, спама и атак на Web-серверы	Теория нейронных сетей; теория цепей Маркова	Адаптивные обнаружения нападения и защиты информации	Потребность в статистическом наборе данных для динамического функционирования
Модель на основе сетей Петри-Маркова	Информационные состояния системы (более 3-х)	Возможность реализации угрозы воздействия на информацию	Теория сетей Петри и теория цепей Маркова	Количественные оценки с учетом временных параметров	Сложность расчетов для практической реализации
Дифференциально-игровая однокритериальная графовая модель	Множество состояний ИС	Оптимальная стратегия защиты информации	Теория графов, дифференциально-игровое моделирование	Позволяет осуществить распределение выделяемых ИР	Не отражает общую динамику воздействия на информацию
Дифференциально-игровые спектральные однокритериальные модели	Множество состояний ИС	Гарантированный уровень защищенности	Дифференциально-игровое моделирование	Низкая вычислительная сложность, учета нестационарности	Неточный пошаговый процесс воздействия на информацию
Гибридная дифференциально-игровая модель	Показатели надежности и защищенности, вероятности угроз, временные параметры	Оптимальное распределение ресурсов защиты	Дифференциально-игровое моделирование	Учет показателя качественного функционирования ИС; высокая точность даже в условиях неопределенности	Точность достигается только при определенном применении (последовательно) математических методов

ров, оснащенных сетевыми экранами и антивирусными программами, среди всех ПК корпоративной сети, и заканчивая расчетом наиболее сложных агрегированных показателей, которые характеризуют уровень защищенности системы в целом.

В большинстве своем для оценки защищенности используются качественные методы, которые на выходе позволяют получить не количественную оценку (например, система защищена на 4,2 балла или на 58%), а качественную — система соответствует определенному классу или уровню защищенности, тому или иному стандарту безопасности.

Таким образом, принимая во внимание необходимость решения конкретных задач выбора системы обеспечения безопасности корпоративных ИС, особую актуальность и практическую значимость приобретает проведение сравнительного анализа имеющихся оценочных процедур и инструментов, позволяющих получить достоверные результаты, которые впоследствии станут основой для принятия решения, что в целом

обуславливает выбор темы данной статьи, а также подтверждает ее важность в текущей ситуации.

Оценкой информационной безопасности занимаются с начала появления самих информационных технологий. По этой тематике на сегодняшний день накоплено много работ отечественных и зарубежных авторов.

Так, разработке систематизированных критериев оценки защиты компьютерных систем посвящены труды Harold, Tipton; Berdik, David; Otoum, Safa; Schmidt, Nikolas; Porter, Dylan; Курносова К.В., Корнеева Д.Б. и др.

Механизм оценки степени защищенности специальных ИС с точки зрения действий системного администратора и действий, выполняемых системой, детально описан Филипповым М.А., Каменских А.Н., Кротовой Е.Л.

Принципиальные особенности задач контроля и оценки защищенности ИС выделены Hadlington, Lee; Binder, Jens; Stanulewicz, Natalia.

Однако, несмотря на имеющиеся исследования, в данной проблемной плоскости существует еще ряд нерешенных вопросов оценки угроз безопасности информации в информационно-телекоммуникационных системах, с позиций обеспечения конфиденциальности данных, их целостности и доступности. Также дополнительной проработки требуют задачи определения наиболее значимых угроз и структуризации пар угроза-уязвимость, что позволило бы оценить состояние защищенности ИС и предотвратить несанкционированные действия.

Таким образом, с учетом вышеизложенного, цель статьи заключается в проведении сравнительного анализа методов оценки защищенности корпоративных ИС, в результате чего систематизация и анализ таких методов позволит оценить их эффективность и повысить уровень защиты ИС.

Как известно, защита корпоративных ИР зависит от уровня используемых программных и аппаратных средств. Внедряя ИС, каждая организация ожидает максимально полезной функциональности для поддержки ее бизнес-процессов. В связи с этим, критический анализ методов оценивания защищенности корпоративных ИС по сути является многокритериальной задачей, включающей в себя не только количественное, но и качественное (нечеткое) описание показателей. Качественные показатели обычно задаются в виде требований безопасности, достижении определенного уровня объективности экспертной информации, это в свою очередь оказывает влияние на выбор того или иного показателя при нечеткой постановке задачи.

В свете вышеизложенного особую значимость приобретает задача трансформации в количественные значения качественного показателя заданного уровня защищенности и проведение оценки полученных результатов. Традиционно для получения количественной оценки защищенности корпоративных ИС используется аппарат теории вероятности, теории массового обслуживания и теории надежности, нейросетевое моделирование, которые позволяют с достаточной точностью описывать (моделировать) процессы, протекающие в защищенной ИС.

В таблице 1 в разрезе ключевых характеристик представлен сравнительный анализ количественных методов оценки защищенности корпоративных ИС.

Особого внимания в процессе исследования методов оценки защищенности корпоративных ИС заслуживает метод экспертных оценок. Этот метод включает в себя комплекс логических и математико-статистических приемов и процедур, связанных с деятельностью эксперта по переработке необходимой для анализа и принятия решений информации [4].

На сегодняшний день существует много вариаций методов экспертного оценивания: метод Дельфи, метод CORAS, метод CSSE, логико-вероятностный метод. В общем виде использование данных методов предполагает прохождение следующих этапов:

1. Определение множества допустимых оценок (МДО). На данном этапе определяется подмножество множества $E = \bigcup_{m=1}^{\infty} E_m$, в котором ищется оценка безопасности ИС.
2. Определение наиболее точной оценки. С МДО выбирается оценка, которая наиболее точно отображает свойства оцениваемой системы, и позволяет представить экспертную оценку в виде задачи принятия решений <Ω, ОП>, где Ω является МДО, а ОП — принцип оптимальности, который выражает представление о наиболее оптимальной оценке и задается функцией:

$$C_{оп}(X) = \begin{cases} a, \text{если а} \in X \subseteq \Omega \\ \emptyset, \text{если а} \notin X \subseteq \Omega \end{cases}$$

где a — оценка системы, которая является решением задачи <Ω, ОП>.

Значительные перспективы на сегодняшний день для оценки защищенности корпоративных ИС имеет метод нечетких множеств, предполагающий использование нечетких когнитивных карт [5].

Нечеткие когнитивные карты представляют собой простой граф из узлов и взвешенных дуг, где узлы — концепты предметной области (например, множество нарушителей, множество способов преодоления системы защиты), а дуги — причинно-следственные связи между ними (например, вероятность наличия определенного вида нарушителей, вероятность реализации атаки и др.).

В общем случае при расчете уровня защищенности ИС используется пробит-функция:

$$PR = a + b + lnD + \gamma ln\tau$$

где a b, γ — коэффициенты, характеризующие степень уязвимости информационного ресурса по отношению к конкретной угрозе или классу угроз;

D — оценка негативного воздействия;

τ — период времени от начала до конца негативного воздействия.

Вес связей в нечетких когнитивных картах задается в нечетком виде: с помощью лингвистических термов или интервальных оценок.

Результатом проведения оценки защищенности корпоративных ИС является расчет интегрального показателя, который включает в себя ряд групповых, к числу которых, по мнению автора, могут быть отнесены следующие: влияние на целостность ($G1_{факт}$); влияние на конфиденциальность ($G2_{факт}$); влияние на доступность ($G3_{факт}$).

Тогда комплексный показатель состояния защищенности ИС (G_z^y может быть рассчитан по следующей формуле:

$$G_z^y = \left(\sum_{i=1}^{3} \left(g_i \cdot G_i^{\text{факт}} \right) \right) \cdot 100\%$$

где g_i — весовые коэффициенты категорий $G_i^{факт}$.

В свою очередь, групповые показатели защищенности аналогичным образом вычисляются через частные показатели, набор которых формируется исходя из особенностей конкретной ИС.

Подводя итоги проведенного исследования, можно сделать следующие выводы. Выбор конкретного метода оценки защищенности корпоративных информационных систем зависит от задач, которые стоят перед экспертом, особенностей самих ИС, имеющихся в наличии финансовых и временных ресурсов, а также квалификации того, кто проводит оценку. В настоящее время предпочтение отдается интеллектуальным методам анализа, которые позволяют получить конкретные количественные оценки.

ЛИТЕРАТУРА

1. Implementing an Information Security Management System: Security Management Based on ISO 27001 Guidelines / Abhishek Chopra, Mukund Chaudhary. Berkeley, CA: Apress L.P. 2020, 284 p.
2. Information security and cryptology: 15th International Conference, Inscrypt 2019, Nanjing, China, December 6–8, 2019. Cham: Springer, 2020. 560 p.
3. Guide to computer network security / Joseph Migga Kizza. Cham: Springer, 2020. 599 p.
4. Information technology. Security techniques. Guidelines for privacy impact assessment. London: British Standards Institution, 2020. 56 p.
5. Jana, Dipak Kumar; Ghosh, Ramkrishna Novel interval type-2 fuzzy logic controller for improving risk assessment model of cyber security // Journal of information security and applications. 2018. Volume 40; pp 173–182.

Журнал «Современная наука: актуальные проблемы теории и практики»