Инженерный вестник Дона, №1 (2025)
ivdon.ru/ru/magazine/archive/n1y2025/9763

Разработка интегрального метода оценки уровня защищенности серверной инфраструктуры организации

Д.А. Рыленков[1], Д.С. Карпов[2]

[1]Московский финансово-юридический университет МФЮА

[2]Российский экономический университет имени Г.В. Плеханова

Аннотация: Управление информационной безопасностью на предприятии является важной задачей, так как число угроз растет и необходимо постоянное совершенствование механизмов защиты. Серверная инфраструктура предприятия применяется для публикации корпоративных сервисов и требования к ней являются высокими с точки зрения производительности, надежности и защищенности. В данной статье рассматривается разработанный метод интегральной оценки уровня защищенности серверной инфраструктуры предприятия от атак различного типа.

Ключевые слова: защита данных, информационные технологии, комплексная оценка, системный анализ, информационные системы, информационная безопасность.

Организация любого масштаба имеет собственные информационные системы, которые могут быть развернуты с использованием серверной инфраструктуры в пределах защищаемого контура [1-3]. Для качественного управления процессом защиты информации необходимо выполнять оценку уровня защищенности систем [4-6]. Разработанный подход отличается от существующих применением экспертных оценок и введением набора показателей, характерных для серверных систем. Экспертные оценки применяются в различных областях исследований – совместные оценки обладают большей точностью, чем отдельное мнение каждого из специалистов по ряду вопросов [7,8].

Предлагаемый анализируемый набор показателей защищенности серверной инфраструктуры представлен в таблице 1.

Таблица № 1

Показатели защищенности серверной инфраструктуры

№	Наименование требования
1	Ограничение на подключение к серверным службам с конкретных диапазонов IP-адресов
2	Выделение отдельной сети управления серверной инфраструктурой
3	Мониторинг серверных приложений
4	Ведение журналов событий активных сервисов
5	Выполнение регулярного резервного копирования данных
6	Внедрение систем бесперебойного питания
7	Отказоустойчивая кластеризация эксплуатируемых систем
8	Резервирование на уровне систем хранения данных
9	Активация шифрования в протоколах управления
10	Реализация централизованной политики обновления программного обеспечения серверных систем

Оценка степени защищенности S будет рассчитываться по следующей формуле:

$$S = \sum_{i=1}^{n} F_i * K_i$$

В данном выражении F – показатель реализации конкретного требования ИБ, K – его вес, n – общее число требований.

Если требование информационной безопасности выполняется, то F для него равно значению 1, в ином случае F будет равно 0.

Весовые коэффициенты требований вычисляются при помощи экспертных оценок на основе метода парных сравнений. Формируется квадратная матрица n*n парного сравнения критериев. В качестве баллов

оценок в матрице используются числовые значения в диапазоне от 1 до 9, указывающие на степень значимости одного критерия над другим.

Далее вычисляется главный собственный вектор матрицы на основе среднего геометрического значения. Данные расчеты выполняются независимо несколькими экспертами, итоговый вектор получается путем расчета среднего значения по каждой из компонент.

Далее показан расчет показателей при оценках двух экспертов.

Сведения о первом эксперте:

- Направление работ – системы защиты информации;
- Научная подготовка – кандидат наук;
- Стаж работы по приоритетному направлению – 30 лет;

Сведения о втором эксперте:

- Направление работ – системы защиты информации;
- Научная подготовка – кандидат наук;
- Стаж работы по приоритетному направлению – 25 лет;

Расчет показателей, выполненный первым экспертом рассмотрен детализировано по шагам. В таблице 2 представлена матрица парного сравнения показателей.

Таблица № 2

Парное сравнение показателей

	1	2	3	4	5	6	7	8	9	10	Ср. геометр.	Нормализованная оценка
1	1	2	2	2	2	5	5	5	5	1	2,51	0,23
2	0,5	1	1	1	2	5	2	2	2	2	1,55	0,14
3	0,5	1	1	1	1	1	1	2	2	2	1,15	0,10
4	0,5	1	1	1	1	5	5	1	1	1	1,29	0,12
5	0,5	0,5	1	1	1	2	2	2	2	1	1,15	0,10
6	0,2	0,2	1	0,2	0,5	1	1	1	2	1	0,62	0,06
7	0,2	0,5	1	0,2	0,5	1	1	2	1	2	0,72	0,07
8	0,2	0,5	0,5	1	0,5	1	0,5	1	1	2	0,69	0,06
9	0,2	0,5	0,5	1	0,5	1	1	1	1	2	0,74	0,07
10	1	0,5	0,5	1	1	0,5	0,5	0,5	0,5	1	0,66	0,06
	4,8	7,7	9,5	9,4	10	22,5	19	17,5	17,5	15		

Для оценки качества полученных данных произведен расчет индекса согласованности (ИС) и отношения согласованности (ОС).

$$ИС = \frac{|\lambda_{max} - n|}{n - 1}$$

В указанном выражении n является размерностью матрицы, а λ_{max} рассчитывается по следующей формуле:

λ_{max}= (4,8*0,23)+(7,7*0,14)+(9,5*0,10)+ (9,4*0,12)+ (10*0,10)+ (22,5*0,06)+

(19*0,07)+(17,5*0,06)+ (17,5*0,07)+ (15*0,06) = 10,93

Расчет индекса согласованности:

$$ИС = \frac{|11{,}85 - 10|}{10 - 1} = 0{,}1$$

Значение случайной согласованности зависит от размерности исходной матрицы (Таблица 3).

Таблица № 3

Значения случайной согласованности

Размерность матрицы	1	2	3	4	5	6	7	8	9	10
Случайная согласованность	0	0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49

Расчет отношения согласованности:

$$ОС = \frac{ИС}{СС} = \frac{0{,}1}{1{,}49} = 0{,}06$$

Значение отношения согласованности равное 0,06 означает, что экспертные оценки согласованны. Данное значение не должно превышать 0,1 [9,10]. На основании результатов аналогичного расчета произведенного вторым экспертом рассчитан итоговый вектор коэффициентов требований

при помощи нормализации оценок средних значений показателей (Таблица 4).

Таблица № 4

Расчет итоговых коэффициентов требований

Номер показателя	Оценки 1 эксперта	Оценки 2 эксперта	Среднее значение	Нормализованная оценка
1	0,23	0,1	0,1650	0,1642
2	0,14	0,1	0,1200	0,1194
3	0,1	0,2	0,1500	0,1493
4	0,12	0,05	0,0850	0,0846
5	0,1	0,05	0,0750	0,0746
6	0,06	0,1	0,0800	0,0796
7	0,07	0,2	0,1350	0,1343
8	0,06	0,07	0,0650	0,0647
9	0,07	0,1	0,0850	0,0846
10	0,06	0,03	0,0450	0,0448

На заключительном этапе произведен расчет итоговой интегральной оценки уровня защищенности инфраструктуры (Таблица 5).

Таблица № 5

Расчет общей оценки защищенности

Номер требования	Выполнение требования	Вес требования
1	1	0,1642
2	0	0,1194
3	1	0,1493
4	1	0,0846
5	1	0,0746
6	1	0,0796
7	1	0,1343
8	1	0,0647
9	0	0,0846
10	0	0,0448
Итоговое значение		0,75

Таким образом, на основе выполненных расчетов итоговая оценка показателя защищенности равна 0,75. Значения 0,9 – 1 соответствуют высокому уровню защищенности, 0,5 – 0,9 среднему уровню защищенности, и ниже 0,5 низкому уровню. Данный метод позволяет оценить и сравнить различные конфигурации системы защиты информации и может быть применим для организаций различного типа.

Литература

1. Бильтаев И. С. Разработка центра управления безопасностью для информационно-аналитической системы предприятия // Студенческие научные исследования: сборник статей XV Международной научно-практической конференции, Пенза, 20 декабря 2022 года. Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2022. С. 35-41.

2. Рыленков Д. А. Применение стандарта IEEE 802.1x для управления доступом в корпоративных сетях // Теория и практика обеспечения информационной безопасности: Сборник научных трудов по материалам всероссийской научно-теоретической конференции, Москва, 03 декабря 2021 года. – Москва: Московский технический университет связи и информатики, 2021. С. 286-289.

3. Магомедрасулов К. О. Проблемы информационной безопасности: алгоритм построения системы информационной безопасности предприятия // Математическое и компьютерное моделирование: Сборник материалов IX Международной научной конференции, посвященной 85-летию профессора В.И. Потапова, Омск, 19 ноября 2021 года. – Омск: Омский государственный университет им. Ф.М. Достоевского, 2021. С. 263-265.

4. Шаго Ф. Н. Методика оценки эффективности системы менеджмента информационной безопасности по времени реакции системы на инциденты

информационной безопасности // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 4(92). С. 115-123.

5. Куркин А. В. Оценка рисков информационной безопасности с применением нечеткого моделирования // Неделя науки Санкт-Петербургского государственного морского технического университета. 2020. – Т. 2, № 4. С. 45.

6. Исаева М. Ф. О внутренних угрозах информационной безопасности // Международный научно-исследовательский журнал. 2019. № 5-1(83). С. 26-28.

7. Олейникова А.А. Концепция управления информационной безопасностью на основе цикла непрерывного детектирования и реагирования на инциденты безопасности информации // Известия ЮФУ. Технические науки. 2023. № 5(235). С. 66-81.

8. Мамхягов, А. З. Информационная безопасность в корпоративной сети // Научный вестник Государственного автономного образовательного учреждения высшего образования "Невинномысский государственный гуманитарно-технический институт". 2023. № 1. С. 26-29.

9. Kafi M. A., Akter N. Securing financial information in the digital realm: case studies in cybersecurity for accounting data protection //American Journal of Trade and Policy. Vol. 10. No. 1. 2023 pp. 15-26.

10. Duc C. Le, & Zincir-Heywood, A. N. Machine learning-based insider threat modeling and detection. In 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM). IEEE. 2019. pp. 1-6.

References

1. Biltaev I. S. Studencheskie nauchnye issledovaniya: sbornik statej XV Mezhdunarodnoj nauchno-prakticheskoj konferencii, Penza, 20 dekabrya 2022 goda. Penza: Nauka i Prosveshhenie (IP Gulyaev G.Yu.), 2022. pp. 35-41.

2. Rylenkov D. A. Teoriya i praktika obespecheniya informacionnoj bezopasnosti: Sbornik nauchnyx trudov po materialam vserossijskoj nauchno-teoreticheskoj konferencii, Moskva, 03 dekabrya 2021 goda. Moskva: Moskovskij texnicheskij universitet svyazi i informatiki, 2021. pp. 286-289.

3. Magomedrasulov K. O. Matematicheskoe i kompyuternoe modelirovanie: Sbornik materialov IX Mezhdunarodnoj nauchnoj konferencii, posvyashhennoj 85-letiyu professora V.I. Potapova, Omsk, 19 noyabrya 2021 goda. Omsk: Omskij gosudarstvennyj universitet im. F.M. Dostoevskogo, 2021. pp. 263-265.

4. Shago F. N. Nauchno-texnicheskij vestnik informacionnyx texnologij, mexaniki i optiki. 2014. № 4(92). pp. 115-123.

5. Kurkin A. V. O Nedelya nauki Sankt-Peterburgskogo gosudarstvennogo morskogo texnicheskogo universiteta. 2020.T. 2, № 4. p. 45.

6. Isaeva M. F. Mezhdunarodnyj nauchno-issledovatel`skij zhurnal. 2019. № 5-1(83). pp. 26-28.

7. Olejnikova A.A. Izvestiya YuFU. Texnicheskie nauki. 2023. № 5(235). pp. 66-81.

8. Mamxyagov, A. Z. Nauchnyj vestnik Gosudarstvennogo avtonomnogo obrazovatelnogo uchrezhdeniya vysshego obrazovaniya "Nevinnomysskij gosudarstvennyj gumanitarno-texnicheskij institut". 2023. № 1. pp. 26-29.

9. Kafi M. A., Akter N. American Journal of Trade and Policy. Vol. 10. No. 1. 2023. pp. 15-26.

10. Duc C. Le, & Zincir-Heywood, A. N. Machine learning-based insider threat modeling and detection. In 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM). IEEE. 2019. pp. 1-6.

Дата поступления: 16.11.2024

Дата публикации: 1.01.2025