DOI: https://doi.org/10.15688/NBIT.jvolsu.2020.3.3

УДК 681.5:004.056
ББК 32.81

МЕТОДЫ РАЗРАБОТКИ РЕКОМЕНДАЦИЙ ДЛЯ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Наталья Алексеевна Головачева

Старший преподаватель кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В работе реализована математическая модель оценки защищенности информационной системы на основе выбранных методов. Сформирована архитектура программного комплекса оценки защищенности информационной системы.

Ключевые слова: информационная безопасность, математическая модель, метод экспертных оценок, оценка защищенности, повышение защищенности.

С появлением информационных технологий широкое применение в организациях и на предприятиях получили информационные системы (ИС). Применение ИС позволяет оптимизировать трудовые ресурсы, автоматизировать полностью или частично бизнес-процессы. Однако применение ИС требует развитие системы информационной безопасность для минимизации злоумышленных воздействий. Для снижения вероятности реализации злоумышленных воздействий существует большое количество программных и программно–аппаратных средств защиты информации. Сложность организации вычислительных сред, распределенность компонентов информационных систем усложняет процесс создания и конфигурирования систем защиты, при этом количество угроз нарушения информационной безопасности (ИБ) ежегодно увеличиваются. Для своевременного реагирования на инциденты ИБ, в том числе и на атаки, необходимо применение средств оценки защищенности ИС для снижения рисков нарушения защищенности. Статистика InfoWath, показывает тенденцию роста различного рода атак, как со стороны внешнего злоумышленника, так и со стороны внутреннего. Следовательно, одной из важнейших задач является корректное определение защищенности ИС [1–3].

Целью данной работы является повышение защищенности информационной системы за счет оценки защищенности ИС.

Для достижения данной цели был определен список методов оценки защищенности ИС, а именно:

– метод экспертных оценок,

– метод оценки защищенности информации от несанкционированного доступа (НСД).

Метод экспертных оценок основывается на взаимодействии работы специалистов (экспертов), получении и обработки сложившихся мнений проведенных экспертов по возникшим вопросам. Экспертные решения формируются с целью подготовки информации для принятия решений о уровня защищенности системы.

Для проведения экспертной оценки необходимо сформировать множество оцениваемых компонентов ИС (1):

$$IS = \{k_1, \ldots\ldots, k_n\}, \quad (1)$$

где IS – множество оцениваемых компонентов ИС; k_n – компоненты ИС; n – количество компонентов ИС.

Далее необходимо определить события безопасности (2), которые могут свидетельствовать о реализации угрозы (3):

$$S = \{s_1, \ldots\ldots, s_n\}, \quad (2)$$

где S – множество совершаемых событий в ИС; s_n – события ИС; n – количество событий в ИС.

$$U = \{u_1 \ldots\ldots, u_m\}, \quad (3)$$

где U – множество актуальных угроз; u_m и $m \in N$ – количество угроз.

В зависимости от сгенерированных в ИС событий безопасности определяют возможность реализации той или иной угрозы. Формализация данного процесса представлена в формуле (4):

$$U = \begin{cases} U_1 = (S_1, S_4) \\ U_2 = (S_4, S_7) \\ U_3 = (S_4, S_7) \\ U_4 = (S_1) \\ U_5 = (S_2, S_8) \\ U_6 = (S_3, S_5, S_6) \end{cases}, \quad (4)$$

где U – множество актуальных угроз; S_1 – вход учетной записи в системы; S_2 – управление учетными записями в системе; S_3 – события маршрутизации и удаленного доступа; S_4 – событие доступа к объекту системы; S_5 – изменение политики системы; S_6 – использование субъектом особых привилегий; S_7 – функционирование процессов системы; S_8 – события входа субъектов в систему; U_1 – угрозы утечки; U_2 – угрозы искажения; U_3 – угрозы утраты; U_4 – угрозы блокирования; U_5 – угрозы взлома; U_6 – угрозы злоупотребления.

После этого следует для каждой угрозы U_i из набора актуальных угроз U определить возможные исходы реализации угроз I_{ij} или другими словами риски, которые зависят от вероятности реализации угрозы A_{ij} и Y_{il} ущерба Y_{il} (5) (см. таблицу):

$$I_{ij} = A_{ij} * Y_{il}, \quad (5)$$

где I_{ij} – риск реализации угрозы i-й угрозы для j-го компонента; A_{ij} – вероятность реализации i-й угрозы для j-го компонента; Y_{il} – ущерб от реализации от i-й угрозы для j-го компонента ИС.

Вероятности реализации оценивается следующим образом:

– маловероятно [0;0,2),
– низкая (0,2;0,4],
– средняя (0,4;0,5],
– выше среднего (0,5;0,8],
– высокая [0,8;1).

В связи с тем, что уровни предприятий различны, соответственно и ущерб будет иметь относительную количественную оценку. Распределение количественных оценок в соответствии с качественными значениями уровня ущерба приведено ниже:

– отсутствует [0;0,2),
– низкий (0,2;0,4],
– средний (0,4;0,5],
– выше среднего (0,5;0,8],
– высокий [0,8;1).

Возможные исходы реализации угрозы

I_i	Вероятность реализации угрозы (A_{ij})	Ущерб от реализации угрозы (Y_{il})
1	Маловероятно	Отсутствует
2	Маловероятно	Низкое
3	Средняя	Низкое
4	Средняя	Среднее
5	Выше среднего	Среднее
6	Выше среднего	Выше среднего
7	Выше среднего	Среднее
8	Выше среднего	Выше среднего
9	Высокая	Выше среднего
10	Высокая	Высокое

Далее рассчитывается сумма рисков реализации *i*-х угроз для *j*-го компонента (6):

$$E_{ij} = \sum_{i=1}^{n} I_{ji}, \quad (6)$$

где E_{ij} – сумма рисков от реализации угроз для *j*-го компонента; I_{ij} – возможные риски реализации *i*-й угрозы для *j*-го компонента ИС.

Суммарная оценка защищенности ИС имеет вид (7):

$$Z = \sum_{i=1}^{n} E_{ij}, \quad (7)$$

где E_{ij} – сумма возможных риски реализации *i*-х угроз для *j*-го компонента; Z – суммарная оценка защищенности ИС.

Качественная оценка защищенности ИС O_z определяется (8):

$$O_z = \begin{cases} \text{если } Z \in (40;90] - \textit{не защищена;} \\ \text{если } Z \in (20;40] - \textit{менее половины} \\ \textit{компонентов не защищены;} \\ \text{если } Z \in (10;20] - \textit{более половины} \\ \textit{компонентов защищены;} \\ \text{если } Z \in [0;10) \textit{ защищена.} \end{cases}, \quad (8)$$

где O_z – оценка защищенности ИС.

По результатам определения оценки защищенности ИС формируются рекомендации по улучшению защищенности ИС.

Рекомендации по повышению уровня защищенности при нарушении свойств безопасности информационного актива (конфиденциальность):

– рекомендуется шифрование конфиденциальной информации;

– рекомендуется настройка встроенных средств защиты ОС;

– рекомендуется установка и настройка СЗИ от НСД;

– рекомендуется установить и настроить системы аутентификации пользователей.

Рекомендации по повышению уровня защищенности при нарушении свойств безопасности информационного актива (целостность):

– рекомендуется шифрование информации;

– рекомендуется использование электронно-цифровой подписи;

– рекомендуется установка и настройка СЗИ от НСД;

– рекомендуется настройка встроенных средства защиты ОС.

Рекомендации по повышению уровня защищенности при нарушении свойств безопасности информационного актива (доступность):

– рекомендуется настройка встроенных средств защиты ОС;

– рекомендуется установка и настройка СЗИ от НСД;

– рекомендуется создание резервирования аппаратного обеспечения;

– рекомендуется резервирование информации.

Архитектура программного комплекса представлена на рисунке.

Данная архитектура состоит из следующих модулей:

– пользовательский интерфейс;

– модуль управления;

– модуль подключения к ИС;

– модуль сбора исходных данных;

– модуль оценки защищенности ИС;

– модуль метода экспертных оценок;

– модуль метода оценки защищенности информации от НСД;

– модуль формирования рекомендаций;

– модуль формирования отчета;

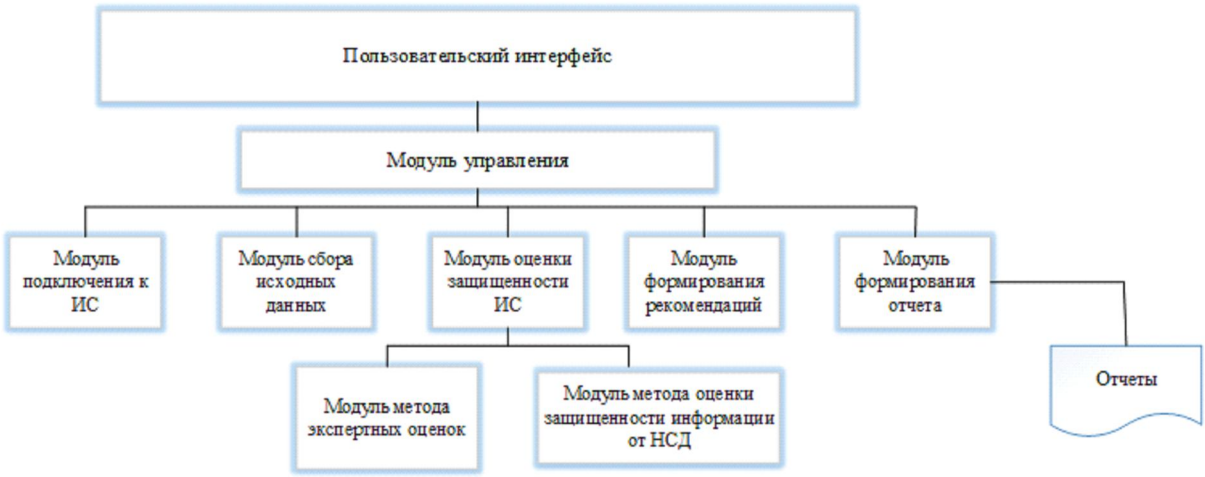
– документ отчетов.

Интерфейс программного комплекса обеспечивает взаимодействие пользователя с программным комплексом «Оценка защищенности информационной системы». Данный интерфейс упрощает взаимодействие по средствам интуитивного понятного расположения кнопок и окон ввода и вывода данных.

Модуль управления обеспечивает синхронизированную работу всех модулей, распределяет потоки данных, которые генерируются смежными модулями и поступают от пользователя.

Модуль подключения к информационной системе позволяет осуществить подключение ко всем компонентам ИС с помощью ввода аутентификационной информации и IP-адреса каждого компонента. Подключение может осуществляться с помощью двух типов подключения: SSH, TELNET.

Модуль сбора исходных данных обеспечивает сбор исходных данных из журналов со-



Архитектура программного комплекса

бытий ИС по каждому компоненту ИС. В данном модуле осуществляется их классификация, кроме того данный модуль реализует анализ угроз.

Модуль оценки защищенности ИС позволяет рассчитать количественную оценку защищенности ИС на основе данных полученных от модуля сбора данных.

Модуль метода экспертных оценок позволяет рассчитать количественную оценку данного метода. Для каждой актуальной угрозы производится расчет возможных реализаций угрозы, далее по каждому компоненту ИС производится расчет суммы рисков реализации угроз. По результатам проведенных расчетов высчитывается суммарная оценка защищенности ИС, на основе которой и определяется качественные оценки защищенности ИС.

Модуль метода оценки защищенности информации от НСД позволяет рассчитать количественную оценку данного метода. Модуль формирования рекомендаций реализует генерацию рекомендации по повышению уровня защищенности ИС на основе имеющихся сведений о состоянии защищенности ИС предприятия.

Модуль формирования отчета позволяет пользователю сохранять результаты работы программного комплекса, что в дальнейшем может служить пользователю основой для проведения сравнительного анализа изменения защищенности ИС в зависимости от применяемых мер по защите информации, кроме того данные отчеты могу быть применены при прогнозировании реализации угроз безопасности при использовании многокритериальных методов экстраполяции.

Документ отчетов позволяет хранить сформированные отчеты оценки защищенности ИС, в формате .docx.

Результат экспериментальных исследований показал повышение защищенности ИС при применении рекомендаций, генерируемых разработанным программным комплексом. В ходе экспериментального исследования подтверждена корректность работы программного комплекса.

СПИСОК ЛИТЕРАТУРЫ

1. Аветисян, А. И. Технологии статического и динамического анализа уязвимостей программного обеспечения / А. И. Аветисян, А. А. Белевацев, И. И. Чукляев // Вопросы кибербезопасности. – 2014. – № 3 (4). – С. 20–28.

2. Щеглов, К. А. Моделирование угроз атак на защищенную информационную систему / К. А. Щеглов, А. Ю. Щеглов // Известия высших учебных заведений. Приборостроение. – 2016. – Т. 59, № 12. – С. 980–990.

3. ISO/IEC 27004 – Информационная технология. Средства обеспечения безопасности. Измерения. – Электрон. текстовые дан. – Режим доступа: http://docs.cntd.ru/document/1200088532.

REFERENCES

1. Avetisyan A.I., Belevantsev A.A., Chuklyayev I.I. Tekhnologii staticheskogo i dinamicheskogo analiza uyazvimostey programmnogo

obespecheniya [Technologies for Static and Dynamic Analysis of Software Vulnerabilities]. *Voprosy kiberbezopasnosti*, 2014, no. 3 (4), pp. 20-28.

2. Shcheglov K.A., Shcheglov A.Yu. Modelirovaniye ugroz atak na zashchishchennuyu informatsionnuyu sistemu [Modeling of Threats of Attacks on a Secure Information System]. *Izvestiya vysshikh uchebnykh zavedeniy. Priborostroyeniye*, 2016, vol. 59, no. 12, pp. 980-990.

3. *ISO/IEC 27004 – Informatsionnaya tekhnologiya. Sredstva obespecheniya bezopasnosti. Izmereniya* [Information Technology. Security Tools. Measurements]. URL: http://docs.cntd.ru/document/1200088532.

METHODS OF DEVELOPING RECOMMENDATIONS FOR IMPROVING THE SECURITY OF INFORMATION SYSTEMS

Natalia A. Golovacheva

Senior Lecturer, Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. With the advent of information technologies, information systems have been widely used in organizations and enterprises. The use of information systems allows optimizing the workforce, automating all or part of business processes. However, the use of information systems requires the development of an information security system to minimize malicious attacks. To reduce the likelihood of malicious attacks, there are a large number of software and hardware-based information security tools. The complexity of computing the distribution of the components of information systems complicates the process of creating and configuring protection systems, the number of threats to security are increasing every year. For a timely response to information security incidents, including attacks, it is necessary to use information system security assessment tools to reduce the risks of security breaches. InfoWath statistics show the growth trend of various types of attacks, both from an external attacker and from an internal one. Therefore, one of the most important tasks is to correctly determine the security of information systems. The paper implements a mathematical model for assessing the security of an information system based on the selected methods. The architecture of the software package for assessing the security of the information system is formed.

Key words: information security, mathematical model, expert assessment method, security assessment, security enhancement.