УДК 004.056

АРХИТЕКТУРА ПРОГРАММНОГО КОМПЛЕКСА ИНТЕЛЛЕКТУАЛЬНОЙ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ ПРОЕКТИРОВАНИИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ

Е. А. Витенбург
Волгоградский государственный университет,
e.vitenburg@ec-rs.ru

В статье определена необходимость внедрения и модернизации системы защиты информации на предприятии, рассмотрена ее типовая структура. Определена актуальность применения методов интеллектуальной поддержки решений при проектировании систем защиты информации. Сформированы математическая модель данной интеллектуальной поддержки и функциональная модель интеллектуального выбора проекта системы защиты информации. Построена архитектура программного комплекса интеллектуальной поддержки принятия решений при проектировании системы защиты информационной системы предприятия.

Ключевые слова: информационная система предприятия, информационная безопасность, система защиты информации, нейронная сеть.

SOFTWARE COMPLEX ARCHITECTURE OF INTELLIGENT DECISION SUPPORT IN DESIGN OF SECURITY SYSTEM FOR ENTERPRISE INFORMATION SYSTEM

E. A. Vitenburg
Volgograd State University,
e.vitenburg@ec-rs.ru

The article identifies the need for the introduction and modernization of the information security system in the enterprise. The typical structure of the information security system in the enterprise is considered. The relevance of methods application of intelligent decision support in the design of information security systems is presented. A mathematical model of intelligent decision support and a functional model of intellectual project selection of information security system are formed. The software complex architecture of intelligent decision support in the design of the security system of the enterprise information system is constructed.

Keywords: enterprise information system, information security, information security system, neural network.

Рост числа предприятий, в том числе опасных производств, отнесенных к критической информационной инфраструктуре (далее – КИИ), определяет необходимость обеспечения информационной безопасности информационных систем (далее – ИС) предприятия, обеспечивающих производственный процесс. Данная необходимость ежегодно подтверждается ведущими в области защиты информации аналитическими центрами. Статистика от аналитического центра PT [1] за 2019 год показывает, что больше половины выявленных уязвимостей информационной системы предприятия относятся к критической и высокой степеням риска в соответствии с оценкой Common Vulnerability Scoring System версии 3 [2]. При этом доля таких уязвимостей выросла на 17 % по сравнению с предыдущим годом. Если уязвимость имеет высокую степень риска, то в большинстве случаев она ставит под удар сразу три свойства безопас-

ности информации: конфиденциальность, целостность и доступность. В 2018 году такое комплексное воздействие имели 58 % уязвимостей (рис. 1).

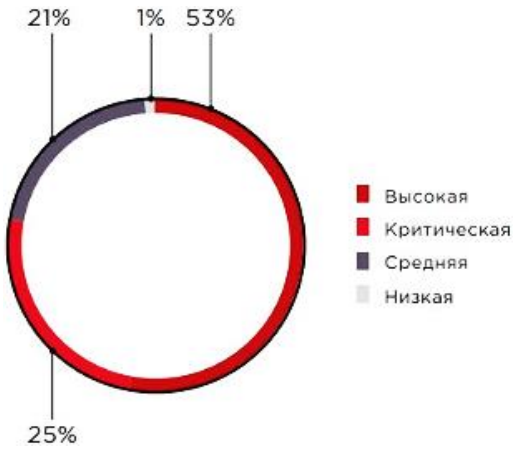

Рис. 1. Степень риска уязвимостей ИС предприятия

При этом среди них только для 4 % сложность атаки была оценена как высокая. Это означает, что в большинстве случаев злоумышленнику не требуется никаких специальных условий, чтобы нарушить защищенность элементов ИС предприятия.

Ввиду ежегодного роста атак на информационные системы предприятий, актуальной задачей является построение и внедрение эффективной системы защиты информации (далее – СЗИ). В случае наличия СЗИ ИС предприятия требуется оперативная корректировка настроек существующих средств защиты информации, входящих в состав системы защиты, корректировка состава подсистем СЗИ, а также установка и настройка новых средств защиты ИС и/или замена устаревших средств защиты информации [3, 4].

Система защиты информации SPI имеет многоуровневую структуру и определяется следующими уровнями (компонентами):

- множество подсистемы защиты информации Subsystem;
- множество средств защиты информации MP.

В общем виде структуру СЗИ можно представить в виде схемы (рис. 2).

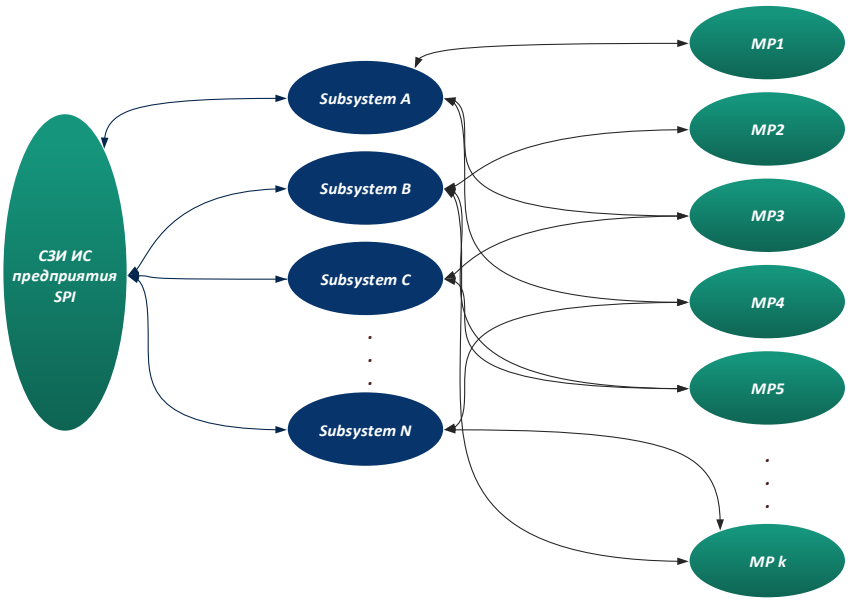

Рис. 2. Обобщенная структура СЗИ ИС предприятия

При формировании СЗИ ИС предприятия SPI в зависимости от исходных данных и модели угроз возможно формирование нескольких проектов системы защиты с различным составом подсистем. Разнообразие подсистем защиты, которые можно использовать для защиты от нескольких видов угроз, усложняет задачу выбора набора подсистем защиты, формирующего систему защиты [5]. Кроме того, выбор подсистем защиты для формирования СЗИ может осуществляться несколько раз в течение жизненного цикла информационной системы. При этом важными характеристиками процесса выбора являются скорость получаемого результата и снижение остаточного риска информационной системе. Поэтому актуальным является применение систем искусственного интеллекта в процессе выбора лучшего набора подсистем защиты – проекта, формирующего систему защиты.

Задача интеллектуального выбора проекта СЗИ сводится к определению важности каждой из типовых подсистем защиты информации. Это позволит специалисту включить в систему защиты именно те средства, которые относятся к наиболее важным подсистемам защиты, т. е. позволит защитить от наиболее актуальных классов угроз.

$$I = N(A), \tag{1}$$

где $I = (I_1, \dots, I_9)$ – вектор важности подсистем защиты информации;

$A = (A_1, \dots, A_6)$ – вектор актуальности классов угроз;

N – функциональная зависимость, представленная нейронной сетью.

Множество угроз нарушения информационной безопасности (далее – ИБ) возможно для удобства разделить на классы CTh, которые определяются в формуле 2:

$$\text{Threat} = \{\text{ Breaking, Leak, Distortion, Loss, Blocking, Abuse}\}, \tag{2}$$

где Breaking – множество угроз, относящихся к классу «взлом»;

Leak – множество угроз, относящихся к классу «утечка»;

Distortion – множество угроз, относящихся к классу «искажение»;

Loss – множество угроз, относящихся к классу «утрата», множество угроз, относящихся к классу «блокирование»;

Blocking – множество угроз, относящихся к классу блокирование;

Abuse – множество угроз, относящихся к классу «злоупотребление».

Причем для того, чтобы определить вектор актуальности классов угроз на основании статистики угроз или данных мониторинга событий безопасности, определены две матрицы соответствия:

Матрица MTh соответствия между множеством угроз $Threat$ и множеством классов угроз *CTh*:

$$MTh = Threat \times Cth = (mth_{ij}),$$

где

$$mth_{ij} = \begin{cases} 1/n, \text{если угроза принадлежит классу угроз} \\ 0, \text{в противном случае} \end{cases}, \tag{3}$$

где n – количество классов угроз, которым принадлежит угроза. При этом $\forall i, \sum_j mth_{ij} = 1$.

Матрица MEv соответствия между множеством событий безопасности Ev и множеством классов угроз CTh:

$$MEv = Ev \times Cth = (mev_{ij}),$$

где $mev_{ij} = \begin{cases} 1, \text{если событие возникает при реализации угрозы класса} \\ 0, \text{в противном случае} \end{cases}$, (4)

Множество событий безопасности Ev включает в себя следующие типы [6]:

$$\text{E}v == \{ EnterEv, ManagementSubEv, AccessObjEv, PolicyChangeEv, UsePrivilegesEv, ISProcessesEv, LevelISEv\}, \quad (5)$$

где $EnterEv$ – множество событий типа «вход субъектов в систему»;

$ManagementSubEv$ – множество событий типа «управление субъектами»;

$AccessObjEv$ – множество событий типа «получение доступа к объектам»;

$PolicyChangeEv$ – множество событий типа «измененийt политики системы»;

$UsePrivilegesEv$ – множество событий типа «использование субъектом особых привилегий»;

$ISProcessesEv$ – множество событий типа «функционирование процессов системы»;

$LevelISEv$ – множество событий типа «уровень системы».

Используемая в программном комплексе нейронная сеть – многослойный персептрон – функционирует согласно формуле 6:

$$\begin{cases} In_{0k} = v_k \\ Out_{ij} = f(\sum_l w_{ijl} In_{ijl} - \theta_{ij}), \\ In_{ijl} = Out_{i-1l} \end{cases} \quad (6)$$

где In_{0k} – k-ый нейрон входного слоя;

v_k – k-ый элемент входного вектора;

Out_{ij} – выходное значение j-го нейрона i-го слоя;

f – функция активации нейрона;

w_{ijl} – вес l-го входа j-го нейрона i-го слоя;

In_{ijl} – значение l-го входа j-го нейрона i-го слоя;

θ_{ij} – уровень активации j-го нейрона i-го слоя;

Out_{i-1l} – выходное значение l-го нейрона (i–1)-го слоя.

Тогда функциональная модель интеллектуального выбора проекта системы защиты информации будет иметь вид (рис. 3) [7].

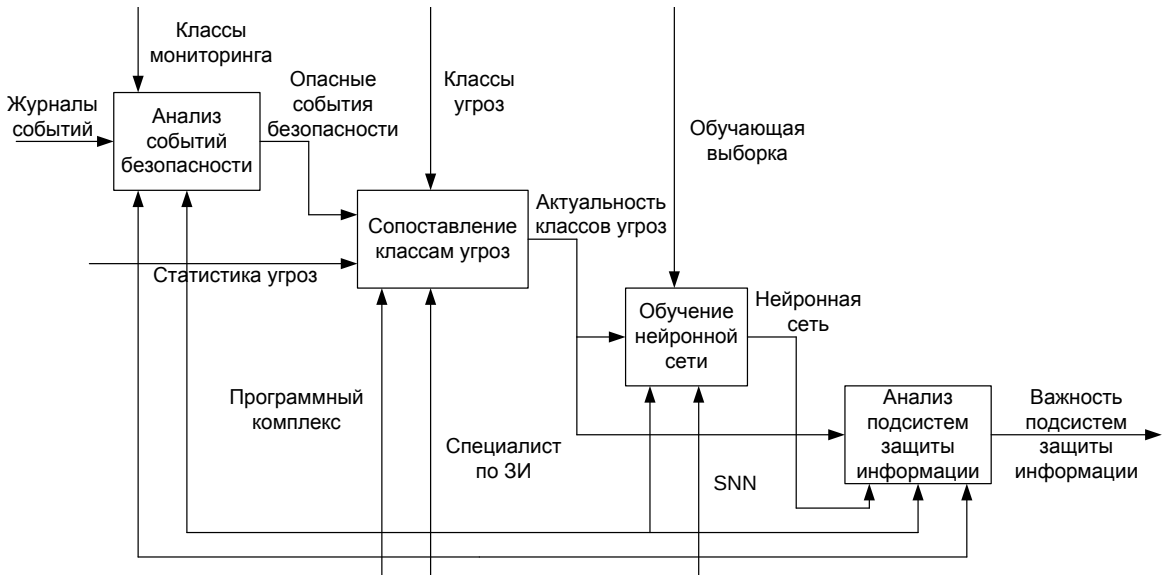

Рис. 3. Функциональная модель интеллектуального выбора проекта системы защиты информации

Входными данными являются либо события безопасности, либо статистика угроз. Из множества событий безопасности выбираются опасные события. Множество опасных со-

бытий безопасности или статистика угроз сопоставляются с классами угроз с помощью матриц соответствия [8]. В результате определяется вектор актуальности классов угроз. Для определения соответствия между актуальностью классов угроз и важностью подсистем защиты информации используется нейронная сеть [9].

Такая нейронная сеть – многослойный персептрон, требует предварительного обучения. Для этого используется обучающая выборка, составленная специалистом по защите информации. Обучение проводится с помощью стороннего ПО Statistica Neural Network.

Вектор важности подсистем защиты позволяет определить, какие подсистемы в первую очередь нуждаются в дополнительных средствах защиты информации [10–11].

На основе разработанной математической модели интеллектуальной поддержки принятия решений при проектировании СЗИ предприятия разработана архитектура программного комплекса интеллектуальной поддержки принятия решений при проектировании системы защиты ИС (рис. 4), состоящая из следующих модулей:

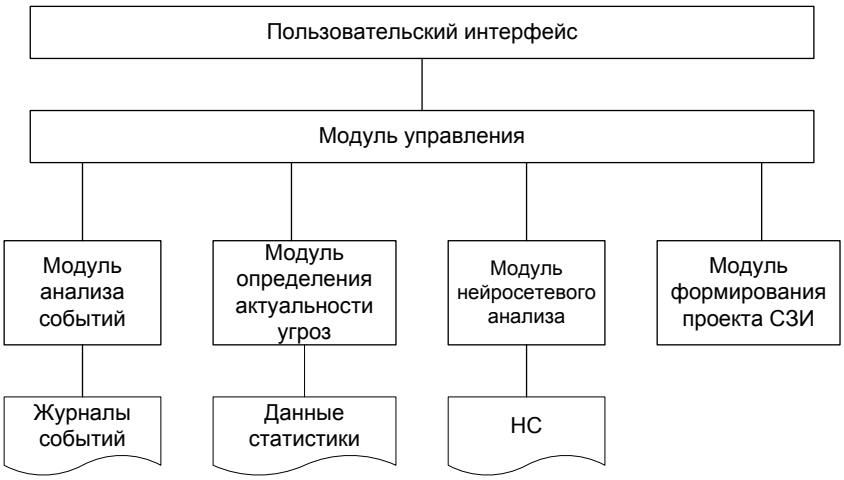

Рис. 4. Архитектура программного комплекса интеллектуальной поддержки принятия решений при проектировании системы защиты информационной системы предприятия

Пользовательский интерфейс необходим для организации интуитивно понятного взаимодействия пользователя с программным комплексом. Модуль управления осуществляет общее управление остальными модулями программного комплекса. Модуль анализа событий осуществляет сбор данных из журналов событий и подсчитывает количество опасных событий безопасности, относящихся к различным классам события (формула 5).

Модуль определения актуальности угроз на основании данных статистики или результата работы модуля анализа данных формирует вектор актуальности классов угроз по формулам 3 и 4.

Модуль нейросетевого анализа формирует вектор входных данных и передает его на вход нейронной сети, а затем получает и интерпретирует ее выход согласно формуле 6.

Модуль формирования проекта СЗИ определяет наиболее важные подсистемы защиты информации, которые нуждаются в дополнительных средствах защиты согласно формуле 6.

На основе описанной математической модели и архитектуры будет разработан программный комплекс, позволяющий как проектировщикам систем защиты информации, так и специалистам по защите информации на предприятии формировать наиболее оптимальные наборы средств защиты информации в проектах, при реализации которых эффективность работы СЗИ будет выше, чем при проектировании без средств принятия решений. Данный вывод следует из того, что при проектировании будет учтено все множество данных о защищаемой системе, что при «ручном» проектировании затруднительно. Кроме того, данный программный комплекс позволит минимизировать субъективные факторы, возникающие при

проектировании со стороны разработчика системы защиты. К ним относятся невнимательность разработчика при анализе исходных данных, сжатые сроки модернизации и/или разработки системы защиты, учет большого количества сведений о защищаемой системе, невозможность в короткие сроки провести глубокий комплексный анализ журналов событий безопасности или статистических данных.

Литература

1. Актуальные киберугрозы: II квартал 2019 года // Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019-q2/ (дата обращения: 28.06.2019).

2. Common Vulnerability Scoring System SIG. URL: https://www.first.org/cvss// (дата обращения: 28.06.2019).

3. Международный стандарт ISO 27001:2013 Информационные технологии. Методы защиты. Системы менеджмента информационной безопасности. Требования. URL: http://www.pqm-online.com/assets/files/pubs/translations/std/iso-mek-27001-2013(rus).pdf (дата обращения 07.07.2019).

4. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. URL: http://docs.cntd.ru/document/1200058320 (дата обращения 07.10.2018).

5. Об информации, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 г. № 149-ФЗ. Доступ из СПС Гарант.

6. Описание событий системы безопасности в Windows 7 и Windows Server 2008 R2. URL: https://support.microsoft.com/ru-ru/help/977519/ description-of-security-events-in-windows-7-and-in-windows-server-2008 (дата обращения: 05.08.2019).

7. Машкина И. В., Сенцова А. Ю., Гузаиров М. Н., Кладов В. Е. Использование методов системного анализа для решения проблемы обеспечения безопасности современных информационных систем // Изв. ЮФУ. Технические науки. 2011. № 12 (125). С. 25–35.

8. Астрахов А. В., Климов С. М., Сычев М. П. Противодействие компьютерным атакам. Технол. основы. М. : МГТУ имени Н.Э. Баумана, 2013. 70 с.

9. Казимир В. В., Серая А. А. Метод построения информационных атак // Математ. машины и системы. 2010. Т. 1, № 4. С. 52–61.

10. Витенбург Е. А., Пушкарская А. И., Оладько В. С. Модель оценки безопасности на основе мониторинга информационной системы // Информацион. системы и технологии. 2017. № 3 (101). С. 21–30.

11. Витенбург Е. А. Обеспечение информационной безопасности информационных ресурсов предприятия // Материалы науч. сессии ВолГУ, 22–27 апреля. Волгоград : Изд-во ВолГУ, 2018. С. 295–299.