DOI 10.21672/2074-1707.2020.49.4.162-169
УДК 004.056

ПОСТРОЕНИЕ ВЗАИМОСВЯЗИ МЕЖДУ НАРУШИТЕЛЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И УЯЗВИМОСТЯМИ ИНФОРМАЦИОННЫХ АКТИВОВ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

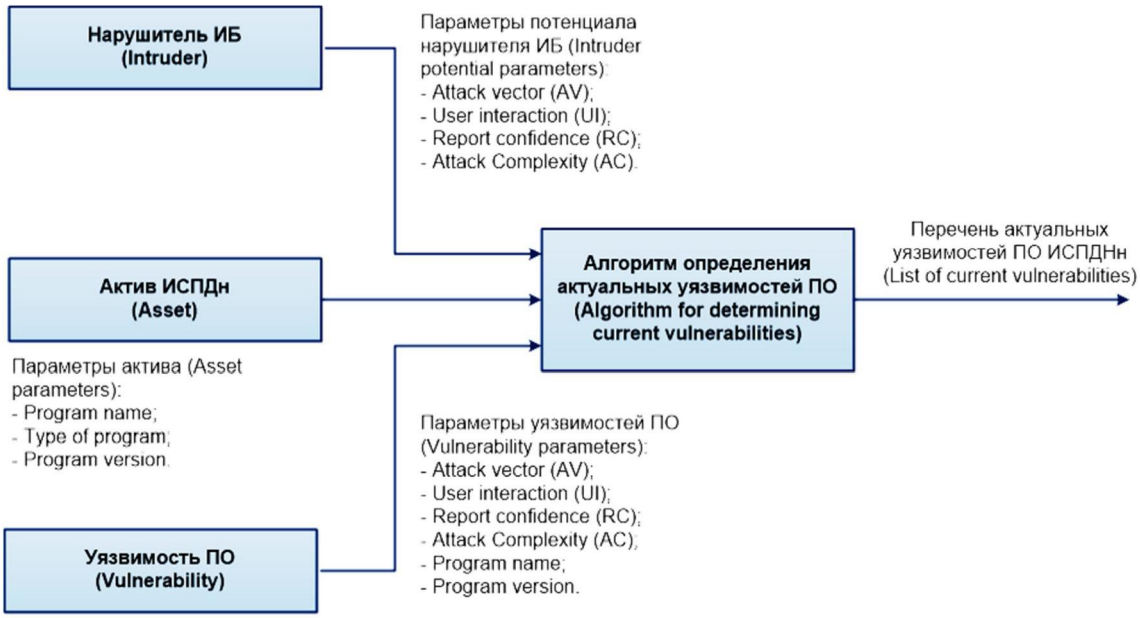
Статья поступила в редакцию 24.01.2020, в окончательном варианте – 05.03.2020.

Жук Роман Владимирович, Филиал «Макрорегион Юг» ООО ИК «СИБИНТЕК», 352800, Российская Федерация, г. Туапсе, ул. Карла Маркса, 36,
главный специалист, e-mail: goonerkrd@gmail.com
Дзьобан Павел Игоревич, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент кафедры компьютерных технологий и информационной безопасности Института компьютерных систем и информационной безопасности, e-mail: antiemoboy@mail.ru
Власенко Александра Владимировна, Кубанский государственный технологический университет, 50072, г. Краснодар, ул. Московская, 2,
кандидат технических наук, доцент, заведующая кафедрой компьютерных технологий и информационной безопасности института компьютерных систем и информационной безопасности, e-mail: Alex_Vlasenko@list.ru

Рассмотрены методики определения активов в информационных системах, выбора уязвимостей программного обеспечения, определения нарушителей и угроз информационной безопасности. Проведен обзор методики оценки уязвимостей программного обеспечения и методики выбора потенциала для нарушителя информационной безопасности с определенными возможностями. Предложена унификация параметров актива информационной системы обработки персональных данных. Предложен способ количественной оценки потенциала нарушителя информационной безопасности, построена взаимосвязь между нарушителем информационной безопасности и уязвимостями программного обеспечения на основе проецирования и унификации метрик вектора оценки уязвимости программного обеспечения на параметры потенциала нарушителя информационной безопасности. Подготовлены продукционные правила, позволяющие установить возможность реализации выявленных уязвимостей программного обеспечения выбранным нарушителем информационной безопасности.

Ключевые слова: актив, вектор, уязвимость программного обеспечения, метрика уязвимости, нарушитель информационной безопасности, продукционная модель, угроза информационной безопасности

Графическая аннотация (Grapchical annotation)



BUILDING A RELATIONSHIP BETWEEN AN INFORMATION SECURITY INTRUDER AND VULNERABILITIES OF INFORMATION ASSETS IN INFORMATION SYSTEMS FOR PROCESSING PERSONAL DATA

The article was received by the editorial board on 24.01.2020, in the final version – 05.03.2020.

Zhuk Roman V., Branch «Macroregion South» Ltd Co IC «SIBINTEK», 36 Karl Marks St., Tuapse, 352800, Russian Federation,

chief specialist, e-mail: goonerkrd@gmail.com

Dzoban Pavel I., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,

Cand. Sci. (Engineering), Associate Professor of the Department of Computer Technologies and Information Security of the Institute of Computer Systems and Information Security, e-mail: antiemoboy@mail.ru

Vlasenko Alexandra V., Kuban State Technological University, 2 Moskovskaya St., Krasnodar, 350072, Russian Federation,

Cand. Sci. (Engineering), Head of the Department of Computer Technologies and Information Security of the Institute of computer systems and information security, e-mail: Vlasenko@kubstu.ru

Methods for determining assets in information systems, selecting software vulnerabilities, and identifying information security intruder and threats to information security are considered. A review of the methodology for assessing software vulnerabilities and the methodology for selecting the potential for an information security intruder with certain capabilities is carried out. Unification of parameters of an asset of an information system for processing personal data is proposed. A method for quantifying the potential of an information security intruder is proposed, and the relationship between an information security intruder and software vulnerabilities is built on the basis of projecting and unifying metrics of the software vulnerability assessment vector on the parameters of the information security intruder's potential. We have prepared production rules that allow us to determine whether the identified software vulnerabilities can be implemented by the selected information security violator.

Key words: vector, software vulnerability, vulnerability metric, information security intruder, production model, information security threat

Введение. Как показывается практика применения международных стандартов по информационной безопасности (ИБ), существует различие между риском ИБ и актуальной угрозой ИБ. А именно, риск ИБ является мерой возможной реализации уязвимости актива определенной угрозой, в результате чего может быть нанесен определенный ущерб организации – владельцу актива [1]. Угроза ИБ в информационных системах обработки персональных данных (ИСПДн) является совокупностью несанкционированного, в том числе, доступа к информации, содержащей персональные данные (далее – ПДн). Результатом такого доступа может стать одно или несколько деструктивных действий (уничтожение, изменение, блокирование, копирование, распространение) [3]. Актуальной угрозой ИБ в ИСПДн считаются угрозы ИБ представляющие потенциальную опасность для ПДн и имеющие возможность реализации, оцененную по методике, представленной в [3].

В [6] представлена классификация угроз несанкционированного доступа в ИСПДн, а также типовые модели угроз ИБ в ИСПДн. Исходя из методик, приведенных в [3] и [6], угроза ИБ представлена как совокупность следующих факторов:

- источник угрозы ИБ;
- уязвимость ИСПДн;
- способ реализации;
- объект воздействия;
- деструктивное действие.

С появлением банка данных угроз безопасности [6] наблюдается тенденция к унификации методик определения угроз ИБ и формирования модели нарушителя ИБ и угроз ИБ в информационных системах (далее – ИС). Дополнительно, регулятором в 2015 г. для обсуждения был опубликован проект методического документа [6]. Однако данный документ на момент написания статьи не был введен в действие.

Рядом нормативных документов отечественных регуляторов в области ИБ для различных видов ИС предусмотрена разработка модели угроз ИБ. Например, данные требования аналогичны для государственных информационных систем [7], автоматизированных систем управления производственными и технологическими процессами [10].

Основным отличием при разработке модели угроз ИБ для ИСПДн от вышеперечисленных ИС является наличие утвержденных методик: [3] и [6].

В настоящее время для определения угроз ИБ в ИСПДн банк данных угроз безопасности представляет справочную информацию о существующих угрозах ИБ и уязвимостях программного обеспечения (далее – ПО). Определение перечня угроз ИБ осуществляется в соответствии с пользовательским фильтром, основными параметрами которого являются:

- тип нарушителя и его потенциал;
- нарушения свойств защищенности информации (конфиденциальность, целостность, доступность) по результатам реализации угрозы.

Определение перечня уязвимостей ИБ осуществляется аналогичным способом с использованием дополнительных параметров, применяемых в методиках оценки уязвимостей [7] и [11]:

- класс уязвимости;
- уровень опасности;
- базовый вектор (Access Vector, Attack Complexity, Authentication);
- идентификатор типа ошибки;
- наличие эксплойта;
- способ эксплуатации;
- способ устранения;
- операционная система.

На основании вышеизложенного разработка модели угроз ИБ посредством банка данных угроз безопасности для различных видов ИС существенным образом зависит от квалификации эксперта, либо группы экспертов, привлекаемых для выбора угроз ИБ. Применение банка данных угроз безопасности для разработки модели угроз ИБ в ИСПДн, совместно с методиками [3] и [6], также является непрактичным в виду отсутствия связи между используемыми банком и параметрами вышеуказанных методик.

Отсутствует взаимосвязь между угрозами ИБ и уязвимостями ПО, приведенными в банке данных угроз безопасности.

Целью данной работы является выбор параметров и организация взаимосвязи между активами ИСПДн, уязвимостями активов и возможностями нарушителя ИБ с целью формирования перечня уязвимостей ПО, которые могут быть реализованы в ИСПДн. Для достижения данной цели необходимо ***решить следующие задачи***:

- классифицировать активы и подготовить перечень параметров для их определения;
- оптимизировать перечень нарушителей и разработать методику оценки их потенциала;
- разработать алгоритм выбора уязвимостей.

Подготовка перечня параметров активов ИСПДн. Классификация активов ИСПДн получена путем проецирования показателей исходной защищенности, приведенных в [3] и в проекте методического документа «Методика определения угроз безопасности информации в информационных системах», а также категорий нарушителя, представленных в [1], на перечень активов представленных в [1]. Учитывая необходимость унификации и автоматизации разрабатываемой методики, а также распределение уязвимостей по параметрам, представленное в банке данных угроз безопасности и общедоступных базах данных уязвимостей ПО, например [11], экспертным путем подготовлены следующие параметры активов:

- наименование ПО;
- тип ПО;
- версия ПО.

Унификация нарушителей информационной безопасности и количественная оценка из потенциала. Согласно классификации, представленной в [1], существует два типа нарушителей, имеющих различные категории в зависимости от наличия определенных возможностей:

- внешний (5 категорий);
- внутренний (8 категорий).

Банки данных угроз безопасности для определения угроз ИБ используют классификацию нарушителей ИБ, представленную в [6] и основанную на потенциале:

- внешний (3 типа потенциала);
- внутренний (3 типа потенциала).

Виды нарушителей ИБ представленные в [1] и [6] могут быть сопоставлены, а их перечень может быть проанализирован и оптимизирован экспертным путем. По результатам оптимизации перечень нарушителей ИБ с присвоенными потенциалами представлен на рисунке 1.

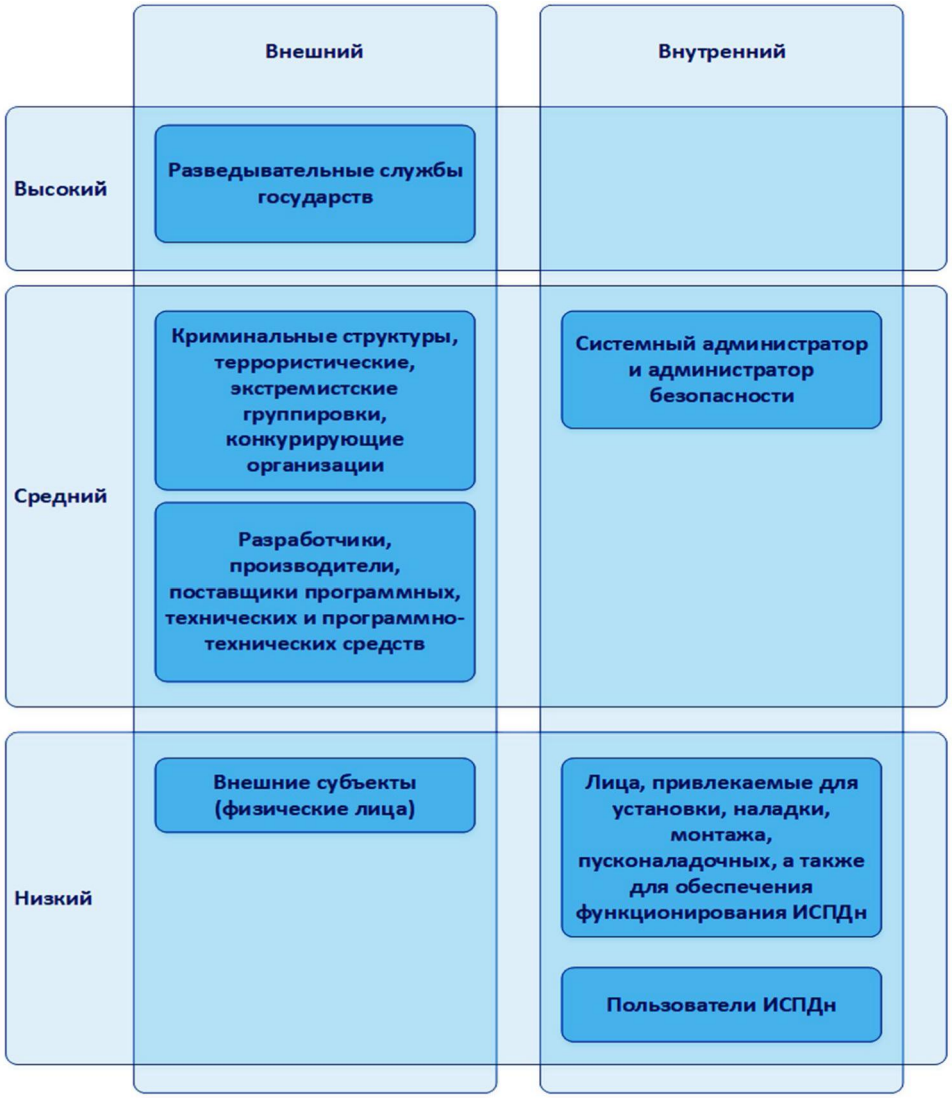


Рисунок 1 – Оптимизированный перечень нарушителей ИБ

Согласно [6], потенциал нарушителя ИБ строго определен. Однако для новых нарушителей ИБ предусмотрен алгоритм и параметры определения потенциала:

- время, затрачиваемое нарушителем ИБ на поиск, определение и использование уязвимости;
- техническая компетентность;
- знание проекта ИС;
- оснащенность;
- возможности доступа к ИСПДн.

Присвоение значений параметрам определения потенциала нарушителя осуществляется экспертным путем. Основной проблемой при определении потенциала нарушителя ИБ по методике [6] является отсутствие связи нарушителя ИБ и уязвимостей ПО активов ИСПДн.

Одним из возможных способов построения связи между потенциалом нарушителя ИБ и уязвимостью ПО активов ИСПДн является проецирование базовых и временных метрик, используемых в общей системе оценки уязвимостей ПО [7] и [8], на параметры потенциала (табл. 1).

Таблица 1 – Метрики, сопоставленные с возможностями нарушителя ИБ

№ п/п	Наименование метрики	Возможность нарушителя ИБ	Метрика
1	Возможности физического доступа к активу:	Возможность доступа к ИС	Attack Vector (AV)
	Через сети общего доступа		Network (N)
	С помощью локально-вычислительной сети		Adjacent Network (A)
	Физический доступ		Physical (P)
2	Необходимость взаимодействия с пользователем	Знание проекта и информационной системы	User Interaction (UI)
	Необходимо		Required (R)
	Нет необходимости		None (N)
3	Наличие информации об уязвимости в общем доступе	Техническая компетентность нарушителя	Report Confidence (RC)
	Отсутствует описание		Unknown (U)
	Частично описана		Reasonable (R)
	Полностью описана		Confirmed (C)
4	Возможность применения специальных средств для эксплуатации уязвимости	Оснащенность нарушителя	Attack Complexity (AC)
	Применение специальных средств		High (H)
	Специальные средства не применяются		Low (L)

Для **разработки алгоритма выбора уязвимостей** проведен анализ различных источников информации об уязвимостях ПО, например [12, 13, 14]. По результатам анализа установлены параметры, которые могут влиять на выбор уязвимостей для подготовленного перечня активов, в состав которого входит ПО:

- наименование ПО;
- версия ПО.

Таким образом, процесс определения уязвимостей ПО будет детализован на два этапа:

1. Определение перечня уязвимостей ПО для выбранных активов.

2. Сопоставление метрик, выбранных на «этапе 1» уязвимостей ПО с параметрами потенциала выбранного нарушителя ИБ.

Используя [4], спроецируем количественные значения на параметры потенциала (табл. 2).

Таблица 2 – Значения метрик уязвимости

№ п/п	Наименование метрики	Метрика	Числовое значение
1	Возможности физического доступа к активу:	Attack Vector (AV)	
	Через сети общего доступа	Network (N)	0,85
	С помощью локально-вычислительной сети	Adjacent Network (A)	0,62
	Физический доступ	Physical (P)	0,2
2	Необходимость взаимодействия с пользователем	User Interaction (UI)	
	Необходимо	Required (R)	0,62
	Нет необходимости	None (N)	0,85
3	Наличие информации об уязвимости в общем доступе	Report Confidence (RC)	
	Отсутствует описание	Unknown (U)	0,92
	Частично описана	Reasonable (R)	0,96
	Подтверждена производителем ПО	Confirmed (C)	1
4	Возможность применения специальных средств для эксплуатации уязвимости	Attack Complexity (AC)	
	Применение специальных средств	High (H)	0,44
	Специальные средства не применяются	Low (L)	0,77

Сопоставление параметров нарушителя с метриками вектора уязвимостей позволит разработать продукционную модель вида:

$$R = < X_1 A_1, X_2 A_2, \dots\dots, X_n A_n : YB >.$$

Левая часть правила является антецедентом X и включает в себя перечень предпосылок для реализации правой части – консеквента Y. Между собой предпосылки связываются посредством операций «И», «ИЛИ».

Для реализации второго этапа создается следующее продукционное правило:

- Vulnerability: если «AV уязвимости актива» <= «AV нарушителя ИБ» И «UI уязвимости актива» <= «UI нарушителя ИБ» И «RC уязвимости актива» <= «RC нарушителя ИБ» И «AC уязвимости актива» <= «AC нарушителя ИБ», то «Уязвимость №» = «Актуальная уязвимость».

Таким образом, для подготовки перечня уязвимостей ПО, которые могут быть реализованы существующим нарушителем ИБ, необходимым условием будет являться превосходство параметров потенциала нарушителя ИБ над метриками уязвимостей ПО из подготовленного списка для ИСПДн, либо их равенство.

По результатам сформированного перечня уязвимостей ПО, которые могут быть реализованы существующим нарушителем ИБ, возможно подготовить перечень угроз ИБ в ИСПДн.

Заключение. Используя параметры актива и проецируя метрики уязвимостей ПО на параметры потенциала нарушителя ИБ, может быть построена связь между нарушителем ИБ и существующими для активов ИСПДн уязвимостями ПО, а также создан объективный алгоритм подготовки перечня актуальных уязвимостей ПО, который может быть реализован в виде ПО или скриптов, для сокращения времени затраченного на разработку модели нарушителя ИБ и подготовку перечня уязвимостей ПО для активов ИСПДн.

Библиографический список

1. Методический документ ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)» – 2008. – 69 с. – Режим доступа: https://fstec.ru/component/attachments/download/289, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 20.01.2020).

2. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – Режим доступа: http://docs.cntd.ru/document/gost-r-iso-mek-27005-2010, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 20.01.2020).

3. Информационное сообщение ФСТЭК России от 6 марта 2015 г. № 240/22/879 «О банке данных угроз безопасности информации». – Режим доступа: https://fstec.ru/normotvorcheskaya/informatsionnye-i-

analiticheskie-materialy/956-informatsionnoe-soobshchenie-fstek-rossii-ot-6-marta-2015-g-240-22-879, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 20.01.2020).

4. Калькулятор метрик уязвимостей. – Режим доступа: https://www.first.org/cvss/calculator/cvsscalc30.js, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 20.01.2020).

5. Методический документ ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», – 2008. – 10 с. – Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 20.01.2020).

6. Методический документ ФСТЭК России «Методика определения угроз безопасности информации в информационных системах» (проект). – 2015. – 43 с. – Режим доступа: https://fstec.ru/component /attachments/download/812, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 20.01.2020).

7. Общая система оценки уязвимостей, версия 2.0, июнь 2007 г., Петер Мелл, Карэн Шарфон, Национальный институт стандартизации и технологий, Саша Романовски, Университет Карнеги Меллон. – Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 17.01.2020).

8. Общая система оценки уязвимостей, версия 3.1, Технический документ, Редакция 1. – Режим доступа: https://www.first.org/cvss/v3.1/specification-document, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 17.01.2020).

9. Приказ ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». – Режим доступа: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 19.01.2020).

10. Приказ ФСТЭК России от 14.03.2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды». – Режим доступа: https://fstec.ru/index?id=868:prikaz-fstek-rossii-ot-14-marta-2014-g-n-31, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 19.01.2020).

11. Сайт базы данных уязвимостей. – Режим доступа: https://nvd.nist.gov/vuln-metrics/cvss, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 20.01.2020).

12. Сайт базы данных уязвимостей. – Режим доступа: https://nvd.nist.gov/vuln/, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 20.01.2020).

13. Сайт базы данных уязвимостей. – Режим доступа: http://www.cvedetails.com, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 20.01.2020).

14. Сайт базы данных уязвимостей. – Режим доступа: http://www.securityfocus.com, свободный. – Заглавие с экрана. – Яз. рус. (дата обращения: 20.01.2020).

References

1. *Metodicheskiy dokument FSTEK Rossii "Bazovaya model ugroz bezopasnosti personalnykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personalnykh dannykh (vypiska)"* [Guidance document of the FSTEC of Russia "The basic model of personal data security threats when they are processed in personal data information systems (extract)"], 2008. 69 p. Available at: https://fstec.ru/component/attachments/download/289 (accessed 20.01.2020).

2. *GOST R ISO/ MEK 27005-2010. Informatsionnaya tehnologiya. Metodi i sredstva obespecheniya informacionnoi bezopashonsti* [GOST R ISO / IEC 27005-2010. Information technology. Methods and means of ensuring security. Information security risk management]. Available at: http://docs.cntd.ru/document/gost-r-iso-mek-27005-2010 (accessed 20.01.2020).

3. *Informatsionnoe pismo FSTEK Rossii ot 6 marta 2015 g. №240/22/879 "O banke dannykh ugroz bezopasnosti informatsii"* [FSTEC information message no. 240/22/879 of March 6, 2015 «On the data Bank of information security threats».] Available at: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/956-informatsionnoe-soobshchenie-fstek-rossii-ot-6-marta-2015-g-240-22-879 (accessed 20.01.2020).

4. *Kalkulator metrik uyazvimostey* [Calculator metrics of the vulnerabilities.] Available at: https://www.first.org/cvss/calculator/cvsscalc30.js (accessed 20.01.2020).

5. *Metodicheskiy dokument FSTEK Rossii "Methodika opredeleniya aktualnykh ugroz bezopasnosti personalnykh dannykh v informatsionnykh sistemakh personalnykh dannkh"* [Guidance document of the FSTEC of Russia "Methodology for determining current threats to the security of personal data when they are processed in personal data information systems"], 2008. 10 p. Available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380 (accessed 20.01.2020).

6. *Metodicheskiy dokument FSTEK Rossii "Methodika opredeleniya ygroz bezopasnosti informacii v informacionnih sistemah" (proekt)* [Methods for determining information security threats in information systems (project)]. Available at: https://fstec.ru/component/attachments/download/812 (accessed 20.01.2020).

7. *Obshchaya otsenka uyazvimostey* [General vulnerability assessment system] version 2.0, June 2007, Peter Mell, Karen Sharfon, national Institute of standardization and technology, Sasha Romanovsky, Carnegie Mellon University]. Available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380 (accessed 17.01.2020).

8. *General vulnerability assessment system, version 3.1, Technical document, Revision 1.* Available at: https://www.first.org/cvss/v3.1/specification-document (accessed 19.01.2020).

9. *Prikaz FSTEK Rossii ot 11.02.2013 №17 "Ob ytvergdenii trebovanii o zashchite informatsii, ne sostavlayushchey gosudarstvennuyu tayny, sodergashcheysya v gosydarstvennykh informatsionnykh sistemakh"* [FSTEC order no. 17.11.2013 «On approval of requirements for the protection of information that does not constitute a state secret contained in state information systems»]. Available at: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702 (accessed 19.01.2020).

10. *Prikaz FSTEK Rossii ot 31.03.2014 № 31 "Ob utverzhdenii trebovaniy o zashchite informatii v avtomatizirovannykh sistemakh upravleniya proizvodstvennymmi i tekhnologicheskimi protsessami na kriticheskihh vazhnykh obektakh, potentsialno opasnykh obektakh, a takzhe obektakh predstavlayushikh povyshennuyu opasnost dlya zhizni izdorovya ludey i dlya okruzhaiyshchey prirodnoy sredy"* [FSTEC order no. 31 of March 14, 2014 «On approval of requirements for ensuring information security in automated production and process control systems at critical facilities, potentially dangerous facilities, as well as objects that pose an increased risk to human life and health and the environment»]. Available at: https://fstec.ru/index?id=868:prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (accessed 19.01.2020).

11. *Sayt bazy dannykh uyazvimostey* [Vulnerability database site]. Available at: https://nvd.nist.gov/vuln-metrics/cvss (accessed 20.01.2020).

12. *Sayt bazy dannykh uyazvimostey* [Vulnerability database site]. Available at: https://nvd.nist.gov/vuln/ (accessed 20.01.2020).

13. *Sayt bazy dannykh uyazvimostey* [Vulnerability database site]. Available at: http://www.cvedetails.com (accessed 20.01.2020).

14. *Sayt bazy dannykh uyazvimostey* [Vulnerability database site]. Available at: http://www.securityfocus.com (accessed 20.01.2020).

DOI 10.21672/2074-1707.2020.49.4.169-178
УДК 004.056

ОПРЕДЕЛЕНИЕ АКТУАЛЬНОСТИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ МАТЕМАТИЧЕСКОГО АППАРАТА НЕЙРОННЫХ СЕТЕЙ

Статья поступила в редакцию 04.02.2020, в окончательном варианте – 09.03.2020.

Жук Роман Владимирович, Филиал «Макрорегион Юг» ООО ИК «СИБИНТЕК», 352800, Российская Федерация, г. Туапсе, ул. Карла Маркса, 36,

главный специалист, e-mail: goonerkrd@gmail.com

Дзьобан Павел Игоревич, Кубанский государственный технологический университет, 350072, Российская Федерация, г. Краснодар, ул. Московская, 2,

кандидат технических наук, доцент кафедры компьютерных технологий и информационной безопасности Института компьютерных систем и информационной безопасности, e-mail: antiemoboy@mail.ru

Власенко Александра Владимировна, Кубанский государственный технологический университет, 50072, г. Краснодар, ул. Московская, 2,

кандидат технических наук, доцент, заведующая кафедрой компьютерных технологий и информационной безопасности института компьютерных систем и информационной безопасности, e-mail: Alex_Vlasenko@list.ru

Рассмотрены методики определения угроз информационной безопасности в информационных системах обработки персональных данных. В связи с отсутствием согласованности существующей утвержденной методики с применяемой банком данных угроз информационной безопасности (https://bdu.fstec.ru/) был проведен анализ параметров актуальности угроз информационной безопасности и предложен способ определения актуальности угроз информационной безопасности с использованием математического аппарата искусственных нейронных сетей. Для реализации этого способа был выполнен анализ топологий искусственных нейронных сетей и методов вычисления ошибок в них. Разработана искусственная нейронная сеть на основании топологии многослойного перцептрона с обратным распространением ошибки. Проведено обучение разработанной искусственной нейронной сети путем подготовки и использования обучающей выборки. Осуществлено сравнение быстродействия функционирования разработанной искусственной нейронной сети с быстродействием привлеченной группы экспертов, действующих по существующей утвержденной методике определения актуальности угроз информационной безопасности в информационных системах обработки персональных данных.

Ключевые слова: показатель исходной защищенности, потенциал нарушителя информационной безопасности, искусственная нейронная сеть, перцептрон, искусственный нейрон, слой, входной сигнал, выходной сигнал, функция активации, сигмоидальная функция, обучающая выборка, угроза информационной безопасности