DOI 10.37882/2223–2966.2023.03.27

МЕТОДИКА ОЦЕНКИ УРОВНЯ ЗАЩИЩЁННОСТИ ПРОГРАММНО-ТЕХНИЧЕСКИХ РЕШЕНИЙ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ

METHODOLOGY FOR ASSESSING THE LEVEL OF SECURITY OF SOFTWARE AND HARDWARE SOLUTIONS OF AN INTEGRATED SYSTEM FOR PROTECTING INFORMATION OF AN ENTERPRISE

P. Nasedkin
M. Bazilevskiy

Summary. The article proposes a method for assessing the level of security of the subsystem of software and hardware solutions (SHS) of an integrated information security system (IISS). A model of the relationship between the objects of influence and the main elements (complexes, subsystems) of the means of protecting information of the SHS level has been developed. Based on the database of threats of the Federal Service for Technical and Export Control (FSTEC), the objects of impact were optimized. In accordance with the SHS level model and the assessments of information security auditors, the efficiency was determined for each level of functionality of the subsystems and for each level of the subsystem. In accordance with the effectiveness assessments for the elements of the SHS, an assessment of the overall level of security of the SHS with the possibility of determining the key elements of the SHS that affect this level is proposed.

Keywords: level efficiency, objects of influence, subsystems, complexes, level of functionality, level assessment.

Наседкин Павел Николаевич
Аспирант, старший преподаватель, Иркутский государственный университет путей сообщения
nasedkin_pn@irgups.ru
Базилевский Михаил Павлович
Кандидат технических наук, Иркутский государственный университет путей сообщения
mik2178@yandex.ru

Аннотация. В статье предложена методика оценки уровня защищённости подсистемы программно-технических решений (ПТР) комплексной системы защиты информации (КСЗИ). Разработана модель взаимосвязи между объектами воздействия и основными элементам (комплексы, подсистемы) средств защиты информации уровня ПТР. На основе базы данных угроз Федеральной службы по техническому и экспортному контролю (ФСТЭК) проведена оптимизация объектов воздействия. В соответствии с моделью уровня ПТР и оценками аудиторов по информационной безопасности определена эффективность по каждому уровню функциональности подсистем и по каждому уровню подсистемы. В соответствие с оценками эффективности по элементам ПТР предложена оценка общего уровня защищённости ПТР с возможностью определения ключевых элементов ПТР, влияющих на данный уровень.

Ключевые слова: эффективность уровня, объекты воздействия, подсистемы, комплексы, уровень функциональности, оценка уровня.

Введение

Растущая зависимость от программных и аппаратных решений сделала измерение уровня их безопасности важнейшим аспектом современных технологий. Безопасность этих систем напрямую влияет на конфиденциальность, целостность и доступность информации, которую они хранят и обрабатывают. В результате научное сообщество активно занимается разработкой методов оценки уровня безопасности этих систем. Оценка уровня безопасности систем предприятия имеет огромное значение в современной быстро меняющейся и технологически развитой бизнес-среде. С ростом использования программного обеспечения и технологий в повседневной деятельности очень важно обеспечить безопасность этих систем и их защиту от потенциальных угроз.

Область формализации знаний при решении задач и обработки информации в процессах управления является хорошо изученной областью, в которой имеется значительный объем работ как зарубежных, так и российских авторов. Среди зарубежных авторов в этой области в настоящее время можно отметить Жан Л., Ван Ю. и Лю [1, 2], В., Садеги А. и Шеллер Р. [3], Алотаиби М. и Али М. [4], Джайн Р. и Джоши А. [5, 6], Маркес С. и Гедес А. [7], Ли Ю., Жан Х. и Лю Ю. [8], Хан Ю., Фан Х. и Жан Л. [9], Ли Х., Ли Ю. и Лю Ю. [10], а среди российских ученых –П.Н. Девянина [11], П.Д. Зегжда [12–14], И.С. Клименко [15], Корниенко А.А. [16] и других.

Кроме того, теоретические основы компьютерной безопасности и защиты сетей были исследованы П.Н. Девяниным [11] и Б.Я. Советовым [17]. Также растет число работ, посвященных изучению различных аспек-

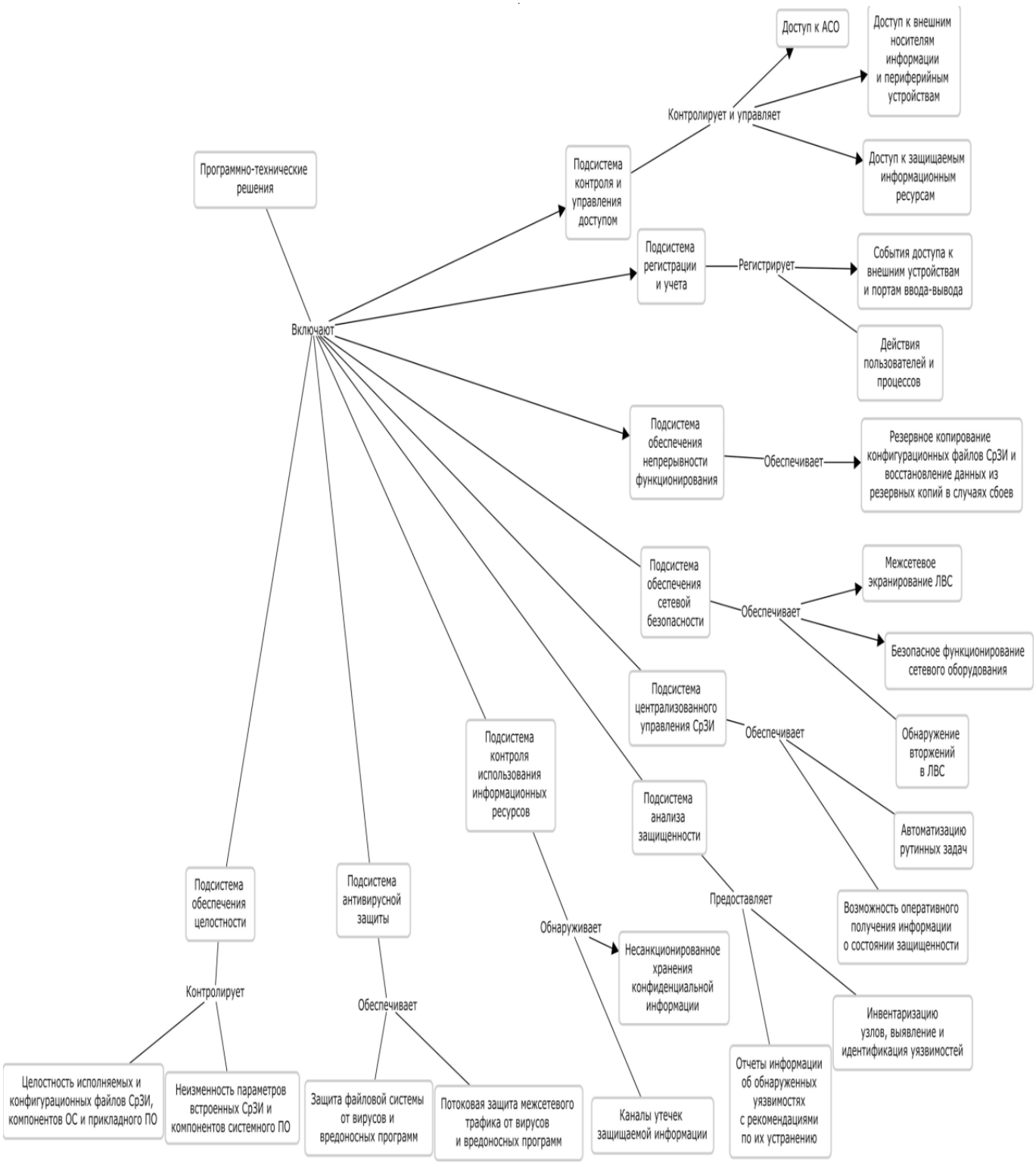

Рис. 1. Структура элементов ПТР и их функциональность

тов защиты информации, заметный вклад в эту область внесли такие авторы, как А.А. Малюк [18], Л.К. Бабенко [19], А.С. Басан [19], А.А. Шумский [20] и А.А. Шелупанов [20]. Эти ученые — лишь несколько примеров из множества российских специалистов, внесших значительный вклад в область информационной безопасности.

Цель настоящей статьи состоит в том, чтобы предложить новый подход к оценке уровня безопасности корпоративных систем, которая учитывает программно-технические решения (ПТР). В основе методики использованы: результаты системного анализа в области построения комплексных систем защиты информации; математические и статистические методы обработки информации для оценки уровня защищённости ПТР комплексной системы защиты информации (КСЗИ) .

Актуальность данной статьи заключается в возрастающем значении информационной безопасности в современном деловом мире и необходимости комплексного и эффективного метода оценки безопасности корпоративных систем. В связи с чем, предлагаемая методика удовлетворяет эту потребность, предлагая научно обоснованный и практичный подход для оценки уровня информационной безопасности этих систем.

Модель базы знаний уровня ПТР КСЗИ

Для внедрения на любом предприятии тех или иных ПТР требуется разработка структуры базы знаний их элементов и выполняемых ими функций. В рамках данной работы определена структура (рис.1), состоящая из девяти подсистем ПТР [15, 20, 21–24]: 1) контроля и управления доступом; 2) регистрации и учета; 3) обеспечения целостности; 4) антивирусной защиты; 5) контроля использования информационных ресурсов; 6) централизованного управления СрЗИ; 7) анализа защищённости; 8) обеспечения сетевой безопасности; 9) обеспечения непрерывности функционирования.

Представленные на рис. 1 подсистемы выполняют следующие функции.

1. Подсистема контроля и управления доступом отвечает за управление учетными записями пользователей и администраторов и их доступом к информационным активам предприятия.
2. Подсистема регистрации и учета отслеживает доступ субъектов к защищенным ресурсам и регистрирует события, связанные с доступом.
3. Подсистема целостности обеспечивает целостность программного обеспечения и конфигурационных файлов, связанных со средствами защиты информации.
4. Подсистема антивирусной защиты обеспечивает непрерывную защиту от вирусов и вредоносных программ.
5. Подсистема контроля информационных ресурсов осуществляет мониторинг и контроль несанкционированного доступа к конфиденциальной информации, а также обеспечивает перехват и анализ различных видов связи, таких как электронная почта и обмен мгновенными сообщениями.
6. Подсистема централизованного управления средствами информационной безопасности: предоставляет администраторам инструменты для управления информационной безопасностью.
7. Подсистема анализа безопасности проводит анализ безопасности различных компонентов сети предприятия и генерирует отчеты о результатах.
8. Подсистема сетевой безопасности использует межсетевые экраны и средства обнаружения вторжений для сети предприятия.
9. Подсистема функциональной непрерывности обеспечивает резервное копирование и восстановление данных для средств защиты информации и активного сетевого оборудования в случае сбоев.

В рамках ПТР выделены пятнадцать комплексов средств защиты информации: 1) комплекс встроенных средств защиты серверов и автоматизированных рабочих машин под управлением операционных систем семейства Windows; 2) антивирусной защиты; 3) резервного копирования; 4) защиты среды виртуализации; 5) сбора, анализа и корреляции событий информационной безопасности; 6) встроенных средств активного сетевого оборудования; 7) резервного копирования конфигурационных файлов активного сетевого оборудования; 8) межсетевого экранирования; 9) обнаружения вторжений; 10) встроенных средств защиты систем хранения данных; 11) централизованного управления средств защиты информации; 12) анализа защищенности; 13) контроля целостности; 14) встроенных средств защиты прикладного программного обеспечения; 15) контроля использования информационных ресурсов.

Сформированная модель базы знаний уровня ПТР КСЗИ позволяет приступить к описанию самой методики оценки уровня её защищённости, которая будет представлена в следующем разделе статьи.

Методика оценки защищённости уровня ПТР КСЗИ

Для оценки уровня защищённости ПТР КСЗИ предприятия предлагается следующая методика.

Таблица 1. Форма для заполнения бинарного массива

Подсистема	Функциональность	Объект воздействия / Комплекс уровня ПТР КСЗИ	1	2	…	58
1	1	1	1	1	…	0
1	2	6	0	1	…	1
2	1	8	1	1	…	0

Шаг 1. Используя данные с сайта БДУ ФСТЭК России (https://bdu.fstec.ru/files/documents/thrlist.xlsx) формируется список объектов воздействия. На данный момент таких объектов оказалось 58. Среди них базы данных, информационные системы, каналы связи, мобильные устройства и т.д.

Шаг 2. Формируется вектор V, состоящий из элементов v_i, показывающих количество функциональностей, входящих в i-ю подсистему. В нашем случае для девяти подсистем этот вектор выглядит так:

$$V = (3,2,2,2,2,2,2,3,1).$$

Формируются множества M_i^j, состоящие из номеров комплексов, входящих в j-ю функциональность i-й подсистемы. В нашем случае эти множества выглядят следующим образом:

$M_1^1 = \{1,4,8,10,14,15\}$, $M_1^2 = \{1,15\}$, $M_1^3 = \{6,8\}$,

$M_2^1 = \{1,2,4,5,6,8,9,10,12,13,14,15\}$, $M_2^2 = \{1,15\}$,

$M_3^1 = \{1,12,13\}$, $M_3^2 = \{1,12,13\}$,

$M_4^1 = \{2\}$, $M_4^2 = \{8\}$,

$M_5^1 = \{1,15\}$, $M_5^2 = \{15\}$,

$M_6^1 = \{11\}$, $M_6^2 = \{11\}$,

$M_7^1 = \{12\}$, $M_7^2 = \{12\}$,

$M_8^1 = \{8\}$, $M_8^2 = \{9\}$, $M_8^3 = \{6,7,8,9\}$,

$M_9^1 = \{3,7\}$.

Шаг 3. Формируется бинарный четырехмерный массив D, состоящий из элементов δ_{ijkp}, где i — номер подсистемы ($i = \overline{1,9}$), j — номер функциональности ($j = \overline{1,v_i}$), k — элементы множества M_i^j, p — номер объекта защиты ($p = \overline{1,58}$). Элементы массива D задаются по правилу:

$$\delta_{ijkp} = \begin{cases} 1, \text{ если в } j-\text{й функциональности } i\text{-й подсистемы} \\ \quad k\text{-й комплекс связан с } p\text{-м объектом защиты;} \\ 0, \text{ в противном случае.} \end{cases}$$

Для удобства заполнения бинарного массива D можно воспользоваться формой, представленной в таблице 1.

Информация, которая будет внесена в массив D по предприятию в дальнейшем будет считаться как «эталон» для расчетов в оценке функциональной эффективности уровня ПТР КСЗИ и оценке его общего уровня защищённости.

Шаг 4. С использованием бинарного массива D для каждого комплекса, входящего в j-ю функциональность i-й подсистемы, вычисляется доля его связей с объектами защиты в общем числе связей всех комплексов j-й функциональности i-й подсистемы с объектами защиты по формуле:

$$N_{ijk}^1 = \begin{cases} \dfrac{\sum\limits_{p=1}^{58} \delta_{ijkp}}{\sum\limits_{s \in M_i^j} \sum\limits_{p=1}^{58} \delta_{ijsp}}, \text{ если } \sum\limits_{s \in M_i^j} \sum\limits_{p=1}^{58} \delta_{ijsp} \neq 0, \\ 0, \text{ если } \sum\limits_{s \in M_i^j} \sum\limits_{p=1}^{58} \delta_{ijsp} = 0, \end{cases}$$

$$i = \overline{1,9},\ j = \overline{1,v_i},\ k \in M_i^j. \quad (1)$$

Затем для каждой функциональности, входящей в i-ю подсистему, вычисляется доля общего числа связей всех её комплексов с объектами защиты в общем числе связей всех комплексов i-й подсистемы с объектами защиты по формуле:

$$N_{ij}^2 = \begin{cases} \dfrac{\sum\limits_{s\in M_i^j}\sum\limits_{p=1}^{58}\delta_{ijsp}}{\sum\limits_{t=1}^{v_i}\sum\limits_{s\in M_i^t}\sum\limits_{p=1}^{58}\delta_{itsp}}, \text{ если } \sum\limits_{t=1}^{v_i}\sum\limits_{s\in M_i^t}\sum\limits_{p=1}^{58}\delta_{itsp} \neq 0, \\ 0, \text{ если } \sum\limits_{t=1}^{v_i}\sum\limits_{s\in M_i^t}\sum\limits_{p=1}^{58}\delta_{itsp} = 0, \end{cases}$$

$$i = \overline{1,9},\ j = \overline{1,v_i}. \quad (2)$$

После чего для каждой подсистемы вычисляется доля общего числа связей всех её комплексов с объектами защиты в общем числе связей всех комплексов с объектами защиты по формуле:

$$N_i^3 = \begin{cases} \dfrac{\sum\limits_{t=1}^{v_i}\sum\limits_{s\in M_i^t}\sum\limits_{p=1}^{58}\delta_{itsp}}{\sum\limits_{s=1}^{9}\sum\limits_{j=1}^{v_s}\sum\limits_{k\in M_s^j}\sum\limits_{p=1}^{58}\delta_{sjkp}}, \text{ если } \sum\limits_{s=1}^{9}\sum\limits_{j=1}^{v_s}\sum\limits_{k\in M_s^j}\sum\limits_{p=1}^{58}\delta_{sjkp} \neq 0, \\ 0, \text{ если } \sum\limits_{s=1}^{9}\sum\limits_{j=1}^{v_s}\sum\limits_{k\in M_s^j}\sum\limits_{p=1}^{58}\delta_{sjkp} = 0, \end{cases}$$

$$i = \overline{1,9}. \quad (3)$$

Шаг 5. Вычисляется эффективность каждого уровня функциональности по формулам:

$$Э_{ij} = \sum_{k\in M_i^j} N_{ijk}^1 \cdot d_{ijk},\ i = \overline{1,9},\ j = \overline{1,v_i}, \quad (4)$$

где d_{ijk} — оценки аудиторов по шкале от 0 до 1. Оценка «1» означает, что k-й комплекс полностью задействован в обеспечении j-й функциональности i-й подсистемы и удовлетворяет требованиям регуляторов по ИБ. Оценка «0» означает, что k-й комплекс совсем не задействован в обеспечении j-й функциональности i-й подсистемы и не удовлетворяет требованиям регуляторов по ИБ. При этом отметим, что на оценку аудиторов могут влиять следующие факторы: уровень компетенции экспертов в области ИБ и результаты вычислений уязвимостей по интерактивному калькулятору, размещенному на сайте БДУ ФСТЭК (https://bdu.fstec.ru/calc31) .

Затем определяется эффективность каждого уровня подсистемы по формулам:

$$Э_i = \sum_{j=1}^{v_i} N_{ij}^2 \cdot Э_{ij},\ i = \overline{1,9}. \quad (5)$$

После чего проводится вычисление оценки общего уровня защищенности подсистемы ПТР КСЗИ по формуле:

$$Э = \sum_{i=1}^{9} N_i^3 \cdot Э_i. \quad (6)$$

Уровень защищённости предприятия по ИБ принимает значения от 0 до 1. Оценка «1» означает, что уровень защищенности ПТР КСЗИ обеспечивается в полном объёме, а «0» — что защищённость уровня ПТР КСЗИ полностью не обеспечивается.

Заключение

В заключение следует отметить, что хорошо спроектированная на предприятии система информационной безопасности на уровне ПТР может эффективно быть применена для подавления негативных последствий, связанных с утечкой конфиденциальной информации и риском кибер-атак. При этом важно постоянно оценивать, обновлять и своевременно модернизировать систему уровня ПТР КСЗИ, чтобы снизить время реагирования на возникающие угрозы.

Согласно предложенной методики по оценке уровня защищённости программно-технических решений КСЗИ (системы информационной безопасности) предприятия были разработаны следующие этапы:

- сформирован перечень из 58 объектов воздействия (базы данных, информационные системы, каналы связи, мобильные устройства и т.п.) с использованием данных сайта БДУ ФСТЭК;
- сформирован бинарный четырехмерный массив с элементами, отображающими связи между подсистемами, функциональными возможностями, объектами воздействия (защиты) и комплексами средств защиты информации;
- с учётом выбранных объектов воздействия предложены шаги для вычисления долей задействованных комплексов, как по функциональности, так и в разрезе подсистем;
- предложен подход к вычислению оценки эффективности каждого уровня функциональности и подсистемы с помощью аудиторских оценок по шкале от 0 до 1, учитывающих такие факторы, как уровень компетентности экспертов ИБ и результаты расчетов уязвимостей по калькуляторам представленным на сайте БДУ ФСТЭК;
- предложен подход к оценке общего уровня безопасности подсистемы ПТР КСЗИ в масштабе [0;1], который принимает значения от 0 до 1. Оценка «1» означает, что информационная безопасность по уровню ПТР КСЗИ достаточно полно обеспечена, а «0» –- нет.

К достоинствам предложенной методики можно отнести возможность автоматизированного проведения агрегированного анализа уровня ПТР КЗСИ с выделением наиболее критичных элементов в общей структуре системы.

В заключение, хотелось бы отметить, что представленная методика представляет практическую значимость для рассмотрения её концептуальных основ при адаптации к разным секторам экономики с целью минимизирования тех или иных угроз безопасности на объекты защиты (воздействия) и оценки средств борьбы с ними.

В рамках следующей работы предполагается описать программную реализацию оценки уровня защищённости ПТР КСЗИ с учётом: механизма аудиторских оценок, доли покрываемых угроз в разрезе свойств информации, формирования данных по «Объекты воздействия — Комплексы защиты» и «Угрозы — Комплексы защиты».

ЛИТЕРАТУРА

1. Zhang, L., Wang, Y., & Liu, W. (2016). A Framework for Knowledge Representation and Reasoning in Information Security Management. Journal of Computer Science and Technology, 31 (2), 195–204.
2. Zhang, L., Wang, Y., & Liu, W. (2017). Representing and Reasoning about Security Requirements for Service-Oriented Architecture. Journal of Computer Science and Technology, 32 (1), 97–104.
3. Sadeghi, A., & Scheller, R. (2016). Modeling and Reasoning about Security Threats and Countermeasures. International Journal of Information Security, 15 (2), 121–133.
4. Alotaibi, M., & Ali, M. (2017). Towards a Knowledge-Based Approach to Information Security Management. Journal of Network and Computer Applications, 100, 89–96.
5. Jain, R., & Joshi, A. (2018). A Semantic-Based Approach to Information Security Management. Journal of Information Security and Applications, 39, 33–39.
6. Jain, R., & Joshi, A. (2020). Formalizing Security Threats and Countermeasures in Service-Oriented Architecture. Journal of Information Security and Applications, 51, 101913.
7. Marques, C., & Guedes, A. (2018). Using ontologies for information security management. Journal of Information Security and Applications, 40, 87–93.
8. Li, Y., Zhang, X., & Liu, Y. (2019). Integrating Knowledge Representation and Reasoning Techniques in Information Security Management. Journal of Computer Science and Technology, 34 (2), 186–192.
9. Han, Y., Fan, X., & Zhang, L. (2020). A knowledge-based framework for security risk assessment in cloud computing environments. Journal of Network and Computer Applications, 157, 102429.
10. Li, X., Li, Y., & Liu, Y. (2021). Knowledge-based approach to threat intelligence in information security management. Journal of Computer Science and Technology, 36 (1), 25–30.
11. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Текст] / П.Н. Девянин. — М.: ГЛТ, 2013. — 338 с.
12. Зегжда Д.П. Основы безопасности информационных систем [Текст] / Д.П. Зегжда. — М.: Горячая линия — Телеком, 2000. — 452 с.
13. Зегжда, П.Д. Методология динамической защиты / П.Д. Зегжда, Д.П. Зегжда // Материалы международной научной конференции по проблемам безопасности и противодействия терроризму. Интеллектуальный центр МГУ. 2–3 ноября 2005 г. — М.: МЦНМО. — 2006. — 480 с., стр. 216–230.
14. Зегжда, П.Д. Системологический подход в информационных технологиях на примере проектирования средств получения и средств защиты информации: дис. … д-ра техн. наук: 05.13.19 / Зегжда Петр Дмитриевич. — СПб, 1996. — 304 с.
15. Клименко, И.С. Информационная безопасность и защита информации: модели и методы управления [Текст] / И.С. Клименко. — Москва: НИЦ ИНФРА-М, 2022–180 с.
16. Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч. / С.Е. Ададуров, А.П. Глухов, А.А. Корниенко; под ред. А.А. Корниенко. — М.: ФГБОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2014. — ч. 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте. — 440 с.
17. Советов Б.Я. Моделирование систем [Текст] / Б.Я. Советов. — М.: Высшая школа, 2009. — 343 с.
18. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации [Текст] / А.А. Малюк. — М.: ГЛТ, 2004. — 280 с.
19. Бабенко Л.К. Защита данных геоинформационных систем [Текст] / Л.К. Бабенко, А.С. Басан, И.Г. Журкин, О.Б. Макаревич. — М.: Гелиос АРВ, 2010. — 336 с.
20. Шумский А.А. Системный анализ в защите информации [Текст]: учебное пособие для вузов / А.А. Шумский, А.А. Шелупанов. — М.: Гелиос АРВ, 2005. — 220 с.
21. ГОСТ Р ИСО/МЭК 27002–2021 Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности. [Электронный ресурс] . — Режим доступа: https://gostassistent.ru/doc/b047942d-1331–48b3–89c7–4840ca3e43cc?ysclid=ldu24miv2s512505396. — Дата доступа: 07.02.2023.
22. ГОСТ Р ИСО/МЭК 27001–2021 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. [Электронный ресурс] . — Режим доступа: https://gostassistent.ru/doc/ec4dfe5d-a428–4404–8613–32edc5826be9. — Дата доступа: 07.02.2023.

23. ГОСТ Р 53114–2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. [Электронный ресурс] .— Режим доступа: https://gostassistent.ru/doc/30273211–2a73–49c6–9ca0–9a49f57be0c8.— Дата доступа: 07.02.2023.
24. ГОСТ Р ИСО/МЭК 18045–2013 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий. [Электронный ресурс] .— Режим доступа: https://gostassistent.ru/doc/41f28fd9–2d3d-4960–9c9d-a6333ba799ca.— Дата доступа: 07.02.2023.

Журнал «Современная наука: актуальные проблемы теории и практики»

г. Иркутск