БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2023. – № 4 (111). – 35–46

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.422 DOI: 10.17212/2782-2230-2023-4-35-46

АНАЛИЗ ПРОЦЕССА СОЗДАНИЯ БЕЗОПАСНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ*

Д.О. КУЛИКОВСКИЙ[1], Д.Н. ХАЛИНА[2]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, магистр кафедры вычислительной техники. E-mail: kulikovskij.2022@stud.nstu.ru*

[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, магистр кафедры вычислительной техники. E-mail: khalinadaria@gmail.com*

Статья представляет собой анализ ключевых этапов разработки безопасной информационной системы предприятия. Основное внимание уделяется освещению этапов определения целей информационной безопасности, оценке рисков, идентификации уязвимостей, а также процессу принятия обоснованных решений в контексте обеспечения безопасности информационной системы. Приводятся детальные рекомендации по созданию отчетов о выполненном анализе рисков и процессе принятия обоснованных решений на основе полученных результатов. В рамках работы также проведен анализ процессов составления матрицы вероятности наступления угроз, построения модели нарушителя и этапы построения модели угроз, обеспечивая понимание эффективных рекомендаций для оценки и управления рисками информационной безопасности предприятия и прогнозирования угроз. Также приведены определения всех применяемых терминов и примеры матрицы доступа, матрицы вероятности наступления угроз. Указаны составляющие моделей нарушителя и модели угроз. Отмечены наиболее распространенные ошибки процесса создания отчета об анализе рисков и его представления руководству. Представленный анализ служит важным ресурсом для специалистов по информационной безопасности и руководителей предприятий, которые заинтересованы в построении надежной и безопасной информационной системы.

Ключевые слова: информационная система, безопасность, модель угроз, модель злоумышленника, матрица доступа, матрица угроз, отчет анализа рисков, контроль доступа

* Статья получена 12 ноября 2023 г.

ВВЕДЕНИЕ

На данный момент каждая организация, использующая информационные технологии в целях автоматизации, сталкивается с проблемой обеспечения информационной безопасности. Угрозы как внешнего, так и внутреннего характера наносят многомиллионный ущерб предприятию и его бизнес-процессам [1].

Информационная безопасность – это действия, направленные на предотвращение злонамеренных действий мошенника по отношению к информации вне зависимости от формы воздействия или характера данных.

1. ОПРЕДЕЛЕНИЕ ЦЕЛЕЙ СОЗДАНИЯ БЕЗОПАСНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Цель построения безопасной информационной системы состоит в сохранении конфиденциальности, доступности и целостности информации. Однако стоимость системы не должна превышать стоимость информации или возможный ущерб от нарушений. Для определения мер, необходимых для вышеуказанных характеристик информации, используется анализ рисков.

2. АНАЛИЗ РИСКОВ

Анализ рисков – это совокупность процедур выявления факторов рисков и оценки их значимости, а также методов снижения вероятности последствий. Поскольку для разных типов информации используются разные методы защиты информации, необходимо четко определить модель злоумышленника. Первоначальная информация о модели злоумышленника запрашивается у руководства, которое имеет представление о ситуации на рынке и располагает сведениями о методах воздействия конкурентов. Наиболее часто используется неформальная модель злоумышленника, отражающая его мотивы или цели (кража информации с целью продажи, нарушение работоспособности сервиса с целью причинения убытков и т. п.) и основные способы их достижения (DDos-атака серверов предприятия, получение удаленного доступа к базам данных с персональной информацией). При моделировании используется теория игр, составляется матрица вероятностей наступления угроз [2]. Рассмотрим пример матрицы вероятностей угроз (табл. 1). В столбцах указан вред, наносимый угрозой в соответствии с ее вероятностью. Обозначим через «Поле **» ситуацию с последствиями, характерными для соответствующей вероятности угрозы.

Таблица 1

Table 1

Матрица вероятности наступления угроз

Threat matrix

Вероятность наступления угрозы	Возможные последствия наступления угрозы			
	Разрушение (Р)	Критические повреждения (К)	Тяжелые повреждения (Т)	Легкие повреждения (Л)
Высокая (В)	Поле ВР	Поле ВК	Поле ВТ	Поле ВЛ
Средняя (С)	Поле СР	Поле СК	Поле СТ	Поле СЛ
Низкая (Н)	Поле НР	Поле НК	Поле НТ	Поле НЛ

После определения основных причин нарушений на них оказывается воздействие или корректируется система защиты. Устранение мотивов или причин, повлекших нарушение, уменьшает вероятность возникновения подобных инцидентов [3]. Также для построения модели нарушителя (рис. 1) используется информация о прецедентах от службы безопасности, сведения о способах хранения и обработки информации, об относящихся к интеллектуальной собственности данных, о способах перехвата передач данных, о конкурентных предприятиях и настроениях в коллективе работников. Дополнительно оцениваются оперативные технические возможности воздействия на системы защищаемого объекта. Технические возможности, или оснащенность, – это средства, оборудование или знания, которыми может располагать злоумышленник. Они подразделяются на физический и логический доступ. Под физическим доступом подразумевается доступ к оборудованию, содержащему искомую злоумышленником информацию. В большинстве случаев физический доступ есть только у сотрудников компании. Логический доступ – это удаленный доступ, реализуемый с использованием вычислительных сетей, позволяющий без физического доступа осуществить доступ к защищаемой информации или выполнить операции по ее обработке [4].

Рис. 1. Модель нарушителя

Fig. 1. Fraudster model

Для проверки нарушения доступа или возможной манипуляции доступом составляется матрица доступа. Это позволяет заметить несанкционированный доступ сотрудников. Матрица доступа представляет собой матрицу, в которой субъекту системы соответствует строка, а объекту – столбец. В клетках матрицы стоят пометки о доступе субъекта к соответствующей системе. Обычно выделяют основные типы разрешенного доступа, такие как «доступ на запись», «доступ на чтение» или «доступ на исполнение». Доступ к объекту может меняться в определенные дни или часы в зависимости от других характеристик объекта или характера проводимых или проведенных работ [5]. В качестве примера матрицы доступа приведена матрица доступов компьютерных пользователей в некоторой сети (рис. 2). За «доступ на запись» отвечает символ «w», за «доступ на чтение» – символ «r» и за «доступ на исполнение» – символ «x». В данной матрице под объектами подразумеваются файлы, а под субъектами – пользователи локальной сети.

Далее в целях создания безопасной информационной системы необходимо построить модель угроз [6]. Важно выяснить связи между информационной инфраструктурой предприятия и информационными активами. Если на предприятии существует четкий регламент обслуживания и эксплуатации оборудования, то сбор информации о типах и вероятностях угроз будет значительно упрощен. Модель угроз состоит из модели нарушителя, информации о системе и базы данных угроз и уязвимостей. Под информацией о системе подразумевается ее программное и аппаратное обеспечение, связи между ее компонентами, задачи и защищаемые ресурсы. База данных содержит пере-

чень угроз информационной безопасности и перечень уязвимостей компонентов системы.

объекты / субъекты	file1	file2	dir1	file3	docA	docB	docC	docD	dir2	file4	pic1
adm	rwx	rwx	rwx	rwx	rwx	rwx	rwx	rwx	rwx	rwx	rwx
pgm1	---	---	---	r-x	---	---	---	---	rwx	rwx	---
pgm2	rwx	rwx	rwx	r-x	---	---	---	---	rwx	rwx	---
pgm3	rwx	rwx	rwx	---	---	---	---	---	---	---	---
op1	---	---	rwx	r-x	---	---	---	---	---	---	---
op2	---	---	rwx	r-x	---	---	---	---	---	---	---
op3	---	---	rwx	r-x	---	---	---	---	---	---	---
us1	--x	---	r--	---	rwx	rwx	---	r--	---	---	---
us2	---	---	r--	---	r--	r--	---	r--	---	---	---
us3	--x	---	r--	---	r--	r--	rwx	rwx	---	---	rwx

Рис. 2. Матрица доступа

Fig. 2. Access matrix

Построение модели угроз состоит из пяти последовательных шагов [7].

1. Определение источников угроз.
2. Выявление уязвимых объектов системы.
3. Определение перечня угроз для каждого объекта.
4. Выявление способов реализации угроз.
5. Оценка ущерба от угроз и их последствий.

После разработки модели угроз необходимо идентифицировать и оценить уязвимости для соответствующих активов. Этот процесс выполняется в рамках аудита. Необходимо разработать критерии оценивания на основании информации, представленной в модели угроз и модели злоумышленника.

3. ОЦЕНКА РИСКОВ

Поскольку ущерб оценивается на этапе построения модели угроз, необходимо провести оценку вероятностей событий рисков. Как и оценка активов, оценка вероятности рассчитывается при помощи сводной статистики по инцидентам, предпосылки к которым совпадают с текущими угрозами или ме-

тодом прогнозирования на основе взвешивания факторов, которые соответствуют модели угроз. Прогнозирование вероятности угроз проводится на основе характеристик уязвимостей и злоумышленников. Величину риска необходимо определить для каждого набора вида «актив – угроза», но не в каждом случае вероятность и ущерб могут быть выражены в формате денежного показателя или числа. В каждой компании существует политика управления рисками. Однако в то время как одна организация ставит превыше всего снижение рисков репутации, другая старается контролировать наиболее вероятные риски средней значимости. Если конкретные действия по обработке риска не определены, то производимые работы по снижению рисков должны основываться на максимальной эффективности применимых мер.

На основе полученных в ходе работ результатов разрабатывается простой и наглядный отчет об анализе рисков, целью которого является презентация данных о структуре и значимости рисков информационной безопасности. Этот отчет представляется высшему руководству для принятия решений [8]. Для достижения наглядности отчета схожие риски агрегируются и ранжируются по значимости, а их классификация должна выполняться в привычных бизнес-терминах.

Отчет анализа рисков содержит:

– информацию о наиболее уязвимых областях информационной безопасности;

– анализ влияния угроз на общую структуру рисков;

– наиболее приоритетные направления работы отдела безопасности.

4. АЛГОРИТМ ПРИНЯТИЯ РЕШЕНИЯ

На основе отчета руководство отдела безопасности формирует план работ на среднесрочный период и закладывает бюджет с учетом характера мероприятий по снижению рисков [10]. Так как требования и риски постоянно изменяются, систему безопасности следует не создавать с нуля, а каждый раз модифицировать и дополнять новыми системами защиты. Однако такой подход усложнит процесс проектирования и внедрения. Для функционирования некоторых систем потребуется более высокая пропускная способность оборудования, дополнительные вычислительные мощности и новые сотрудники, обеспечивающие мониторинг и обслуживание средств защиты. В рамках настоящей статьи невозможно рассмотреть конкретные механизмы защиты и их функционал, однако следует заметить, что защитить требуется всю информационную систему. Это влечет за собой повышенные требования к пропускной способности и предельной нагрузке оборудования. Наиболее распространен-

ная ошибка при создании отчета анализа рисков – это представление промежуточных итогов руководству. Отчет должен быть полным, однако в процессе его написания стоит фиксировать этапы готовности.

5. ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ

Процесс, описанный в настоящей работе, может быть применен на различных уровнях организации, в которой обеспечение информационной безопасности представляет существенное значение.

Применение этого процесса особенно критично для корпоративных предприятий, в которых информационные ресурсы представляют критическую ценность. В этом контексте процесс создания безопасной информационной системы обеспечивает защиту от утечки конфиденциальных данных и нежелательного доступа к корпоративным ресурсам.

Банки, инвестиционные фирмы и другие финансовые учреждения обрабатывают огромные объемы чувствительной информации. Применение данного процесса в этой области позволяет обеспечить безопасность финансовых транзакций, защитить персональные данные клиентов и предотвратить мошенничество.

Защита государственной тайны, информационной безопасности и обеспечение работоспособности критически важных систем – основные моменты, когда применение данного процесса обеспечивает надежную защиту.

Защита медицинской информации, включая конфиденциальные данные пациентов, требует особого внимания к информационной безопасности. Применение рассматриваемого процесса в медицинских учреждениях помогает обеспечить конфиденциальность данных и защиту от угроз нарушения безопасности.

В свете растущей ценности информации ИТ-компании и стартапы обращают всё большее внимание на обеспечение безопасности своих скоростных и инновационных продуктов. Применение данного процесса позволяет им обеспечить надежную защиту своих разработок и данных пользователей.

ЗАКЛЮЧЕНИЕ

Создание систем информационной безопасности предприятия – требующий значительных ресурсов и специализированных знаний и навыков процесс, который включает как проектирование и внедрение средств и систем защиты информации, так и их последующее сопровождение с использованием современных средств, таких как Security Operations Centers.

Анализ рисков, инцидентный менеджмент и аудит информационной безопасности взаимосвязаны, поскольку являются входными и выходными данными вышеуказанных процессов. Внедрение процесса управления рисками необходимо осуществлять с учетом управления инцидентами и аудитом информационной безопасности.

Необходимость проведения анализа рисков становится критической, если организация принимает решение пройти сертификацию по международному стандарту ISO/IEC 27001:2013. Аккредитация соответствующими агентствами проходит поэтапно: сначала изучение аудитором документации системы менеджмента, затем детальный аудит внедренных мер и их эффективности, далее инспекционный аудит соответствия требованиям [11]. Последний этап периодически повторяется в сертифицированных компаниях.

Установление режима защиты конфиденциальной информации и личных данных тесно связано с анализом рисков, поскольку все перечисленные процессы используют сходные методы идентификации и оценки активов, а также разработки моделей нарушителя и моделей угроз.

СПИСОК ЛИТЕРАТУРЫ

1. Создание систем информационной безопасности / Компания «Открытые технологии». – URL: https://www.ot.ru/services/creation-of-information-security/ (дата обращения: 04.12.2023).

2. Матрица вероятностей (рисков) и влияния управления проектов. – URL: https://habr.com/ru/articles/680524/ (дата обращения: 04.12.2023).

3. *Теренин А.* Модель типового злоумышленника и охрана информации. – URL: https://wiseeconomist.ru/poleznoe/57236-model-tipovogo-zloumyshlennika-oxrana-informacii (дата обращения: 04.12.2023).

4. ГОСТ Р 57580.1–2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. – М.: Стандартинформ, 2017. – 61 с.

5. *Ясенев В.Н.* Конспект лекций по информационной безопасности / Нижегородский государственный университет им. Н.И. Лобачевского. – Н. Новгород, 2017. – 253 с.

6. Пишем модель угроз // Блог компании «Информационный центр». – 2019, 25 июня. – URL: https://www.google.com/amp/s/habr.com/ru/amp/publications/457516/ (дата обращения: 04.12.2023).

7. *Дроботун Е.Б., Цветков О.В.* Построение модели угроз безопасности информации в автоматизированной системе управления критически важными объектами на основе сценариев действий нарушителя // Программные про-

дукты и системы. – 2016. – № 3. – С. 42–50. – DOI: 10.15827/0236-235X.115.042-050.

8. *Суханов А.* Анализ рисков в управлении информационной безопасностью // Байт. – 2008. – № 11. – С. 25–29.

9. *Емельянников М.* Информационные системы персональных данных // Журнал «Сіо». – 2008. – № 10. – С. 17–20.

10 *Селищев В.А., Чечуга О.В., Наседкин М.Н.* Построение системы информационной безопасности предприятия // Известия Тульского государственного университета. Технические науки. – 2009. – № 1-2. – С. 137–144.

11. *Бирюков Д., Токарева Е.* Международный стандарт ISO/IEC 27001:2013. Взгляд в будущее индустрии ИБ // Информационная безопасность. – 2013. – № 2. – С. 52–55. – URL: https://lib.itsec.ru/articles2/pravo/mezhdunarodnyy-standart-iso-iec-270012013.-vzglyad-v-buduschee-industrii-ib (дата обращения: 05.12.2023).

12. *Бирюков А.А.* Информационная безопасность: защита и нападение. – М.: ДМК Пресс, 2013. – 474 с.

13. AEGIS. White paper on research and innovation in cybersecurity. – AEGIS Consortium, 2018.

14. *Mani V.* Cybersecurity and fintech at a crossroads // ISACA Journal. – 2019. – Vol. 2. – P. 1–7.

15. *Dupont B.* The cyber-resilience of financial institutions: significance and applicability // Journal of Cybersecurity. – 2019. – Vol. 5 (1). – P. 1–17.

16. Current cyber-defense trends in industrial control systems / J.E. Rubio, C. Alcaraz, R. Roman, J. Lopez // Computer Security. – 2019. – Vol. 87. – P. 101561.

17. Analysis of intrusion detection systems in industrial ecosystems / J.E. Rubio, C. Alcaraz, R. Roman, J. Lopez // 14th International Conference on Security and Cryptography (SECRYPT 2017). – 2017. – Vol. 6. – P. 116–128.

18. How can organizations develop situation awareness for incident response: a case study of management practice / A. Ahmad, S.B. Maynard, K.C. Desouza, J. Kotsias, M.T. Whitty, R.L. Baskerville // Computer Security. – 2021. – Vol. 101. – P. 102122.

19. Solution-aware data flow diagrams for security threat modeling / L. Sion, K. Yskout, D. van Landuyt, W. Joosen // SAC ’18: Proceedings of the 33rd Annual ACM Symposium on Applied Computing. – ACM, 2018. – P. 1425–1432. – DOI: 10.1145/3167132.3167285.

20. Risk-based design security analysis / L. Sion, K. Yskout, D. van Landuyt, W. Joosen // SEAD ’18: Proceedings of the 1st International Workshop on Security Awareness from Design to Deployment. – ACM, 2018. – P. 11–18. – DOI: 10.1145/3194707.3194710.

Куликовский Дмитрий Олегович, студент магистратуры Новосибирского государственного технического университета. Основное направление научных исследований – информационная безопасность. E-mail: kulikovskij.2022@stud.nstu.ru

Халина Дарья Николаевна, студент магистратуры Новосибирского государственного технического университета. Основное направление научных исследований – информационная безопасность. E-mail: khalinadaria@gmail.com

DOI: 10.17212/2782-2230-2023-4-35-46

Analysis creation process of a secure enterprise information system*

D.O. Kulikovskij[1], D.N. Khalina[2]

[1] *Novosibirsk State Technical University, 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation, master's student of the Department of Computer Science. E-mail: kulikovskij.2022@stud.nstu.ru*

[2] *Novosibirsk State Technical University, 20 K. Marx Prospekt, Novosibirsk, 630073, Russian Federation, master's student of the Department of Computer Science. E-mail: khalinadaria@gmail.com*

The article is an analysis of the key stages of the development of a secure enterprise information system. The focus is on highlighting the stages of determining information security objectives, risk assessment, vulnerability identification, as well as the process of making informed decisions in the context of information system security. The article provides detailed recommendations for creating reports on the completed risk analysis and the process of making informed decisions based on the results obtained. As part of the work, the analysis of the processes of compiling a matrix of the probability of the occurrence of threats, building a model of the violator and the stages of building a threat model was also carried out, providing an understanding of effective recommendations for assessing and managing the risks of information security of the enterprise and forecasting threats. The definitions of all the terms used and examples of the access matrix, the threat probability matrix are also given. The components of the intruder models and threat models are indicated. The most common errors in the process of creating a risk analysis report and presenting it to management are noted. The presented analysis serves as an important resource for information security specialists and business managers who are interested in building a reliable and secure information system.

Keywords: information system, security, threat model, fraudster model, access matrix, threat matrix, risk analysis report, access control

* *Received 12 November 2023.*

REFERENCES

1. Open Technologies. *Sozdanie sistem informatsionnoi bezopasnosti* [Creation of information security systems]. Available at: https://www.ot.ru/services/creation-of-information-security/ (accessed 04.12.2023).

2. *Matritsa veroyatnostei (riskov) i vliyaniya upravleniya proektov* [Matrix of probabilities (risks) and impact of project management] Available at: https://habr.com/ru/articles/680524/ (accessed 04.12.2023).

3. Terenin A. *Model' tipovogo zloumyshlennika i okhrana informatsii* [The model of a typical attacker and information security]. Available at: https://wiseeconomist.ru/poleznoe/57236-model-tipovogo-zloumyshlennika-oxrana-informacii (accessed 04.12.2023).

4. GOST R 57580.1–2017. *Bezopasnost' finansovykh (bankovskikh) operatsii. Zashchita informatsii finansovykh organizatsii. Bazovyi sostav organizatsionnykh i tekhnicheskikh mer* [State Standard R 57580.1–2017. Security of financial (banking) operations. Information protection of financial organizations. Basic set of organizational and technical measures]. Moscow, Standartinform Publ., 2017. 61 p.

5. Yasenev V.N. *Konspekt lektsii po informatsionnoi bezopasnosti* [Lecture notes on information security]. National Research Lobachevsky State University of Nizhni Novgorod, 2017. 253 p.

6. Information Center LLC. *Pishem model' ugroz* [Writing a threat model]. Available at: https://www.google.com/amp/s/habr.com/ru/amp/publications/457516/ (accessed 04.12.2023).

7. Drobotun E.B., Tsvetkov O.V. Postroenie modeli ugroz bezopasnosti informatsii v avtomatizirovannoi sisteme upravleniya kriticheski vazhnymi ob"ektami na osnove stsenariev deistvii narushitelya [Modeling information security threats in the automated control system for crucial objects on the basis of attack scenarios]. *Programmnye produkty i sistemy = Software and Systems*, 2016, no. 3, pp. 42–50. DOI: 10.15827/0236-235X.115.042-050.

8. Sukhanov A. Analiz riskov v upravlenii informatsionnoi bezopasnost'yu [Risk analysis in information security management]. *Bait*, 2008, no. 11, pp. 25–29. (In Russian).

9. Emel'yannikov M. Informatsionnye sistemy personal'nykh dannykh [Information systems of personal data]. *Zhurnal «Cio»*, 2008, no. 10, pp. 17–20. (In Russian).

10. Selischev V.A., Chechuga O.V., Nasedkin M.N. Postroenie sistemy informatsionnoi bezopasnosti predpriyatiya [Building of the system information safety of the enterprise]. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki = News of the Tula state university. Technical sciences*, 2009, no. 1-2, pp. 137–144.

11. Biryukov D., Tokareva E. Mezhdunarodnyi standart ISO/IEC 27001:2013. Vzglyad v budushchee industrii IB [International standard ISO/IEC 27001:2013. A look into the future of information security industry]. *Informatsionnaya bezopasnost' = Information Security*, 2013, no. 2, pp. 52–55. (In Russian). Available at: https://lib.itsec.ru/articles2/pravo/mezhdunarodnyy-standart-iso-iec-270012013.-vzglyad-v-buduschee-industrii-ib (accessed 05.12.2023).

12. Biryukov A.A. *Informatsionnaya bezopasnost': zashchita i napadenie* [Information security: protection and attack]. Moscow, DMK Press, 2013. 474 p.

13. AEGIS. *White paper on research and innovation in cybersecurity*. AEGIS Consortium, 2018.

14. Mani V. Cybersecurity and fintech at a crossroads. *ISACA Journal*, 2019, vol. 2, pp. 1–7.

15. Dupont B. The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity*, 2019, vol. 5 (1), pp. 1–17.

16. Rubio J.E., Alcaraz C., Roman R., Lopez J. Current cyber-defense trends in industrial control systems. *Computer Security*, 2019, vol. 87, p. 101561.

17. Rubio J.E., Alcaraz C., Roman R., Lopez J. Analysis of intrusion detection systems in industrial ecosystems. *14th International Conference on Security and Cryptography (SECRYPT 2017)*, 2017, vol. 6, pp. 116–128.

18. Ahmad A., Maynard S.B., Desouza K.C., Kotsias J., Whitty M.T., Baskerville R.L. How can organizations develop situation awareness for incident response: a case study of management practice. *Computer Security*, 2021, vol. 101, p. 102122.

19. Sion L., Yskout K., Landuyt D. van, Joosen W. Solution-aware data flow diagrams for security threat modeling. *SAC '18: Proceedings of the 33rd Annual ACM Symposium on Applied Computing*. ACM, 2018, pp. 1425–1432. DOI: 10.1145/3167132.3167285.

20. Sion L., Yskout K., Landuyt D. van, Joosen W. Risk-based design security analysis. *SEAD '18: Proceedings of the 1st International Workshop on Security Awareness from Design to Deployment*. ACM, 2018, pp. 11–18. DOI: 10.1145/3194707.3194710.

Для цитирования:

Куликовский Д.О., Халина Д.Н. Анализ процесса создания безопасной информационной системы предприятия // Безопасность цифровых технологий. – 2023. – № 4 (111). – С. 35–46. – DOI: 10.17212/2782-2230-2023-4-35-46.

For citation:

Kulikovskij D.O., Khalina D.N. Analiz protsessa sozdaniya bezopasnoi informatsionnoi sistemy predpriyatiya [Analysis creation process of a secure enterprise information system]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2023, no. 4 (111), pp. 35–46. DOI: 10.17212/2782-2230-2023-4-35-46.