Научная статья
УДК 004.624
DOI: 10.17072/1993-0550-2022-4-54-60

Разработка специальной классификации информационных активов в сфере информационной безопасности

А. В. Манжосов[1], **И. П. Болодурина**[1], **В. С. Сабуров**[1], **Н. А. Долгушев**[1]
[1]Оренбургский государственный университет, Оренбург, Россия

Автор, ответственный за переписку: Артём Владимирович Манжосов, a.v.manzhosov@gmail.com

Аннотация. Проведен анализ определений понятия "информационный актив", который показал разностороннюю направленность информационных активов в сфере информационной безопасности. Выполнен обзор источников по теме исследования, в результате которого определено, что тема исследования является обсуждаемой, актуальной в российской и международной повестке. Проведено сравнение классификаций информационных активов в нормативно-правовых актах, которое позволило определить рекомендуемый базовый перечень информационных активов. Разработана специальная классификация информационных активов, которая систематизирует классы информационных активов по критерию возможности воздействия рисков информационной безопасности на информационный актив.

Ключевые слова: *специальная классификация; информационный актив; информационная безопасность*

Для цитирования: *Манжосов А. В., Болодурина И. П., Сабуров В. С., Долгушев Н. А.* Разработка специальной классификации информационных активов в сфере информационной безопасности // Вестник Пермского университета. Математика. Механика. Информатика. 2022. Вып. 4(59). С. 54–60. DOI: 10.17072/1993-0550-2022-4-54-60.

Благодарности: исследование выполнено при финансовой поддержке РНФ в рамках научного проекта №22-71-10124 "Разработка комплексной системы оценки устойчивости моделей машинного обучения по отношению к состязательным атакам".

Статья поступила в редакцию 21.10.2022; одобрена после рецензирования 11.11.2022; принята к публикации 14.11.2022.

Research article

Development of a Special Classification of Information Assets in the Information Security Field

A. V. Manzhosov[1], I. P. Bolodurina[1], V. S. Saburov[1], N. A. Dolgushev[1]
[1]Orenburg State University, Orenburg, Russia

Corresponding author: Artyom V. Manzhosov, a.v.manzhosov@gmail.com

Abstract. The analysis of definitions of the concept of "information asset" was carried out, which showed the versatility of information assets in the information security field. A review of sources on the topic of research was performed, which determined that the topic of research is discussed and relevant to the Russian and international agendas. Classification of information assets in legal acts was compared, which made it possible to determine the recommended basic list of information assets. A special classification of information assets was developed, which systematizes classes of information assets by the criterion of possibility of information security risks impact on the information asset.

Keywords: *special classification; information asset; Information Security*

For citation: *Manzhosov A. V., Bolodurina I. P., Saburov V. S., Dolgushev N. A*. Development of a Special Classification of Information Assets in the Information Security Field // Bulletin of Perm University. Mathematics. Mechanics. Computer Science. 2022;4(59):54-60. (In Russ.). DOI: 10.17072/1993-0550-2022-4-54-60.

Acknowledgments: the study was supported by the Russian Science Foundation, project № 22-71-10124 "Development of a comprehensive system for evaluating the stability of machine learning models against adversarial attacks".

The article was submitted 21.10.2022; approved after reviewing 11.11.2022; accepted for publication 14.11.2022.

Введение

Ключевым составным элементом любого риска является актив. Наличие рисков информационной безопасности (далее – ИБ) как раз и обусловлено наличием информационных активов (далее – ИА). Значительную часть капитализации всей организации составляет информация, циркулирующая в ее информационных системах. К ИА относится практически любая информация, которая представляет ценность для предприятия. К ним можно отнести и имущество предприятия, его финансы, кадры, технологии и инновации, информационную систему предприятия, а также его организационную структуру. Под активами (ресурсами) понимаются не только материальные объекты, но и сервисы, функционирование которых критично для процессов, а также данные, используемые в процессе операционной деятельности.

Цель идентификации активов – определение перечня активов, в отношении которых требуется управление рисками, а также перечня связанных с активами бизнес-процессов.

1. Обзор определений понятия "информационный актив"

В настоящее время определение понятия "информационный актив" представлено в разных источниках.

Информационный актив – информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для организации банковской системы Российской Федерации; находящаяся в распоряжении организации банковской системы Российской Федерации и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме [1].

Информационный актив – информационные ресурсы или средства обработки информации организации [2]. Информационный актив – знания или данные, которые имеют значение для организации [3].

Информационные ресурсы – документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, депозитариях, музейных хранилищах и т.п. [4].

Защищаемые ресурсы (информационной системы) – ресурсы, использующиеся в информационной системе при обработке защищаемой информации с требуемым уровнем ее защищенности [5].

Защищаемые информационные ресурсы (автоматизированной информационной системы) – информационные ресурсы автоматизированной информационной системы, для которых должен быть обеспечен требуемый уровень их защищенности [3].

Информационный актив – это поддающийся измерению результат деятельности компании за определенный период времени [6].

Информационный актив – это информация, находящаяся в распоряжении организации и имеющая ценность для нее, в независимости от вида ее представления [7].

Для каждой организации чаще всего ценными являются свои индивидуальные ИА. Определить их можно, ответив на вопрос: "Потеря или нанесение ущерба каким ИА или информационным ресурсам причинит вред всей организации"?

2. Обзор источников

Статья [8] содержит исследования, касающиеся классификации ИА и предлагает собственную систему классификации, учитывающую особенности небольших IT организаций и бизнес-процессов. В частности, авторы дифференцируют ИА с помощью метода качественного наблюдения и статистического метода. Статья "A Study on Classification of Information Asset Considering Business Process Characteristics for Small IT Service Organization" предлагает исключительно теоретическое описание классификации ИА, без конкретной модели построения классификации, статья не связана с законодательством РФ, а также не предо-

ставляет механизм получения итогового перечня ИА.

В статье "Information Asset Classification and Labelling Model Using Fuzzy Approach for Effective Security Risk Assessment" [9] авторы анализируют эффективность моделей классификации ИА по соответствующим уровням риска безопасности, требуемому уровню защиты и приоритету. В исследовании предложена структура классификации и маркировки ИА на основе нечеткой оценки безопасности и классификации ИА (FIACL) и их экспертной оценки, базирующаяся на стандарте безопасности ISO/IEC 27001.

Публикация автора [10] посвящена динамической когнитивной модели оценки уровня безопасности ИА, также основанной на нечетком методе оценки. Статья посвящена повышению уровня ИБ высших учебных заведений по законодательству РФ.

В статье "Идентификация активов как ключевых факторов риска информационной безопасности" [11] представлен сравнительный анализ классификаций активов по международным и российским стандартам ИБ. Автор также предлагает пример реестра ИА на примере отдельной организации. Статья содержит примеры классифицированных активов.

Автор статьи "Совершенствование системы обеспечения информационной безопасности финансовой организации с применением процессов моделирования, классификации информационных активов и учетных записей" [12] рассматривает процессы моделирования и классификации ИА банковского сектора, а также приводит базовые классификации активов и учетных записей подконтрольного объекта с целью выявления возможных путей совершенствования системы обеспечения ИБ. Статья предлагает анализ законодательства банковского сектора и механизм определения актуальных угроз ИБ.

Зарегистрированный модуль ePlat4m [13] "Управление категорированием объектов КИИ (УКИИ)" разработан с целью автоматизации процессов сбора, учета и обработки результатов инвентаризации информационных ресурсов (программных и аппаратных компонентов) АСУ ТП.

Проведенный анализ литературы показал, что тема исследования является обсуждаемой, актуальной в российской и международной повестке. Уровень проработанности темы остается низким, требует проведения исследований и общественной дискуссии на форумах и конференциях.

3. Сопоставительный анализ существующих классификаций информационных активов нормативно-правовых актов

Стандарт BS 7799-3 описывает ресурсы как "то, что имеет ценность или находит полезное применение для организации, ее деловых операций и их непрерывности" [14]. Информацию и другие ресурсы стандарт рекомендует классифицировать в соответствии с идентифицированной стоимостью ресурсов, законодательными и бизнес-требованиями, и уровнем критичности, а реестры этих ресурсов должны быть собраны вместе и поддерживаться в актуальном состоянии. Допускается объединение похожих или связанных ресурсов в управляемые наборы, чтобы сократить усилия, затрачиваемые на процесс.

Определение классификации, а также ее пересмотр с целью предоставления гарантий того, что классификация остается на соответствующем уровне, входит в обязанности владельца ресурса. Информация должна быть защищена, независимо от того, какую форму она принимает, например, базы данных или файлы данных, документация компании или системная документации, контракты, руководства пользователя, учебный материал, операционные процедуры и процедуры поддержки, инструкции, документы, содержащие важные бизнес-результаты, планы обеспечения непрерывности или соглашения о переходе на аварийный режим.

Для каждого из идентифицированных ресурсов или группы ресурсов должен быть определен их владелец, и ответственность за сопровождение соответствующих механизмов безопасности должна быть возложена на этого владельца. Обязанности по внедрению механизмов безопасности могут быть делегированы, однако ответственность должна оставаться за назначенным владельцем ресурса.

Стандарт ISO/IEC 27005 понимает под ИА нечто, имеющее ценность для организации и, следовательно, нуждающееся в защите [15]. Стандарт также отмечает, что под влиянием угрозы может оказаться не только один, но и большее количество активов, а также только отдельная часть актива.

В связи с этим, ценность активов может быть определена в зависимости от их финансовой стоимости и масштабов последствий для бизнеса в случае их порчи или компрометации. Так же, как и BS 7799-3, стандарт ISO/IEC 27005 допускает группировку активов или их разбиение на элементы и связывание сценариев с элементами. Основными активами обычно являются базовые процессы и информация о деятельности организации в границах процесса менеджмента риска. Могут рассматриваться также и другие основные активы, такие как процессы жизнедеятельности организации, которые будут иметь отношение к формированию политики ИБ или плана непрерывности бизнеса. Процессы и информация, которые не были идентифицированы как чувствительные относительно данной деятельности, не будут иметь определенной классификации в оставшейся части исследования. Это означает, что, если даже такие процессы или информация будут скомпрометированы, организация по-прежнему будет успешно осуществлять свою деятельность. Тем не менее, они часто будут наследовать средства управления, реализуемые для защиты процессов и информации, идентифицированных как чувствительные.

Методический документ ФСТЭК России от 5 февраля 2021 года "Методика оценки угроз безопасности информации» определяет информационный ресурс как «информацию, данные, представленные в форме, предназначенной для хранения и обработки в системах и сетях" [16].

Документ предписывает определять ценность активов с помощью их классификации, в соответствии с их критичностью и их важности для осуществления бизнес-целей организации. Ценность определяется с использованием двух мер: восстановительной стоимости актива (стоимости очистки с целью восстановления и замены информации) и последствий для бизнеса от потери или компрометации актива (например, возможные неблагоприятные деловые и/или законодательные или регулирующие последствия раскрытия, модификации, недоступности и/или разрушения информации и других ИА).

В таблице представлен сопоставительный анализ существующих классификаций ИА нормативно-правовых актов.

Сопоставительный анализ существующих классификаций ИА нормативно-правовых актов

	Стандарт ISO/IEC 27005	**Стандарт BS 7799-3**		**Методика оценки угроз безопасности информации**
Типы ИА	бизнес-процессы	первичные активы	информация	информация, содержащаяся в системах и сетях
	действия		бизнес-процессы	программно-аппаратные средства обработки и хранения информации
	информация	активы поддержки	сервисы	программные средства
	аппаратные средства		программное обеспечение	машинные носители информации
	программное обеспечение		физические объекты, используемые для поддержки обработки информации	телекоммуникационное оборудование
	сеть		люди, участвующие в процессах хранения или обработки информации	средства защиты информации
	персонал			пользователи систем и сетей
	организационная структура			обеспечивающие системы

Опираясь на Методический документ ФСТЭК России от 5 февраля 2021 года "Методика оценки угроз безопасности информации", можно получить перечень ИА.

Такой список носит общий характер, и для более эффективного формирования перечня ИА необходимо составить классификацию на основе вышеупомянутого методического документа.

4. Специальная классификация информационных активов

Идентификацию ИА с целью управления рисками ИБ, необходимо проводить с той степенью точности детализации, которая обеспечила бы получение достаточной информации для оценки критичности риска. Классификацию ИА следует начинать "сверху вниз", а не наоборот, как это делает в последнее время большое количество ИТ-специалистов, формируя таким образом списки различных ни к чему не привязанных активов.

Критерий разработки специальной классификации: ИА считается такой актив, на который распространяются риски ИБ.

Первый ярус классификационного иерархического древа преимущественно основан на методическом документе ФСТЭК России от 5 февраля 2021 года "Методика оценки угроз безопасности информации".

На рис. 1 представлена базовая версия специальной классификации ИА в сфере ИБ.

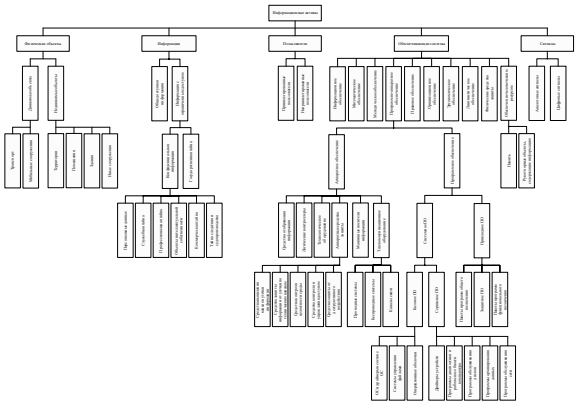

Рис. 1. *Базовая версия специальной классификации ИА в сфере ИБ*

Разработанная специальная классификация позволит упростить процесс идентификации ИА на предприятии за счет систематизации и структурирования ИА.

Полная специальная классификация ИА в сфере ИБ в исходном размере доступна к скачиванию по ссылке https://nextcloud.ussc.ru/index.php/s/YfS5tMiR6mTzfoX или QR-коду, представленному на рис. 2.

Рис. 2. *Ссылка для скачивания специальной классификации информационных активов в сфере информационной безопасности*

Заключение

При разработке специальной классификации ИА в сфере ИБ поэтапно были выполнены нескольких аналитических задач.

Проведен анализ определений понятия "информационный актив", который показал разностороннюю направленность ИА в сфере ИБ.

Проведен обзор источников по теме исследования, в результате которого определено, что тема исследования является обсуждаемой, актуальной в российской и международной повестке.

Выполнен сопоставительный анализ классификаций ИА нормативно-правовых актов. Определен рекомендуемый базовый перечень ИА, на который можно опираться при разработке классификации информационных активов и управлением рисками ИБ.

Разработанная специальная классификация ИА, которая предлагает систематизацию классов ИА по критерию распространения рисков ИБ на классифицированный тип ИА.

Список источников

1. *Стандарт* Банка России СТО БР ИББС-1.0-2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. Взамен СТО БР ИББС-1.0-2010. М.: Изд-во стандартов, 2014. 101 с.
2. *ГОСТ* Р ИСО/ТО 13569-2007. Финансовые услуги. Рекомендации по информационной безопасности. М.: Изд-во стандартов, 2008. 16 с.
3. *ГОСТ* Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации. М.: Изд-во стандартов, 2005. 11 с.
4. *Федеральный* закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 № 149-ФЗ (последняя редакция). Ст. 2.
5. *ГОСТ* Р 50.1.056-2005. Техническая защита информации. Основные термины и определения. М.: Изд-во стандартов, 2005. 15 с.
6. *Топсахалова Ф. М-Г.* Англо-русский толковый словарь бухгалтерских и финансовых терминов. М., 2012. 122 с.
7. *Ясенев В.Н.* Конспект лекций по информационной безопасности: учеб.-метод. пособие; Федер. агентство по образованию. Нижний Новгород: изд-во ННГУ им. Н.И. Лобачевского, 2017. 235 с.

8. *Kang J.* A Study on Classification of Information Asset Considering Business Process Characteristics for Small IT Service Organization / J. Kang; L. Lim // The Journal of Society for e-Business Studies. 2011. № 16. P. 97–108.
9. *Alonge C.* Information Asset Classification and Labelling Model Using Fuzzy Approach for Effective Security Risk Assessment / O. Arogundade, C. Alonge // International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS). 2020. № 3. P. 71–90.
10. *Ажмухамедов И.М.* Динамическая нечеткая когнитивная модель оценки уровня безопасности информационных активов вуза // Вестник АГТУ. Сер.: Управление, вычислительная техника и информатика. 2012. № 2. С. 137–142.
11. *Собакин И.Б.* Идентификация активов как ключевых факторов риска информационной безопасности // Вопросы защиты информации. 2011. № 2 (93). С. 45–49.
12. *Зайцев А.С.* Совершенствование системы обеспечения информационной безопасности финансовой организации с применением процессов моделирования, классификации информационных активов и учетных записей // Безопасность информационных технологий. 2013. № 4. С. 39–45.
13. *Кудряшова К.А.* Общество с ограниченной ответственностью "Уральский центр систем безопасности". Модуль ePlat4m "Управление категорированием объектов КИИ (УКИИ) ". Патент № 2021611572 РФ; Заявл. 2021610202 08.01.2021; Опубл. 01.02.2021, Бюл. № 2.
14. *Британский* стандарт BS 7799-3. Системы управления информационной безопасностью. BSI, 2006. 70 с.
15. *ГОСТ* Р ИСО/МЭК 27000-2012. Информационная технология. Методы и средства обеспечения безопасности. М.: Изд-во стандартов, 2012. 69 с.
16. *Методический* документ ФСТЭК России от 5 февраля 2021 года. Методика оценки угроз безопасности информации. М.: Изд-во стандартов, 2021. 83 с.

References

1. *Standart* Banka Rossii STO BR IBBS-1.0-2014. Obespechenie informacionnoj bezopasnosti organizacij bankovskoj sistemy Rossijskoj Federacii. Obshchie polozheniya. Vzamen STO BR IBBS-1.0-2010. M.: Izd-vo standartov; 2014. 101 p. (In Russ.).
2. *GOST R* ISO/TO 13569-2007. Finansovye uslugi. Rekomendacii po informacionnoj bezopasnosti. M.: Izd-vo standartov; 2008. 16 p. (In Russ.).
3. *GOST R* 50.1.053-2005. Informacionnye tekhnologii. Osnovnye terminy i opredeleniya v oblasti tekhnicheskoj zashchity informacii. M.: Izd-vo standartov; 2005. 11 p. (In Russ.).
4. *Federal'nyj* zakon "Ob informacii, informacionnyh tekhnologiyah i o zashchite informacii" ot 27.07.2006 № 149-FZ (poslednyaya redakciya). St. 2. (In Russ.).
5. *GOST R* 50.1.056-2005. Tekhnicheskaya zashchita informacii. Osnovnye terminy i opredeleniya. M.: Izd-vo standartov; 2005. 15 p. (In Russ.).
6. *Topsahalova F. M-G.* Anglo-russkij tolkovyj slovar' buhgalterskih i finansovyh terminov. M., 2012. 122 p. (In Russ.).
7. *Yasenev V.N.* Konspekt lekcij po informacionnoj bezopasnosti: ucheb.-metod. posobie; Feder. agentstvo po obrazovaniyu. Nizhnij Novgorod, izd-vo NNGU im. N.I. Lobachevskogo; 2017. 235 p. (In Russ.).
8. *J. Kang, L. Lim.* A Study on Classification of Information Asset Considering Business Process Characteristics for Small IT Service Organization. The Journal of Society for e-Business Studies. 2011;(16):97–108.
9. *Arogundade O., Alonge C.* Information Asset Classification and Labelling Model Using Fuzzy Approach for Effective Security Risk Assessment. International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS). 2020;(3):71–90.
10. *Azhmuhamedov I.M.* Dinamicheskaya nechetkaya kognitivnaya model' ocenki urovnya bezopasnosti informacionnyh aktivov vuza // Vestnik AGTU. Ser.: Upravlenie, vychislitel'naya tekhnika i informatika. 2012;(2):137–142. (In Russ.).
11. *Sobakin I.B.* Identifikaciya aktivov kak klyuchevyh faktorov riska informacionnoj bezopasnosti // Voprosy zashchity informacii. 2011;(2 (93)):45–49. (In Russ.).
12. *Zajcev A.S.* Sovershenstvovanie sistemy obespecheniya informacionnoj bezopasnosti finansovoj organizacii s primeneniem processov modelirovaniya, klassifikacii informacionnyh aktivov i uchetnyh zapisej // Bezopasnost' informacionnyh tekhnologij. 2013;(4):39–45. (In Russ.).

13. *Kudryashova K.A.* Obshchestvo s ogranichennoj otvetstvennost'yu "Ural'skij centr sistem bezopasnosti". Modul' ePlat4m "Upravlenie kategorirovaniem ob'ektov KII (UKII)". Patent № 2021611572 RF; Zayavl. 2021610202 08.01.2021; Opubl. 01.02.2021, Byul. № 2. (In Russ.).
14. *Britanskij* standart BS 7799-3. Sistemy upravleniya informacionnoj bezopasnost'yu. BSI; 2006. 70 p. (In Russ.).
15. *GOST R* ISO/MEK 27000-2012. Informacionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. M.: Izd-vo standartov; 2012. 69 p. (In Russ.).
16. *Metodicheskij* dokument FSTEK Rossii ot 5 fevralya 2021 goda. Metodika ocenki ugroz bezopasnosti informacii. M.: Izd-vo standartov; 2021. 83 p. (In Russ.).

Информация об авторах:

Артём Владимирович Манжосов – научный сотрудник научно-исследовательского института цифровых интеллектуальных технологий Оренбургского государственного университета (460018, Россия, Оренбургская область, г. Оренбург, просп. Победы, д. 13), a.v.manzhoosv@gmail.com;

Ирина Павловна Болодурина – доктор технических наук, профессор, заведующий кафедрой прикладной математики Оренбургского государственного университета (460018, Россия, Оренбургская область, г. Оренбург, просп. Победы, д. 13), ipbolodurina@yandex.ru, https://orcid.org/0000-0003-0096-2587, AuthorID 118837;

Никита Александрович Долгушев – студент факультета математики и информационных технологий Оренбургского государственного университета (460018, Россия, Оренбургская область, г. Оренбург, просп. Победы, д. 13), ndolgushev@ussc.ru;

Вадим Сергеевич Сабуров – студент факультета математики и информационных технологий Оренбургского государственного университета (460018, Россия, Оренбургская область, г. Оренбург, просп. Победы, д. 13), byzantineglory1025@gmail.com.

Information about the authors:

Artyom V. Manzhosov – Researcher of the Research Institute of Digital Intelligent Technologies of Orenburg State University (13, Pobedy ave., Orenburg, Orenburg region, Russia, 460018), a.v.manzhoosv@gmail.com;

Irina P. Bolodurina – Doctor of Technical Sciences, Professor, Head of Applied Mathematics Department, Orenburg State University (13, Pobedy ave., Orenburg, Orenburg region, Russia, 460018), ipbolodurina@yandex.ru, https://orcid.org/0000-0003-0096-2587, AuthorID 118837;

Nikita A. Dolgushev – Student of the Faculty of Mathematics and Information Technology, Orenburg State University (13, Pobedy ave., Orenburg, Orenburg region, Russia, 460018), ndolgushev@ussc.ru;

Vadim S. Saburov – Student of the Department of Mathematics and Information Technology of Orenburg State University (13, Pobedy ave., Orenburg, Orenburg region, Russia, 460018), byzantineglory1025@gmail.com.