Для цитирования
Трофимов В.В., Трофимов С.В. Онтологические аспекты безопасности информационных технологий / III Научно-практическая конференция «Стандартизация: траектория науки», приуроченная ко Всемирному дню стандартов, Москва, 15 октября 2025 г. // Информационно-экономические аспекты стандартизации и технического регулирования. 2025. № 6(87). С. 599–605.

УДК 004.9

ОНТОЛОГИЧЕСКИЕ АСПЕКТЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Трофимов В.В., *аспирант, ФГБУ «Институт стандартизации», Россия, г. Москва,*
Трофимов С.В.*, канд. экон. наук, ФГБУ «Российский институт стандартизации», Россия, г. Москва*

Целью исследования является определение потенциальной связи между нормативно-техническими и методическими документами и существующими подходами к классификации объектов (сущностей, логических единиц, таксономических и онтологических элементов) и структурированию предметной области в сфере безопасности информационных технологий. На основе проведенного анализа описания объектов и их взаимосвязей применительно к сфере информационной безопасности и защиты информации представлены возможные классификации (выделения сущностей и их группировка по классам) в привязке к источникам данных.

Ключевые слова: онтология, графы, таксономия, классификация, информационная безопасность, угрозы, уязвимости, активы, база данных и знаний.

ONTOLOGICAL ASPECTS OF INFORMATION TECHNOLOGY SECURITY

Trofimov V.V., *graduate student, Russian Standardization Institute, Moscow*
Trofimov S.V., *Cand. Sci. (Econ.), Russian Standardization Institute, Moscow*

The purpose of the study is to determine the potential relationship between regulatory, technical and methodological documents and existing approaches to the classification of objects (entities, logical units, taxonomic and ontological elements) and the structuring of the subject area in the field of information technology security. based on the analysis of the description of objects and their interrelationships in relation to the field of information security and information protection, possible classifications (separation of entities and their grouping by classes) are presented in relation to data sources.

Keywords: ontology, graphs, taxonomy, classification, information security, threats, vulnerabilities, assets, database and knowledge.

Вопросы онтологического описания объектов и их взаимосвязей являются важным инструментом для структурирования знаний в различных предметных областях, включая вопросы безопасности использования информационно-коммуникационных технологий (ИКТ). Онтологии позволяют формализовать понятия, их свойства и отношения, что способствует более эффективному анализу, моделированию и управлению сложными системами. В контексте информационной безопасности (ИБ) онтологии используются для описания угроз, уязвимостей, активов, контрмер и их взаимосвязей, что помогает в проектировании и создании комплексных систем защиты информации, в анализе рисков и в поддержке принятия решений по обеспечению ИБ.

Онтологический аспект любого исследования позволяет сформировать структурное представление описания определенной реальности (предметной области) за счет системы

понятий, связанных с помощью логических отношений «общее – единичное». Словарь понятий строится на терминологии нормативно-методических документов и стандартов в области информационных технологий и кибербезопасности. Онтологические модели позволяют на основе информации о взаимосвязях сущностей выявить возможные пути доступа к информационным активам, чтобы на этапах проектирования, например, программных продуктов нейтрализовать возможные уязвимости [1].

Эксперты по кибербезопасности прогнозируют увеличение числа кибератак на российскую инфраструктуру, что делает задачу обнаружения сетевых вторжений серьезной исследовательской задачей [2].

Безопасность ИКТ строится на основе обеспечения конфиденциальности и безопасности данных, реализуя возможности программного и аппаратного обеспечения, стратегии управления данными [3].

Возрастающая потребность в обработке неструктурированной текстовой информации, в повышении качества и эффективности методов обработки текстовых документов, в разработке систем поиска информации, в организации рубрикации и кластеризации документов, автоматического аннотирования документов во многом может быть разрешена благодаря структурной организации баз данных и знаний (БДЗ) на основе онтологического подхода [4].

В целом безопасность связана с вопросом защиты активов организации от угроз. При этом угрозы рассматриваются как потенциальные возможности для неправомерного использования активов. Защита и поддержание целостности активов организации особенно важны для знаний, уникальных и критически важных навыков и ресурсов, которыми владеет организация [5]. В условиях роста информационной сложности и междисциплинарных исследований взаимопонимание и использование точно определенной терминологии становится все более проблематичным для профессионалов из разных предметных областей (ПрО), что затрудняет общение между коллегами. По мере того как процесс принятия решений становится центральным и стратегическим преимуществом, успех организации все больше зависит от ее способности производить, собирать, хранить, управлять и распространять знания. В этом процессе роль «первой скрипки» принадлежит онтологии знаний, и в частности онтологии безопасности информационных технологий (БИТ).

Онтология определяет общий словарь для исследователей, которым необходимо обмениваться информацией в рамках предметной области. Она включает в себя машинные интерпретирующие определения основных понятий в ПрО и взаимосвязей между ними. Области применения онтологического подхода в условиях роста интеллектуализации в анализе данных постоянно расширяются: это распознавание нештатных ситуаций на основе агентных моделей при диагностике бортового оборудования космической техники [6]; автоматическое реагирование на угрозы с целью минимизации ущерба за счет обработки больших объемов данных на основе алгоритмов искусственного интеллекта [7]; развитие адаптивных механизмов подсистемы информационной безопасности в организационных системах поддержки принятия решений на основе метода вывода по прецедентам в условиях динамики конфликтного взаимодействия, отличающейся возможностью выработки управляющего воздействия для координации механизмов подсистемы информационного обмена [8].

Унифицированные и формализованные модели знаний в области информационной безопасности являются фундаментальными требованиями для поддержки и совершенствования существующих подходов к управлению рисками, основная первопричина которых заключается в неполноте знаний о ПрО [9]. Концептуально- аналитический подход, включающий поиск и анализ существующей литературы по ИБ, является основой для создания формальной модели знаний и соответствующей БДЗ (артефактов), упорядочение которой для систематизации и рационального поиска информации будет обеспечивать предлагаемая онтология безопасности в формате БИТ.

Целью исследования является определение потенциальных связей между нормативно-техническими, методическими и научно-техническими источниками, существующими

подходами к классификации объектов (сущностей, логических единиц, таксономических и онтологических элементов) и структурированию предметной области в сфере информационной безопасности.

В основе онтоло́гии в информатике лежит подход, базирующийся на подробной формализации заданной области знаний с помощью определенной концептуальной схемы. Обычно такая схема состоит из структуры данных, содержащей все релевантные[1] классы объектов, их связи и правила, принятые в этой области [10].

Концептуализация – это абстрактный, упрощенный взгляд на мир, который мы хотим представить для какой-либо цели. Каждая база знаний, система, основанная на знаниях, или агент уровня знаний (управляющая программа или сценарий) придерживаются некоторой концептуализации явно или неявно. Для целей обмена знаниями формальные онтологии служат спецификациями общих взаимодействий между агентами (концептуализаций или многоаспектной переработкой данных) [11].

Онтология является средством, обеспечивающим концептуальный уровень представления знаний, необходимых при разработке как конкретной информационной системы (ИС), так и системы ИБ для нее. В частности, использование онтологии дает возможность сформировать структуру ИС, описать набор компонентов и их взаимосвязей, сформировать список решаемых задач с привязкой к данным и программным компонентам, а также обеспечить гибкий интерфейс с учетом потребностей конкретного пользователя [12].

Основные подходы к понятию «онтология научного исследования» представлены в следующей таблице.

Основные подходы к определению понятия «онтология» предметной области

№	Онтология (О) исследования информационных процессов	Источники
1	О. – формализованное представление набора наименований понятий в предметной области и отношений между этими наименованиями понятий.	ГОСТ Р 59277–2020; п. 3.35[2]
2	О. – формальная эксплицитная спецификация совместно используемой *концептуализации*.	Gruber T.R [10, с. 4]
3	Общая онтология определяет словарь, с помощью которого агенты обмениваются запросами и утверждениями.	Gruber T.R [11]
4	О. – модель предметной области, использующая все доступные средства представления знаний, релевантные для данной области.	Соловьев И.В. [13]
5	О. – совокупность терминов, выражений отношений и связанных с ними определений на естественном языке вместе с одной или несколькими формальными теориями, предназначенными для отражения заданных интерпретаций этих определений.	ГОСТ Р 70846.3–2023, п. 3.26[3]

Обобщая представленные определения, запишем в формальном виде модель онтологии в виде следующего кортежа [4]:

$$O = \langle C,\ E,\ At,\ R,\ A \rangle, \quad (1)$$

где O – онтология; C – понятия (классы) онтологии; E – экземпляры онтологии; At – атрибуты понятий и экземпляров онтологии; R – отношения между понятиями; A – аксиомы онтологии. Термину «онтология» удовлетворяет широкий спектр структур, представляющих знания о той или иной ПрО. В большинстве случаев при рассмотрении онтологий в рамках информационных процессов и ИС и решаемых ими задач в качестве ПрО анализируются различные вычислительные ресурсы, например базы данных и знаний. При этом в отдельных

[1] *Релевантность* – степень соответствия найденного документа (набора документов) информационным потребностям пользователя.

[2] ГОСТ Р 59277–2020 Системы искусственного интеллекта. Классификация систем искусственного интеллекта. (Дата введ. 01.03.2021).

[3] ГОСТ Р 70846.3–2023 Национальная система пространственных данных. Онтология. Общие положения. (Дата введ. 01.03.2024).

типах онтологий некоторые из перечисленных в выражении (1) компонентов могут быть не определены. Так, структура рубрикаторов обычно не включает экземпляры и атрибуты; тогда формальной моделью рубрикаторов является модель вида [4]:

$$O = \langle C, \emptyset, \emptyset, R, A \rangle = \langle C,\ R,\ A \rangle. \quad (2)$$

Основными компонентами, составляющими онтологию, являются: понятия (классы), отношения, аксиомы, свойства (атрибуты) и экземпляры. Понятия – это абстрактные термины, обычно организованные в таксономии, которые могут обладать свойствами (или атрибутами), которые помогают установить связь между неиерархическими понятиями, описывающими общие характеристики экземпляров классов или классовые отношения, и могут иметь определенный тип (например, *СТРОКА*, *ЦЕЛОЕ* число, логическое значение и т.д.). Аксиомы – это правила, которые применяются в моделируемой предметной области и ограничивают возможные интерпретации определенных понятий. Онтологии обеспечивают наследование объектно-ориентированным способом, где примеры представляют собой реальное возникновение абстрактных понятий.

Для работы с онтологиями чаще всего используются *языки описания онтологий* – формальный язык, используемый для кодирования онтологии. Существует несколько подобных языков (*список неполон*) [14]:

- Web Ontology Language (OWL) – стандарт W3C (World Wide Web Consortium), язык для семантических утверждений, разработанный как расширение модели данных Resource Description Framework (RDF), которая позволяет объединить разнородную информацию, включая базы данных, системы и базы знаний;
- *Knowledge Interchange Format* (KIF) – универсальный машинно-ориентированный язык для обмена данными в рамках выбранной ПрО. KIF имеет декларативную семантику и логическую всесторонность;
- Common Logic (CL) – логическая структура, стандартизованная для упрощения обмена и передачи знаний в компьютерных системах, – является стандартным языком разработки онтологий[4] ;
- Cycorp Language (CycL) – онтологический язык, синтаксис которого базируется на логике первого порядка Основан на исчислении предикатов с некоторыми расширениями более высокого порядка.

Для работы с языками онтологий существует несколько видов технологий: редакторы онтологий (для создания онтологий), СУБД онтологий (для хранения и обращения к онтологии) и хранилища онтологий (для работы с несколькими онтологиями).

Под моделью безопасности информационных технологий будем понимать системы, определяющие правила доступа к данным и работы с ними для обеспечения информационной безопасности. При этом БИТ относится только к процессам переработки данных (обработке, хранению, поиску, отображению и др.), не касаясь процессов передачи данных, свойственных понятию ИКТ [3].

Точно так же, как концепция ИБ включает в себя БИТ, чтобы защитить саму информацию, независимо от ее текущей формы и/или местоположения, кибербезопасность необходимо рассматривать как расширение информационной безопасности. Кибербезопасность также связана с защитой человека (лиц, организаций), использующих ресурсы в киберпространстве, и с защитой любых других активов, в том числе принадлежащих обществу в целом, которые подверглись риску в результате уязвимостей, связанных с использованием ИКТ. Взаимосвязь между этими тремя пересекающимися понятиями проиллюстрирована на рис. 1 [3]. Объектами защиты для представленных трех областей являются: 1) информационные активы, хранящиеся и передаваемые без использования ИКТ (документы, архивы, объекты в неоцифрованном виде); 2) неинформационные активы,

[4] ГОСТ Р ИСО/МЭК 21838-1–2021. Информационные технологии. Онтологии высшего уровня (TLO). Ч. 1. Требования. (Дата введ. 30.04.2022).

уязвимые угрозам с использованием ИКТ; 3) информационные активы, хранящиеся и передаваемые с использованием ИКТ.

Основные типы моделей безопасности

- Концептуальные модели
  - Представляют собой набор понятий и связей между ними, которые определяют смысловую структуру предметной области.
  - Они помогают понять, какие аспекты ИБ важны, и служат основой для дальнейшего построения систем безопасности.
- Математические модели
  - Формализуют сценарии угроз и мер защиты в виде логических алгоритмов.
  - Используются для количественных оценок уязвимостей, построения алгоритмов защиты и расчета рисков.

Информация – это актив, который наряду с другими важными активами представляет собой огромную ценность для бизнеса организации и, следовательно, должен быть надежно защищен[5].

Причем ИС представляется как набор приложений, услуг, информационно-технических активов или других компонентов для обработки информации[6].

Организации осознают, что информация и связанные с ней процессы, системы, сети и персонал являются важными активами для достижения целей, стоящих перед организацией;

ИТ-актив (IT asset) – это оборудование, программное обеспечение, элемент или сущность, которые могут быть использованы для получения, обработки, хранения и распространения информации, способствовать предоставлению ИТ-продукта/услуги, а также имеют потенциальную или фактическую ценность для организации[7].

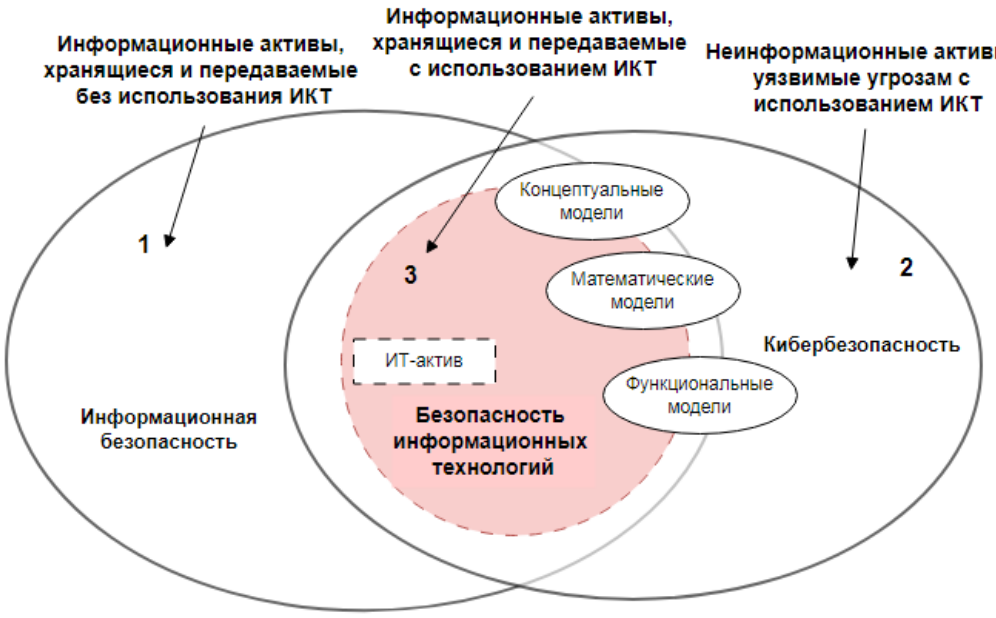

Рис. 1. Взаимоотношения между информационной безопасностью, кибербезопасностью и безопасностью информационных технологий

Эти модели обеспечивают иерархию прав на выполнение конкретных действий:

– дискреционное управление доступом (discretionary access control, DAC) – доступ определяется владельцами ресурсов и требует сложных настроек для контроля;

[5] ГОСТ Р ИСО/МЭК 27000–2021 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. (Дата введ. 30.11.2021).
[6] Там же, п. 3.35.
[7] ГОСТ Р 72161–2025 Информационные технологии. Управление ИТ-активами. Ч. 1. Системы управления ИТ-активами. Требования. (Дата введ.: 28.07.2025); п.3.10.

– мандатное управление доступом (mandatory access control, MAC) – доступ регулируется системой на основе фиксированных правил, часто с использованием меток секретности;

– ролевое управление доступом (role-based access control, RBAC) – более гибкий и масштабируемый по администрированию механизм на основе ролей, которые присваиваются пользователям.

Для обеспечения БИТ решаются задачи, свойственные указанным на рис. 1 направлениям [3, 9, 12], связанным с переработкой данных:

– накопление и анализ поступающих данных;

– мониторинг данных – их интерпретация в реальном масштабе времени;

– диагностика работы компьютерных систем управления и выявление отклонений от нормального режима работы;

– прогнозирование последствий некоторых событий;

– поддержка принятия решений в виде своевременного предоставления необходимой информации и рекомендаций.

На рис. 2 показан пример построения онтологии безопасности с учетом множества разнообразных факторов, отражающих особенности всех заинтересованных участников, их ресурсов, возможных угроз для организации и построения соответствующих мер защиты от киберопасностей [12].

Рис. 2. Онтология безопасности информационных технологий

Представленная онтология отражает только один из начальных этапов рассмотрения проблемы кибербезопасности, так как не затрагивает такие сферы, как информационная безопасность, безопасность приложений, сетей, информационных систем и другие.

Онтологическое описание объектов и их взаимосвязей в сфере информационной безопасности является мощным инструментом для структурирования знаний, анализа рисков, проведения аудита и разработки систем защиты информации. Различные подходы и методологии, такие как OWL, RDF, Protégé и UML, позволяют создавать гибкие и расширяемые онтологии, которые могут быть использованы для автоматизации процессов анализа и принятия решений в области информационной безопасности.

Вместе с тем отдельным вопросом стоит увязывание вопросов классификаций (угроз, уязвимостей и ряда других составляющих, представленных на рис. 2 на онтологическом уровне со сведениями, содержащимися в нормативно-правовых, нормативно-технических и методических документах, к которым следует отнести объекты регулирования, их атрибуты, требования к ним, при формировании единой онтологической модели ПрО и БИТ.

Список литературы

1. Леонов Н.В. Противодействие уязвимостям программного обеспечения. Часть 1. Онтологическая модель // Вопросы кибербезопасности. 2024. № 2(60). С. 87–92. DOI: 10.21681/2311-3456-2024-2-87-92 /
   Leonov N.V. Protivodejstvie uyazvimostyam programmnogo obespecheniya. Part 1. Ontologicheskaya model'. Voprosy kiberbezopasnosti. 2024;2(60):87–92. DOI: 10.21681/2311-3456-2024-2-87-92 (In Russ.).
2. Лось В.П., Маланьин Д.Д. Методы интеллектуального анализа данных, применяемые в задаче обнаружения вторжений // Информация и безопасность. 2022. Т. 25, № 4. С. 599–608. DOI 10.36622/VSTU.2022.25.4.014 /
   Los V.P., Malanin D.D. Metody intellektual'nogo analiza dannyh, primenyaemye v zadache obnaruzheniya vtorzhenij. Informaciya i bezopasnost'. 2022; 25(4):599–608. DOI: 10.36622/VSTU.2022.25.4.014 (In Russ.).
3. Бурый А.С., Исаенко И.В. Обеспечение проактивной безопасности информационно-коммуникационных технологий // Информационно-экономические аспекты стандартизации и технического регулирования. 2024. № 5(80). С. 73–78. /
   Buryi A.S., Isaenko I.V. Obespechenie proaktivnoj bezopasnosti informacionno-kommunikacionnyh tekhnologij. Information and Economic Aspects of Standardization and Technical Regulation. 2024;5(80):73–78. (In Russ.).
4. Лукашевич Н.В., Добров Б.В. Проектирование лингвистических онтологий для информационных систем в широких предметных областях // Онтология проектирования. 2015. Т. 5, № 1(15). С. 47–69. /
   Lukashevich N.V., Dobrov B.V. Proektirovanie lingvisticheskih ontologij dlya informacionnyh sistem v shirokih predmetnyh oblastyah. Ontologiya proektirovaniya. 2015;5(1):47–69. (In Russ.).
5. Arbanas K., Čubrilo M. Ontology in information security. Journal of information and organizational sciences. 2015; 39(2):107–36.
6. Юрыгина Ю.С., Скорюпина Е.Г. [и др.]. Подход к разработке системы распознавания и предупреждения нештатных ситуаций транспортного грузового корабля "Прогресс" на основе мультиагентных технологий и онтологий // Информационно-управляющие системы. 2016. № 1(80). С. 50–57. DOI: 10.15217/issn1684-8853.2016.1.50 /
   Yurygina Yu.S., Skoryupina E.G., et al. Podhod k razrabotke sistemy raspoznavaniya i preduprezhdeniya neshtatnyh situacij transportnogo gruzovogo korablya "Progress" na osnove mul'tiagentnyh tekhnologij i ontologij. Informacionno-upravlyayushchie sistemy. 2016;1(80):50–57. DOI: 10.15217/issn1684-8853.2016.1.50 (In Russ.).
7. Мельников С.Ю., Мещеряков Р.В., Пересыпкин В.А. Некоторые аспекты применения технологий искусственного интеллекта в задачах защиты информации (обзор) // Известия ЮФУ. Технические науки. 2024. № 5(241). С. 58–68. DOI: 10.18522/2311-3103-2024-5-58-68 /
   Melnikov S.Yu., Meshcheryakov R.V., Peresypkin V.A. Nekotorye aspekty primeneniya tekhnologij iskusstvennogo intellekta v zadachah zashchity informacii (obzor). Izvestiya YuFU. Tekhnicheskie nauki. 2024;5(241):58–68. DOI: 10.18522/2311-3103-2024-5-58-68 (In Russ.).
8. Бурый А.С., Усцелемов В.Н. Развитие систем поддержки принятия решений на основе прецедентов в распределенных информационных структурах // Правовая информатика. 2024. № 1. С. 88–95.
   Buryi A.S., Ustselemov V.N. Razvitie sistem podderzhki prinyatiya reshenij na osnove precedentov v raspredelennyh informacionnyh strukturah. Legal Informatics. 2024;1:88–95. (In Russ.).
9. Fenz S., Ekelhart A. Formalizing information security knowledge // In Proceedings of the 4th international Symposium on information, Computer, and Communications Security. 2009. С. 183–194.
10. Gruber T.R. A translation approach to portable ontology specifications. Knowledge acquisition. 1993;5(2):199–220.
11. Gruber T.R., Olsen G.R. An ontology for engineering mathematics. In Principles of Knowledge Representation and Reasoning (KR’94). Morgan Kaufmann. 1994, pp. 258–269.
12. Ворожцова Т.Н. Онтология как основа для разработки интеллектуальной системы обеспечения кибербезопасности // Онтология проектирования. 2014. № 4(14). С. 69–77. /
    Vorozhtsova T.N. Ontologiya kak osnova dlya razrabotki intellektual'noj sistemy obespecheniya kiberbezopasnosti. Ontologiya proektirovaniya. 2014;4(14): 69–77. (In Russ.).
13. Соловьев И.В. Онтологии предметной области в науках о Земле // Перспективы науки и образования. 2014. № 1(7). С. 74–78. /
    Solovev I.V. Ontologii predmetnoj oblasti v naukah o Zemle. Perspektivy nauki i obrazovaniya. 2014;1(7):74–78. (In Russ.).
14. Бурый А.С. Информационно-поисковые социотехнические системы: термины и определения. – М.: Горячая линия-Телеком, 2018. – 166 с./
    Buryi A.S. Informacionno-poiskovye sociotekhnicheskie sistemy: terminy i opredeleniya. Moscow: Goryachaya liniya-Telekom Publ., 2018, 166 p. (In Russ.).
15. Бойтунова М.Д., Шукенбаева Н.Ш., Шукенбаев А.Б. Исследование принципов построения и разработки онтологии инцидентов информационной безопасности // REDS: Телекоммуникационные устройства и системы. 2022. Т. 12, № 3. С. 4–9. /
    Bojtunova M.D., Shukenbaeva N.Sh., Shukenbaev A.B. Issledovanie principov postroeniya i razrabotki ontologii incidentov informacionnoj bezopasnostiю REDS: Telekommunikacionnye ustrojstva i sistemy. 2022;12(3):4–9. (In Russ.).