УДК 004.056.5

Н. И. Глухов [1]***, П.Н. Наседкин*** [1]

[1] *Иркутский государственный университет путей и сообщений, г. Иркутск, Российская Федерация*

ОНТОЛОГИЧЕСКИЕ МОДЕЛИ В ПРОЦЕССЕ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ХОЗЯЙСТВУЮЩИХ СУБЪЕКТОВ

Аннотация. В данной работе проводится построение онтологических моделей в процессе управления информационными рисками и информационной безопасности (ИБ) хозяйствующих субъектов на основе отношений между основными концептами в области информационной безопасности предприятий. Определяется перечень основных объектов защиты предприятий, состав и структура информационной системы управления предприятий (ИСУП), информационные системы, информационные потоки, виды и уровни информации, обрабатываемой в ИСУП, технические меры защиты с учетом которых определяются основной спектр средств защиты информации и их связей между собой, а также раскрываются основные связи онтологических моделей по информационной безопасности и управлению информационными рисками, что в дальнейшем позволит при их рассмотрении и анализе принять оптимально достаточные управленческие решения по минимизации угроз и получения прогностических оценок уровня возможного ущерба с учетом источников и свойств информации в разрезе каждого информационного актива с применением различных методик в оценке рисков ИБ (качественных, количественных, гибридных).

Ключевые слова: источники угроз, риски, онтологическая модель, концепты, информационные системы, управленческие решения по информационной безопасности, объекты защиты.

N.I. Glukhov[1]***, P.N. Nasedkin*** [1]

[1] *Irkutsk State University of Railways and Communications, Irkutsk, Russian Federation*

ONTOLOGICAL MODELS IN THE PROCESS OF MANAGING INFORMATION RISKS AND INFORMATION SECURITY OF ECONOMIC SUBJECTS

Abstract. In this paper, ontological models are constructed in the process of managing information risks and information security (IS) of business entities based on the relationship between the basic concepts in the field of information security of enterprises. The list of the main objects of enterprise protection, the composition and structure of the enterprise management information system (EMIS), information systems, information flows, types and levels of information processed by the EMIS, technical protection measures, taking into account which the main range of information protection means and their connections are determined, are determined with each other, and also reveals the main relationships of ontological models for information security and information risk management, which in the future will allow for their consideration and analysis to take optimally sufficient managerial decisions to minimize threats and obtain prognostic estimates of the level of possible damage, taking into account the sources and properties of information in the context each information asset using various methods in assessing the risks of information security (qualitative, quantitative, hybrid).

Keywords**:** sources of threats, risks, ontological model, concepts, information systems, management decisions on information security, objects of protection.

Введение

Обеспечение защиты основных информационных активов хозяйствующих субъектов, включая бизнес-процессы, от искажения, уничтожения, несанкционированного доступа является актуальной проблемой информационной безопасности. Для ее решения задействован теоретический и практический подходы, включающие в себя как системный анализ и теорию принятия решений, так и различные методики в оценке уровня угроз.

В настоящее время анализ и оценка текущего уровня обеспечения информационной безопасности хозяйствующих субъектов проводится в основном в рамках договорных отношений силами организаций имеющих соответствующий уровень компетенции на проведение аудита по информационной безопасности (ИБ). На основании отчетов полученных от ауди-

торов по ИБ руководство хозяйствующих субъектов (далее – предприятий) определяет стратегические и тактические цели достижения оптимальных соотношений между затратами на ИБ и средствами защиты информации (СрЗИ), имеющихся и необходимых для последующего интегрирования в информационную систему управления предприятия (ИСУП) и его инженерно-технических систем охраны (ИТСО). При этом, под «Объектом» защиты предприятий понимается комплекс зданий, сооружений и иных объектов производственного назначения, находящихся в пределах контролируемой зоны предприятий и в случае наличия у него дочерних обществ соответствующих территорий, находящихся обособленно за пределами от основной. В связи с чем, в перечень объектов защиты информационной инфраструктуры предприятия влияющих на принятие решений по управлению информационными рисками и обеспечению информационной безопасности ИСУП должны входить:

1. Автоматизированные процессы и процедуры основного и вспомогательных производств;
2. системы и установки АСУТП (автоматизированных систем управления технологическим процессом) с подключением и без подключения к локальной вычислительной сети предприятий.

Несмотря на то, что в установках АСУТП не обрабатывается и не хранится информация, составляющая коммерческую тайну предприятий, их деловых партнёров и контрагентов руководству предприятий при этом необходимо обеспечить непротиворечивость, целостность и доступность информации. В состав объекта защиты АСУТП входят программное обеспечение (ПО), автоматизированные рабочие места (АРМ) и серверы АСУТП, а также активное сетевое оборудование (АСО), входящее в состав локальной вычислительной сети (ЛВС) АСУТП. Однако, в состав объекта защиты в части АСУТП не входят контроллеры (уровень автоматического управления) и исполнительные механизмы (уровень ввода (вывода) данных, исполнительных устройств) по следующим причинам:

1. При применении известных на сегодняшний день СрЗИ на уровне контрольно-измерительных приборов и автоматики (КИПиА) есть потенциальная опасность создания задержек и искажений при передаче информации между измерительными и исполнительными механизмами и системами управления, что может повлечь риски нарушения непрерывности технологического процесса;
2. нейтрализация угроз безопасности информации на уровнях использования стека протоколов TCP/IP (рабочие станции АСУТП, серверы АСУТП, АСО, входящее в состав ЛВС АСУТП) без нарушения логики функционирования КИПиА и АСУТП в целом.

Отношения между концептами управления СрЗИ информационной безопасности предприятий и их онтологическая модель.

Для построения онтологических моделей в процессе управления информационными рисками и информационной безопасности хозяйствующих субъектов (рис.1) необходимо определить основные отношения между концептами в области информационной безопасности предприятий (табл.1), которые должны учитывать, как объекты защиты - информационные системы (ИС), обрабатывающие конфиденциальную информацию; ИС обрабатывающих персональные данные (ИСПДн); АСУТП и при этом выделяются автоматизированные рабочие места (АРМ) ИС, обрабатывающих конфиденциальную информацию с повышенными требованиями к безопасности (далее – АРМ ПТБ), так и следующую информацию:

1. Состав и структуру ИСУП:
   1.1. Состав технических средств, входящих в ИСУП;
   1.2. каналы передачи данных;
   1.3. беспроводные каналы передачи данных Wi-Fi;
   1.4. структурные и функциональные схемы локальной и корпоративной системы передачи данных;
   1.5. состав общесистемных программных средств;
   1.6. состав прикладного программного обеспечения;

1.7. состав применяемых средств защиты информации;
1.8. антивирусную защиту;
1.9. систему резервного копирования и аварийного восстановления данных.

2. Информационные системы, информационные потоки, виды и уровни информации, обрабатываемой в ИСУП:
   2.1. Информационные системы, входящие в ИСУП (ИС, обрабатывающие как конфиденциальную, так и открытого доступа информацию, ИСДн, АСУТП);
   2.2. информационные потоки, циркулирующие в ИСУП;
   2.3. виды и уровни информации, обрабатываемой и накапливаемой в ИСУП.
3. Систему доступа и разграничения прав пользователей ИСУП;
4. Физическую защиту и технические меры защиты:
   4.1. ИТСО в составе:
      4.1.1. Инженерно-технических средств защиты (ИТСЗ) объекта (инженерные заграждения, инженерные средства и сооружения, контрольно-пропускные пункты; помещения для размещения подразделений охраны);
      4.1.2. ТСО (система охранной сигнализации; система охранная телевизионная; система контроля и управления доступом; система сбора и обработки информации, включающая подсистему связи и передачи извещений к пультам централизованного наблюдения; технические средства досмотра);
      4.1.3. вспомогательных систем (система охранного освещения; система оповещения о тревоге, чрезвычайной ситуации и др.; система электропитания; система оперативной связи подразделений охраны).
5. Уровень подготовки персонала.

В разрезе системы ИТСО выделяется состав систем ТСО подлежащих защите информации в соответствие с требованиями локальных нормативных документов предприятий и Федерального законодательства России. Для защиты ТСО должна создаваться и использоваться собственная выделенная физически локальная вычислительная сеть (ЛВС). При этом, необходимо учитывать то обстоятельство, что совместное использование сетей передачи данных на предприятиях может привести к непредсказуемым нарушениям в работе систем безопасности и нарушению пропускной способности каждой из сетей. Совместное использование сети также недопустимо из-за возможности несанкционированного воздействия на работу подсистем комплекса ТСО через ЛВС предприятия общего пользования.

Определение концептов безопасности для ИТСО в составе ТСО в рамках данной исследовательской работы в части построения онтологической модели не рассматриваются по соображениям закрытости данной информации, которая входит в перечень паспортов по антитеррористической защищенности объектов на предприятиях.

Таблица 1

Отношения между концептами управления СрЗИ информационной безопасности предприятий

№ п.п.	Наименование	Действия (Функции)
1	Контроль и управление доступом	контроль и управление доступом к **защищаемым информационным ресурсам.**
		контроль и управление доступом к **внешним носителям информации и периферийным устройствам.**
		контроль доступа к **АСО [активное сетевое оборудование], ЛВС, межсетевым экранам, СрЗИ.**
2	Регистрация и учет	регистрация и учет **действий, пользователей и процессов поиска вирусов и вредоносного программного обеспечения.**
		регистрация событий доступа к в**нешним устройствам и портам ввода-вывода.**
3	Обеспечение целостности	контроль целостности **исполняемых и конфигурационных файлов СрЗИ, АСО, компонентов ОС, прикладного и системного ПО, файлы данных.**

№ п.п.	Наименование	Действия (Функции)
		контроль неизменности **параметров встроенных СрЗИ и компонентов системного ПО.**
4	Антивирусная защита	защита **файловой системы от вирусов и вредоносных программ.**
		потоковая защита **межсетевого трафика от вирусов и вредоносных программ.**
5	Обеспечение сетевой безопасности	**межсетевое экранирование** ЛВС.
		обнаружение **вторжений** в ЛВС.
		обеспечение безопасного функционирования **сетевого оборудования, ИС, АСО,ВНИ,СрЗИ, Переферийное оборудование**
6	Обеспечение непрерывности(функционирования	резервное копирование **исполняемых и конфигурационных файлов СрЗИ, АСО, прикладного и системного ПО ,компонентов ОС и восстановление данных из резервных копий** в случаях сбоев.
7	Контроль использования информационных ресурсов	контроль каналов утечек **защищаемой информации**.
		обнаружение несанкционированного **хранения конфиденциальной информации.**
8	Анализ защищенности	предоставление в виде отчетов информации об обнаруженных **уязвимостях** с рекомендациями по их устранению.
		обеспечение инвентаризации **узлов**, выявление и идентификация **уязвимостей.**
9	Централизованное управление СрЗИ	обеспечение возможности оперативного получения **информации о состоянии защищенности.**
		обеспечение автоматизации **рутинных задач.**

Онтологическая модель управления СрЗИ ИБ предприятий.

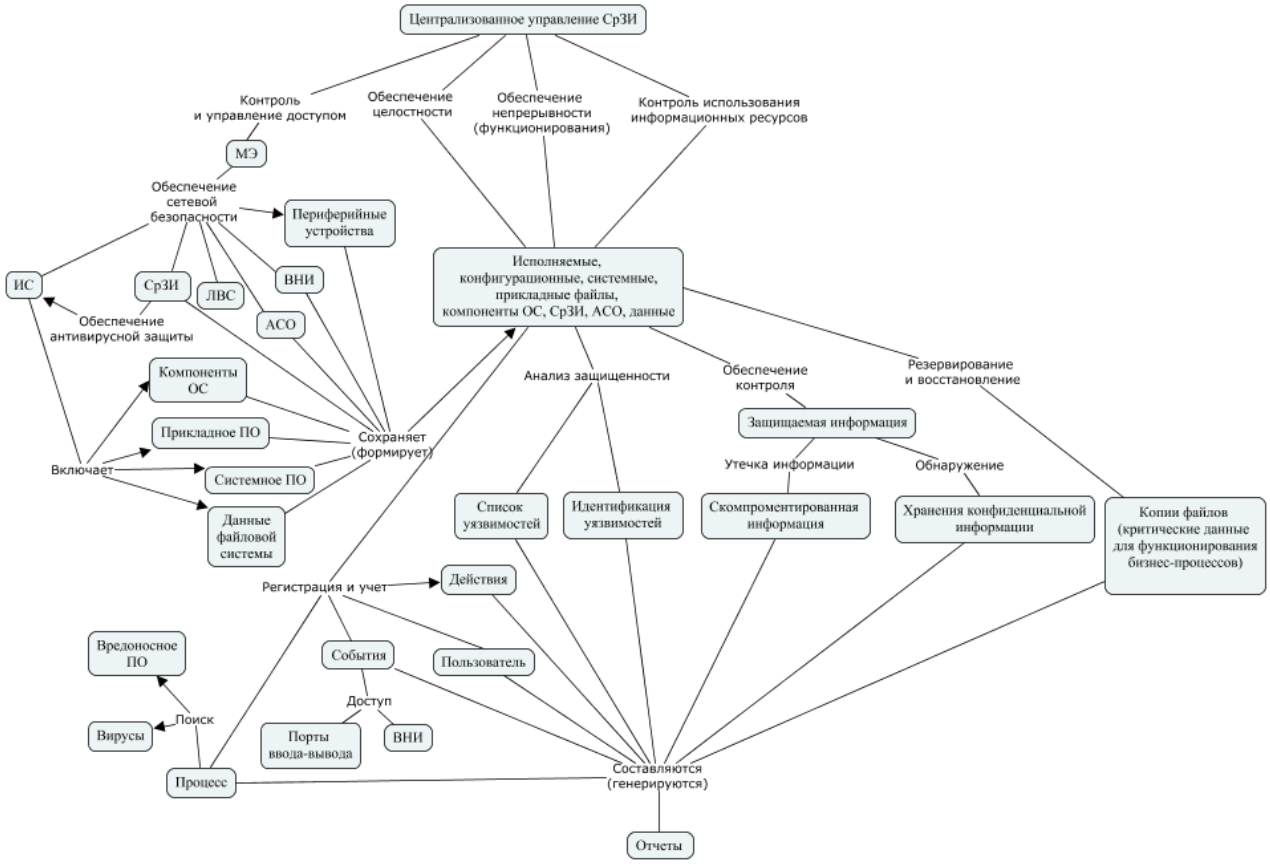

Рис. 1 . Онтологическая модель управления СрЗИ ИБ предприятий.

Онтологическая модель взаимосвязи основных концептов в процессе управления информационными рисками и информационной безопасности предприятий.

Анализ научной литературы с учетом ГОСТ Р ИСО/МЭК 15408-1-2012 [1-17] позволил определить состав концептов в области понятий в аналитике внутренних угроз информационной безопасности предприятий, их взаимосвязей и влияния на возможный ущерб предприятий, что позволило построить онтологическую модель, представленную на рис. 2, которая может быть адаптирована и применена к различным предметным областям данного направления исследований, а также в области принятия управленческих решений по ИБ.

Онтологические модели, представленные выше на рис.1 и рис.2 выполнены в приложении «CmapTools», которое позволяет проектировать и легко создавать концепт-карты.

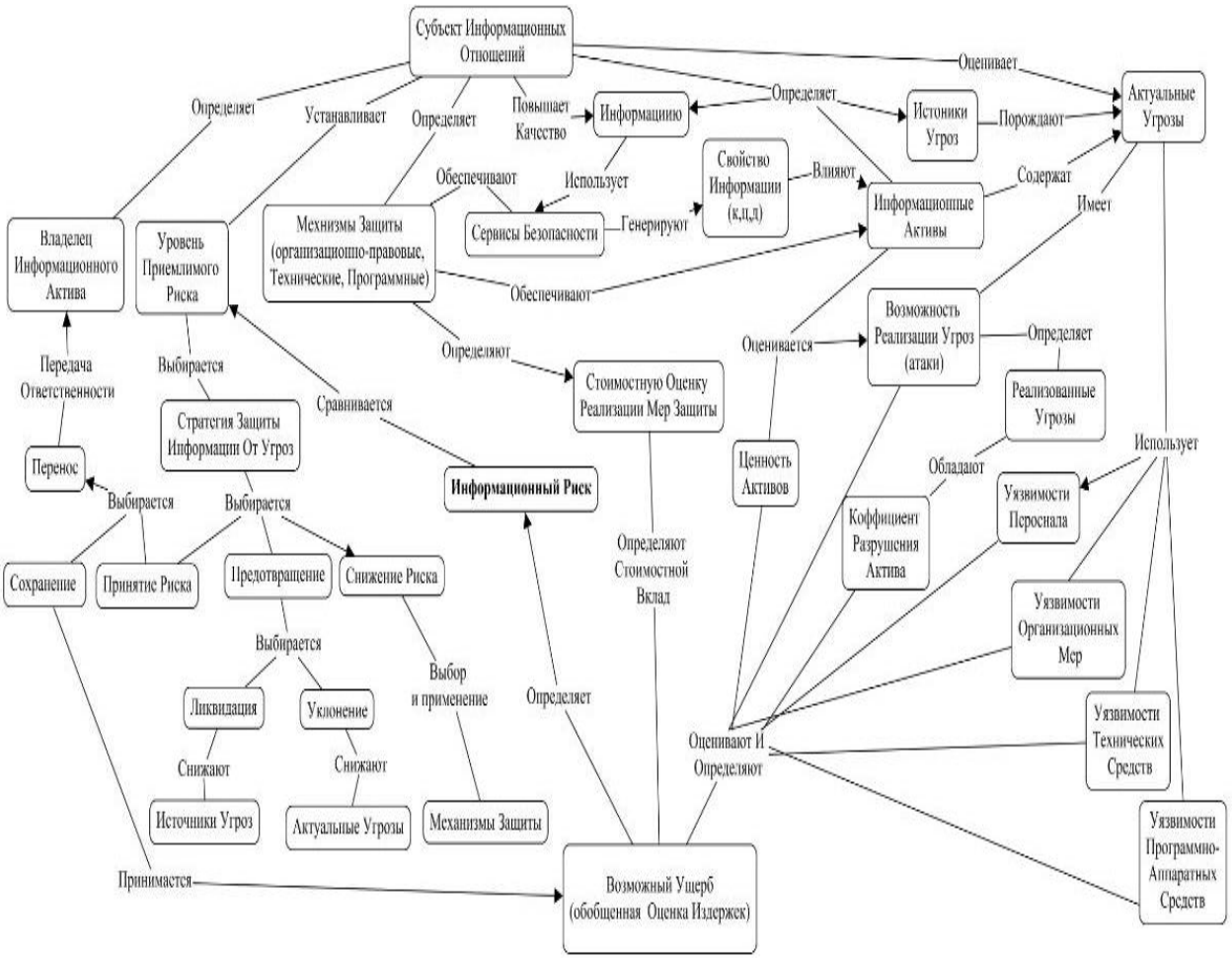

Рис. 2. Онтологическая модель взаимосвязи основных концептов в процессе управления информационными рисками и информационной безопасности предприятий.

Заключение

Большое влияние на принятие управленческих решений по защите информации на предприятии оказывают результаты полученные входе аудита ИБ и профилактических внутренних мероприятий. Однако, стоит отметить, что немаловажным является и проведение системного анализа соответствующих угроз ИБ в разрезе классификации угроз по определенным основным признакам в результате которых будут получены прогностические оценки разных вариантов негативного влияния на ИБ и их последующий результат воздействия. Следует подчеркнуть, что по результатам аналитического отчета компании «СёрчИнформ» (Россия) за 2019 год в области оценки уровня информационной защиты и подходов к вопро-

сам информационной безопасности в России, стран СНГ прослеживается рост угроз для предприятий, вызванных под воздействием антропогенного фактора который ведет к существенному имиджевому ущербу предприятий [10].

Таким образом, предложенные онтологические модели управления информационными рисками и информационной безопасности хозяйствующих субъектов показывают основные компоненты информационной безопасности предприятий и связи между ними в части управления и контроля механизмами ИБ, а также показывают необходимый к рассмотрению руководством предприятий путь принятия управленческих решений по минимизации угроз информационной безопасности.

В связи с чем, это позволит выбрать более точный подход к оценке уровня возможного ущерба с применением методик в оценке рисков ИБ (качественных, количественных, гибридных) с учетом источников и свойств информации в разрезе каждого информационного актива.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения» [Электронный ресурс] / Утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373–ст. – Режим доступа: http://docs.cntd.ru/document/ 1200058320, свободный (дата обращения: 18.05.2020).
2. ГОСТ Р ИСО/МЭК 15408–1–2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. [Электронный ресурс] / Утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 15 ноября 2012 г. № 814–ст. – Режим доступа: http://docs.cntd.ru/document/ 1200101777, свободный (дата обращения: 18.05.2020).
3. ГОСТ Р ИСО/МЭК 27002–2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности [Электронный ресурс] / Утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии 24 сентября 2012 г. N 423–ст. – Режим доступа: http://docs.cntd.ru/document/1200103619, свободный (дата обращения: 18.05.2020).
4. ГОСТ Р ИСО 31000–2010. Менеджмент риска. Принципы и руководство. – М.: Стандартинформ, 2012. –24 с.
5. ГОСТ Р ИСО 31010–2011. Менеджмент риска. Методы оценки риска. – М.: Стандартинформ, 2012. – 74 с.
6. ГОСТ Р ИСО/МЭК 27001–2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – М.: Стандартинформ, 2008. –31 с.
7. ГОСТ Р ИСО/МЭК 27005:2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – М.: Стандартинформ, 2011. – 94 с.
8. ГОСТ Р 53114–2008. Защита информации. Обеспечение информационной безопасности организации. Основные термины и определения. – М.: Стандартинформ, 2009. – 20 с.
9. Блинов А.М. Информационная безопасность: учеб. пособие. – СПб: Изд. СПБГУЭФ, 2010. – 96 с.
10. Исследование уровня информационной безопасности в компаниях России и СНГ за 2019 год [Электронный ресурс]. – Режим доступа: https://searchinform.ru/research–2019, свободный (дата обращения: 17.04.2020).
11. Климов С.М. Методика оценки возможного ущерба от нарушения безопасности информации автоматизированной системы // Известия ТРТУ. – 2003. – № 4 (33). – С. 27–31.
12. Легчекова Е.В. Метод расчета риска информационной безопасности / Е.В. Легчекова, О.В. Титов // Сборник научных статей международной научно–практической конфе-

ренции «Проблемы и перспективы электронного бизнеса». – Гомель: Изд. Белорусский торгово–экономический университет потребительской кооперации. – 2017. – С. 87–89.

13. Нестеров С.А. Анализ и управление рисками в сфере информационной безопасности [Электронный ресурс] – Режим доступа: http://window.edu.ru/resource/443/57443, свободный (дата обращения: 18.05.2020). – С–Пб, 2007. – 1 эл. архив (nesterov–security.zip).

14. Управление рисками. Модель безопасности с полным перекрытием. [Электронный ресурс]. – Режим доступа: https://www.intuit.ru/studies/courses/531/387/lecture/8990, свободный (дата обращения: 17.04.2020 г.).

15. Шинаков К.Е. Минимизация рисков нарушения безопасности при построении системы защиты персональных данных: автореф. дис. канд. техн. наук: 05.13.19 – Брянск, 2017. – С. 70–97.

16. ISO/IEC 27000–1:2018 Information technology – Service management – Part 1: Service managment system requirements [Электронный ресурс]. – Режим доступа:https://www.iso.org/obp/ui/#iso:std:iso-iec:20000:–1:ed–3:v1:en, свободный (дата обращения: 18.05.2020).

17. ISO 31000:2018 – Risk management – Guidelines [Электронный ресурс] – Режим доступа: https://risk-academy.ru/download/iso31000/, свободный (дата обращения: 18.05.2020).

REFERENCES

1. GOST R 50922–2006. Data protection. Basic terms and definitions. Available at: http://docs.cntd.ru/document/ 1200058320 (Access: May 05,2020) (in Russ.).

2. GOST R ISO /IEC 15408–1–2012. Information technology. Security methods and tools. Criteria for assessing the security of information technology. Part 1. Introduction and general model. [Electronic resource] Available at: http://docs.cntd.ru/document/ 1200101777, (Access: May 05,2020) (in Russ.).

3. GOST R ISO /IEC 27002–2012 Information Technology (IT). Security methods and tools. Code of norms and rules of information security management [Electronic resource] Available at: http://docs.cntd.ru/document/1200103619, (Access: May 05,2020) (in Russ.).

4. GOST R ISO 31000–2010. Risk management. Principles and guidelines. – M.: Standartinform, 2012 –24 p.

5. GOST R ISO 31010–2011. Risk management. Risk assessment methods. – M.: Standartinform, 2012. –74 p.

6. GOST R ISO /IEC 27001–2006. Information technology. Security methods and tools. Information Security Management Systems. Requirements. – M.: Standartinform, 2008. – 31 p.

7. .. GOST R ISO / IEC 27005:2010. Information technology. Security methods and tools. Information Security Risk Management. – M .: Standartinform, 2011. – 94 p.

8. .. GOST R 53114–2008. Data protection. Ensuring the information security of the organization. Key terms and definitions. – M .: Standartinform, 2009. – 20 p.

9. .. Blinov A. M. *Informacionnaya bezopasnost: ucheb. posobiye* [Information security]. SPb: SPbGUEF, 2010. – 96 p. (in Russ.).

10. . *Issledovanie urovnya informazionnoy bezopfsnosti v kompaniyach Rossia i SNG za 2019 god* [A study of the level of information security in companies in Russia and the CIS for 2019]. [Electronic resource]. – Available at: https://searchinform.ru/research–2019/ (Access April date: 04 2020) (in Russ.).

11. . Klimov S.M. *Metodika ozenki vozmozhnogo ucherba ot narushenya bezopasnosty informazii avtomatizirovannoy sistemy* [Methodology for assessing the possible damage from information security breaches of the automated system]. Izvestia TRTU, 2003, no. 4 (33). – P. 27–31. (in Russ.).

12. . Legchekova E.V, Titov O.V *Metod rasheta riska informazionnoy bezopasnosty* [The method of calculating information security risk]. Collection of scientific articles of the international scientific-practical conference "Problems and prospects of electronic business" – Gomel,

Publishing House of the Belarusian Trade and Economic University of Consumer Cooperatives, 2017 P. 87–89.

13. . Nesterov S.A. *Analiz i upravlenie riskami v sfere informazionnoy bezopasnosty* [Analysis and risk management in the field of information security]. [Electronic resource] – Available at: http://window.edu.ru/resource/443/57443, (Access May 18 2020). – St. Petersburg, 2007. – 1 email. Archive (nesterov-security.zip) (in Russ.).

14. . Upravlenye riskami. *Model bezopasnosty s polnym perecrytiem*.[Risk management. Security model with full overlap]. Available at: https://www.intuit.ru/studies/courses/531/387/lecture/8990 (Access May 18 2020) (in Russ.)..

15. . Shinakov K.E. *Minimizazia riskov narushenya bezopasnosty pri postroenyii sistemyzachity personalnych dannych: avtoreferat dissertazii* [Minimizing the risks of security breaches when building a personal data protection system]. Bryansk, 2017. – P. 70–97 (in Russ.).

16. . ISO / IEC 27000–1: 2018. Information technology – Service management – Part 1: Service management system requirements [Electronic resource]. – Available at: https: //www.iso.org/obp/ui/#iso: std: iso–iec: 20000: –1: ed–3: v1: en, (Access May 18 2020).

17. . ISO 31000:2018 – Risk management – Guidelines [Electronic resource] – Available at: https://risk-academy.ru/download/iso31000/, (Access May 18 2020).

Информация об авторах

Наседкин Павел Николаевич – инженер по сетевой безопасности Управления информатизации, Иркутский государственный университет путей и сообщений, г. Иркутск, e-mail: nasedkin_pn@irgups.ru

Глухов Николай Иванович – канд. экон. наук, доцент кафедры «Информационные системы и защита информации», Иркутского государственного университета путей сообщения», г. Иркутск, e-mail: gni1953@mail.ru

Authors

Nasedkin Pavel Nikolaevich – network security engineer Network Security Engineer, Informatization Departmen, Irkutsk State Transport University, Irkutsk, e-mail: nasedkin_pn@irgups.ru

Nikolay Ivanovich Glukhov, candidate in Economics, Associate Professor, chair of Information Systems and Information Protection of the Irkutsk State Transport University, Irkutsk, gni1953@mail.ru

Для цитирования

Наседкин П.Н. , Глухов Н.И. Онтологические модели в процессе управления информационными рисками и информационной безопасности хозяйствующих субъектов // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2020. – №2(7). – С. 24-31 – DOI: 10.26731/2658-3704.2020.2(7).24-31 – Режим доступа: http://ismm-irgups.ru/toma/27-2020, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 01.06.2020)

For citation

Nasedkin P.N., Glukhov N.I., Ontological models in the process of managing information risks and information security of business entities // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2020. No. 2(7). P. 24-31. DOI: 10.26731/2658-3704.2020.2(7).24-31 [Accessed 01/06/20]