УДК *004.056.5*

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

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

РАЗРАБОТКА ЭЛЕМЕНТОВ ОНТОЛОГИИ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ

Аннотация. В данной работе рассмотрена онтология элементов комплексной системы защиты информации (далее – КСЗИ) предприятия. Отмечены основные базовые концепты и взаимосвязи, которые обеспечивают выявление, блокирование, минимизацию актуальных угроз и выполнение законодательных, нормативных требований по информационной безопасности в рамках защиты информации в периметре предприятия. В работе впервые предложена общая онтология КСЗИ предприятия, учитывающая основные аспекты развертывания и эксплуатации подобных систем.

В результате исследования рассмотренная в данной работе разработка элементов онтологии КСЗИ позволяет в дальнейшем построить более полные онтологические модели, которые могут быть положены в основу получения агрегированных оценок эффективности защиты информации на предприятии.

Ключевые слова: защита информации, комплексная система защиты информации, КСЗИ, онтология, агрегированная оценка.

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

[1] *Irkutsk State University of Railway Transport, Irkutsk, Russian Federation*

DEVELOPMENT OF ELEMENTS OF ONTOLOGY OF COMPLEX SYSTEM OF PROTECTION OF THE ENTERPRISE INFORMATION

Abstract. In this work the ontology of elements of the complex system of information protection (hereinafter referred to as CSPI) of the enterprise is considered. The main basic concepts and interrelations which provide revealing, blocking, minimization of actual threats and fulfillment of legislative, normative requirements on information security within the framework of information protection in perimeter of enterprise are noted. For the first time the general ontology of enterprise CSPI is proposed, which takes into account the main aspects of deployment and operation of such systems.

As a result of research the development of elements of ontology of CSPI considered in this work allows to construct more complete ontological models which can be put in a basis of reception of the aggregated estimations of efficiency of protection of the information at the enterprise.

Keywords: information protection, complex system of information protection, CSPI, ontology, aggregated assessment.

В условиях экономической деятельности предприятия информация выступает как один из основных ценных информационных активов. Как и любой другой ценный актив на предприятии информация может быть подвержена разрушению, хищению. В связи с чем, проблема защиты информации становится одной из актуальных задач в обеспечении защищенности информационных систем и информационных ресурсов, а также автоматизированных управляющих систем технологическим процессом (АСУ ТП) от внешних и внутренних угроз.

В данной работе рассмотрена онтология отдельных элементов комплексной системы защиты информации (далее – КСЗИ) предприятия. Отмечены основные базовые концепты и взаимосвязи, которые обеспечивают выявление, блокирование, минимизацию актуальных угроз и выполнение законодательных, нормативных требований по информационной безопасности в рамках защиты информации в периметре предприятия.

Новизна работы - в работе впервые предложена общая онтология КСЗИ предприятия, учитывающая основные аспекты развертывания и эксплуатации подобных систем.

В основе разработки общей модели онтологии КСЗИ предприятия должна быть учтена необходимость решения следующих задач:

–защита информации и средств ее обработки от несанкционированного доступа;

–защита персональных данных, обрабатываемых в ИС предприятия в соответствии с действующим законодательством Российской Федерации в области защиты персональных данных;

–защита информационных ресурсов ИС предприятия от внешних программно-технических воздействий, контроль входящих и исходящих информационных потоков и их содержания;

–защита информационных ресурсов, хранимых и обрабатываемых в прикладных информационных системах;

–защита информационных ресурсов от вредоносного кода.

Защита информации в рамках предприятия должна обеспечиваться на всех технологических этапах ее обработки и во всех режимах функционирования ИС и автоматизированных систем управления технологическим процессом (АСУ ТП). Для построения КСЗИ предпочтительно должны быть использованы сертифицированные средства защиты информации.

Разрабатываемые решения в рамках построения отдельных элементов онтологии, как и самой КСЗИ, не должны препятствовать достижению целей создания информационных систем предприятия и их функционирования. Разработка КСЗИ, как и построение отдельных элементов онтологии, осуществляется в соответствии с техническим заданием на создание КСЗИ и (или) техническим заданием (частным техническим заданием) на создание КСЗИ с учетом общих требований к КСЗИ в целом

Элементы верхнего уровня в онтологии КСЗИ предприятия, представленные на рис. 1 включают:

1. Комплект документации на КСЗИ (рис.2);
2. Организационно-распорядительные документы (рис.3);
3. Инженерно-технические решения (рис.4);
4. Программно-технические решения в составе подсистем КСЗИ (рис.5).

Разрабатываемая онтология КСЗИ (рис. 1) предприятия должна в основе своей структуры включать следующие элементы: организационно-распорядительные документы, комплект документации на КСЗИ, программно-технические и инженерно-технические решения [5].

Рис. 1. Элементы верхнего уровня в онтологии КСЗИ

Комплект документации на КСЗИ (рис. 2) в рамках онтологии с учетом использованных материалов, оборудования и режимов работы должна содержать:

1. Проектно-эксплуатационную и рабочую документацию КСЗИ в составе следующих документов:

1.1. Пояснительная записка к техническому проекту на создание КСЗИ;

1.2. Ведомость технического проекта на КСЗИ;

1.3. Схема функциональной структуры на КСЗИ;

1.4. Структурная схема комплекса технических средств КСЗИ;

1.5. Спецификация оборудования КСЗИ;

1.6. Локально-сметные расчеты на проведение монтажных и пуско-наладочных работ по созданию КСЗИ;

1.7. Разделительные ведомости на КСЗИ.

2. Комплект документации на сертифицированные комплексы КСЗИ (лицензии, технические паспорта, формуляры и т.п.) и дистрибутивы программ.

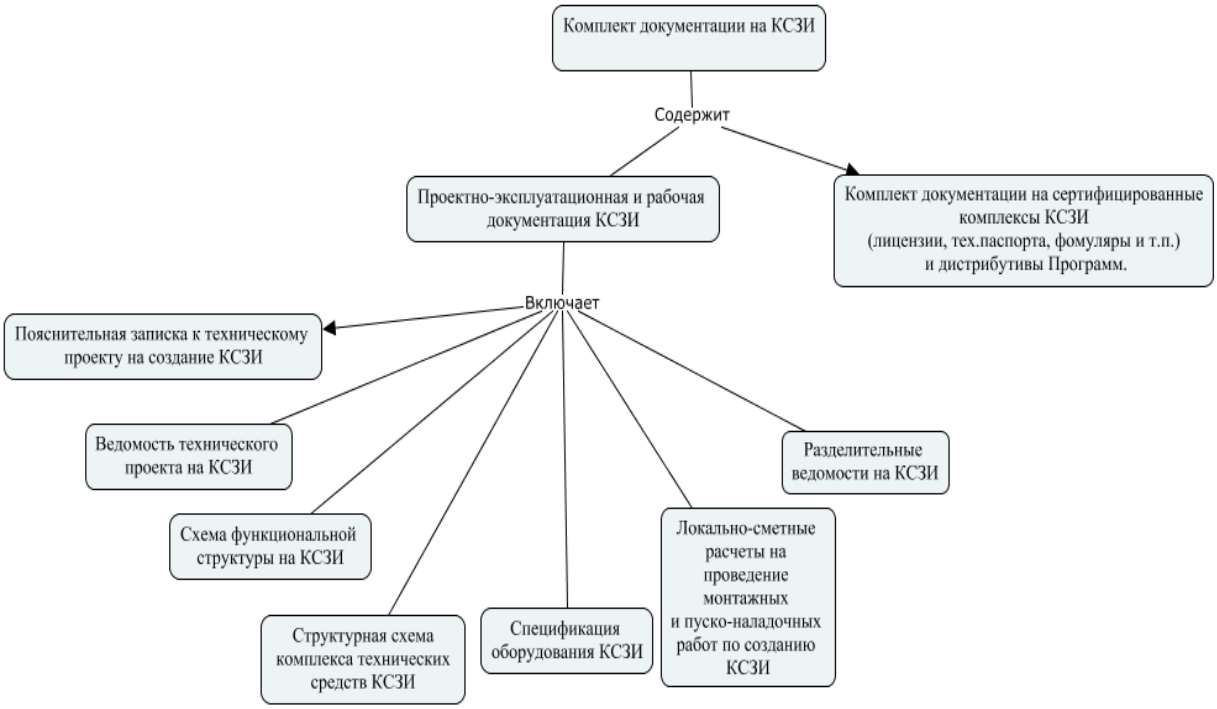

Рис. 2. Элементы уровня комплекта документации на КСЗИ в онтологии КСЗИ

Общая структура создания организационно-распорядительных документов в разрезе элементов и их взаимосвязей в рамках разрабатываемой онтологии КСЗИ отражена на рис. 3 без учета нормативных документов, необходимых для реализации инженерно-технических решений (ИТР) по защите объектов предприятия в силу их конфиденциальности.

Разработка организационных и технических решений должна осуществляется в соответствие с действующей нормативно-методической документацией ФСТЭК России и ФСБ России, а также с учётом стандартов в области информационной безопасности предприятия.

В основе разработки онтологии КСЗИ должны использоваться требования законодательных актов РФ в области защиты информации, нормативно-методических документов ФСТЭК России, а также организационно распорядительные локально-нормативные документы (ОРЛНД) предприятия.

Организационно-распорядительные локально-нормативные документы (ОРЛНД) предприятия в общей базовой структуре создания КСЗИ должны содержать:

1. Стандарт «Политики информационной безопасности».
2. Политика «Концепция информационно-технической безопасности».
3. Стандарт «Руководство по информационной безопасности».
4. Иные локально-нормативные документы предприятия, регламентирующие обеспечение информационной безопасности, а также требования законодательных актов РФ и нормативно-методических документов ФСТЭК России.

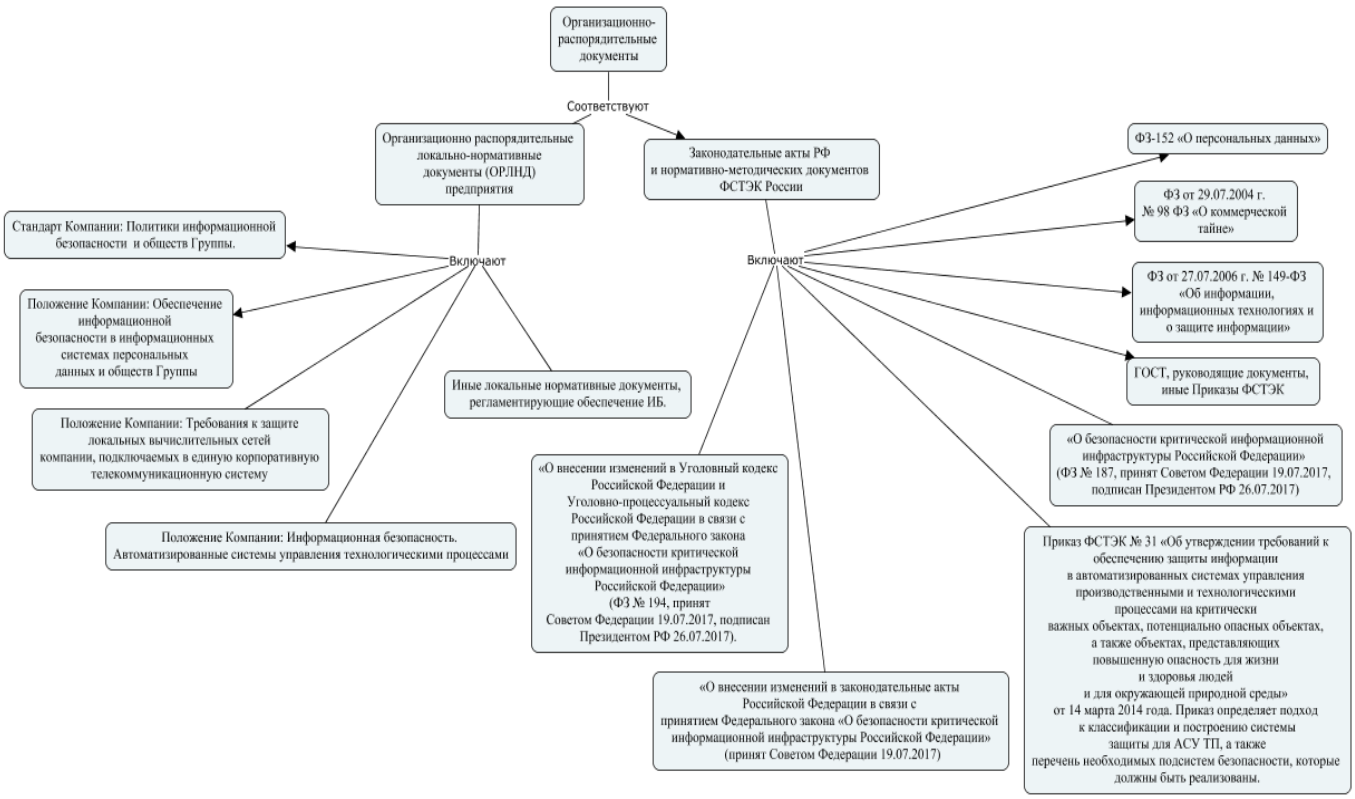

Рис. 3. Элементы уровня ОРД в онтологии КСЗИ

В общем виде в структуру элементов уровня инженерно-технических решений (ИТР) в онтологии КСЗИ (рис. 4) в разрезе защиты и охраны объектов предприятия должны входить и включать в себя:

– средства инженерно-технической укрепленности объекта;
– система охранной и тревожной сигнализации;
– система периметральной сигнализации;
– система охранного телевидения;
– система контроля и управления доступом;
– система охранного освещения;
– устройства обнаружения диверсионно-террористических средств;
– система связи;
– система оповещения;
– средства и системы досмотра (устройства обнаружения диверсионно-террористических средств и запрещенных предметов);
– система электроснабжения технических систем охраны (ТСО);
– система кабельных коммуникаций.

Элементы ИТР решений в рамках инженерно-технической защиты и охраны объектов предприятия создаваемой онтологии КСЗИ должны обеспечивать реализацию следующих функций в разрезе защиты и охраны объектов предприятия:

– Предупреждение и пресечение угроз (несанкционированный доступ на объекты предприятия, террористических, криминальных);
– минимизацию и устранение последствий угроз.

Дальнейшая детализация и разработка онтологии КСЗИ в направлении элементов ИТР требует участия служб безопасности предприятий в каждом конкретном случае в виду действующих ограничений на доступ к данному виду информации.

Уровень ИТР в онтологии элементов инженерной инфраструктуры КСЗИ должен обеспечивать реализацию следующих функций:

– кондиционирование серверных помещений, приборов АСУ ТП;

– бесперебойное электроснабжение серверных, АСУ ТП и АРМ;

– функционирование пожарной сигнализации серверных помещений, АСУ ТП и коммутационных шкафов.

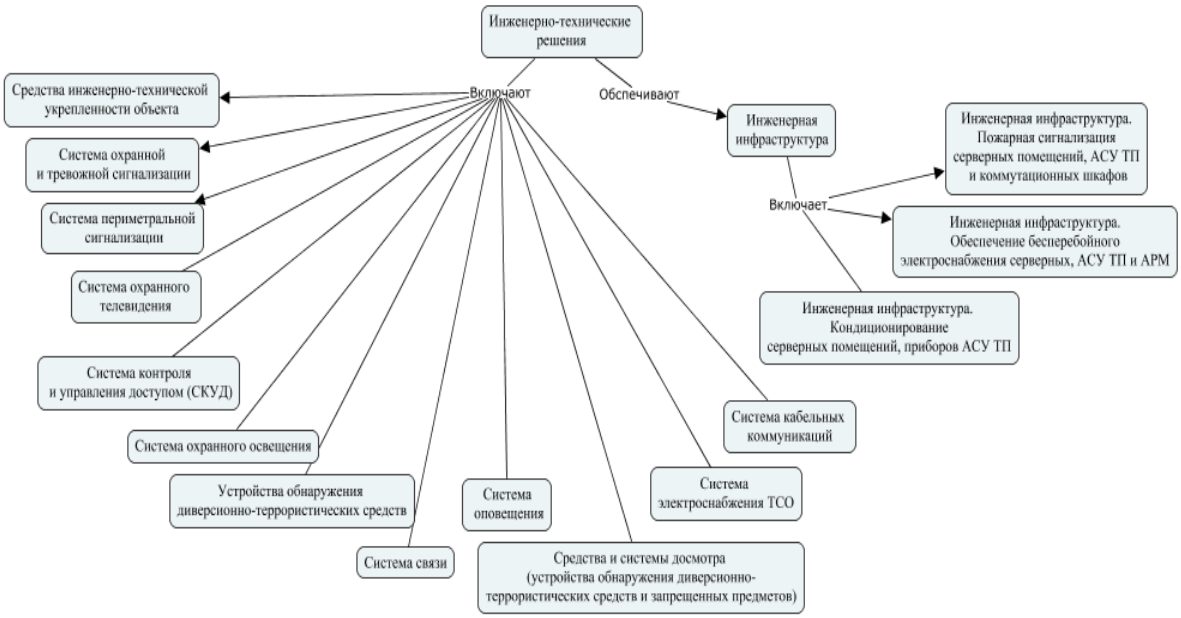

Рис. 4. Элементы уровня ИТР в онтологии КСЗИ

Структура создания онтологии КСЗИ в разрезе элементов уровня программно-технических решений (ПТР) приведена на рис. 5 и включает следующие позиции:

1. Подсистема контроля и управления доступом;
2. Подсистема регистрации и учета;
3. Подсистема обеспечения целостности;
4. Подсистема антивирусной защиты;
5. Подсистема контроля использования информационных ресурсов;
6. Подсистема централизованного управления СрЗИ;
7. Подсистема анализа защищенности;
8. Подсистема обеспечения сетевой безопасности;
9. Подсистема обеспечения непрерывности функционирования.

Рис. 5. Элементы уровня ПТР в разрезе подсистем онтологии КСЗИ

1. Подсистема контроля и управления доступом должна выполнять функции идентификации, аутентификации, создания, активации, модификации, пересмотра (с установленной периодичностью), отключение (блокирование) и удаление учетных записей, а также обеспечение контроля за действиями пользователей и администраторов при доступе их к информационным активам предприятия. В рамках данной подсистемы обеспечивается идентификация программ, томов, каталогов, файлов на АРМ и серверах.

2. Подсистема регистрации и учета. В рамках подсистемы регистрации и учета должны регистрироваться вход/выход субъектов доступа к защищаемым ресурсам, запуск и завершение программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов, регистрация попыток доступа субъектов (пользователей и процессов) к защищаемым объектам доступа (файлам, каталогам). В рамках подсистемы должны обеспечиваться функции по обработке, корреляции событий ИБ и управления активами из единой консоли (web-интерфейса).

3. Подсистема обеспечения целостности. В рамках подсистемы обеспечения целостности должны выполняться функции контроля целостности исполняемых и конфигурационных файлов средств защиты информации (СрЗИ), операционных систем (ОС), прикладного программного обеспечения (ППО) и неизменности параметров встроенных СрЗИ, ОС, АРМ и серверов, входящих в состав ИС и АСУ ТП.

4. Подсистема антивирусной защиты. В рамках подсистемы обеспечивается постоянная защита файловой системы АРМ и серверов под управлением различных версий ОС Windows от вирусов, троянских программ и червей, как с использованием баз вирусных описаний, так и с помощью эвристического анализа, а также потоковая защита межсетевого трафика от вирусов и вредоносных программ.

5. Подсистема контроля использования информационных ресурсов. В рамках подсистемы контроля использования информационных ресурсов должны выполняться функции: обнаружения несанкционированного хранения конфиденциальной информации в информационных ресурсах (файловые серверы, файловые хранилища, АРМ пользователей, БД); контроля каналов утечек защищаемой информации; аутентификации пользователей и формирования профилей доступа к ресурсам сети Интернет; расшифровка SSL (TLS) трафика средствами агентов на АРМ; контроль действий по отправке информации когда агент находится вне ЛВС предприятия; перехват и анализ с возможностью блокировки сообщений, отправляемых с использованием корпоративной электронной почты (протокол SMTP); перехват и анализ сообщений, отправляемых с использованием веб-сервисов (веб-почта, социальные сети, файловые Интернет-ресурсы, облачные хранилища и т.п.); перехват и анализ информации в системах мгновенных сообщений (ICQ, Skype, Jabber, Mail.ru); централизованное хранение истории инцидентов, исходных почтовых сообщений и перехваченных данных; автоматический разбор сообщения на составляющие на этапе приема сообщения с возможностью анализа сообщения по его атрибутам (заголовки, тело, вложения); создание, редактирование и удаление правил фильтрации, анализа и архивирования; детектирование заполненных форм – определение заполненных и незаполненных бланков документов с возможностью обнаружения в форме документа (бланке) персональной информации; возможность оперативного оповещения по электронной почте ответственных работников о зафиксированных событиях ИБ; перехват документов, отправляемых на печать (сетевые и локальные принтеры).

6. Подсистема централизованного управления СрЗИ. В рамках подсистемы централизованного управления СрЗИ должны выполняться функции: обеспечение возможности оперативного получения информации о состоянии защищенности ИС и АСУ ТП, а также оперативного реагирования на инциденты ИБ; предоставление администраторам инструментов для выполнения функций контроля, управления по обеспечению информационной безопасности и автоматизации рутинных задач.

7. Подсистема анализа защищенности. В рамках подсистемы анализа защищенности должны выполняться следующие функции: обнаружение и учет защищаемых ресур-

сов; анализ защищенности компонентов ЛВС предприятия (ОС серверов ИС, АСУ ТП и СрЗИ, АСО, сетевые сервисы серверов ИС, АСУ ТП и СрЗИ, прикладное программное обеспечение); анализ защищенности информационных систем предприятия; сканирование узла ЛВС; принятие решений о соответствии или несоответствии узлов ИС и информационных систем в целом принятым предприятием технических стандартов; регулярное централизованное обновление компонентов подсистемы; централизованное управление компонентами подсистемы и доступом пользователей к функциям подсистемы; генерация отчетов о результатах сканирования, а также доставка отчетов уполномоченным сотрудникам предприятия.

8. Подсистема обеспечения сетевой безопасности. В рамках подсистемы обеспечения сетевой безопасности должны выполняться следующие функции: межсетевое экранирование и сегментирование ЛВС предприятия; обнаружение вторжений; централизованное управление подсистемой; интеграция с периметральной системой защиты информации предприятия.

9. Подсистема обеспечения непрерывности функционирования. В рамках подсистемы обеспечения непрерывности функционирования должны выполняться функции: резервное копирование конфигурационных файлов СрЗИ и АСО и восстановление данных из резервных копий в случаях сбоев; хранение резервных копий; восстановление данных из резервных копий; реализация отказоустойчивой конфигурации МЭ и АСО.

В результате исследования рассмотренная в данной работе разработка отдельных элементов онтологии КСЗИ позволяет в дальнейшем построить онтологические модели, которые могут быть положены в основу получения агрегированных оценок эффективности защиты информации на предприятии, как это предлагается в работах [1-3].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Аршинский Л.В. Логико-аксиологический подход к оценке состояния систем // Современные технологии. Системный анализ. Моделирование. Иркутск: ИрГУПС. 2013. № 3(39). С. 140-146.

2. Аршинский Л.В. Методика агрегированного оценивания систем с поддержкой ключевых компонентов // Онтология проектирования. 2015. Т. 5. № 2 (16). С. 223-232.

3. Аршинский В.Л., Аршинский Л.В., Доржсурэн Х. Оценка качества функционирования станции Улан-Баторской железной дороги на основе онтологического и продукционного моделирования // Современные наукоемкие технологии, 2018, № 5. С. 16-20.

4. Конев А. А. Подход к описанию структуры системы защиты информации / А. А. Конев, Е. М. Давыдова // Доклады ТУСУР. – 2013. – № 2(28). – С. 107–111.

5. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: учебное пособие. М.: Форум, Инфра-М, 2010. 592 с.ISBN 978-5-16-003746-2.

REFERENCES

1. Arshinskiy, L.V. Logical-axiological approach to the systems state estimation (in Russian) // So-time technologies. System analysis. Modeling. Irkutsk: IrGUPS. 2013. № 3(39). C. 140-146.

2. Arshinskiy, L.V. A technique of the aggregate estimation of the systems with the key components support (in Russian) // Design ontology. 2015. T. 5. № 2 (16). C. 223-232.

3. Arshinskiy V.L., Arshinskiy L.V., Dorzhsuren H. Quality estimation of Ulan Bator railroad station functioning on the basis of ontological and production modeling // Modern high technology, 2018, ¹ 5. C. 16-20.

4. Konev, A.A. Approach to the information protection system structure description (in Russian) / A.A. Konev, E.M. Davydova // TUSUR reports. - – 2013. - – № 2(28). - – C. 107–111.

5. Shangin V. F. Comprehensive protection of information in corporate systems: a training manual. Moscow: Forum, Infra-M, 2010. 592 p.ISBN 978-5-16-003746-2.

Информация об авторах

Николай Иванович Глухов - к.э.н., доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: gni1953@mail.ru

Павел Николаевич Наседкин - аспирант кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: nasedkin_pn@irgups.ru

Authors

Nikolai Ivanovich Glukhov - Candidate of Science, Associate Professor of the Department of Information Systems and Information Protection, Irkutsk State University of Railway Transport, Irkutsk, e-mail: gni1953@mail.ru.

Pavel Nikolaevich Nasedkin - postgraduate student of the department Information Systems and Information Protection, Irkutsk State University of Railways, Irkutsk, e-mail: nasedkin_pn@irgups.ru.

Для цитирования

Глухов Н.И., Наседкин П.Н. Разработка элементов онтологии комплексной системы защиты информации предприятия // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2021. – №1(9). – С. 35-42 – DOI: 10.26731/2658-3704.2021.1(9).35-42 – Режим доступа: http://ismm-irgups.ru/toma/19-2021, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 01.02.2021)

For citation

Glukhov, N.I.; Nasedkin, P.N. Development of elements of ontology of complex system of protection of the enterprise information [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2021. No. 1(9). P. 35-42. DOI: 10.26731/2658-3704.2021.1(9).35-42 [Accessed 01/02/21]