УДК 004.056.5

Н.И. Глухов [1], П.Н. Наседкин[1], Д.С. Милько[1]

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

ОНТОЛОГИЧЕСКАЯ МОДЕЛЬ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ ПОТОКАМИ НА ПРЕДПРИЯТИИ С УЧЕТОМ УРОВНЕЙ КОНФИДЕНЦИАЛЬНОСТИ

Аннотация. В соответствие с развитием цифровой экономики страны увеличиваются потоки информации в ходе финансово-хозяйственной деятельности предприятий, что требует обеспечения требуемого уровня безопасности объектов критической информационной инфраструктуры.

В данной работе рассматривается структура управления информационными потоками на предприятии с учетом уровней конфиденциальности и методов управления. Определены виды и уровни конфиденциальности информации, степень критичности. Приведена краткая классификация информации по уровням конфиденциальности.

В результате исследования с помощью предложенной в данной работе онтологической модели введены основные базовые концепты и их взаимосвязи, которые задействованы в информационных потоках в периметре предприятия и влияющих на оценку критичности информации и/или информационного актива предприятия в целом.

Ключевые слова: защита информации, риск, онтологическая модель управления, степень критичности.

N. I. Glukhov [1], P.N. Nasedkin [1], D.S. Milko [1]

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

ONTOLOGICAL MODEL OF INFORMATION FLOW MANAGEMENT AT THE ENTERPRISE, TAKING INTO ACCOUNT CONFIDENTIALITY LEVELS

Abstract. This article examines the ontological model of information flow management in the enterprise, taking into account the levels of confidentiality and for the first time proposed a general ontology in terms of the main basic concepts and their relationships affecting the determination of the negative consequences and assessment of the criticality of information and/or information asset of the enterprise.

As a result of the study, considered in this work ontological model of information flow management in the enterprise, taking into account the levels of confidentiality can be further laid down in the basis of a comprehensive assessment of information security enterprise and get an aggregate assessment of the effectiveness of information protection at the enterprise.

***Keywords*:** information protection, risk, ontological management model, degree of criticality

Увеличивающиеся потоки информации в ходе финансово-хозяйственной деятельности (ФХД) предприятия являются факторами, которые оказывают значительное влияние на внедрение новых информационных технологий и тем самым определяют основную цель в области информационной безопасности (ИБ), а именно: обеспечение защищенности интересов предприятия от угроз в информационной сфере путем создания условий, препятствующих проявлению неприемлемых рисков. Защищенность предприятия достигается установлением режима коммерческой тайны на предприятии и обеспечением состояния защищенности информационных ресурсов с точки зрения свойств ИБ - конфиденциальности, целостности и доступности информации, а также обеспечением её безотказности и аутентичности.

В настоящее время для достижения основных целей в управлении ФХД и обеспечения ИБ предприятия любого сектора экономики необходимо обеспечить эффективное использование всех его технических, экономических, организационных и социальных ресурсов. В связи с чем, на предприятии разрабатывается и утверждается одна из существующих в настоящее время организационных структур (линейная, функциональная, дивизиональная, либо процессная структура) с учетом основной миссии предприятия.

В результате финансово-хозяйственной деятельности на предприятии выделяют следующие приоритеты в сфере развития ИБ, которые требуют в части себя в условиях конкурентной среды обеспечения управления, их контроля и защиты:

– приоритет защищенности критичных информационных ресурсов (ключевые технологические, производственные и бизнес-процессы);

– приоритет обеспечения мероприятия в области ИБ при внедрении средств автоматизации бизнес-процессов и документооборота предприятия, а также производственных и технологических процессов;

– приоритет обеспечения непрерывного контроля соответствия требованиям законодательства;

– приоритет создания условий для безопасного применения инноваций и прогрессивных технологий (мобильных рабочих мест, виртуализации, облачных технологий и т.п.);

– приоритет формирования и систематического совершенствование политики импортозамещения систем и средств защиты.

В зависимости от форм собственности предприятия, характера обрабатываемой информации, размера и сферы деятельности создаётся корпоративная информационная система, комплексная защита информации которой должна строиться на основе различных законов [1-4] и дополняющих их нормативных документов ФСТЭК [5,6].

Научная новизна работы состоит в том, что впервые предложен подход к определению негативных последствий и категорированию информации по степени критичности с точки зрения построения онтологической модели управления информационными потоками на предприятии с учетом уровней конфиденциальности.

Методы управления. В настоящее время на предприятии выделяются методы управления, которые объединяются в иерархический стек технологий, т.е. обеспечивают обмен информацией с использованием всех уровней управления (рис.1) в рамках технологических процессов предприятия, которые включают:

– Системы промышленной автоматизации в составе автоматизированных систем управления технологическим процессом (далее - АСУ ТП), автоматизированных систем диспетчерского и технологического управления (далее - АСДТУ), автоматизированных информационно-измерительных систем (далее - АИИС). На данном уровне автоматизации диспетчерское управление и сбор информации осуществляется с применением SCADA – систем на основе данных получаемых с измерительного оборудования, исполнительных устройств и программируемых логических контроллеров (ПЛК);

– Управление производством (MES - система управления и оптимизации производственной деятельности предприятия). На данном уровне руководство контролирует весь производственный процесс на предприятии от сырья до готовой продукции. В связи с чем, это позволяет видеть, что происходит, и принимать управленческие решения на основе этой информации, т.е. проводить корректировку заказов на сырье или планов отгрузки на основе реальных данных;

– Финансово-хозяйственное управление (далее - ФХД), т.е. ERP уровень планирования ресурсами предприятия. На данном уровне управления высшее руководство предприятия может видеть и контролировать свою деятельность. ERP обычно представляет собой набор различных компьютерных приложений, которые могут видеть все, что происходит внутри предприятия. Таким образом, данный уровень использует все технологии предыдущих уровней и дополнительно у нему еще несколько программ для достижения этого уровня интеграции. Иными словами, это позволяет иметь возможность контролировать все уровни управления на предприятии от производства до продаж, закупок, финансирования и расчета заработной платы, а также многие другие процессы;

– Уровень стратегии и маркетинга (бизнес-аналитика) на основе BI-платформы для загрузки, очистки и преобразования данных из различных источников и обработки информации (далее - OLAP).

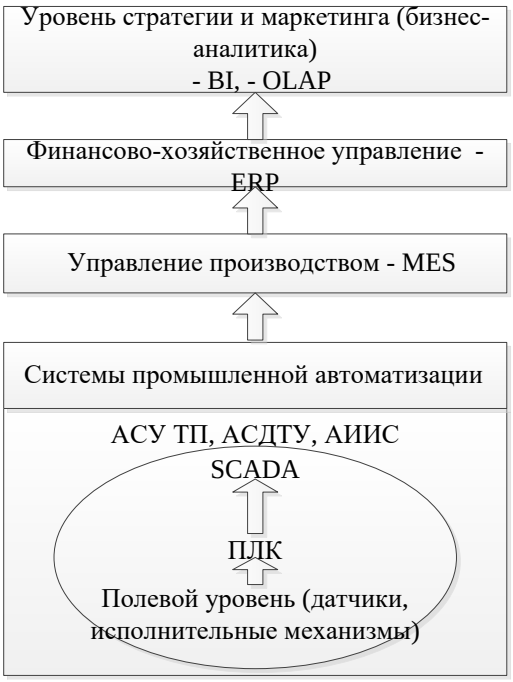

Рис. 1. Уровни управления предприятием в рамках технологических процессов

Информационные потоки. В процессе финансово-хозяйственной деятельности на предприятии и установленного режима коммерческой тайны выделяются следующие информационные потоки:

– информационные потоки, связанные с внешними сетями и системами;

– внутренние информационные потоки АСУ ТП, АСУ ФХД, в том числе системы электронного документооборота (СЭД), а также потоки информации связанные с сервером печати.

К объектам защиты на предприятии, как правило, относят следующие информационные активы (ИА):

– информация, обрабатываемая на предприятии и представленная в электронном виде;

– информационные системы (ИС) и АСУ ФХД, обеспечивающие хранение, обработку и передачу информации бизнес-процессов и находящиеся в собственности или распоряжении предприятия (в отношении которых предприятие может устанавливать требования по защите);

– АСУ ТП, обеспечивающие хранение, обработку и передачу информации технологических и производственных процессов;

– информационно-телекоммуникационные системы (ИТКС);

– средства и системы защиты, обеспечивающие реализацию и контроль требований по информационной безопасности.

В процессе ФХД на предприятии обрабатывается и накапливается информация, характеризующаяся:

1. По виду и уровню конфиденциальности:

– открытая информация:

– информация ограниченного доступа (конфиденциальная информация): информация для служебного пользования, коммерческая тайна, персональные данные, инсайдерская информация.

2. По степени критичности.

Классификация информации по уровням конфиденциальности на предприятии отражается в локальных нормативных документах. Для всех видов информации обрабатываемой на предприятии в рамках управления ИБ обеспечивается защита свойств информации (доступность, целостность и конфиденциальность).

Информации обрабатываемая и хранящаяся на предприятии имеет следующие характеристики:

– открытая информация – информация, разглашение которой не влечёт негативных последствий для предприятия, В связи с чем, требуется только обеспечить доступность и целостность.

– информация для служебного пользования – информация конфиденциальная, которая формируется в структурных подразделениях предприятия и используется в соответствии с утвержденным на предприятии порядком. В связи с чем, требуется обеспечить доступность, целостность, конфиденциальность информации.

– информация, составляющая коммерческую тайну – информация конфиденциальная. Гриф «Коммерческая тайна» присваивается информации при её производстве в соответствии с утвержденными нормативными документами, определяющими перечень сведений, составляющих коммерческую тайну предприятия. В перечень включается информация по направлениям деятельности предприятия в части: управления, планов и научно-технической деятельности, проектов и контрактов, совещаний и переговоров, финансов, рынка, экономики и производства, собственности и корпоративного управления, партнеров и контрагентов, геодезии и картографии, цен, защита информации. Таким образом, требуется обеспечить доступность, целостность, конфиденциальность информации.

– информация, содержащая персональные данные – информация конфиденциальная. Отметка о конфиденциальности присваивается данному виду информации в соответствии с утвержденными нормативными документами, определяющими перечень сведений, составляющих персональные данные предприятия. Требуется обеспечить доступность, целостность, конфиденциальность информации.

– инсайдерская информация – информация, которая может оказать значимое влияние на цены финансовых инструментов предприятия. Требуется обеспечение доступности, целостности, конфиденциальности.

Онтологическая модель управления информационными потоками на предприятии с учетом уровней конфиденциальности (рис.2). В онтологической модели отражены концепты и взаимосвязи, влияющие на определение перечня негативных последствий и оценку степени критичности информации предприятия с помощью которых степень критичности информации для предприятия определяется исходя из [7, 8]:

– ценности информации в целом для предприятия в разрезе вида информации, ограничения доступа к ней;

– потерь и вероятности реализации угроз.

Негативные последствия для предприятия определяются из взаимосвязи составляющих его элементов (систем, процессов), влияющих на определение возможного ущерба через оценку рисков ИБ для каждого информационного актива предприятия, являющегося объектом защиты. В рамках деятельности предприятия по реализации системы управления ИБ (СУИБ) оценка рисков ИБ должна включать в себя:

– идентификацию информации и объектов защиты, их ценности для целей и задач деятельности;

– оценку величины риска ИБ на основе анализа ценности информации и объектов защиты, моделей угроз безопасности информации и нарушителей ИБ предприятия. Величина риска ИБ при этом зависит от ценности информации и/или информационного актива, вероятности реализации угрозы безопасности, уязвимости, коэффициентов (конфиденциальность, целостность, доступность, разрушительность), частоты возникновения за фиксированный

промежуток времени неблагоприятного события и эффективности существующих или планируемых мер защиты;

– определение характеристик рисков ИБ информации и/или объектов защиты.

Таким образом, в результате определения негативных последствий и оценки степени критичности информации для предприятия в работе проведен анализ критичности информации и/или объекта защиты для ФХД предприятия и предъявляемых к нему базовых требований, а также наличия актуальных угроз безопасности и уязвимостей.

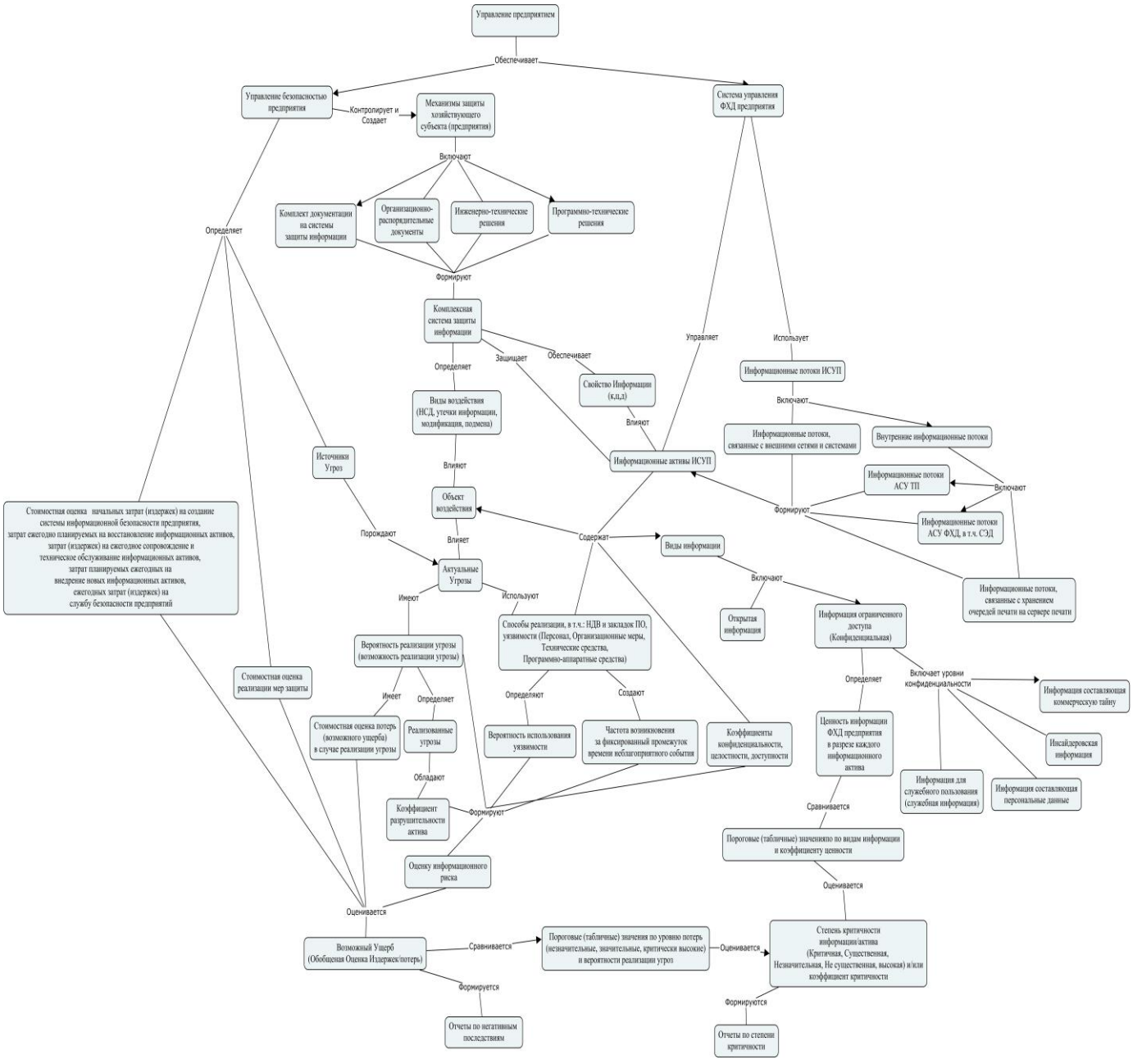

Рис. 2. Онтологическая модель управления информационными потоками на предприятии с учетом уровней конфиденциальности

Заключение. В результате исследования рассмотренная в данной работе онтологическая модель управления информационными потоками на предприятии с учетом уровней конфиденциальности может быть в дальнейшем положена в основу методики комплексной оценки информационной безопасности предприятия и получения агрегированных оценок эффективности защиты информации на предприятии, как это предлагается в работах [9-11].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 29.04.2004 № 98-ФЗ «О коммерческой тайне».

2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

4. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

5. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

6. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при из обработке в информационных системах персональных данных».

7. Глухов Н.И. Оценка информационных рисков предприятия: учебное пособие. – Иркутск: - Иркутск: ИрГУПС, 2013. – 148 с.

8. ISO/IEC TR 13335 Information technology – Guidelines for the management of IT Security (Информационная технология. Методы безопасности. Руководство по управлению безопасностью).

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

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

11. 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.

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

13. 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. Federal Law No. 98-FZ of 29.04.2004 «O kommrcheskoy tayne» [«On Commercial Secrets»].

2. Federal Law No. 149-FZ dated 27.07.2006 «O Informazii, Informazionyh Technologiah i ozachite informazii» [«On Information, Information Technologies and Information Protection»].

3. Federal Law dated 27.07.2006 No. 152-FZ «O personalnyh dannyh [«On Personal Data»].

4. Federal Law No. 187-FZ of 26.07.2017 «O bezopasnoti kriyicheskoy informazionnoy infrastructury Rossiyskoy Federazii» [«On Security of Critical Information Infrastructure of the Russian Federation»].

5. Order of the FSTEC of Russia No. 17 dated 11.02.2013 «Ob utverzhdenii Trebovaniy o zashite informatsii, ne sostavlayushei gosudarstvennuyu tainu, soderzhasheisya v gosudarstvennih informatsiohnnyh sistemah» [*«On Approval of the Requirements for the Protection of information that does not constitute a State secret contained in State Information Systems»*].

6. Order of the FSTEC of Russia No. 21 of 18.02.2013 «Ob utverzhdenii Sostava i soderzhaniya organizatsionnyh i technicheskih mer po obespecheniyu bezopasnosti personalnih dannih pri ih obrabotke v informatsionnyh sistemah personalbyh dannyh» [*«On approval of the Composition and content of organi-*

zational and technical measures to ensure the security of personal data during their processing in personal data information systems»].

7. Glukhov N.I. Otsenka informazionnyh riskov predriatia: a textbook [Assessment of information risks of the enterprise]/Irkutsk: IrGUPS, 2013. - 148 pp.

8. ISO/IEC TR 13335 Information technology - Guidelines for the management of IT security.

9. Arshinskiy, L.V. Logiko-aksiologicheskiy podhod r otsenke sostoyania system [Logical-axiological approach to the systems state estimation (in Russian)] // So-time technologies. System analysis. Modeling. Irkutsk: IrGUPS. 2013. № 3(39). pp. 140-146.

10.Arshinskiy, L.V. Metodika agregirovannogo otsenivania system s podderzhekoy klyuchevih komponentov [A technique of the aggregate estimation of the systems with the key components support] // Design ontology. 2015. T. 5. № 2 (16). pp. 223-232.

11. Arshinskiy V.L., Arshinskiy L.V., Dorzhsuren H. Otsenka kachestva fukzionirovanya stanzii Ulan-Batorskoy xhelexnoy dorogi na osnove ontologicheskogo I produktivnogo modelirovanya [Quality estimation of Ulan Bator railroad station functioning on the basis of ontological and production modeling]// Modern high technology, 2018, ¹ 5. pp. 16-20.

12. Konev, A.A. Podhod k opisanyu strucruty sistemi zachity infirmazii [Approach to the information protection system structure description] / A.A. Konev, E.M. Davydova // TUSUR reports. - – 2013. - – № 2(28). - – pp. 107–111.

13. Shangin V. F. Kompeksnaya zachita informazii v korporativnyh sistemah: a training manual [Comprehensive protection of information in corporate systems]/ Moscow: Forum, Infra-M, 2010. 592 p.ISBN 978-5-16-003746-2.

Информация об авторах

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

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

Милько Дмитрий Сергеевич - аспирант кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск,e-mail: dmitry.s.milko@gmail.com

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 Nasedkin - Postgraduate student, Department of Information Systems, Irkutsk State University of Railways, Irkutsk, e-mail: nasedkin_pn@irgups.ru.

Dmitry Milko - Postgraduate student, Department of Information Systems, Irkutsk State University of Railways, Irkutsk, e-mail: dmitry.s.milko@gmail.com

Для цитирования

Глухов Н.И., Наседкин П.Н., Милько Д.С. Онтологическая модель управления информационными потоками на предприятии с учетом уровней конфиденциальности // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2021. – №3(11). – С. 59-66 – DOI: 10.26731/2658-3704.2021.3(11).59-66 – Режим доступа: http://ismm-irgups.ru/toma/311-2021, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 01.09.2021)

For citation

Glukhov, N.I.; Nasedkin, P.N., Milko D.S. Ontological model of information flow management in the enterprise, taking into account the levels of confidentiality [Ontologicheskaya model upravlenia informazionnimi potokami na predpriiyatii s uchetom urovnia konfidenzialnosty] // 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], 2021. No. 3(11). P. 59-66. DOI: 10.26731/2658-3704.2021.3(11).59-66. [Accessed 01/09/21]