УДК 338.3

ОРГАНИЗАЦИОННО-ЭКОНОМИЧЕСКИЕ РИСКИ ВНЕДРЕНИЯ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

ORGANIZATIONAL AND ECONOMIC RISKS OF INTRODUCTION OF INFORMATION SECURITY SYSTEMS OF THE ENTERPRISE

В.В. ФИЛАТОВ, В.Ю. МИШАКОВ, Н.П. РОДИНОВА, В.М. ОСТРОУХОВ, И.В. ПОЛОЖЕНЦЕВА, Х.Г. АХМЕДОВА

V.V. FILATOV, V.YU. MISHAKOV, N.P. RODINOVA, V.M. OSTROUKHOV, I.V. POLOZHENTSEVA, KH.G. AKHMEDOVA

(Российский экономический университет имени Г.В. Плеханова, Российский государственный университет имени А.Н. Косыгина (Технологии. Дизайн. Искусство), Московский государственный университет технологий и управления им. К.Г. Разумовского)

(Russian University of Economics+ named after G.V. Plekhanov, Russian State University named after A.N. Kosygin (Technologies. Design. Art), Moscow State University of Technologies and Management named after K.G. Razumovsky)

E-mail: filatov_vl@mail.ru; mishakovviktor@yandex.ru; naduxa57@mail.ru; ovmvmo56@yandex.ru; vip-perh@yandex.ru; htanya21@yandex.ru

Обеспечение безопасности информации, циркулирующей на предприятии, а также между предприятиями и государственными учреждениями – одна из составных частей информационной безопасности государства, в частности, и национальной безопасности государства в целом.

Целью работы является конкретизация отдельных подходов менеджмента информационной безопасности на предприятии с учетом организационных, технологических, технических, правовых и экономических факторов. Для достижения поставленной цели необходимо решить следующие задачи: проанализировать теоретические аспекты возможных угроз при потере коммерческой и технологической информации, а также рассмотреть положения комплекса менеджмента управления информационной безопасностью в текущей деятельности руководителя.

Security of information circulating in the enterprise, and between enterprises and public institutions is one of the components of information security in particular and national security in general. The purpose of the work is to specify individual approaches to information security management at the enterprise, taking into account organizational, technological, technical, legal and economic factors. To achieve this goal, it is necessary to solve the following tasks: to analyze the theoretical aspects of possible threats to the loss of commercial and technological information, as well as to consider the provisions of the complex management of information security management in the current activities of the head.

Ключевые слова: информационная безопасность, предприятие, менеджмент, организационно-экономическое обеспечение.

Keywords: information security, enterprise, management, organizational and economic support.

Проблемы информационной безопасности (ИБ) связаны с необходимостью защиты формируемого массива всесторонней информации о различных аспектах хозяйствования, разглашение которого может привести к коммерческим потерям различного рода (включая имиджевые). Конфиденциальная информация может быть как коммерческой, так и технологической и похищение или повреждение ее возможно различными способами. Важной проблемой при этом является осознание системы угроз, которые формируются, нарастают, трансформируются. Именно система угроз и формирует причины развития менеджмента информационной безопасности [1].

Проблемы информационной безопасности становятся первостепенными с учетом следующих факторов [2]:

- несовершенство международных стандартов и законодательной базы, обеспечивающих необходимый уровень защиты информации;
- создание единого информационного пространства, которое не обеспечивает достаточного уровня информационной безопасности.

Целью работы является анализ рисков внедрения систем информационной безопасности предприятия с учетом организационных, технологических, технических, правовых и экономических факторов. Для достижения поставленной цели необходимо решить следующие задачи: проанализировать теоретические аспекты возможных угроз при потере коммерческой и технологической информации, а также рассмотреть положения комплекса менеджмента управления информационной безопасностью в текущей деятельности руководителя.

В последние годы решению проблем информационной безопасности посвящены работы школ ряда научных направлений – по разработке информационных технологий, программных продуктов, в том числе и защитного плана, по разработке компьютерного оборудования, по обоснованию правовых основ, а также по реализации организационно-управленческих систем, имеющих целью – обеспечение информационной безопасности бизнеса (для любой организации по масштабам, подчиненности, расположению).

Известны работы Мельникова В.П.[3], Уткина В.Б. [4], Гафнер В.В. [5], Исаева Г.Н. [6] , Тарасова А.В. [7], Слиньковой И.П. [8], Шаньгина В.Ф. [9] и других ученых. Следует отметить, что значительное число разработок имеют техническую направленность и вследствие этого реализуются специальным персоналом по информационному сопровождению бизнеса. Кроме того, несмотря на растущее внимание к исследованиям в области информационной безопасности, вопросы управления процессом обеспечения информационной безопасности промышленных предприятий и коммерческих организаций не получили всестороннего исследования.

Вопросу оценки эффективности инвестиций в информационную безопасность посвящены работы российских ученых Абрамова М.А. [10], Родиной Ю.В. [11], Кострова А.В. [12], а также работы зарубежных ученых Heimo C. (2004) [13], R. Anderson (2008) [14], Ian Brown (2009) [15], Evered Rob (2010) [16], Carty Matt (2012) [17], Moltedo A.(2014) [18], Jim Breithaupt (2014) [19], Malcolm W. Harkins (2016) [20], в которых отражаются различные решения задачи оценки затрат на информационную безопасность с точки зрения ее эффективности. Однако проблема оценки затрат в информационную безопасность до сих пор не решена и является актуальной.

Обеспечение безопасности информации, циркулирующей на предприятии, а также между предприятиями и государственными учреждениями – одна из составных частей информационной безопасности государства, в частности, и национальной безопасности государства в целом [1].

В нашей стране ежегодно выносится около полусотни приговоров инсайдерам, которые передают персональные данные конкретных лиц заказчикам, обычно найденным через сеть. Однако ни спрос, ни предложение меньше не становятся – убедиться в этом можно, набрав запрос в любой поисковой системе [21].

В России допустившие утечку организации чаще всего рискуют только потерей репутации и, как следствие, возможным оттоком клиентов и снижением дохода. За рубежом же компаниям грозят не только скандалы, но и крупные штрафы. К примеру, в новом GDPR (Общий регламент по защите данных ЕС) для тех, кто нарушил правила обработки и хранения персональных данных, предусмотрены серьезные санкции – до 20 млн. евро или 4% дохода на мировом рынке за год [22].

Волноваться по поводу информационной безопасности стоит не только крупным корпорациям. В Verizon Data Breach Investigations Report 2019 были проанализированы более 40 тыс. сообщений об утечках данных из 86 стран мира. Выяснилось, что в 43% случаев жертвами становились предприятия малого бизнеса [23].

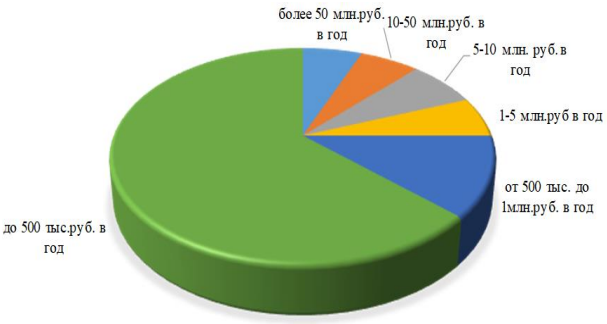

Рис. 1

Наиболее интересной оказалась статистика по размерам бюджетов, выделяемых на информационную безопасность в опрошенных российских организациях. В 63% компаний на ИБ выделяется минимальный бюджет — до 500 тыс. руб. в год, рис. 1 (размер бюджета на информационную безопасность в год [24]). Еще 12% опрошенных имеют годовой бюджет от 500 тыс. до 1 млн. руб. в год. Только 12% респондентов могут похвастаться бюджетом на ИБ более 10 млн. руб. в год. Из них лишь 6% крупных компаний имеют бюджет на ИБ более 50 млн. руб. в год. 7% опрошенных располагают бюджетом от 5 до 10 млн. руб. в год, и еще 6% — бюджетом от 1 до 5 млн. руб. в год [24].

Как видно, у подавляющего числа российских компаний на информационную безопасность выделяются минимальные бюджеты, которых может хватить лишь на базовые средства защиты (такие, как антивирусы или межсетевые экраны) [25].

В результате приоритетных направлений развития ИБ оказалось несколько, см. рис. 2 (приоритетные направления развития информационной безопасности [25]). В равной мере для опрошенных организаций оказались актуальны задачи защиты от внутренних угроз (включая утечки информации), автоматизации процесса управления ИБ, защиты периметра и создания SOC (центров оперативного мониторинга, анализа и реагирования на инциденты) [26].

Рис. 2

Оценивая названные угрозы информационной безопасности, можно признать, что в основе формирования их лежат объективные физиологические и психологические закономерности (механизмы) – человек часто не выполняет правила (в рассматриваемом случае относительно сохранения информации) в связи с тем, что их исполнение требует систематически выполнять предписанные повторяющиеся действия, операции, имеющие для человека при многократном повторении рутинный, сниженный по остроте восприятия характер. А если в процессе работы человек не выполнил требуемую процедуру и ничего не произошло (нет отрицательного результата, нет явного проявления недовольства со стороны контролирующих систем, нет нарушения собственно процесса работы), то возникает переоценка значения распоряжений по выполнению регламентов, формируется облегченное отношение

к регламентам. И именно такое восприятие определяет психологическую установку работника к нарушениям нужных для регулятора действий – "я это делаю или не делаю, ничего ведь страшного не происходит, значит, ничего плохого я не совершаю". По отношению к менеджменту информационной безопасности эта особенная трансформация установок работников создает угрозы в силу того, что сложно поддается контролю, поскольку лежит в плоскости внутренних оценок и мотивов и может быть преодолен лишь в результате специальных систем регулирования поведения (предупредительные, разъяснительные меры, поощрение за строгое соблюдение правил и наказание при нарушении правил деятельности любого уровня опасности, выявление повторяемости нарушений и др.) и систематических комплексных проверок.

Злоумышленники-инсайдеры используют для кражи информации несколько основных каналов. И для защиты каждого из них есть технические решения, которые позволяют предотвратить утечки или, как минимум, найти и наказать виновного [27].

1. Съемные носители. Самый простой способ пресечь копирование на диск – заблокировать USB-порты. Но часто это нереально, так как съемные носители используются в работе. Тогда на помощь приходят программы, которые защищают как от нежелательной записи информации на внешнее устройство, так и от загрузки с него посторонних файлов. Например, мониторинг активности пользователей (UAM) – позволяет контролировать трафик и события в Сети, останавливать подозрительные операции и сообщать в службу безопасности о нарушениях. С помощью IDS/IPS-систем можно засечь запуск вредоносных программ и удалить зараженные файлы, а средства DRM и IRM ограничивают использование файлов, в том числе их копирование.

Также в борьбе с нежелательными операциями внутри Сети полезны DLP-сервисы. Они анализируют информацию внутри корпоративной системы, буквально узнавая секретные документы "в лицо". Для этого программа проверяет наличие в файле определенных слов, меток, таблиц или изображений (например, фотографий паспортов клиентов). Если они обнаружены, документ считается конфиденциальным, и DLP-система блокирует опасные действия с ним.

2. Бумажные копии и фотографии экранов. С помощью технологии ILD после ее установки при каждом открытии файла в корпоративной системе или отправке его на печать программа создает уникальную копию документа (всего существует более 205 триллионов комбинаций страницы А4). Изменения незаметны человеческому глазу, но затрагивают каждый элемент на странице. Получается, что каждый сотрудник всегда работает со своей личной версией документа. И если этот документ однажды всплывет в даркнете или просто обнаружится в неположенном месте, то ILD-система легко определит "слабое звено". Исправлять или рвать бумагу бесполезно. Программе хватит клочка с парой слов, чтобы указать на нарушителя.

3. Облачные хранилища. Специальные сервисы позволяют просто обмениваться информацией с коллегами и партнерами. Работают они со всеми популярными форматами, включая pdf, текстовые и графические файлы, таблицы и презентации, для загружаемых данных можно устанавливать различные уровни доступа. На страже информации стоит та же технология ILD. Когда онлайн-пользователь обращается к документу, алгоритм создает его уникальную копию, число которых неограничено. И в случае проблем службе безопасности будет легко установить, через кого из сотрудников, имевших доступ к хранилищу, произошла утечка.

В реальной жизни преступники обычно используют самые простые средства и человеческие слабости, а потому противостоять им можно и нужно. Перечисленные технические решения, грамотная политика безопасности и обучение сотрудников помогают предотвратить большую часть утечек персональных данных и сберечь репутацию и деньги компании.

Далее проанализируем организационно-экономические риски внедрения систем информационной безопасности предприятия.

1. Автоматизация без оптимизации. Проект автоматизации начинается с правильной постановки задач управления. Все автоматизируемые бизнес-процессы рассматриваются, согласуются с бизнес-моделью предприятия, затем рассматривается возможность автоматизации. Все процессы и функции производства, подлежащие автоматизации, описываются и формализуются. Это может привести к необходимости реорганизации структуры и методов деятельности [28].

2. Приоритет одной службы. Службы IT, департамент развития, технологи. Любая служба может быть драйвером проекта, но ни одна из них не должна получить приоритет в решениях по автоматизации.

3. Компьютеризация вместо автоматизации. Попытка перенести алгоритм неавтоматизированных операций в новую систему. Возможности новых IT-систем превосходят способность организаций осваивать новые методы работы.

4. Измеримые показатели. Цели подкрепляются метриками, уровни по которым отображают прогресс в достижении показателей. Трудно развивать то, что не измеряется.

5. Снижение производительности на период освоения. Новые инструменты требуют сил и времени на освоение. Некоторое время придется поддерживать старую и новую систему параллельно. Резервируйте время на обучение и оптимизацию.

6. Начинать с планирования. Многие заказчики, зная о сложности планирования и постоянном срыве планов, пытаются развивать IT-системы с автоматизации планирования. Не имея достоверной картины происходящего и реальных норм – составить реальный план невозможно.

7. Комплексная автоматизация. Комплексное внедрение может быть успешным только на новых предприятиях. На действующих предприятиях автоматизация любого действия (даже провальная) приводит к изменению всех значимых факторов. Изменяется видение, ресурсы, навыки, взаимоотношения с подрядчиками, навыки персонала, время реакции, требования к инфраструктуре, смещаются узкие места и базис оценки. Невнимательные последователи по семь лет разрабатывают концепцию внедрения Manufacturing Execution System, вкладывая средства в детализацию своих иллюзий [29].

8. Реструктурирование предприятия. Внедрение начинается с полного обследования всех аспектов деятельности предприятия. Формируется заключение. Описываются бизнес-процессы. Под них формируются алгоритмы. Инфраструктура и функционал приводятся в соответствие с алгоритмами работы. Формализуются необходимые изменения, необходимые до внедрения (кто примет обязательные роли, например), во время внедрения, на переходный период, по итогам внедрения. Это приведет к необходимости введения новых субъектов деятельности и ликвидации или ограничению полномочий некоторых из старых [30].

9. Реорганизация деятельности предприятия. Подразделения и участки, затронутые автоматизацией (это не только владельцы систем, а и смежники), придется реорганизовать. Сохраняем полезные наработки и достижения. Изменяем только там, где можно упростить. Предусматриваем резервы во избежание "авралов".

Чтобы хеджировать риски внедрения систем информационной безопасности предприятия, необходимо учитывать следующие риски, исходящие от персонала.

1. Временное увеличение нагрузки. На период тестирования и настройки системы нагрузка на персонал может возрасти. При задаче поддержки двух систем персонал обычно сохраняет старые методы работы, относя новые к фоновым и второстепенным – отрицая новые методы, обозначая их как причину срыва производственных планов.

2. Нормативные документы. Есть обязательные законы и нормативы, ограничивающие применение современных средств и технологий автоматизации.

3. Стремление автоматизировать вчерашний день. Предусматриваем функционал, покрывающий текущие задачи, и задачи развития.

4. Кастомизация. Готовые модули должны решать 80% задач. Кастомизация только в крайних случаях.

5. Фрагментарное рассмотрение ресурсов. Отсутствие оценки полной стоимости IT-решений. Заказчик может не видеть "подводных камней", а исполнитель избегает указывать на них при заключении сделки.

6. Игнорирование рисков. Этому посвящено содержание статьи. Рассматривайте не только выгоды, а и возможные жертвы на пути к успеху.

7. Масштабирование ошибок. Перекладывая действия на АСУП, надо смоделировать развитие ошибок. Люди все еще лучше роботов оценивают адекватность команд.

8. Необеспеченная автономность. Насколько работоспособна АСУП при неработоспособности отдельных систем. Manufacturing Execution System обязана продолжить работу, даже когда ERP-система "лежит на боку". Эта обязанность прописана в стандарте.

9. Несогласованность с исполнителем. Подрядчик, отрицающий риски или считающий все запросы выполнимыми – не до конца понимает задачу.

10. Формирование группы по автоматизации. Рабочая комиссия должна включать экспертную группу, группу внедрения, возглавляться представителем высшего руководства и формироваться приказом по предприятию, утверждающим состав группы, основные задачи, порядок работы группы, контрольные показатели, периодичность отчетности и контроля.

11. Опора на внешние компетенции. Нужны специалисты, оперативно решающие рабочие вопросы настройки и эксплуатации АСУП. Обучать своих сотрудников дешевле аутсорсинга. Есть и другие мотивы накапливать компетенции на стороне эксплуатации.

12. Потеря ключевых специалистов. Увольнение любого сотрудника не должно остановить развитие АСУП.

13. Упущения планирования поддержки и сопровождения. Многие сервисы (особенно зарубежные) переходят на схему по подписке. Лучше предварительно представлять условия поддержки, гарантии, обновления, доработки, расширения, интеграции системы.

14. Неполный функционал. Система должна закрывать некий участок IT-ландшафта полностью и иметь бесшовную интеграцию со смежными системами. Упущения вынудят допустить сопутствующее существование неконтролируемых дополнений или приведут к отказу от использования системы.

15. Обновления с разрывом целостности данных. Политика обновлений должна предусматривать щадящее продление лицензий и комфортный регламент обновлений.

16. Незамкнутый информационный контур. Система должна учитывать все ресурсы и все операции, ни одно их отклонений не должно вызывать пробелов в информации.

17. Недостаточность механизмов контроля. Встроенные в систему возможности запроса на подтверждение, подключение автоматических механизмов контроля, замера и сравнения технологических параметров с плановыми и нормативными.

18. Недостаточная скорость работы. Реакция системы для управления производством должна соответствовать скорости техпроцесса и превосходить скорость неавтоматизированной работы.

19. Нецелостность данных. АСУП не должна позволять правку данных о производстве задним числом. Исправление ошибочных параметров должно приводить к автоматическому их обновлению во всех частях системы. Данные, собираемые человеком, должны сопоставляться с данными из других источников.

В Ы В О Д Ы

Оценивая названные угрозы информационной безопасности, можно признать, что

в основе формирования их лежат объективные физиологические и психологические закономерности (механизмы) – человек часто не выполняет правила (в рассматриваемом случае относительно сохранения информации) в связи с тем, что их исполнение требует систематически выполнять предписанные повторяющиеся действия, операции, имеющие для человека при многократном повторении рутинный, сниженный по остроте восприятия характер. А если в процессе работы человек не выполнил требуемую процедуру и ничего не произошло (нет отрицательного результата, нет явного проявления недовольства со стороны контролирующих систем, нет нарушения собственно процесса работы), то возникает переоценка значения распоряжений по выполнению регламентов, формируется облегченное отношение к регламентам.

ЛИТЕРАТУРА

1. *Zinchuk G.M., Anokhina M.Y., Yashkin A.V., Petrovskaya S.A.* Food security of Russia in the context of import substitution // European Research Studies Journal. – 2017. Т. 20, № 3. С. 371...382.

2. *Ветрова Н.М., Гайсарова А.А.* Особенности менеджмента информационной безопасности на современном этапе // Экономика строительства и природопользования. – 2017, №1(2). С. 64...80.

3. *Мельников В.П., Клейменов С.А., Петраков А.М.* Информационная безопасность и защита информации / Под ред. С.А. Клейменова. – М.: Изд-во "Академия", 2008.

4. *Балдин К.В., Уткин В.Б.* Информационные системы в экономике. – М.: Издательско-торговая корпорация "Дашков и Ко", 2006.

5. *Гафнер В.В.* Информационная безопасность. – Ростов н/Д: Феникс, 2010.

6. *Исаев Г.Н.* Информационные системы в экономике. – 6-е изд.. – М.: Изд-во "Омега-Л", 2013.

7. *Тарасов А.В.* Управление промышленным предприятием на основе формирования эффективной системы информационной безопасности: Дис... канд. эконом. наук. – Орел: ОГТУ, 2006.

8. *Петров С.В., Слинькова И.П., Гафнер В.В.* Информационная безопасность. – М.: АРТА, 2012.

9. *Шаньгин В.Ф.* Информационная безопасность компьютерных систем и сетей. – М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013.

10. *Абрамов М.А.* Стандарты в области информационной безопасности необходимы в управлении организацией // Стандарты и качество. – 2011, № 1 (883). С. 42...46.

11. *Рудакова О.С., Родина Ю.В.* Анализ угроз информационной безопасности кредитных организаций // Национальные интересы: приоритеты и безопасность. –2009, №23 (56). С. 61...67.

12. *Костров А.В.* Основы информационного менеджмента. – М.: Финансы и статистика, 2001.

13. *Heimo C.* Policy foundation review. GMF-Global Monitoring for Food Security. – 2004. From http://www.gmfs.info/uk/publications/documents/C1_av2.3.pdf. Viewed April 12, 2017

14. *R. Anderson et al.* (2008), Security Economics and European policy, Proceedings of the Workshop on Economics and Information Security, at http://weis2008.econinfosec.org/papers/MooreSecurity.pdf

15. *Ian Brown, Lilian Edwards and Chris Marsden.* (2009), Information security and cybercrime, https://www.researchgate.net/publication/228226770

16. *Evered Rob and Jerzy Rub.* (2010). "Maintaining Information Security while Allowing Personal Hand-held Devices in the Enterprise." Intel Corporation. http://www.intel.com/ Assets/PDF/whitepaper/ Maintaining_Info_Security_Allowing_Personal_Hand_Held_Devices_Enterprise.pdf

17. *Carty Matt, Vincent Pimont and David W. Schmid*. (2012). "Measuring the Value of Information Security Investments." Intel Corporation. http://www.intel.com/content/dam/www/public/us/en/documents/best-practices/information-securityinvestments-paper.pdf

18. *Moltedo A., Troubat N., Lokshin M., & Saja Z.* (2014). Analysing food security using household survey data. Washington DC: World Bank.

19. *Mark S. Merkow, Jim Breithaupt.* (2014) Information Security: Principles and Practices Second Edition, 800 East 96th Street, Indianapolis, Indiana 46240 USA, p.349.

20. *Malcolm W. Harkins.* (2016) Managing Risk and Information Security: Protect to Enable. Folsom, California, USA, p.208

21. Число утечек из муниципальных организаций // https://www.infowatch.ru/analytics/digest/15364

22. Главные утечки 2018 года // https://www.infowatch.ru/analytics/digest/15203

23. *Шабанов И.* Анализ рынка информационной безопасности в России. Часть 1 //Источник: https://www.anti-malware.ru/analytics/Market_Analysis/analysis-information-security-market-russia-part-1

24. *Шабанов И.* Анализ рынка информационной безопасности в России Источник: https://www.anti-malware.ru/analytics/Market_Analysis/analysis-information-security-market-russia-part-3

25. *Филатов В.В., Кудрявцев В.В., Родина Е.Е., Пащук С.М.* Организационно-экономические меры по защите предприятия от промышленного шпионажа и фишинговых атак // Проблемы правовой и технической защиты информации. – 2019 № 7. С.109...112.

26. *Родина Е.Е., Филатов В.В., Кудрявцев В.В., Притчина А.А* . Теоретико-методологические подхо-

ды к определению понятия "инвестиционная безопасность" // Проблемы правовой и технической защиты информации. – 2019, № 7. С. 99...102.

27. *Сергей Войнов.* Почему утекают персональные данные клиентов и как их защитить. IT-менеджмент. https://www.e-xecutive.ru/management/itforbusiness/1991577-kak-utekaut-personalnye-dannye-klientov-i-kak-ih-zaschitit?utm_campaign=2175&utm_medium=menedzhment&utm_source=email

28. *Рудакова О.С., Родина Ю.В.* Анализ угроз информационной безопасности кредитных организаций // Национальные интересы: приоритеты и безопасность. – 2009, №23 (56). С. 61...67.

29. *Zaitseva N.A., Filatov V.V., Larionova A.A., Rodina E.E., Makarova L.M., Palastina I.P., Hramchenko A.A.* Project management of revitalization of urban areas through the creation of industrial parks // Modern Journal of Language Teaching Methods. – V.8, №12. 2018. P. 284…297.

30. *Тарасов А.В.* Политика информационной безопасности предприятия как основа управления информационной безопасностью // Современные аспекты экономики. – 2006, № 17 (110). С. 45...50.

R E F E R E N C E S

1. Zinchuk G.M., Anokhina M.Y., Yashkin A.V., Petrovskaya S.A. Food security of Russia in the context of import substitution // European Research Studies Journal. – 2017. T. 20, № 3. S. 371...382.

2. Vetrova N.M., Gaysarova A.A. Osobennosti menedzhmenta informatsionnoy bezopasnosti na sovremennom etape // Ekonomika stroitel'stva i prirodopol'zovaniya. – 2017, №1(2). S. 64...80.

3. Mel'nikov V.P., Kleymenov S.A., Petrakov A.M. Informatsionnaya bezopasnost' i zashchita informatsii / Pod red. S.A. Kleymenova. – M.: Izd-vo "Akademiya", 2008.

4. Baldin K.V., Utkin V.B. Informatsionnye sistemy v ekonomike. – M.: Izdatel'sko-torgovaya korporatsiya "Dashkov i Ko", 2006.

5. Gafner V.V. Informatsionnaya bezopasnost'. – Rostov n/D: Feniks, 2010.

6. Isaev G.N. Informatsionnye sistemy v ekonomike. – 6-e izd.. – M.: Izd-vo "Omega-L", 2013.

7. Tarasov A.V. Upravlenie promyshlennym predpriyatiem na osnove formirovaniya effektivnoy sistemy informatsionnoy bezopasnosti: Dis... kand. ekonom. nauk. – Orel: OGTU, 2006.

8. Petrov S.V., Slin'kova I.P., Gafner V.V. Informatsionnaya bezopasnost'. – M.: ARTA, 2012.

9. Shan'gin V.F. Informatsionnaya bezopasnost' komp'yuternykh sistem i setey. – M.: ID FO-RUM, NITs INFRA-M, 2013.

10. Abramov M.A. Standarty v oblasti informatsionnoy bezopasnosti neobkhodimy v upravlenii organizatsiey // Standarty i kachestvo. – 2011, № 1 (883). S. 42...46.

11. Rudakova O.S., Rodina Yu.V. Analiz ugroz informatsionnoy bezopasnosti kreditnykh organizatsiy // Natsional'nye interesy: prioritety i bezopasnost'. – 2009, №23 (56). S. 61...67.

12. Kostrov A.V. Osnovy informatsionnogo menedzhmenta. – M.: Finansy i statistika, 2001.

13. Heimo C. Policy foundation review. GMF-Global Monitoring for Food Security. – 2004. From http://www.gmfs.info/uk/publications/documents/C1_av2.3.pdf. Viewed April 12, 2017

14. R. Anderson et al. (2008), Security Economics and European policy, Proceedings of the Workshop on Economics and Information Security, at http://weis2008.econinfosec.org/papers/MooreSecurity.pdf

15. Ian Brown, Lilian Edwards and Chris Marsden. (2009), Information security and cyber-crime, https://www.researchgate.net/publication/228226770

16. Evered Rob and Jerzy Rub. (2010). "Maintaining Information Security while Allowing Personal Hand-held Devices in the Enterprise." Intel Corporation. http://www.intel.com/ As-sets/PDF/whitepaper/Maintaining_Info_Security_Allowing_Personal_Hand_Held_Devices_Enterprise.pdf

17. Carty Matt, Vincent Pimont and David W. Schmid. (2012). "Measuring the Value of Information Security Investments." Intel Corporation. http://www.intel.com/content/dam/www/public/us/en/documents/best-practices/information-securityinvestments-paper.pdf

18. Moltedo A., Troubat N., Lokshin M., & Saja Z. (2014). Analysing food security using household survey data. Washington DC: World Bank.

19. Mark S. Merkow, Jim Breithaupt. (2014) Information Security: Principles and Practices Second Edition, 800 East 96th Street, Indianapolis, Indiana 46240 USA, r.349.

20. Malcolm W. Harkins. (2016) Managing Risk and Information Security: Protect to Enable. Folsom, California, USA, r.208

21. Chislo utechek iz munitsipal'nykh organizatsiy // https://www.infowatch.ru/analytics/digest/15364

22. Glavnye utechki 2018 goda // https://www.infowatch.ru/analytics/digest/15203

23. Shabanov I. Analiz rynka informatsionnoy bezopasnosti v Rossii. Chast' 1 //Istochnik: https://www.anti-malware.ru/analytics/Market_Analysis/analysis-information-security-market-russia-part-1

24. Shabanov I. Analiz rynka informatsionnoy bezopasnosti v Rossii Istochnik: https://www.anti-malware.ru/analytics/Market_Analysis/analysis-information-security-market-russia-part-3

25. Filatov V.V., Kudryavtsev V.V., Rodina E.E., Pashchuk S.M. Organizatsionno-ekonomicheskie mery po zashchite predpriyatiya ot promyshlennogo shpionazha i fishingovykh atak // Problemy pravovoy i tekhnicheskoy zashchity informatsii. – 2019 № 7. S.109...112.

26. Rodina E.E., Filatov V.V., Kudryavtsev V.V., Pritchina A.A. Teoretiko-metodologicheskie podkhody k opredeleniyu ponyatiya "investitsionnaya bezopasnost'" // Problemy pravovoy i tekhnicheskoy zashchity informatsii. – 2019, № 7. S. 99...102.

27. Sergey Voynov. Pochemu utekayut personal'nye dannye klientov i kak ikh zashchitit'. IT-menedzhment. https://www.e-xecutive.ru/management/itforbusiness/1991577-kak-utekaut-personalnye-dannye

klientov-i-kak-ih-zaschitit?utm_campaign=2175&utm_medium=menedzhment&utm_source=email

28. Rudakova O.S., Rodina Yu.V. Analiz ugroz informatsionnoy bezopasnosti kreditnykh organizatsiy // Natsional'nye interesy: prioritety i bezopasnost'. – 2009, №23 (56). S. 61...67.

29. Zaitseva N.A., Filatov V.V., Larionova A.A., Rodina E.E., Makarova L.M., Palastina I.P., Hramchenko A.A. Project management of revitalization of urban areas through the creation of industrial parks // Modern Journal of Language Teaching Methods. – V.8, №12. 2018. P. 284…297.

30. Tarasov A.V. Politika informatsionnoy bezopasnosti predpriyatiya kak osnova upravleniya informatsionnoy bezopasnost'yu // Sovremennye aspekty ekonomiki. – 2006, № 17 (110). S. 45...50.

Рекомендована кафедрой информации и сервиса РГУ имени А.Н. Косыгина. Поступила 20.01.20.