УДК 004.056.53
DOI: http://dx.doi.org/10.21686/1818-4243-2019-3-25-32

А.В. Гаврилов, В.А. Сизов
Российский экономический университет им. Г.В Плеханова, Москва, Россия

Повышение эффективности формирования профессиональных компетенций магистров по направлению «Информационная безопасность» на основе применения CASE-технологий

Цель исследования. *В современных условиях для построения эффективной системы информационной безопасности предприятия требуются специалисты, обладающие соответствующими профессиональными компетенциями и навыками системного подхода при анализе совокупности факторов, оказывающих влияние на состояние информационной безопасности предприятия. Для подготовки такого рода специалистов требуются качественные изменения в содержании учебных дисциплин, основанные на использовании в процессе построения системы информационной безопасности методов и средств системного анализа.*

Существующие в настоящее время подходы в оценке рисков предприятия основаны на формировании реестра его информационных ресурсов, необходимого для дальнейшей обработки рисков. Адекватная оценка стоимости ресурса невозможна без правильного понимания семантики этого ресурса и его роли в реализуемых бизнес-процессах. Современные подходы к вопросу формирования реестра информационных ресурсов предприятия, по мнению авторов, не предлагают эффективной методики выявления ресурсов и оценки их стоимости.

В настоящей работе рассматривается подход, основанный на применении в подготовке магистров по направлению «Информационная безопасность» методики структурно-функционального анализа и CASE-технологий при формировании реестра информационных ресурсов предприятия.

Материалы и методы. *Для формирования реестра информационных ресурсов предприятия предлагается выполнять построение структурно-функциональной модели предприятия с использованием нотации IDEF0. Моделирование бизнес-процессов выполнялось в среде Business Studio компании «Современные технологии управления».*

В качестве примера для анализа рисков рассматривалась деятельность типовой компании IT-индустрии, занимающейся разработкой и внедрением информационных систем управления предприятием.

Результаты. *Методика прошла успешную апробацию в учебном процессе. По мнению авторов статьи, использование данной методики при проведении лабораторных занятий для магистров, обучающихся по направлению «Информационная безопасность» позволило повысить эффективность формирования у обучающихся профессиональных компетенций и, следовательно, в целом, качество обучения.*

Полученные результаты могут быть использованы не только в качестве методики обучения специалистов в области информационной безопасности. Применение рассматриваемой в статье методики формирования реестра информационных ресурсов предприятия в практической деятельности по обеспечению информационной безопасности предприятия позволит повысить обоснованность решений по защите информации предприятия.

Заключение. *В работе предложена методика, позволяющая обосновать выбор основных направлений по защите информации предприятия на основе анализа его бизнес-процессов. Отличительной особенностью методики является использование современных CASE-технологий для принятия решений в области информационной безопасности предприятия.*

Реализация методики позволяет сформировать реестр информационных ресурсов предприятия, включающий оценку вероятного ущерба по каждому ресурсу. Реестр показывает узкие места в организации защиты, на которые следует обратить первоочередное внимание при планировании мероприятий по защите информации. На основе полученных данных можно сформировать обоснованную с экономической точки зрения стратегию и тактику развития системы защиты информации предприятия.

Ключевые слова: *CASE-технологии, IDEF0, защита информации, бизнес-процесс*

Aleksandr V. Gavrilov, Valeriy A. Sizov
Plekhanov Russian University of Economics, Moscow, Russia

Improving the efficiency of the formation of professional competencies Masters in “Information Security” based on the use o CASE-technologies

Purpose of the study. *In modern conditions, building an effective information security system for an enterprise requires specialists with appropriate professional competencies and systems approach skills in analyzing a combination of factors that influence the state of information security of an enterprise. For the preparation of such kind of specialists, qualitative changes in the content of educational disciplines are required, based on the use of methods and means of system analysis in the process of building an information security system.*

The current approaches to assessing the risk of an enterprise are based on the formation of a register of its information resources necessary for the further processing of risks. Adequate assessment of the value of a resource is impossible without a correct understanding of the semantics of this resource and its role in the implemented business processes. Modern approaches to the formation of the register of enterprise information resources, according to the authors, do not offer an effective method of identifying resources and estimating their value.

This paper considers an approach based on the use of structural and functional analysis methods and CASE-technologies in the formation of a register of information resources of the enterprise in the training of masters in the direction of "Information Security".

Materials and methods. *For the formation of the register of enterprise information resources, it is proposed to build a structural-functional enterprise model using the IDEF0 notation. Business process modeling was performed in the Business Studio environment of «Modern Control Technologies».*

As an example for risk analysis, the activities of a typical IT-industry company engaged in the development and implementation of enterprise management information systems were considered.

Results. *The technique was successfully tested in the educational process. According to the authors of the article, the use of this technique in conducting laboratory classes for masters enrolled in the "Information Security" direction has made it possible to increase the efficiency of the formation of professional competencies in students and, consequently, in general, the quality of education.*

The results obtained can be used not only as a training method for specialists in the field of information security. The application of the methodology of forming the register of information resources of an enterprise considered in the article in practical activities to ensure the information security of an enterprise will increase the validity of decisions to protect the information of the enterprise.

Conclusion. *The paper proposes a method to justify the choice of the main directions for the protection of enterprise information based on the analysis of its business processes. A distinctive feature of the technique is the use of modern CASE-technologies for decision-making in the field of enterprise information security.*

The implementation of the methodology allows you to create a register of information resources of the enterprise, including an assessment of the likely damage for each resource. The registry shows the bottlenecks in the organization of protection, which should be given priority when planning measures to protect information. On the basis of the data obtained, it is possible to form a strategy and tactics for developing an enterprise information protection system that is reasonable from an economic point of view.

Keywords: *CASE-technology, IDEF0, information security, business process*

Введение

В современных условиях для построения эффективной системы информационной безопасности предприятия требуются специалисты, обладающие навыками системного подхода при анализе совокупности факторов, оказывающих влияние на состояние информационной безопасности предприятия. Для подготовки такого рода специалистов требуются качественные изменения в содержании учебных дисциплин, основанные на использовании в процессе построения системы информационной безопасности методов и средств системного анализа.

К числу таких методов относится и методика структурно-функционального анализа, базирующаяся, как правило, на широком применении CASE-технологий.

Основой системы информационной безопасности (ИБ) предприятия является процесс управления рисками, направленный на противодействие угрозам и пресечение нарушений ИБ. Процесс управления рисками включает в себя следующие составляющие: описание бизнес-процессов, выявление информационных ресурсов предприятия, выявление степени подверженности предприятия угрозам, которые могут нанести существенный ущерб, планирования мероприятий по минимизации рисков, реализацию мероприятий по минимизации рисков, оценку эффективности системы управления информационной безопасностью.

Существующие в настоящее время подходы в оценке рисков информационной безопасности предприятия основаны на применении стандартов ГОСТ Р ИСО/МЭК 27005-2010 [1], ГОСТ Р ИСО 31000-2010 [2], ISO/IEC 27001-2013 [3], ГОСТ Р ИСО/МЭК 17799-2005 [4]. При оценивании рисков информационной безопасности необходимо сформировать реестр информационных ресурсов предприятия. Реестр информационных ресурсов представляет собой таблицу, содержащую основную информацию обо всех ресурсах, задействованных в бизнес-процессах, которые попадают в область действия системы управления информационной безопасностью предприятия. Составление такой таблицы необходимо для дальнейшей обработки рисков: выбор методов устранения тех или иных угроз, понижения уровня риска.

Трудность при составлении данного документа заключается, с одной стороны, в необходимости учета всех информационных ресурсов предприятия, с другой – в необходимости (для дальнейшей оценки стоимости ресурса) понимания его семантики и роли в реализуемых бизнес-процессах. Так как информационный ресурс зачастую используется несколькими подразделениями и должностными лицами, то существует также вероятность его дублирования (с различными наименованиями) при построении реестра ресурсов. В настоящее существует ряд работ, касающихся методик выявления и оценки рисков информационной безопасности предприятия.

В частности, в работе [5] рассматривается методика оценки рисков информационной безопасности предприятия, один из этапов которой – формирование перечня информационных активов предприятия. К информационным активам авторы относят: программное обеспечение, оборудование, обрабатываемую информацию. Математическое ожидание потерь для каждого риска предлагается рассчитывать, как произведение стоимости информационного актива на вероятность реализации угрозы для данного актива. В статье не описывается способ формирования перечня информационных активов. Приводимый пример расчета стоимости актива рассматривает лишь частный случай, не давая представления об общих

принципах оценки стоимости информационных активов предприятия.

В работах [6-9] предлагаются методики расчета рисков информационной безопасности предприятия. В рамках реализации методики выделяются активы организации, однако способы формирования перечня активов авторами не рассматриваются.

По мнению Е.К. Барановой [10], А.М. Астахова [11] величину возможного ущерба для каждого информационного актива предлагается определять с учетом стоимости активов и тяжести последствий нарушения их безопасности. В работе [10] приводится классификация существующих методик оценки рисков информационной безопасности, рассматриваются программные инструменты для управления рисками ИБ.

В работе [12] рассматривается формализованный подход применения деловых игр для повышения эффективности подготовки магистров по программе «Защита информационного пространства субъектов экономической деятельности», однако не рассматривается вопрос разработки игрового профессионального контента.

Авторами [13] обсуждаются проблемы оценивания рисков с использованием метода оценивания на основе нечеткой логики. В контексте решения задач управления рисками авторами предлагается применять методы структурного анализа и проектирования, однако практическая реализация подхода не рассматривается.

Отличительной особенностью работы [14] является определение понятия риска, а также классификация рисков экономической безопасности предприятия. В статье рассматриваются подходы ПАО «Газпром» к обеспечению экономической безопасности предприятия и управлению финансовыми рисками.

Перечисленные исследования внесли серьезный вклад в развитие и совершенствование методик оценки рисков информационной безопасности предприятия, однако их общим недостатком является отсутствие формальных методов выявления информационных ресурсов предприятия, подлежащих защите. В этой связи представляется весьма актуальной задача разработки эффективных методов формирования перечня информационных ресурсов предприятия.

1. Постановка задачи

В настоящей статье ставится задача разработки методики выявления и экономического обоснования основных направлений развития системы защиты информации предприятия, основанной на анализе модели его бизнес-процессов и построении реестра информационных ресурсов.

В качестве примера рассматривается деятельность предприятия ИТ-индустрии, занимающегося разработкой и внедрением информационных систем управления на предприятиях заказчиков. Как правило, предприятия ИТ-индустрии используют в своей деятельности 3 подхода: 1) Установка и адаптация готовых решений компании; 2) Модернизация программного обеспечения заказчика и перевод его на новую технологическую платформу; 3) Быстрая разработка новых решений.

Предприятие владеет большим количеством подлежащих защите информационных ресурсов. В результате применения излагаемой методики должны быть определены ключевые информационные ресурсы, на защиту которых должны, в первую очередь, быть направлены мероприятия по защите информации.

2. Методика оценки рисков на основе модели бизнес-процессов предприятия

Особенностью предлагаемой методики является формирование реестра информационных ресурсов предприятия на основе анализа модели его бизнес-процессов. Информационные ресурсы отображаются на диаграммах IDEF0 как выходы процессов/операций и специфицируются в соответствующих таблицах. Анализ диаграмм и таблиц спецификаций позволяет выявить все информационные ресурсы предприятия в контексте протекающих бизнес-процессов. Такого рода подход позволяет на системной основе выявить все информационные ресурсы предприятия, будет способствовать пониманию семантики ресурсов, их значимости в деятельности предприятия и, как следствие, более точной оценке их стоимости. Рассмотрим предлагаемую методику детально.

Шаг 1. Построение модели бизнес-процессов предприятия

На первом шаге методики выполняется построение модели бизнес-процессов предприятия. В качестве примера для анализа рисков рассматривается деятельность типовой компании IT-индустрии, занимающейся разработкой и внедрением информационных систем управления предприятием.

При моделировании бизнес-процессов использовались структурно-функциональные диаграммы на основе нотации IDEF0 [15]. Построение модели бизнес-процессов осуществлялось при помощи программного продукта Business Studio от российского разработчика ГК «Современные технологии управления» [16-17]. Пример модели бизнес-процессов предприятия IT-индустрии приведен в приложениях 1, 2. Диаграмма A0 (декомпозиция первого уровня) иллюстрирует взаимодействие

основных бизнес-процессов предприятия. Диаграмма А4 (декомпозиция второго уровня) соответствует ключевому бизнес-процессу «Планирование, реализация и сопровождение ИТ-проектов». При построении IDEF0-диаграмм для компании IT-индустрии использовались типовые структуры бизнес-процессов [18, 19].

Шаг 2. Анализ моделей бизнес-процессов с целью выявления подлежащих защите информационных ресурсов предприятия.

Для определения подлежащих защите информационных ресурсов необходимо составить таблицу, содержащую описание выходов процессов IDEF0-модели. В качестве примера рассмотрим выходы процесса «Планирование, реализация и сопровождение ИТ-проектов».

В табл. 1 описываются выходы процесса А4 «Планирование, реализация и сопровождение ИТ-проектов». Содержимое графы «Выход» соответствует наименованию дуг на IDEF0-диаграмме. Дуга соответствует информационному (в ряде случаев материальному) потоку, порождаемому функциональным блоком. В графе «Объекты» отображаются компоненты информационного потока (перечень документов, описание информационных единиц). Графа «Получатель» содержит сведения о получателе информационного ресурса. В качестве получателя может выступать структурное подразделение, конкретное должностное лицо. Получатель может также являться внешней по отношению к моделируемой системе сущностью, например, заказчик, аутсорсер и пр. В графе «Процесс/Внешняя среда» приводятся данные о процессе – получателе информационного ресурса.

Шаг 3. Формирование реестра информационных ресурсов предприятия, оценка стоимости ресурсов.

Следующим шагом методики оценки рисков является непосредственное формирование реестра информационных ресурсов. При этом для каждого ресурса выполняется экспертная оценка его стоимости, оценивается вероятность их реализации. Исходными данными при формировании реестра ресурсов служат сведения о выходах процессов, полученные на предыдущем шаге.

При оценке стоимости (C_i) информационного ресурса необходимо учитывать:

– стоимость возможных потерь при получении информации заинтересованными лицами (конкурентами, клиентами и пр.);

– стоимость восстановления информации при ее утрате;

– затраты на восстановление нормального процесса функционирования предприятия в случае, если потеря информации приведет к частичной или полной остановке его бизнес-процессов и т.д.

Таблица 1

Выходы процесса А4 «Планирование, реализация и сопровождение ИТ-проектов»

№	Выход	Объекты	Передается	
			Получатель	Процесс/Внешняя среда
1.	Бюджет расходов проекта	Бюджет расходов проекта	Бухгалтерия	А6.1 Формирование бюджета доходов и расходов
2.	Обязательства перед аутсорсерами	Договор на выполнение работ Акт выполненных работ	Бухгалтерия	А6.1 Формирование бюджета доходов и расходов
3.	Обязательства заказчика	Договор на реализацию ИТ-проекта Акт ввода в эксплуатацию	Бухгалтерия	А6.2 Контроль доходов
4.	ИТ-проект, сданный в эксплуатацию	ИТ-проект, сданный в эксплуатацию Проектная документация		Внешняя среда – заказчик
5.	Отчет об удовлетворенности клиента	Отчет об удовлетворенности клиента	Начальник отдела продаж	А1.1 Анализ рынка
6.	Отчетность по выполнению проектных работ	Акт ввода в эксплуатацию Акт выполненных работ и счет-фактура Акт выполненных работ по пуско-наладке Отчет о предпроектном обследовании Отчет о пуско-наладочных работах Техно-рабочий проект Сдаточная документация	Бухгалтерия	А6.6 Подготовка отчетности
7.	Задачи на выполнение работ по аутсорсингу	Описание задачи проекта	Аутсорсеры	Внешняя среда – аутсорсеры
8.	Потребность в специалистах	План привлечения специалистов для реализации проекта	Начальник отдела кадров	А3.1 Определение потребностей в персонале
9.	Потребность программно-технических средствах	Ведомость потребности в программно-технических средствах	Начальник отдела снабжения	Заказчик
10.	Заявка на программно-техническое обеспечение	Заявка на программно-техническое обеспечение	Инженерно-технический отдел	А5.2 Выполнение профилактических и ремонтно-восстановительных работ

Для определения максимальной вероятности реализации угроз для i-го информационного ресурса следует оценить вероятность реализации каждой из этих угроз и выбрать максимальную из них:

$$P_i = \max_j \left(P_{ij} \right),$$

где P_i – максимальная вероятность реализации угроз для *i*-го информационного ресурса,

P_{ij} – вероятность реализации *j*-ой угрозы для *i*-го информационного ресурса.

При оценке вероятности реализации *j*-ой угрозы для *i*-го информационного ресурса следует учитывать:

– существующий уровень защиты данного ресурса. Например, если на момент оценки вероятности уже реализованы мероприятия по резервному копированию информации, то вероятность потери информации вследствие непреднамеренных действий персонала близка к нулю;

– стоимость информационного ресурса как фактор, повышающий вероятность его кражи заинтересованными лицами (конкурентами, клиентами и пр.).

Расчет вероятного ущерба $У_i$ для *i*-го информационного ресурса определим по формуле:

$$У_i = P_i \cdot C_i.$$

Суммарный вероятный ущерб оценивается путем суммирования вероятных ущербов по всем информационным ресурсом предприятия:

$$У_{\Sigma} = \sum_{i=1}^{n} У_i,$$

где $У_{\Sigma}$ – суммарный вероятный ущерб,

n – общее число информационных ресурсов предприятия.

Реестр информационных ресурсов для рассматриваемого примера приведен в табл. 2. В связи с тем, что рассматривалось типовое предприятие, экспертная оценка стоимости ресурсов рассматривается гипотетически. В условиях реального предприятия стоимость ресурсов оценивается на основе методик, рассматриваемых в [6, 9].

Таблица 2

Реестр информационных ресурсов на основе анализа выходов процесса А4

№	Информационный ресурс	Ценность ресурса, руб.	Максимальная вероятность реализации угроз	Вероятный ущерб, руб.
1.	Сведения по бюджетам реализованных проектов	1 000 000	0,1	100 000
2.	База аутсорсеров с данными о выполненных работах и выплатах	2 000 000	0,1	200 000
3.	База заказчиков с данными о заключенных договорах	10 000 000	0,35	3 500 000
4.	Программное обеспечение, разработанное компанией – интеллектуальная собственность (исходные коды программ)	100 000 000	0,1	10 000 000
5.	Типовые проектные решения – интеллектуальная собственность (проектные модели, скрипты баз данных и пр.)	100 000 000	0,1	10 000 000
6.	Данные по программно-техническому обеспечению предприятия	500 000	0,1	50 000
7.	Сведения об удовлетворенности заказчиков реализованными проектами	1 000 000	0,4	400 000
8.	Документация по выполненным проектам	50 000 000	0,15	7 500 000
9.	Сведения по заявкам на программно-техническое обслуживание	100 000	0,0	0,0

Исходя из полученного результата можно выделить 4 ключевых ресурса, нуждающихся в первую очередь в реализации мероприятий по защите информации: 1) Программное обеспечение, разработанное компанией – исходные коды программ, 2) Типовые проектные решения – проектные модели, скрипты баз данных и пр., 3) Документация по выполненным проектам, 4) База заказчиков с данными о заключенных договорах.

Заключение

В работе предложена методика, позволяющая обосновать выбор основных направлений по защите информации предприятия на основе анализа его бизнес-процессов. Отличительной особенностью методики является использование CASE-технологий для принятия решений в области информационной безопасности предприятия.

Реализация методики позволяет сформировать реестр информационных ресурсов предприятия, включающий оценку вероятного ущерба по каждому ресурсу. Реестр показывает узкие места в организации защиты, на которые следует обратить первоочередное внимание при планировании мероприятий по защите информации. На основе полученных данных можно сформировать обоснованную с экономической точки зрения стратегию и тактику развития системы защиты информации предприятия.

Реализация мероприятий по защите информации позволит снизить суммарный вероятный ущерб. В этом случае повторная оценка суммарного вероятного ущерба позволит оце-

нить эффективность затрат на защиту информации.

Повышение эффективности формирования профессиональных компетенций магистров по направлению «Информационная безопасность» основано на формализованном доступном языке представления системного подхода при анализе совокупности факторов, оказывающих влияние на состояние информационной безопасности предприятия. Представленная в работе методика основана на использовании с этой целью структурно-функционального моделирования, а также CASE-технологий.

Методика прошла успешную апробацию в учебном процессе. По мнению авторов статьи, использование данной методики при проведении лабораторных занятий для магистров, обучающихся по направлению «Информационная безопасность» позволило повысить эффективность формирования у обучающихся профессиональных компетенций, в частности: ПК-2 – способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности, ПК-3 – способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов [20].

Полученные результаты могут быть полезны не только как методика обучения специалистов в области информационной безопасности, но и в практической деятельности по обеспечению информационной безопасности предприятия.

Литература

1. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Взамен ГОСТ Р ИСО/МЭК ТО 13335-3-2007 и ГОСТ Р ИСО/МЭК ТО 13335-4-2007; Введ. с 30.11.2010. М.: Стандартинформ, 2011.
2. ГОСТ Р ИСО 31000-2010. Менеджмент риска. Принципы и руководство.; Введен с 01.09.2011. М.: Стандартинформ, 2012.
3. Международный стандарт ISO/IEC 27001-2013. Информационные технологии – Методы защиты – Системы менеджмента информационной безопасности – Требования.
4. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2005 г. № 447-ст.
5. Кривякин К.С., Изотова А.Р., Федоров В.М. Методический подход к оценке рисков информационной безопасности предприятия // Экономинфо. 2018. Т. 15. № 2. С. 82–90.
6. Ильченко Л.М., Брагина Е.К., Егоров И.Э., Зайцев С.И. Расчет рисков информационной безопасности телекоммуникационного предприятия // Открытое образование. 2018. Т. 22. № 2. С. 61–70.
7. Плетнев П.В., Белов В.М. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса // Доклады Томского государственного университета систем управления и радиоэлектроники. 2012. № 1–2 (25). С. 83–86.
8. Одинцова М.А. Методика управления рисками для малого и среднего бизнеса // Экономический журнал. 2014. № 3 (35).
9. Выборнова О.Н., Давидюк Н.В., Кравченко К.Л. Оценка информационных рисков на основе экспертной информации (на примере ГБУЗ АО «Центр медицинской профилактики») // Инженерный вестник Дона. 2016. № 4 (43). С. 86.
10. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности // Вестник Московского университета им. С.Ю. Витте. 2015. № 1. С. 73–79.
11. Астахов А.М. Искусство управления информационными рисками. М.: ДМК Пресс, 2010. 312 с.
12. Сизов В.А. Применение деловых игр в подготовке магистров по программе «Защита информационного пространства субъектов экономической деятельности» // Открытое образование. 2018. Т. 22. № 6. С. 59–64.
13. Замула А.А., Одарченко А.С., Дейнеко А.А. Методы оценивания и управления информационными рисками // Прикладная радиоэлектроника. 2015. № 3. С. 182–187.
14. Зарипова А. И., Коваленко С.В. Финансовые риски при обеспечении экономической безопасности предприятий [Электрон. ресурс] // Молодой ученый. 2018. № 1. С. 61–63. URL: https://moluch.ru/archive/187/47652/ (дата обращения: 16.05.2019)
15. Р 50.1.028-2001. Методология функционального моделирования. Рекомендации по стандартизации. Приняты и введены в действие Постановлением Госстандарта России от 02.07.2001 № 256 ст.
16. Гаврилов А.В. Методика выбора CASE-средств структурного проектирования для обучения по направлению подготовки «Прикладная информатика» // (ИП&УЗ-2015): сборник научных трудов XVIII научно-практической конференции (21–24 апреля 2015 г., Москва) Под науч. ред. Ю. Ф. Тельнова. М.: Московский государственный университет экономи-

ки, статистики и информатики (МЭСИ), 2015. С. 230–241.

17. Гаврилов А.В. Анализ функциональных возможностей бесплатных CASE-средств проектирования баз данных // Открытое образование. 2016. Т. 20. № 4. С. 39–43.

18. Пример функциональной модели (IDEF0) промышленного предприятия в Business Studio. [Электрон. ресурс] URL: http://www.businessstudio.ru/publication/proizv_predpr_abc/businessmodel.php?lang=ru-ru (дата обращения 02.02.2019).

19. Пример функциональной модели компании, осуществляющей деятельность по проектированию, монтажу и обслуживанию инженерно-технических систем. [Электрон. ресурс] URL http://publication.businessstudio.ru/businessmodel.php?lang=ru-ru&oguid=2be70b1c-a108-4228-b272-1c9eefbc464e (дата обращения 02.02.2019).

20. Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратуры). Утвержден приказом Министерства образования и науки Российской Федерации от 01.12.2016 г. № 1513.

References

1. GOST R ISO / IEC 27005-2010. Information technology. Methods and means of security. Information security risk management. Instead, GOST R ISO / IEC 13335-3-2007 and GOST R ISO / IEC 13335-4-2007; Enter from 11/30/2010. Moscow: Standardinform; 2011. (In Russ.)

2. GOST R ISO 31000-2010. Risk management. Principles and guidelines .; Entered from 09/01/2011. Moscow: Standardinform; 2012. (In Russ.)

3. The international standard ISO / IEC 27001-2013. Information technology - Protection methods - Information security management systems - Requirements. (In Russ.)

4. GOST R ISO / IEC 17799-2005. Information technology. Practical rules of information security management. Approved and enacted by the Order of the Federal Agency for Technical Regulation and Metrology of December 29; 2005 No. 447-st. (In Russ.)

5. Krivyakin K.S., Izotova A.R., Fedorov V.M. Methodical approach to risk assessment of information security of an enterprise. Ekonominfo. 2018; 15 (2): 82-90. (In Russ.)

6. Il'chenko L.M., Bragina E.K., Egorov I.E., Zaytsev S.I. Calculation of risks of information security of a telecommunications enterprise. Otkrytoye obrazovaniye = Open Education. 2018; 22 (2): 61-70. (In Russ.)

7. Pletnev P.V., Belov V.M. Methods of assessing information security risks in small and medium-sized businesses. Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki = Reports of Tomsk State University of Control Systems and Radioelectronics. 2012; 1–2 (25): 83–86. (In Russ.)

8. Odintsova M.A. Risk Management Technique for Small and Medium Businesses. Ekonomicheskiy zhurnal = Economic Journal. 2014; 3 (35). (In Russ.)

9. Vybornova O.N., Davidyuk N.V., Kravchenko K.L. Information risk assessment based on expert information (for example, GBUZ JSC "Center for Medical Prevention"). Inzhenernyy vestnik Dona = Engineering Bulletin of the Don. 2016; 4 (43): 86. (In Russ.)

10. Baranova E.K. Methods of analysis and risk assessment of information security. Vestnik Moskovskogo universiteta im. S.YU. Vitte = Bulletin of Vitte Moscow University. 2015 (1): 73-79. (In Russ.)

11. Astakhov A.M. Iskusstvo upravleniya informatsionnymi riskami = The art of information risk management. Moscow: DMK Press; 2010. 312 p. (In Russ.)

12. Sizov V.A. The use of business games in the preparation of masters program "Protection of the information space of subjects of economic activity". Otkrytoye obrazovaniye = Open Education. 2018; 22 (6): 59-64. (In Russ.)

13. Zamula A.A., Odarchenko A.S., Deyneko A.A. Methods of evaluation and information risk management. Prikladnaya radioelektronika = Applied Radio Electronics. 2015 (3): 182-187. (In Russ.)

14. Zaripova A. I., Kovalenko: V. Financial Risks in Ensuring the Economic Security of Enterprises [Internet]. Molodoy uchenyy = Young scientist. 2018; 1: 61-63. URL: https://moluch.ru/archive/187/47652/ (Cited: 16.05.2019). (In Russ.)

15. R 50.1.028-2001. Methodology of functional modeling. Recommendations for standardization. Adopted and put into effect by the Resolution of the State Standard of Russia of July 2; 2001 No. 256, Art. (In Russ.)

16. Gavrilov A.V. Methods of selecting CASE-tools of structural design for training in the direction of training "Applied Informatics". (IP&UZ-2015): sbornik nauchnykh trudov XVIII nauchno-prakticheskoy konferentsii = (IP & UZ-2015): collection of scientific papers of the XVIII scientific-practical conference (April 21-24, 2015, Moscow) Ed. Yu. F. Telnov. Moscow: Moscow State University of Economics, Statistics and Informatics (MESI); 2015: 230-241. (In Russ.)

17. Gavrilov A.V. Analysis of the functionality of free CASE-database design tools. Otkrytoye obrazovaniye = Open Education. 2016; 20 (4): 39-43. (In Russ.)

18. An example of a functional model (IDEF0) of an industrial enterprise in Business Studio.

[Internet] URL: http://www.businessstudio.ru/publication/proizv_predpr_abc/businessmodel.php?lang=ru-ru (Cited 02.02.2019). (In Russ.)

19. An example of a functional model of a company engaged in the design, installation and maintenance of engineering systems. [Internet] URL http://publication.businessstudio.ru/businessmodel.php?lang=ru-ru&oguid=2be70b1c-a108-4228-b272-1c9eefbc464e (Cited 02.02.2019). (In Russ.)

20. Federal State Educational Standard of Higher Education in the field of preparation 10.04.01 Information security (master's level). Approved by order of the Ministry of Education and Science of the Russian Federation of 01.12.2016, № 1513. (In Russ.)

Сведения об авторах

Александр Викторович Гаврилов
к.т.н., доцент, доцент кафедры Прикладной информатики и информационной безопасности
Российский экономический университет им. Г.В Плеханова, Москва, Россия
Эл. почта: Gavrilov.AV@rea.ru

Валерий Александрович Сизов
д.т.н., профессор, профессор кафедры Прикладной информатики и информационной безопасности
Российский экономический университет им. Г.В Плеханова, Москва, Россия
Эл. почта: Sizov.VA@rea.ru

Information about the authors

Aleksandr V. Gavrilov
Cand. Sci. (Engineering) Associate Professor, Associate Professor at the Department of Applied Informatics and Information Security
Plekhanov Russian University of Economics, Moscow, Russia
E-mail: Gavrilov.AV@rea.ru

Valeriy A. Sizov
Dr. Sci. (Engineering), Professor, Professor at the Department of Applied Informatics and Information Security
Plekhanov Russian University of Economics, Moscow, Russia
E-mail: Sizov.VA@rea.ru