УДК 004.056.53
DOI: http://dx.doi.org/10.21686/1818-4243-2021-5-41-49

А.В. Гаврилов, В.А. Сизов, Е.В. Ярошенко

Российский экономический университет им. Г.В Плеханова, Москва, Россия

Методика оценки рисков информационной безопасности предприятия с использованием CASE-технологий

Цель исследования. *Построение эффективной системы информационной безопасности предприятия невозможно без адекватной оценки рисков, которым подвержены его активы. Результаты такой оценки должны стать основой для принятия решений в области информационной безопасности предприятия. Идентификация информационных активов и оценка их стоимости, определение уровня угроз безопасности активов позволяют спланировать мероприятия по созданию системы информационной безопасности предприятия.*

В настоящей работе рассматривается методика оценки рисков информационной безопасности предприятия, отличительной особенностью и новизной которой является применение современных средств и методов построения и анализа бизнес-процессов с целью выявления подлежащих защите информационных активов предприятия.

Материалы и методы. *Идентификацию информационных активов предлагается выполнять, опираясь на модель бизнес-процессов предприятия, выполняемую с использованием методики 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.

Результаты. *Описываемая в статье методика оценки рисков информационной безопасности предприятия прошла успешную апробацию в учебном процессе. Её использование при проведении лабораторных занятий по дисциплине «Проектирование системы информационной безопасности предприятий и организаций» для магистров, обучающихся по направлению «Информационная безопасность» позволило, по мнению авторов статьи, повысить эффективность формирования у обучающихся профессиональных компетенций.*

Заключение. *В работе предложена методика оценки рисков информационной безопасности для объектов информационной инфраструктуры предприятия, позволяющая выделить приоритетные направления защиты информации на предприятии. В результате применения методики формируется матрица потерь, показывающая проблемные места в организации защиты информации, на которые следует обратить первоочередное внимание при планировании мероприятий информационной безопасности. На основе полученных данных можно сформировать обоснованную с экономической точки зрения стратегию и тактику развития системы информационной безопасности предприятия.*

Ключевые слова: *информационная безопасность, риски, CASE-технологии, бизнес-процесс, IDEF0.*

Aleksandr V. Gavrilov, Valeriy A. Sizov, Elena V. Yaroshenko

Plekhanov Russian University of Economics, Moscow, Russia

Methodology for Assessing the Risks of Information Enterprise Security Using Case Technologies

Purpose of the study. *Creating an effective information security system of an enterprise is impossible without an adequate assessment of the risks to which its assets are exposed. The results of such an assessment should become the basis for making decisions in the field of information security of the enterprise. Identification of information assets and assessment of their value, determination of the level of threats to the security of assets allow planning measures to create an enterprise information security system.*

This paper discusses a methodology for assessing the risks of information security of an enterprise, a distinctive feature and novelty of which is the use of modern tools and methods for constructing and analyzing business processes in order to identify the information assets of an enterprise to be protected.

Materials and methods. *It is proposed to identify information assets based on the model of business processes of the enterprise, performed using the IDEF0 methodology. Modeling of business processes was carried out in the Business Studio environment of the "Modern Management Technologies" company.*

The activity of a typical IT-industry company was considered as an example for the risk analysis.

Results. *The methodology for assessing the risks of information security of an enterprise described in the article has been successfully tested in the educational process. Its use in conducting laboratory classes in the discipline "Designing the information security system of enterprises and organizations" for masters studying in the direction of "Information security" allowed, according to the authors of the article, to increase the effectiveness of the formation of students' professional competencies.*

Conclusion. *The paper proposes a methodology for assessing information security risks for objects of an enterprise's information infrastructure, which makes it possible to identify priority areas of information security at an enterprise. As a result of the application of the technique, a loss matrix is formed, showing the problem areas in the organization of information protection, which should be given priority attention when planning information security measures. Based on the data obtained, it is possible to form an economically justified strategy and tactics for the development of an enterprise information security system.*

Keywords: *information security, risks, CASE technologies, business process, IDEF0.*

Введение

Процесс управления рисками информационной безопасности (ИБ) направлен на противодействие угрозам и пресечение нарушений ИБ предприятия. Эффективное управление рисками требует их адекватной оценки, результаты которой станут основой для принятия решений в области информационной безопасности предприятия.

Практически все современные подходы к оценке рисков информационной безопасности предприятия основаны на последовательном решении следующих задач:

1. Идентификация активов предприятия и оценка их ценности.
2. Идентификация угроз активам и выявление уязвимостей в системе защиты информации.
3. Определение вероятностей реализации угроз и оценка их последствий.
4. Формирование предложений по обработке выявленных рисков [1-4].

Ключевым фактором построения эффективной системы информационной безопасности предприятия является идентификация подлежащих защите информационных активов предприятия. Не случайно данному вопросу посвящено немалое число исследований. Так, например, в работах [5-8] предлагаются методики расчета рисков информационной безопасности предприятия, в рамках реализации которых выделяются информационные активы предприятия. Однако конкретные способы идентификации активов авторами не рассматриваются.

Идентификация информационных активов и оценка их стоимости, определение уровня угроз безопасности активов позволяет спланировать мероприятия по созданию системы информационной безопасности предприятия. В то же время адекватная оценка стоимости информационного актива невозможна без правильного понимания его роли и значения в реализуемых бизнес-процессах [9]. Существующие подходы к вопросу формирования реестра подлежащих защите активов предприятия не предполагают использования для решения данной задачи современных методов и программных средств построения и анализа бизнес-процессов предприятия.

В настоящей работе рассматривается методика оценки рисков информационной безопасности предприятия, отличительной особенностью и новизной которой является применение современных средств и методов построения и анализа бизнес-процессов с целью определения подлежащих защите информационных активов предприятия.

Для выявления подлежащих защите информационных активов предприятия производится построение функциональной модели бизнес-процессов с использованием методики IDEF0 [10]. Моделирование бизнес-процессов выполняется в среде Business Studio компании «Современные технологии управления» [11].

1. Обзор методик оценки рисков информационной безопасности предприятия

Выявление, анализ и оценка рисков информационной безопасности является ключевым этапом проектирования систем информационной безопасности (СИБ) предприятия. От того, насколько правильно будут оценены риски зависит и эффективность системы информационной безопасности предприятия в целом. Кратко охарактеризуем наиболее популярные в настоящее время методики управления рисками ИБ.

Метод CRAMM (CCTA Risk Analysis and Managment Method) и реализующий его одноименный программный продукт от компании Insight Consulting Limited является мощным и универсальным инструментом проведения обследования информационных систем и анализа рисков ИБ. Данный метод используется уже более 30 лет и за это время приобрел популярность во всем мире. Основным недостатком метода в контексте поставленной задачи исследования является то, что идентификация защищаемых ресурсов производится без привязки к бизнес-процессам предприятия. Данный недостаток CRAMM отмечается, в частности, в работе [12], автор которой утверждает, что методика не учитывает сопроводительной документации, такой как описание бизнес-процессов компании.

Указанного недостатка не лишена и методика FRAP (Facilitated Risk Analysis Process), предлагаемая компанией Peltier and Associates. В данной методике определение защищаемых ресурсов производится с использованием опросных листов, изучения документации на систему, использования инструментов автоматизированного анализа (сканирования) сетей [13]. Идентификация защищаемых ресурсов производится также без привязки к бизнес-процессам предприятия.

Метод CORAS представляет собой методику и программный инструмент моделирования риска. Программный продукт, реализующий методологию CORAS распространяется бесплатно. В методике CORAS не предусмотрена периодичность проведения оценки рисков и актуализация их значений [14]. CORAS не позволяет оценить эффективность инвестиций, вложенных во внедрение мер безопасности. Так же, как и в вышерассмотренных методиках CORAS не дает возможности анализа бизнес-процессов предприя-

тия с целью выявления защищаемых ресурсов.

Разработанная компанией RiskWatch одноименная методика ориентирована на количественные способы оценки рисков. Величина риска определяется как математическое ожидание потерь за год. Эффект от внедрения средств защиты количественно рассчитывается с помощью показателя ROI (Return on Investment - возврат инвестиций). Данный метод целесообразно использовать для проведения анализа рисков на программно-техническом уровне защиты без учета организационных и административных факторов [15].

Методика MSAT (Microsoft Security Assessment Tool), реализованная в соответствующем программном продукте от компании Microsoft использует качественные оценки рисков информационной безопасности. Методика позволяет оценить эффективность инвестиций от внедрения средств защиты информационных активов, но не дает возможность принимать во внимание протекающие в компании бизнес-процессы с целью идентификации объектов защиты [16].

Приведенный обзор позволяет сделать вывод о том, что на сегодняшний день не существует общепринятой научно обоснованной методики выявления рисков. Используемые при проектировании СИБ предприятий и организаций частные методики в большинстве своем опираются на эмпирические подходы в оценке рисков ИБ, основанные на накопленном компаниями-разработчиками опыте разработки систем управления рисками ИБ.

По мнению авторов статьи, основным недостатком большинства работ по данной проблематике является их ориентация на эмпирический подход, недостаточное внимание возможностям, возникающим при использовании методов и средств проектирования информационных систем. К числу таких методов относится и методика структурно-функционального анализа, опирающаяся на применении CASE[1]-технологий.

2. Методика оценки рисков информационной безопасности с использованием функциональной модели бизнес-процессов предприятия

Предлагаемая методика оценки рисков информационной безопасности предприятия включает в себя следующие составляющие:

1) построение и анализ модели бизнес-процессов предприятия с целью идентификации активов предприятия,

2) экспертную оценку ценности активов,

3) идентификацию угроз активам предприятия,

4) определение вероятностей реализации угроз,

5) стоимостную оценку последствий реализации угроз (ущерб предприятия).

Современное предприятие владеет большим количеством подлежащих защите информационных активов, и эффективность системы его информационной безопасности во многом зависит от правильности расстановки приоритетов защиты, грамотного выбора наиболее ценных и уязвимых информационных ресурсов. В результате применения предлагаемой методики должны быть определены ключевые информационные ресурсы, на защиту которых должны, в первую очередь, быть направлены мероприятия по защите информации.

Трудность идентификации активов предприятия состоит, с одной стороны, в необходимости выявления и анализа всех информационных ресурсов предприятия, с другой – в необходимости (для дальнейшей оценки стоимости актива) понимания его значения для успешного и эффективного протекания реализуемых бизнес-процессов. Так как информационный ресурс зачастую используется несколькими подразделениями и должностными лицами, то существует также вероятность его дублирования (с различными наименованиями) при построении реестра ресурсов.

Отличительная особенность методики – формирование реестра подлежащих защите информационных активов предприятия на основе анализа его функциональной модели, выполненной с применением методики IDEF0 [17, 18]. Информационные потоки, являющиеся выходами блоков IDEF0, заносятся в соответствующую таблицу. Такой подход позволяет на системной основе выявить все информационные активы предприятия, понять их значение в контексте протекающих бизнес-процессов и, как следствие, произвести более точную оценку стоимости этих активов. Рассмотрим предлагаемую методику детально.

На *первом этапе* выполняется построение модели бизнес-процессов предприятия с использованием методики IDEF0. В качестве примера рассматривается предприятие IT-индустрии. При построении модели были использованы типовые функциональные модели компаний [19, 20]. Пример модели приведен в приложениях 1, 2. Диаграмма A0 иллюстрирует взаимодействие основных процессов предприятия. Диаграмма A4 соответствует ключевому процессу «Планирование, реализация и сопровождение ИТ-проектов».

На *втором этапе* составляется таблица, содержащая описание выходов функциональных блоков IDEF0-мо-

[1] CASE – программные средства автоматизации разработки программ.

дели. В табл. 1 описываются выходы процесса А4 «Планирование, реализация и сопровождение ИТ-проектов». Содержимое графы «Выход» соответствует наименованию дуг на IDEF0-диаграмме, соответствующих информационным потокам, порождаемым функциональными блоками. 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.

На *третьем этапе* выполняется формирование реестра информационных ресурсов. Для каждого ресурса выполняется экспертная оценка его стоимости. Исходными данными при формировании реестра ресурсов служат сведения о выходах процессов, полученные на предыдущем шаге.

При оценке стоимости (C_k) 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.

По каждому информационному ресурсу определяется перечень объектов защиты (таблица 2). При этом учитываются:

– все ресурсы, на которых хранится ценная информация;

– все сетевые группы, в которых находятся ресурсы системы (т.е. физические связи ресурсов друг с другом);

– отделы, к которым относятся ресурсы;

– виды ценной информации;

– ущерб для каждого вида ценной информации по трем видам угроз: внешние, внутренние, комбинированные;

– бизнес-процессы, в которых обрабатывается информация;

– группы пользователей, имеющих доступ к ценной информации;

Таблица 1

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

Table 1

Outputs of the A4 process “Planning, implementation and maintenance of IT projects”

№	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

– класс группы пользователей;

– доступ группы пользователей к информации;

– характеристики этого доступа (вид и права);

– средства защиты информации;

– средства защиты рабочего места группы пользователей.

Рассмотрим информационный ресурс «Программное обеспечение, разработанное компанией – интеллектуальная собственность (исходные коды программ)». Предположим, что данный ресурс хранится на сервере отдела разработки программного обеспечения (ПО) и доступ к нему в настоящее время имеют следующие лица: системный администратор, начальник отдела. Данная информация используется при реализации проектов, поэтому копируется на рабочие станции участников проектов (менеджер проекта, архитектор(ы) проекта, системные аналитики, программисты). Таким образом, к числу объектов защиты можно отнести: сервер отдела разработок, каналы передачи данных, средства вычислительной техники (СВТ) сотрудников отдела – участников проектов. Рассуждая подобным образом, заполним в таблице 2 графу «объекты защиты».

Задачей *четвертого этапа* является непосредственная оценка рисков для объектов защиты с учетом потенциальных угроз.

Таблица 2

Реестр информационных ресурсов предприятия

Table 2

Register of information resources of the enterprise

№	Информационный ресурс	Ценность ресурса, руб.	Объекты защиты
1.	Сведения по бюджетам реализованных проектов	1 000 000	1. Сервер бухгалтерии 2.СВТ сотрудников бухгалтерии 3. Каналы передачи данных
2.	База внештатных исполнителей (аутсорсеров) с данными о выполненных работах и выплатах	2 000 000	1. Компьютер начальника отдела разработки ПО 2.Сервер отдела разработки ПО
3.	База заказчиков с данными о заключенных договорах	10 000 000	1. Компьютер начальника отдела разработки ПО 2. Компьютер начальника отдела продаж 3. Сервер отдела разработки ПО 4. Сервер отдела продаж 5. Сервер бухгалтерии 6.СВТ сотрудников бухгалтерии
4.	Программное обеспечение, разработанное компанией – интеллектуальная собственность (исходные коды программ)	100 000 000	1. Компьютер начальника отдела разработки ПО 2. Компьютер системного администратора 3. Сервер отдела разработки ПО 4. СВТ системных аналитиков 5. СВТ программистов 6. СВТ менеджеров проектов 7. Каналы передачи данных
5.	Типовые проектные решения – интеллектуальная собственность (проектные модели, скрипты баз данных и пр.)	100 000 000	1. Компьютер начальника отдела разработки ПО 2. Компьютер системного администратора 3. Сервер отдела разработки ПО 4. СВТ системных аналитиков 5. СВТ программистов 6. СВТ менеджеров проектов 7. Каналы передачи данных
6.	Данные по программно-техническому обеспечению предприятия	500 000	1. Компьютер начальника ИТ-отдела 2. Сервер ИТ-отдела 3. СВТ сотрудников ИТ-отдела
7.	Сведения об удовлетворенности заказчиков реализованными проектами	1 000 000	1. Компьютер начальника отдела продаж 2. Сервер отдела продаж 3. СВТ сотрудников отдела продаж
8.	Дополнительная документация по выполненным проектам	50 000 000	1. Компьютер начальника отдела разработки ПО 2. Компьютер системного администратора 3. Сервер отдела разработки ПО 4. СВТ системных аналитиков 5. СВТ программистов 6. СВТ менеджеров проектов 7. Каналы передачи данных
9.	Сведения по заявкам на программно-техническое обслуживание	100 000	1. Компьютер начальника ИТ-отдела 2. Сервер ИТ-отдела 3. СВТ сотрудников ИТ-отдела
...	...	...	...

Обозначим объекты, подлежащие защите O_i, например, компьютер начальника отдела разработки ПО – O_1, сервер отдела продаж – O_2, сервер отдела разработки ПО – O_3 и т.д.

С каждым объектом, требующим защиты O_i, связывается некоторое множество действий, к которым может прибегнуть нарушитель для получения несанкционированного доступа к объекту (в случае преднамеренного воздействия), а также некоторое множество случайных событий (в случае непреднамеренного/случайного воздействия). Обозначим j-ую угрозу объекту защиты $У_j$, например, угроза несанкционированного доступа нарушителя к защищаемым файлам на локальном компьютере – $У_1$, угроза доступа к файлам сервера – $У_2$, угроза несанкционированного удаления защищаемой информации $У_3$ т.д. Потенциальные злоумышленные действия по отношению ко всем объектам формируют набор угроз информационной безопасности – множество $У_j$.

Множество отношений «объект-угроза-вероятность реализации» представим в виде таблицы (табл. 3), в ячейки которой внесем оценки вероятности реализации $У_j$ угрозы для O_i объекта – P_{ij}, полученные экспертным путем. Определение вероятности должно основываться на оценке текущего уровня уязвимости (степени защищенности данного объекта) с учетом как числа прецедентов нарушения информационной безопасности объекта, так и стоимости связанного информационного ресурса как фактора, повышающий вероятность его кражи.

Отсутствие числа в ячейке таблицы соответственно означает, что для i-го объекта j-ой угрозы не существует.

Для определения риска нарушения безопасности информации на i-ом объекте следует учесть стоимость связанного с

Таблица 3

Оценки вероятности реализации угроз

Table 3

Estimates of the probability of threat implementation

	$У_1$	$У_2$	...	...	$У_j$	...	...	...	$У_m$
O_1	0,1				0,01				0,1
O_2		0,05							
...									
O_i	0,03				0,01				
...									
O_n	0,2								0,01

ним информационного ресурса. Например, объект O_i – СВТ сотрудников отдела продаж связан с обработкой информационного ресурса C_k – сведения об удовлетворенности заказчиков реализованными проектами, оценочная стоимость которого составляет 1 000 000 руб. (см. табл. 2). Назовем полученное значение приведенной стоимостью объекта защиты информации и обозначим ее для i-ого объекта – C_{Oi}.

Как видно из таблицы 2 обеспечение безопасности различных информационных ресурсов может производиться путем организации защиты одних и тех же объектов. В этом случае для расчета приведенной стоимости объекта защиты нужно использовать стоимость наиболее ценного из информационных ресурсов, связанных с этим объектом (см. табл. 2).

$$C_{Oi} = \max(C_k)\ \{O_i\},$$

где C_k – стоимость связанного с объектом защиты информационного ресурса.

Так, например, в соответствии с таблицей 2 сервер отдела разработки ПО – объект O_3 связан с обработкой/хранением трех информационных ресурсов: 1) База аутсорсеров с данными о выполненных работах и выплатах (C_1 = 2 000 000 руб.), 2) База заказчиков с данными о заключенных договорах (C_2 = 10 000 000 руб.), 3) Программное обеспечение, разработанное компанией (C_3 = 100 000 000 руб.), 4) Типовые проектные решения (C_4 = 100 000 000 руб.), 5) Дополнительная документация по выполненным проектам (C_5 = 50 000 000 руб.).

$$C_{O3} = \max\{C_1,\ C_2,\ C_3,\ C_4,\ C_5\} = 100\ 000\ 000 \text{ руб.}$$

Определив приведенную стоимость объектов защиты информации, рассчитаем матрицу вероятных потерь.

Расчет вероятных потерь для i-ого объекта при реализации j-ой угрозы определим по формуле:

$$П_{ij} = P_{ij} \times C_{Oi},$$

где $П_{ij}$ – величина вероятных потерь для i-ого объекта при реализации j-ой угрозы,

Таблица 4

Матрица вероятных потерь

Table 4

Matrix of probable losses

	$У_1$	$У_2$	...	$У_j$	...	$У_m$
O_1	10 000 000			400 000		3 000 000
O_2		500 000				
...						
O_i	5 000 000			1 000 000		
...						
O_n	2 000 000					100 000

P_{ij} – вероятность реализации *j*-ой угрозы для *i*-ого объекта.

В результате выполненного анализа получим таблицу с оценкой вероятных потерь (таблица 4).

Основываясь на полученной таким образом матрице вероятных потерь можно выделить приоритетные направления защиты информации на предприятии. Это, в свою очередь, позволит не только оценить риски информационной безопасности для объектов информационной инфраструктуры предприятия, но и выделить угрозы безопасности информации, от которых защищать объекты инфраструктуры предприятия нужно в первую очередь. Матрица потерь показывает узкие места в организации защиты информации, на которые следует обратить первоочередное внимание при планировании мероприятий информационной безопасности. На основе полученных данных можно сформировать обоснованную с экономической точки зрения стратегию и тактику развития системы 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. 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.

6. 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.

7. Одинцова М.А. Методика управления рисками для малого и среднего бизнеса // Экономический журнал. 2014. № 3(35).

8. 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.

9. Гаврилов А.В., Сизов В.А. Повышение эффективности формирования профессиональных компетенций магистров по направлению «Информационная безопасность» на основе применения CASE-технологий // Открытое образование. 2019. Т. 23. № 3. С. 25–32.

10. Р 50.1.028-2001. Методология функционального моделирования. Рекомендации по стандартизации. Приняты и введены в действие Постановлением Госстандарта России от 2.07.201 № 256 ст.

11. Официальный сайт компании «Современные технологии управления». Инструмент для проектирования – система Business Studio [Электрон. ресурс]. Режим доступа: https://www.businessstudio.ru/products/business_studio/intro/ (Дата обращения: 20.05.2021).

12. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности // Вестник Московского университета им. С.Ю. Витте. 2015. № 1. С. 73-79.

13. Сухаревская Е.В., Михальченко С.В., Шамин И.М., Никишова А.В. Анализ методов оценки рисков при применении ERP-систем [Электрон. ресурс] // Современные научные исследования и инновации. 2016. № 9. Режим доступа: http://web.snauka.ru/issues/2016/09/72016. (Дата обращения: 21.05.2021).

14. Файзулаев Д. Ф., Морозов Б. Б. Методы и средства анализа рисков информационной безопасности предприятия // Безопасность информационных технологий. 2017. Т. 24. № 3. С. 72–77.

15. Пугин В.В., Губарева О.Ю. Обзор методик анализа рисков информационной безопасности информационной системы предприятия // T-COMM – Телекоммуникации и транспорт. 2012. № 6. С. 54-57.

16. Абрамов А.С., Писарев В.Д., Шилов А.К. Применение методологии MSAT для оценки защищенности предприятия // Аллея науки. 2017. Т. 3. № 13. С. 961–965.

17. Гаврилов А.В. Использование современных CASE-средств структурного проектирования при обучении студентов по направлению подготовки «прикладная информатика» // Открытое образование. 2015. № 4(111). С. 22–27.

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

19. Пример функциональной модели (IDEF0) промышленного предприятия в Business Studio [Электрон. ресурс]. Режим доступа: http://www.businessstudio.ru/publication/proizv_predpr_abc/businessmodel.php?lang=ru-ru. (Дата обращения: 21.05.2021).

20. Пример функциональной модели компании, осуществляющей деятельность по проектированию, монтажу и обслуживанию инженерно-технических систем [Электрон. ресурс]. Режим доступа: http://publication.businessstudio.ru/businessmodel.php?lang=ru-ru&oguid=2be70b1c-a108-4228-b272-1c9eefbc464e. (Дата обращения: 21.05.2021).

References

1. GOST R ISO/MEK 27005-2010. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Menedzhment riska informatsionnoy bezopasnosti. Vzamen GOST R ISO/MEK TO 13335-3-2007 i GOST R ISO/ MEK TO 13335-4-2007; Vved. s 30.11.2010 = GOST R ISO / IEC 27005-2010. Information technology. Methods and means of ensuring safety. Information security risk management. Instead of GOST R ISO / MEK TO 13335-3-2007 and GOST R ISO / MEK TO 13335-4-2007; Enter. from 30.11.2010. Moscow: Standartinform; 2011. (In Russ.)

2. GOST R ISO 31000-2010. Menedzhment riska. Printsipy i rukovodstvo.; Vveden s 01.09.2011 = GOST R ISO 31000-2010. Risk management. Principles and guidelines .; Introduced from 01.09.2011. Moscow: Standartinform; 2012. (In Russ.)

3. Mezhdunarodnyy standart ISO/IEC 27001-2013. Informatsionnyye tekhnologii – Metody zashchity – Sistemy menedzhmenta informatsionnoy bezopasnosti – Trebovaniya = International standard ISO / IEC 27001-2013. Information technology - Security methods - Information security management systems - Requirements. (In Russ.)

4. GOST R ISO/MEK 17799-2005. Informatsionnaya tekhnologiya. Prakticheskiye pravila upravleniya informatsionnoy bezopasnost'yu. Utverzhden i vveden v deystviye Prikazom Federal'nogo agentstva po tekhnicheskomu regulirovaniyu i metrologii ot 29 dekabrya 2005 g. №447-st = GOST R ISO / IEC 17799-2005. Information technology. Practical rules for information security management. Approved and put into effect by the Order of the Federal Agency for Technical Regulation and Metrology dated December 29, 2005 No. 447-st. (In Russ.)

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

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

7. Odintsova M.A. Methodology of risk management for small and medium-sized businesses. Ekonomicheskiy zhurnal = Economic Journal. 2014: 3(35). (In Russ.)

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

9. Gavrilov A.V., Sizov V.A. Increasing the effectiveness of the formation of professional competencies of masters in the direction of «Information Security» based on the use of CASE-technologies. Otkrytoye obrazovaniye = Open Education. 2019; 23; 3: 25-32. (In Russ.)

10. R 50.1.028-2001. Metodologiya funktsional'nogo modelirovaniya. Rekomendatsii po standartizatsii. Prinyaty i vvedeny v deystviye Postanovleniyem Gosstandarta Rossii ot 2.07.201 № 256 st = R 50.1.028-2001. Functional modeling methodology. Recommendations for standardization. Adopted and put into effect by the Resolution of the Gosstandart of Russia dated 2.07.201 No. 256 Art. (In Russ.)

11. Ofitsial'nyy sayt kompanii «Sovremennyye tekhnologii upravleniya». Instrument dlya proyektirovaniya – sistema Business Studio = Official site of the company «Modern technologies of management». Design tool - Business Studio system [Internet]. Available from: https://www.businessstudio.ru/products/business_studio/intro/ (cited 20.05.2021). (In Russ.)

12. Baranova Ye.K. Methods of analysis and assessment of information security risks. Vestnik Moskovskogo universiteta im. S.YU. Vitte = Bulletin of the Moscow University. S.Yu. Witte. 2015; 1: 73-79. (In Russ.)

13. Sukharevskaya Ye. V., Mikhal'chenko S. V., Shamin I. M., Nikishova A. V. Analysis of risk assessment methods when using ERP systems [Internet]. Sovremennyye nauchnyye issledovaniya i innovatsii = Modern scientific research and innovations. 2016: 9. Available from: http://web.snauka.ru/issues/2016/09/72016. (cited 21.05.2021). (In Russ.)

14. Fayzulayev D. F., Morozov B. B. Methods and tools for risk analysis of information security of an enterprise. Bezopasnost' informatsionnykh tekhnologiy = Security of information technologies. 2017; 24; 3: 72-77. (In Russ.)

15. Pugin V.V., Gubareva O.YU. Review of methods for analyzing information security risks of an enterprise information system. T-COMM – Telekommunikatsii i transport = T-COMM - Telecommunications and transport. 2012; 6: 54-57. (In Russ.)

16. Abramov A.S., Pisarev V.D., Shilov A.K. Application of the MSAT methodology for assessing the security of an enterprise. Alleya nauki = Alley of Science. 2017; 3; 13: 961-965. (In Russ.)

17. Gavrilov A.V. The use of modern CASE-tools for structural design in teaching students in the direction of training «Applied Informatics». Otkrytoye obrazovaniye = Open Education. 2015; 4(111): 22-27. (In Russ.)

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

19. Primer funktsional'noy modeli (IDEF0) promyshlennogo predpriyatiya v Business Studio = An example of a functional model (IDEF0) of an industrial enterprise in Business Studio [Internet]. Available from: http://www.businessstudio.ru/publication/proizv_predpr_abc/businessmodel.php?lang=ru-ru. (cited 21.05.2021). (In Russ.)

20. Primer funktsional'noy modeli kompanii, osushchestvlyayushchey deyatel'nost' po proyektirovaniyu, montazhu i obsluzhivaniyu inzhenerno-tekhnicheskikh system = An example of a functional model of a company engaged in the design, installation and maintenance of engineering systems [Internet]. Available from: http://publication.businessstudio.ru/businessmodel.php?lang=ru-ru&oguid=2be70b1c-a108-4228-b272-1c9eefbc464e. (cited 21.05.2021). (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

Елена Валерьевна Ярошенко
К.э.н. доцент кафедры прикладной информатики и информационной безопасности
Российский экономический университет им. Г.В. Плеханова,
Москва, Россия
yaroshenko.ev@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

Elena V. Yaroshenko
Cand. Sci. (Economics), Associate professor of the Academic Department of Applied Information Technology and Information Security
Plekhanov Russian University of Economics, Moscow, Russia
E-mail: yaroshenko.ev@rea.ru