DOI: https://doi.org/10.15688/NBIT.jvolsu.2022.4.2
УДК 004.942
ББК 32.971.35

МОДЕЛЬ ОПРЕДЕЛЕНИЯ СОСТАВА СИСТЕМЫ ЗАЩИТЫ ERP-СИСТЕМ

Алексей Александрович Бабенко

Кандидат педагогических наук, доцент,
кафедра информационной безопасности,
Волгоградский государственный университет
babenko.aleksey@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Ангелина Вячеславовна Рыбалкина

Студент, кафедра информационной безопасности,
Волгоградский государственный университет
angelina.rybalkina@rambler.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Рассмотрена роль ERP-систем в современной цифровой экономике. Приведены результаты работ в области защиты ERP-систем. Определены архитектура и функции ERP-систем, влияющие на их безопасность. Проанализирован рынок ERP-систем в мире и Российской Федерации. Рассмотрены угрозы информационной безопасности ERP-систем. Приведена модель угроз безопасности ERP-системы организации. Представлена функциональная модель определения состава системы защиты ERP-систем. Описан программный комплекс для определения состава системы защиты ERP-систем. Приведены результаты экспериментальных исследований с помощью разработанной модели.

Ключевые слова: ERP-система, оценка рисков, определение состава системы защиты, модель угроз, цифровая экономика.

Особую роль в развитии цифровой экономики в Российской Федерации приобретают ERP-системы. Основное назначение ERP-систем – поддержка функционала всех составляющих работы предприятия и обеспечение взаимодействия их друг с другом. ERP-система позволяет автоматизировать работу сотрудников на всех этапах работы предприятия, включая разработку и внедрения новых продуктов, а также оптимизировать работу уже существующих. Важно отметить, что ERP – не просто класс систем, позволяющий контролировать работу, а целая методика по организации и управлению бизнес-процессов предприятия. По этой причине для отечественных компаний внедрение подобной технологии предполагает существенные изменения в работе. Одна из особенностей при построении системы управления предприятием, основанной на принципах ERP – это ориентация на планирование и учет всех аспектов планирования ресурсов производства. Основной задачей ERP-систем является составление планов поставок материалов, производства. В то

время как многие функции учета, реализованные в данных системах, являются лишь дополнительными свойствами к основной задаче. Учитывая особую роль ERP-системы в деятельности предприятия особую роль приобретают задачи обеспечения информационной безопасности этих систем.

Основные теоретические и практические аспекты проблем создания, внедрения, эксплуатации и обеспечения безопасности ERP-систем нашли свое отражение в работах [4–6] ряда современных российских ученых: А. Нестерова, А.И. Дмитренко, Т.Г. Долговой, Е.Н. Горбачевской, Т.И. Булдаковой, А.В. Коршунова, Е.Ю. Виноградовой, А.И. Галимовой и др. Анализ результатов исследований, представленных в научно-практических работах данных ученых, показал, что актуальными являются следующие направления:

а) решение задач выбора оптимальной ERP-системы;

б) решение задач эффективной интеграции ERP-систем в предприятиях различных отраслей с целью повышения эффективности управления ресурсами, снижения производственных издержек и трудозатрат;

в) анализ и устранения технических проблем, связанных с разработкой и эксплуатацией ERP-систем различного типа;

г) анализ угроз кибербезопасности при использовании ERP-систем;

д) обеспечение безопасности и исследование механизмов защиты данных при эксплуатации ERP-систем.

Решение задач определения состава системы защиты различных типов информационных систем с использованием экспертного метода рассмотрены в работах [1–3].

Выделенные направления позволяют сделать вывод о том, что при внедрении и эксплуатации ERP-систем актуальной задачей является обеспечение информационной безопасности (ИБ) как ERP-системы, так и всей информационной инфраструктуры системы цифровой экономики в целом. Для проведения контроля над состоянием безопасности часто используют процедуры управления рисками ИБ, позволяющие своевременно идентифицировать источники и объекты риска, оценить существующие угрозы и выработать решения по управлению недопустимыми.

Под ERP-системой будем понимать автоматизированную систему, управляющую всеми процессами производства, реализованную в виде приложения с общим пользовательским интерфейсом и представляющую собой единую централизованную базу данных. Комплекс программных средств, находящийся в ERP-системе, предназначен для планирования и контроля всех стадий работы производства, включая активы и финансово-экономическую деятельность, управление персоналом, покупку материалов, цепочки поставок, финансовый учет. Система используется для непрерывного оптимального баланса ресурсов организации с помощью специализированного программного пакета, осуществляющего общую конфигурацию данных и процессов для всех управленческих деятельностей.

Анализ существующих ERP-систем позволил выделить их архитектуру и функции:

1. Платформа – среда для работы компонентов и модулей, основных возможностей и полномочий. Изменять код платформы может только инженер-разработчик. Пользователи системы и специалисты по внедрению не обладают правами доступа к программному коду.

2. Компонент управления данными – центральное хранилище, которое включает в себя базы данных, пакет программ для работы с ними, инструменты для обработки и анализа данных, а также экспресс-отправки их в программные модули.

3. Модули – элементы, подключаемые к платформе по мере необходимости. Они работают с единой базой данных и используют базовый функционал. Важно отметить, что модули работают независимо друг от друга. Такая структура модулей является главной отличительной особенностью ERP-систем.

Базовыми функциями всех ERP-систем являются:

а) разработка технического задания на производимые изделия, а также распределение ресурсов, необходимых для их изготовления;

б) составление планов по производству и продажам продукции;

в) распределение материалов, а также планирование их закупок по мере необходимости;

г) контролирование своевременности и объемов поставок;

д) руководство отделами закупок и снабжения, обеспечение учета, оптимизация и рационализация складских и производственных резервов;

е) составление плана производственной деятельности от полного планирования работы всего предприятия до использования некоторых видов оборудования;

ж) организация управления финансами, включая разработку финансово-экономических планов, а также контроль их исполнения;

з) управление всеми проектами предприятия.

Распределение ERP-систем на российском рынке в 2022 г. имеет следующий вид (рис. 1) [7].

Наибольшую долю рынка занимает российская ERP-система «1С:Предприятие» – 39 %; в совокупности на долю ERP-решений от Microsoft приходится 11 % рынка – это второе место; третье место с 8 % занимают самая популярная в мире ERP-система – SAP и система «Галактика».

Анализ угроз информационной безопасности ERP-систем

Учитывая особую роль ERP-системы в деятельности предприятия, отметим, что каждый элемент ее сложной архитектуры должен быть надежно защищен. Поскольку любое негативное воздействие (неважно, внешнее или внутреннее) может сказаться на деятельности организации и привести к серьезным последствиям. Следующие объекты, как правило, являются наиболее уязвимыми к возникновению ошибок (см. рис. 2):

– вычислительный процесс, который отвечает за автоматизацию подготовки решений и выработку управляющих воздействий в ERP-системе;

– базы данных в целом или информация, находящаяся в них;

– объектный код, выполняемый вычислительными средствами в ходе работы ERP-системы;

– информация, передаваемая между сотрудниками компании и подаваемая для потребителей.

Возникшие ошибки приводят к возникновению уязвимостей, через которые реализуется большинство угроз ИБ. Последствия каждой угрозы могут привести как к материальному, так и не материальному ущербу. Это опасно не только для организации в целом, но и для отдельных субъектов, использующих ERP-систему.

Большинство угроз по объектам воздействия распределяются по следующим уровням: уровень сети; уровень базы данных (единое хранилище информации), уровень приложений и подсистем ERP; уровень представлений (пользовательский).

Внешние угрозы могут исходить от конкурентов, преступных группировок, отдельных физических лиц, а также организации административно-управленческого аппарата. Работники предприятия, руководство и разные технические средства являются непосредственными источниками внутренних угроз.

Последствия каждой угрозы тесно связаны с вероятностью (частотой) ее реализации и могут привести к материальному и не

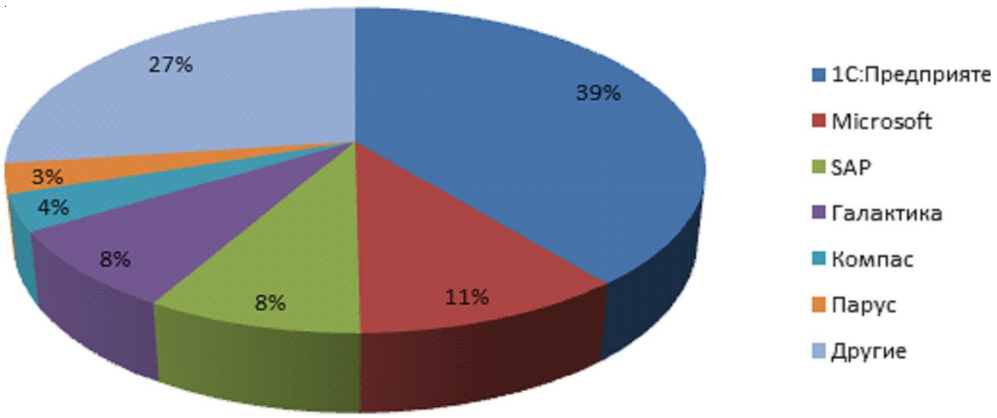

Рис. 1. Рейтинг ERP-систем на Российском рынке

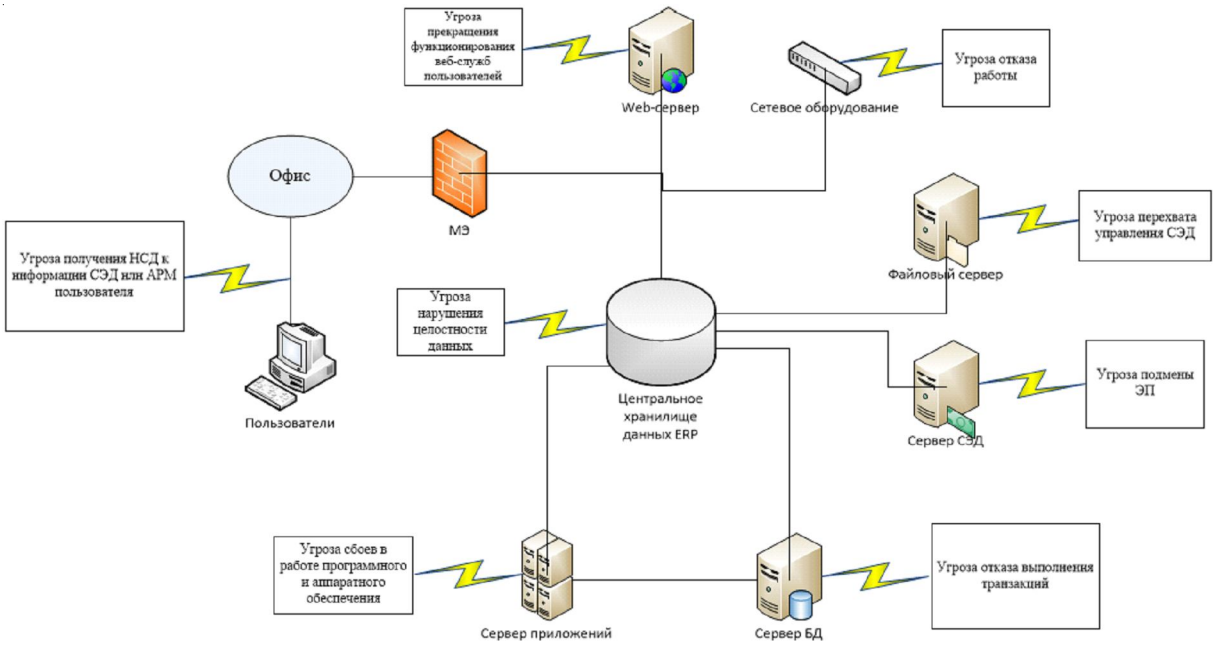

Рис. 2. Модель угроз безопасности ERP-системы организации

материальному ущербу, как для отдельных субъектов, использующих ERP-систему, так и для всей организации в целом. Поэтому любая ERP-система должна иметь надежные средства защиты.

Разработка функциональной модели определения состава системы защиты ERP-систем

Контекстная IDEF0-диаграмма процесса определения состава системы защиты ERP-системы представляет функциональный блок, на который воздействуют (см. рис. 3):

– входные данные – ERP-система, угрозы ее компонентам и уязвимости;

– управляющая информация: ГОСТ Р 57317-2016, ГОСТ Р ИСО/МЭК 27005-2010 и меры защиты;

– механизмы, необходимые для произведения данного процесса – пользователь и программа;

– выходной результат – состав системы защиты ERP-системы.

Декомпозиция функционального блока представлена на рисунке 4.

Функциональная модель позволила разработать программный комплекс для определения состава системы защиты ERP-систем.

Экспериментальные исследования модели определения состава системы защиты ERP-систем

В разработанном программном комплексе пользователь выбирает ERP-систему, далее загружаются активы, потенциальные угрозы и уязвимости этой системы (см. рис. 5). На функциональной вкладке «Активы» пользователь выбирает активы. Выбранные активы записываются в таблицу, где пользователь оценивает их ценность по количественной шкале от 1 до 4.

На функциональной вкладке «Угрозы и уязвимости» пользователь выбирает из списков угрозы и уязвимости, добавляет их в таблицу. Затем дает качественную оценку каждому выбранному компоненту и записывает данные об оценках. На основе полученных оценок определяется вероятность реализации угроз, после чего рассчитывается вероятность реализации угроз (см. рис. 6).

На основании ранее полученных данных формируется итоговая таблица, где указывается ценность активов и вероятность реализации угроз. Затем рассчитывается значение риска реализации угроз. Для снижения среднего и высокого уровня риска в программе определяются контрмеры и выбираются наиболее эффективные средства защиты.

Рис. 3. Контекстная IDEF0-диаграмма процесса определения состава системы защиты ERP-системы

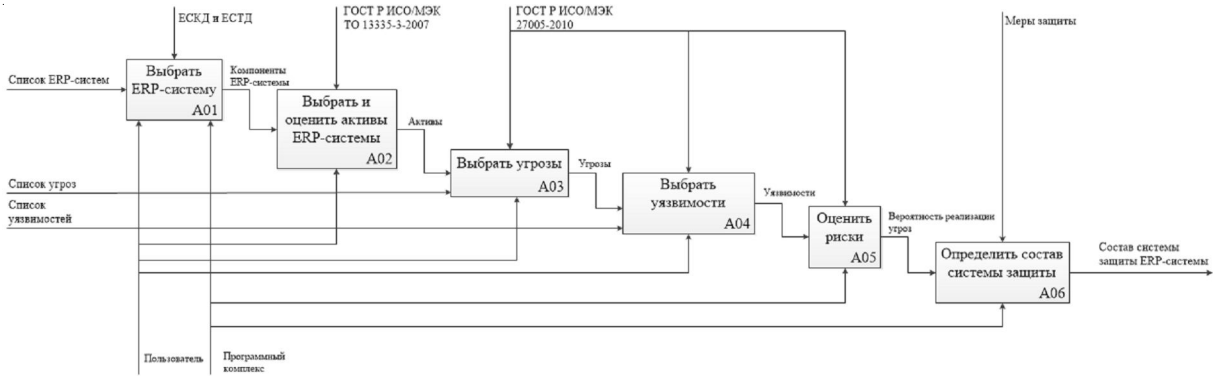

Рис. 4. Декомпозиция функционального блока процесса определения состава системы защиты ERP-системы

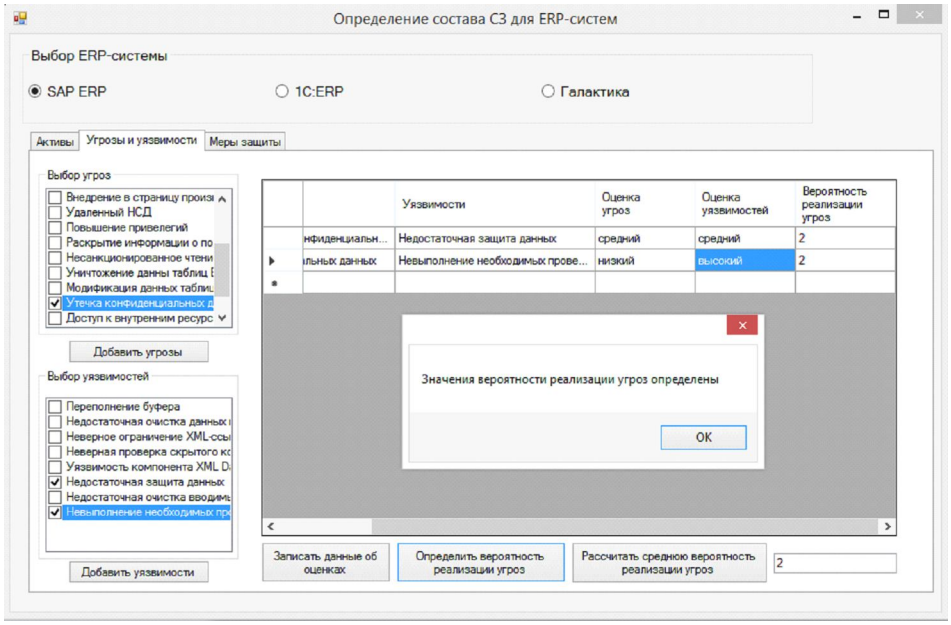

Рис. 5. Интерфейс программного комплекса для определения состава системы защиты ERP-системы (экранная копия)

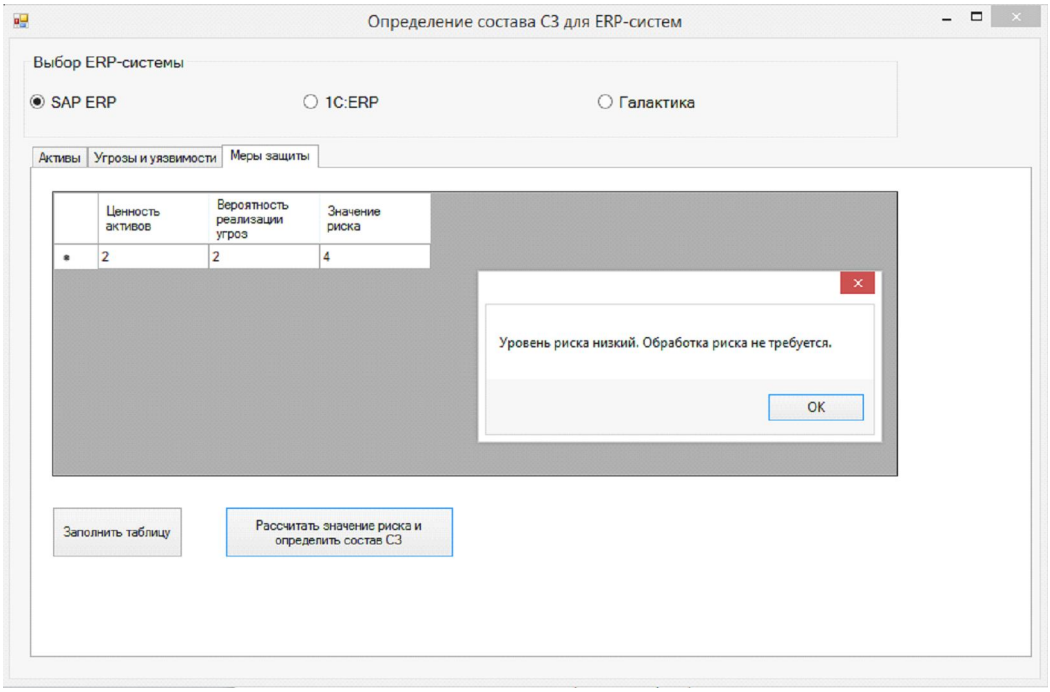

Рис. 6. Результаты первого эксперимента (экранная копия)

Экспериментальные исследования показали для SAP ERP-системы низкий уровень риска, поэтому обработка риска и внедрение контрмер не требуется. Для ERP-системы «Галактика» уровень риска до внедрения контрмер равен 6 (средний), поэтому для минимизации уровня риска использовался состав средств защиты, состоящий из программно-аппаратного комплекса «StoneGateIPS». После внедрения контрмер уровень риска снизился до 3, что является низким. Для ERP-системы 1С уровень риска до внедрения контрмер равен 12 и является высоким. Для снижения риска определен состав системы защиты, состоящий из средства антивирусной защиты «Dr.Web», межсетевого экрана «ImpervaSecureSphere» и криптографического средства защиты «Best Crypt». После внедрения контрмер уровень риска уменьшился в 3 раза (рис. 7).

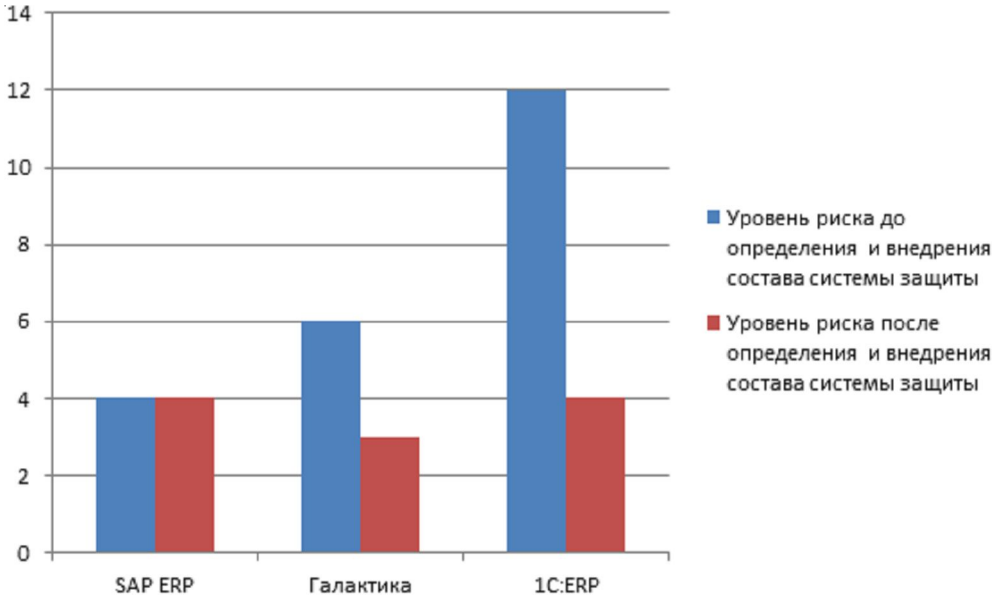

Рис. 7. Уровни риска до и после внедрения системы защиты

Заключение

Разработанная модель позволяет на основании оценки ценности активов, определения их угроз и степени реализации этих угроз, а также вероятности их появления, определить состав системы защиты ERP-систем, снижающий риски информационной безопасности до приемлемого уровня. Предложенная модель и ее программная реализация может использоваться в системах принятия решений для обеспечения информационной безопасности ERP-систем.

СПИСОК ЛИТЕРАТУРЫ

1. Бабенко, А. А. Алгоритм оценки риска информационной безопасности автоматизированной системы управления технологическими процессами нефтегазовой отрасли / А. А. Бабенко, А. А. Вдовкин // Перспективные информационные технологии (ПИТ 2022) : тр. Междунар. науч.-техн. конф. – Самара : Изд-во Самар. науч. центра РАН, 2022. – С. 105–108.

2. Бабенко, А. А. Разработка модели управления составом технических средств защиты информации в государственных информационных системах / А. А. Бабенко // НБИ технологии. – 2019. – Т. 13. – № 2. – С. 6–11.

3. Бабенко, А. А. Разработка системы управления рисками информационной безопасности в государственных информационных системах / А. А. Бабенко // Перспективные информационные технологии (ПИТ 2022) : тр. Междунар. науч.-техн. конф. – Самара : Изд-во Самар. науч. центра РАН, 2022. – С. 102–105.

4. Виноградова, Е. Ю. Информационная система планирования и управления предприятием как элемент цифровой экономики / Е. Ю. Виноградова, А. И. Галимова // Фундаментальные и прикладные исследования в области управления, экономики и торговли : сб. тр. науч. и учеб.-практ. конф. – СПб. : Изд-во С.-Петерб. политехн. ун-та Петра Великого, 2017. – С. 168–176.

5. Модели и методы исследования информационных систем : монография / А. Д. Хомоненко, А. Г. Басыров, В. П. Бубнов [и др.]. – СПб. : Лань, 2019. – 204 с.

6. Пугин, В. В. Обзор методик анализа риска информационной безопасности информационной системы предприятия / В. В. Пугин, О. Ю. Губарева // T-Comm – Телекоммуникации и Транспорт. – 2012. – № 6. – С. 54–57.

7. Рейтинг ERP-систем 2022 // Market.CNews. – Электрон. текстовые дан. – Режим доступа: https://market.cnews.ru/research/erp_2022/table?p=review (дата обращения: 03.10.2022). – Загл. с экрана.

REFERENCES

1. Babenko A.A., Vdovkin A.A. Algoritm ocenki riska informacionnoj bezopasnosti avtomatizirovannoj sistemy upravlenija tehnologicheskimi processami neftegazovoj otrasli [Algorithm for Information Security Risk Assessment of the Automated Process Control System of the Oil and Gas Industry]. *Perspektivnye informacionnye tehnologii (PIT 2022): tr. Mezhdunar. nauch.-tehn. konf.* [Promising Information Technologies (PIT 2022): Proceedings of the International Scientific and Technical Conference]. Samara, Izd-vo Samar. nauch. tsentra RAN, 2022, pp. 105-108.

2. Babenko A.A. Razrabotka modeli upravlenija sostavom tehnicheskih sredstv zashhity informacii v gosudarstvennyh informacionnyh sistemah [Development of a Model for Managing the Composition of Technical Means of Information Protection in State Information Systems]. *NBI tehnologii* [NBI Technologies], 2019, vol. 13, no. 2, pp. 6-11.

3. Babenko A.A. *Razrabotka sistemy upravlenija riskami informacionnoj bezopasnosti v gosudarstvennyh informacionnyh sistemah* [Development of Information Security Risk Management System in State Information Systems]. *Perspektivnye informacionnye tehnologii (PIT 2022): tr. Mezhdunar. nauch.-tehn. konf.* [Promising Information Technologies (PIT 2022): Proceedings of the International Scientific and Technical Conference]. Samara, Izd-vo Samar. nauch. tsentra RAN, 2022, pp. 102-105.

4. Vinogradova E.Yu., Galimova A.I. Informacionnaja sistema planirovanija i upravlenija predprijatiem kak jelement cifrovoj jekonomiki [Enterprise Planning and Management Information System as an Element of the Digital Economy]. *Fundamental'nye i prikladnye issledovanija v oblasti upravlenija, jekonomiki i torgovli: sb. tr. nauch. i ucheb.-prakt. konf.* [Basic and Applied Research in Management, Economics and Trade. A Collection of Works of a Scientific and Educational-Practical Conference]. Saint Petersburg, Izd-vo S.-Peterb. politekhn. un-ta Petra Velikogo, 2017, pp. 168-176.

5. Khomonenko A.D., Basyrov A.G., Bubnov V.P. et al., eds. *Modeli i metody issledovanija informacionnyh sistem: monografija* [Designs and Methods for Researching Information Systems: Monograph]. Saint Petersburg, Lan' Publ., 2019. 204 p.

6. Pugin V.V., Gubareva O.Yu. Obzor metodik analiza riska informacionnoj bezopasnosti informacionnoj sistemy predprijatija [Overview of

Enterprise Information System Information Security Risk Analysis Techniques]. *T-Comm – Telekommunikacii i Transport* [T-Comm – Telecommunications and Transport], 2012, no. 6, pp. 54-57.

7. Rejting ERP sistem 2022 (Rating of ERP systems 2022). *Market.CNews*. URL: https://market.cnews.ru/research/erp_2022/table?p=review (accessed 3 October 2022).

MODEL FOR DETERMINING THE COMPOSITION OF THE ERP SYSTEM PROTECTION SYSTEM

Aleksey A. Babenko

Candidate of Sciences (Pedagogy), Associate Professor,
Department of Information Security,
Volgograd State University
babenko.aleksey@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Angelina V. Rybalkina

Student, Department of Information Security,
Volgograd State University
angelina.rybalkina@rambler.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. The role of ERP systems in the modern digital economy is considered. The results of work in the field of protection of ERP systems are presented. The architecture and functions of ERP systems that affect their security are determined. The market of ERP systems in the world and the Russian Federation is analyzed. Threats to information security of ERP systems are considered. A model of security threats to the organization's ERP system is presented. A functional model for determining the composition of the ERP systems protection system is presented. A software package for determining the composition of the ERP systems protection system is described. The results of experimental studies using the developed model are presented.

Key words: ERP system, risk assessment, determination of the composition of the protection system, threat model, digital economy.