ЭКОНОМИЧЕСКИЕ ИССЛЕДОВАНИЯ

ECONOMIC STUDIES

DOI: 10.12731/2070-7568-2024-13-1-226
УДК 004.056

Научная статья | Региональная и отраслевая экономика

ОБОСНОВАНИЕ НЕОБХОДИМОСТИ ВНЕДРЕНИЯ НЕПРЕРЫВНОГО ПРОЦЕССА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИЯХ

Е.Н. Сыщикова, Е.Е. Макарова, М.Н. Муратова

В статье рассматривается информационная безопасность в системе работы промышленного предприятия. Акцентируется внимание на необходимости внедрения непрерывного процесса обеспечения информационной безопасности для защиты всех информационных активов от утечек, краж и несанкционированного раскрытия, проанализированы основные положения стандартов по управлению информационной безопасностью.

Цель работы: *оптимизировать способы программных средств защиты современных промышленных предприятий, а также снизить угрозы и виды уязвимости, связанные с безопасностью информации на предприятиях.*

Метод исследования: *в процессе исследования проблемы использовались аналитические методы анализа.*

Результаты: *необходимость использования стандартов ГОСТ Р ИСО/МЭК 27001-2021 и модели PDCA (Plan-Do-Check-Act) на промышленных предприятиях высокотехнологичных отраслей экономики с целью снижения угроз и потерь информационной безопасности, выявления критических факторов, негативно влияющих на бизнес-процессы и сами предприятия.*

Область применения результатов: *полученные результаты могут быть использованы в качестве теоретической основы для существующих оценок средств защиты информации и автоматизированных систем безопасности на высокотехнологичных промышленных предприятиях в современных условиях хозяйствования.*

Ключевые слова: *информационная безопасность; промышленные предприятия; управление; защита информации; угрозы информационной безопасности; риски информационной безопасности*

Для цитирования. *Сыщикова Е.Н., Макарова Е.Е., Муратова М.Н. Обоснование необходимости внедрения непрерывного процесса обеспечения информационной безопасности на предприятиях // Наука Красноярья: экономический журнал. 2024. Т. 13, №1. С. 7-21. DOI: 10.12731/2070-7568-2024-13-1-226*

Original article | Regional and Branch Economy

SUBSTANTIATION OF THE NEED TO IMPLEMENT A CONTINUOUS INFORMATION SECURITY PROCESS AT ENTERPRISES

E.N. Syshchikova, E.E. Makarova, M.N. Muratova

The article discusses information security in the system of an industrial enterprise. Attention is focused on the need to implement a continuous information security process to protect all information assets from leaks, theft and unauthorized disclosure, the main provisions of information security management standards are analyzed.

Objective: *To optimize the methods of software protection of modern industrial enterprises, as well as to reduce threats and vulnerabilities related to information security at enterprises.*

Method or methodology of the work: *In the process of investigating the problem, analytical methods of analysis were used.*

Results: *The need to use ISO/IEC 27001 standards and the PDCA (Plan-Do-Check-Act) model at industrial enterprises of high-tech sectors of the economy in order to reduce threats and losses of information security, identify critical factors that negatively affect business processes and the enterprises themselves.*

Practical implications: *The results obtained can be used as a theoretical basis for existing assessments of information security tools and automated security systems at high-tech industrial enterprises in modern economic conditions.*

Keywords: *information security; industrial enterprises; management; information protection; threats of information security; risks of information security*

For citation. *Syshchikova E.N., Makarova E.E., Muratova M.N. Substantiation of the Need to Implement a Continuous Information Security Process at Enterprises. Krasnoyarsk Science: Economic Journal, 2024, vol. 13, no. 1, pp. 7-21. DOI: 10.12731/2070-7568-2024-13-1-226*

Введение

Промышленные предприятия являются важным сектором российской экономики [16, 17]. По этой причине важно обеспечить безопасность их деятельности, при этом в условиях перехода к цифровой экономике большое значение имеет обеспечение информационной безопасности [1, 2, 7].

Навык введения передовых информационных технологий в процессы предоставления различного рода сведений и документов для выполнения различных работ и услуг значительно меняет понимание роли и места информации в этих процессах [15, с. 584-589].

Внедрение современных информационных технологий предусматривает возможность максимально повысить эффективность и качество как самой производственной деятельности, так и выпускаемой продукции (услуг) [9, с. 101-110]. Однако активное использование информационных технологий повышает уязвимость предприятия, что подтверждается большим числом компьютерных преступлений [11, с. 1305-1309].

Взяв за основу определение Д.Н. Шакина и др. [18] информационная безопасность по своей сути является состоянием защищенности информационных ресурсов (информационной среды) от внутренних и внешних угроз, способных нанести ущерб интересам личности, общества, государства (национальным интересам). Вместе с этим, отдельно выделяется подпункт, связанный с нанесением урона по репутации предприятия. К потерям в сфере экономической составляющей, как правило, относят: - подделка электронных подписей, - предоставление в открытый доступ личных данных, что является следствием недостаточно совершенной системы информационной безопасности [18].

Промышленным предприятиям для поддержания конфиденциальности необходимо правильно проектировать, разрабатывать и внедрять современные программы, позволяющие, на постоянной основе осуществлять экономический мониторинг рисков и угроз, который обеспечит информационную поддержку деятельности предприятия.

Постоянное осуществление мониторинга рисков и угроз информационной безопасности является важным элементом в комплексе мер по обеспечению безопасности информации на промышленном предприятии. Процесс устроенный таким образом, позволит выявить риски и спрогнозировать угрозы, определить их последствия и вероятность наступления, а также подготовить действия по нивелированию.

Подобные подходы к формированию систем защиты информации предприятия выстраиваются комплексно, с опорой на нормативно-правовую

базу Российской Федерации, а также с учетом особенностей осуществления основной деятельности предприятия. Основной задачей подобных систем защиты является предотвращение неблагоприятных событий в сфере информационной безопасности, а не их выявление постфактум.

Условием предотвращения наступления неблагоприятных событий в сфере информационной безопасности будет являться бесперебойность и непрерывность работы системы. Именно непрерывный контроль внутренних и внешних угроз информационной безопасности является залогом снижения рисков и образования узких мест в общей системе защиты информации.

Цель исследования: разработка рекомендаций по обеспечению информационной безопасности промышленных предприятий.

Методы и материалы

В качестве основы контроля угроз информационной безопасности можно выделить анализ рисков. По мнению авторов, осуществление анализа в свою очередь необходимо проводить поэтапно:

1 этап: идентификация активов: мониторинг всех информационных активов, баз данных, приложений, и т.д.;

2 этап: определение угроз: выявление потенциальных угроз по каждому ввиду активов;

3 этап: оценка уязвимостей: описание «узких мест» системы потенциально уязвимых для преступников;

4 этап: определение последствий: оценка возможных последствий при использовании злоумышленниками потенциально уязвимых составных частей системы;

5 этап: оценка вероятности возникновения неблагоприятных событий;

6 этап: оценка уровня риска: определение уровня риска для каждого актива;

7 этап: разработка мероприятий по снижению рисков: внедрение технических решений, разработка мер безопасности, информирование сотрудников и т. д.

8 этап (непрерывный): регулярное обновление и мониторинг: отслеживание реализации принятых мер и их корректировка с учетом новых вызовов.

Таким образом, непрерывный анализ рисков и угроз информационной безопасности позволит предприятию своевременно выявить и нивелировать уязвимости и угрозы, связанные с обеспечением защиты информации.

Одной из основных составляющих, а также базовым элементом формирования системы управления информационной безопасностью промышленного предприятия будет являться внедрение международных стандартов по информационной безопасности, так как стандартизированные принципы и методы управления качеством оказывают влияние на все сферы деятельности предприятия, в том числе и на информационную безопасность.

В серии международных стандартов по обеспечению информационной безопасности «ГОСТ Р ИСО/МЭК 27001-2021. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. и введен в действие Приказом Росстандарта от 30.11.2021 N 1653-ст и идентичен международному стандарту ISO/IEC 27000) содержатся основы и рекомендации для формирования, применения и внедрения системы управления информационной безопасностью в работу предприятия.

Несомненными плюсами ГОСТ Р ИСО/МЭК 27001-2021 является то, что он обеспечивает:

- устойчивость к кибератакам;
- быструю реакцию и перестройку системы ус учетом новых угроз;
- обеспечение секретности данных;
- формирование защиты информации по всему контуру предприятия;
- экономию средств.

Поскольку в условиях турбулентной экономической среды надежная и практичная система управления информационной безопасностью необходима всем промышленным предприятиям, так как системы, разработанные на уровне предприятия, не могут в полной мере учесть все современные угрозы и вызовы, стандарты в области обеспечения и управления информационной безопасностью становятся прекрасной альтернативой разработкам самих предприятий. Вышеуказанный стандарт ГОСТ Р ИСО/МЭК 27001-2021 многие специалисты, такие как И.В. Мандрица, В.И. Петренко, А.П. Жук [5, с. 20-29] выделяют в качестве основного, так как именно в нем наиболее полно и с описанием требуемых результатов представлен процесс внедрения на предприятии системы управления информационной безопасностью.

В настоящий момент, согласно данным Международной организация по стандартизации ИСО, опубликованным в ежегодном исследовании рынка сертифицированных систем менеджмента за 2022-2023 годы (исследование охватывает сертификаты соответствия ИСО 9001, ИСО 14001, ИСО 45001 и другим стандартам, выданным под аккредитацией членов Международ-

ного форума по аккредитации IAF, исследование проводилось по количеству сертификатов в мире), результаты по действующим сертификатам по стандартам следующие:

- ISO 9001 (менеджмент качества) - 1 265 215 сертификатов,
- ISO 14001 (экологический менеджмент) - 529 853 сертификата,
- ISO 45001 (менеджмент охраны труда) - 397 339 сертификатов,
- ISO/IEC 27001 (менеджмент IT безопасности) - 71 549 сертификатов,
- ISO 22000 (менеджмент пищевой безопасности) - 45 459 сертификатов,
- ISO 13485 (менеджмент качества производителей медицинских изделий) - 29 741 сертификатов,
- ISO 50001 (энергетический менеджмент) - 28 164 сертификата,
- ISO 20000-1 (менеджмент безопасности ITсервисов) - 27 009 сертификатов,
- ISO 37001 (менеджмент противодействия взяточничеству) - 5 969 сертификатов,
- ISO 22301 (менеджмент непрерывности бизнеса) - 3 200 сертификатов,
- ISO 39001 (менеджмент дорожной безопасности) - 1 550 сертификатов,
- ISO 55001 (менеджмент активов) - 997 сертификатов,
- ISO 29001 (менеджмент качества поставщиков нефтегазовой отрасли) - 177 сертификатов [4].

ГОСТ Р ИСО/МЭК 27001-2021 используется банками, страховыми компаниями и другими финансовыми учреждениями для обеспечения безопасности своих операций и защиты данных:

- здравоохранение: в медицинской индустрии имеется много конфиденциальной информации пациентов, включая медицинские записи и личные данные. Организации в сфере здравоохранения часто используют ISO/IEC 27001 для обеспечения безопасности этих данных и соблюдения законодательства о конфиденциальности здравоохранения;

- IT-сектор: ИСО/МЭК 27001-2021 также широко применяется в IT-секторе, где безопасность данных и защита сетей являются первоочередными задачами. Он используется как руководство по улучшению практик безопасности информации в разработке и управлении программным обеспечением, а также в предоставлении облачных и IT-услуг.

Однако стандарт ИСО/МЭК 27001-2021 может быть применен практически в любой организации, для которой информационная безопасность играет важную роль. Они помогают организациям установить системный подход к управлению безопасностью информации и снизить риски, связанные с нарушением информационной безопасности.

Рассмотрим общую модель непрерывного совершенствования процессов PDCA (Plan-Do-Check-Act), известную как цикл Деминга-Шухарта. Он является основой организационной модели ИСО/МЭК 27001-2021 для систем управления информационной безопасностью [6, с. 3-4]. Цикл Деминга-Шухарта показывает последовательность управления, состоящую из четырёх действий:

- цели и результаты(бизнес-планирование) P;
- организация D;
- соответствие полученных результатов поставленным целям C;
- действие A.

В организационной среде модель PDCA (Plan-Do-Check-Act) может и должна применяться в различных областях [6, с. 3-4].

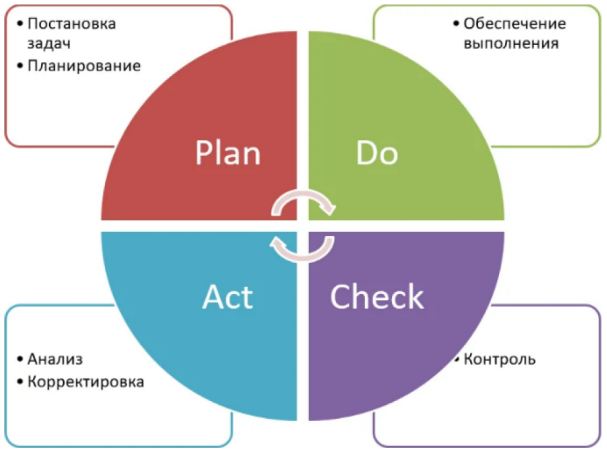

Рис. 1. Цикл Деминга-Шухарта [3, 19]

Цикл Деминга-Шухарта состоит из четырех последовательно повторяющихся этапов, предложенных Джозефом Демингом и Уильямом Шухартом, которые необходимы для достижения непрерывного улучшения (рис. 1):

- P(Plan) планирование – включает в себя определение проблемы, сбор, анализ информации и разработку плана, что определяет стратегию цели и методы достижения результата;
- D(Do) организация – включает в себя выполнение запанированных задач и процессов по достижению цели;
- A(Act) действие – включает меры для стабилизации и стандартизации улучшенных процессов;

- C(Check) проверка – включает в себя сбор и анализ данных, контроль и оценку результатов.

Цикл Деминга-Шухарта может повторяться, т.к. этот системный подход к управлению качеством в организациях позволяет достичь непрерывного улучшения и совершенствования.

Результаты исследования

Трудности и возможные пути их решения, которые могут возникнуть при настройке систем защиты информации для промышленных предприятий, могут возникнуть из-за:

- низкая квалификация персонала предприятия. Необходимо создавать максимально автономные системы защиты с повышенной надежностью, требующие минимального участия оператора на удаленном производственном участке;

- отсутствие взаимодействия между различными подразделениями предприятия. Необходимо распределить обязанности между сотрудниками и закрепить их в должностных инструкциях;

- устаревшая программно-аппаратная база и проблема регулярных исправлений для систем реального времени. Решение – организация компенсационных мероприятий по охране труда и функциональной безопасности, разработка регламентов технического обслуживания на период технологического простоя, составление планов модернизации;

- непрерывность работы систем автоматизации производства. Здесь могут помочь предварительные испытания с участием производителей для определения совместимости предлагаемых решений с целевой системой.

Если не внедрить систему безопасности своевременно, предприятие может ожидать три критических последствия: потеря пользовательских данных, техногенная катастрофа или перерыв в работе. После этого предприятие рискует столкнуться с гораздо более опасными проблемами, чем кибератаки.

Чтобы защитить себя в этой области, предприятиям теперь следует подумать, какие средства защиты они выбирают и каких атак следует опасаться больше всего [13, с. 3].

Проще говоря, это комплекс мер, который охватывает три основных уровня:

- производительность некритичных для бизнеса сервисов, таких как веб-сайт компании. Компания должна быть готова к обычным DDoS-атакам и другим методам кибератак;

- защита критической информации, включая персональные данные и коммерческую тайну. Задача специалистов по информационной безопасности – защитить ИТ-узлы таким образом, чтобы организация могла функционировать без репутационных или финансовых потерь;

- нормативные требования. Часто руководство предприятия, оценив затраты на решения по информационной безопасности, пытается максимально снизить издержки. Государство понимает нежелание организаций тратить деньги на то, что может и не произойти, но, с другой стороны, есть критические процессы, которые необходимо предотвращать, поэтому власти юридически обязаны рекомендовать предприятиям принятие мер по обеспечению экономической безопасности.

Также важным моментом является то, кто атакует, это могут быть просто квалифицированные студенты, которые совершают атаку для развлечения или для повышения своей репутации в хакерском сообществе, но могут быть и спецслужбы или военизированные группировки, для которых нанесение критического урона является прямой задачей.

Те методы защиты, что работают против студентов, вряд ли остановят хакеров, работающих на чужое государство. Соответственно предприятиям нужен такой уровень систем информационной безопасности, который позволит противостоять всем видам атак. В условиях санкций для поддержания высокого уровня безопасности информации необходимы отечественные разработки.

Рынок обеспечения информационной безопасности в России в ближайшие годы станет рынком только отечественных производителей. Это подтвердил В.В. Путин, выступая на пленарном заседании Международного конгресса по кибербезопасности, организованного ПАО «Сбербанк» [14].

В связи с этим, на сегодняшний день особенно актуализируется задача, связанная с кодированием и шифрованием информации, а также изучением, развитием и использованием инновационных методов защиты информации. В современном секторе обеспечения информационной безопасности для различных организаций особенную актуальность приобретают вопросы развития и применения биометрических методов защиты информации [10, с. 1236-1239].

Бизнес это понимает, поэтому инвестиции в сферу информационной безопасности за последний год значительно возросли.

С развитием технологий и все большей цифровизацией бизнес-процессов, угрозы и риски в области информационной безопасности также увеличиваются. В связи с этим растет спрос на системы обеспечения информационной безопасности, что может привести к повышению их цены.

Также системы информационной безопасности должны включать инструменты обнаружения новых сложных систем, которые способствуют развитию продвинутых технологий и устранению новых угроз.

Исходя из этого необходимо своевременно развивать, актуализировать и реконструировать современные технологии информационной безопасности, чтобы обезопасить предприятие от внешних атак и угроз.

Современные средства защиты информации можно разделить на несколько основных направлений развития: физические, аппаратные, организационные, программные, законодательные [12, с. 62-67]. И каждая составная часть должна быть охвачена современными наработками.

Все это требует времени и дополнительных затрат, которые могут отразится на стоимости системы информационной безопасности, так как влекут за собой не только своевременное обновление и актуализацию технологий, но и своевременное обучение сотрудников новым технологиям.

Выводы и предложения

В настоящий момент существует необходимость формирования благоприятных условий для повышения уровня информационной безопасности предприятий. Используя в качестве инструмента совершенствование законодательной базы государство сможет сформировать подходящую среду для недопущения возникновения угроз критическим отраслям российской экономики. Промышленные предприятия смогут разрабатывать и реализовывать стратегию обеспечения своей информационной безопасности, с учетом технических и организационных мер по использованию современных технологий защиты данных.

Резюмируя выше сказанное, можно сказать, что правильное восприятие требований к информационной безопасности должно соответствовать соблюдениям нормативных и законодательных стандартов, оценки предполагаемых рисков и угроз уязвимости предприятия, а также соответствовать требованиям, принципам и целям защиты информации предприятия.

Список литературы

1. Апатова Н.В. Кибербезопасность: проблемы бизнеса // Проблемы информационной безопасности социально-экономических систем: VIII Всероссийская с международным участием научно-практическая конференция, Симферополь - Гурзуф, 17–19 февраля 2022 года. Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2022. С. 3.

2. Голубев В.С., Пирогова О.Е. Проблемные вопросы внедрения информационных технологий в целях обеспечения безопасности бизнеса // Сборник материалов XXII Международной научно-практической конференции «Смирновские чтения – 2023», Санкт-Петербург, 22–24 марта 2023 года / Международный банковский институт имени Анатолия Собчака. Том Часть 1. Санкт-Петербург: Международный банковский институт имени Анатолия Собчака, 2023. С. 37-44.
3. Деминг Э. Выход из кризиса: Новая парадигма управления людьми, системами и процессами. М.: Альпина Паблишер, 2012. 419 с.
4. ИСО опубликовала очередное исследование рынка сертификации за 2022 год. URL: https://ajaregistrars.ru/blog/iso-opublikovala-ocherednoe-issledovanie-rynka-sertifikatsii-za-2022-god/
5. Исследование рисков бизнес-информации по этапам бизнес-процесса организации / И. В. Мандрица, В. И. Петренко, А. П. Жук [и др.] // Проблемы информационной безопасности социально-экономических систем: VII Всероссийская с международным участием научно-практическая конференция, Гурзуф, 18–20 февраля 2021 года. Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2021. С. 20-29.
6. Каюмова Д.Д. Проектирование системы управления информационной безопасностью в организациях // Молодой ученый. 2019. № 4(242). С. 3-4.
7. Лебедева Т.С., Усольцев Н.С. Кибербезопасность в торговле: как обезопасить данные клиентов и защитить бизнес от кибератак // Фундаментальные и прикладные исследования в области управления, экономики и торговли : Сборник трудов Всероссийской научно-практической и учебно-методической конференции. В 8-ми частях, Санкт-Петербург, 15–19 мая 2023 года. Том Часть 4. Санкт-Петербург: ПОЛИТЕХ-ПРЕСС, 2023. С. 216-223.
8. Макаров А.Н., Макаров Э.А. Информационная и цифровая экономика в контексте экономической методологии и теории. Курск: Закрытое акционерное общество «Университетская книга», 2023. 185 с.
9. Милкина Ю.А., Макарова Е.Е. Внедрение современных информационных технологий в строительную отрасль // Организатор производства. 2021. Т. 29. № 3. С. 101-110.
10. Муратова М.Н. Информационная безопасность в области оценки недвижимости // Экономика и предпринимательство. 2023. № 1 (150). С. 1236-1239.
11. Муратова М.Н. Информационная безопасность в системе управления проектами развития промышленного предприятия // Экономика и предпринимательство. 2022. № 10 (147). С. 1305-1309.

12. Муратова М.Н., Камчатова Е.Ю. Реализация ресурсного эффекта при оценке проекта развития промышленного предприятия // Ученые записки Российской академии предпринимательства. 2022. Т. 21. № 3. С. 62-67.
13. Пашков Н.Н., Дрозд В.Г. Анализ рисков информационной безопасности и оценка эффективности систем защиты информации на предприятии // Современные научные исследования и инновации. 2020. № 1(105). С. 3.
14. Пленарное заседание Международного конгресса по кибербезопасности. URL: http://www.kremlin.ru/events/president/news/57957
15. Проскурина З.Б., Макарова Е.Е. Доверительное управление имущественным комплексом как фактор инновационного развития экономики // Экономика и предпринимательство. 2018. № 8 (97). С. 584-589.
16. Сыщикова Е.Н. Направления повышения эффективности производства на основе модернизации системы управления предприятием. Монография. Saint-Louis, Missouri, USA: Science and Innovation Center Publishing House, 2017. 216 с. https://doi.org/10.12731/Syshchikova.2017.216
17. Сыщикова Е.Н. Теория и методы повышения эффективности системы управления на предприятии: монография / ГОУВПО «Воронежский гос. технический ун-т». Воронеж: Воронежский гос. технический ун-т, 2010. 206 с.
18. Шакин Д.Н., Бунев Е.Г., Доценко С.М., Ильин А.П., Марголин П.С., Пирумов В.С., Тынянкин С.И. Информационная безопасность. М.: ЗАО «Издательский дом «Оружие и технологии»», 2009. 256 с.
19. Shewhart W.A. Statistical method from the viewpoint of quality control. Washington: The Graduate School, the Department of Agriculture, 1939. P. 155. Цитировано по: Нив Генри Р. Пространство доктора Деминга: принципы построения устойчивого бизнеса. М.: Альпина Бизнес Букс, 2005. 370 с.

References

1. Apatova N.V. *Problemy informatsionnoy bezopasnosti sotsial'no-ekonomicheskikh sistem: VIII Vserossiyskaya s mezhdunarodnym uchastiem nauchno-prakticheskaya konferentsiya, Simferopol'- Gurzuf, 17–19 fevralya 2022 goda* [Problems of information security of socio-economic systems: VIII All-Russian scientific and practical conference with international participation, Simferopol - Gurzuf, February 17–19, 2022]. Simferopol: Crimean Federal University, 2022, p. 3.
2. Golubev V.S., Pirogova O.E. *Sbornik materialov XXII Mezhdunarodnoy nauchno-prakticheskoy konferentsii "Smirnovskie chteniya – 2023", Sankt-Peterburg, 22–24 marta 2023 goda* [Collection of materials of the XXII International Scientific and Practical Conference "Smirnov Readings - 2023", St. Petersburg,

March 22–24, 2023] / International Banking Institute named after Anatoly Sobchak. Part 1. St. Petersburg: International Banking Institute named after Anatoly Sobchak, 2023, pp. 37-44.
3. Deming E. *Vykhod iz krizisa: Novaya paradigma upravleniya lyud'mi, sistemami i protsessami* [Out of the crisis: A new paradigm for managing people, systems and processes]. M.: Alpina Pablisher, 2012, 419 p.
4. ISO has published another certification market study for 2022. URL: https://ajaregistrars.ru/blog/iso-opublikovala-ocherednoe-issledovanie-rynka-sertifikatsii-za-2022-god/
5. Mandritsa I.V., Petrenko V.I., Zhuk A.P. et al. *Problemy informatsionnoy bezopasnosti sotsial'no-ekonomicheskikh sistem: VII Vserossiyskaya s mezhdunarodnym uchastiem nauchno-prakticheskaya konferentsiya, Gurzuf, 18–20 fevralya 2021 goda* [Problems of information security of socio-economic systems: VII All-Russian with international participation of scientific and practical conference, Gurzuf, February 18–20, 2021]. Simferopol: Crimean Federal University, 2021, pp. 20-29.
6. Kayumova D.D. *Molodoy uchenyy,* 2019, no. 4(242), pp. 3-4.
7. Lebedeva T.S., Usol'tsev N.S. *Fundamental'nye i prikladnye issledovaniya v oblasti upravleniya, ekonomiki i torgovli : Sbornik trudov Vserossiyskoy nauchno-prakticheskoy i uchebno-metodicheskoy konferentsii. V 8-mi chastyakh, Sankt-Peterburg, 15–19 maya 2023 goda* [Fundamental and applied research in the field of management, economics and trade: Collection of proceedings of the All-Russian scientific, practical and educational conference. In 8 parts, St. Petersburg, May 15–19, 2023]. Part 4. St. Petersburg: Polytech-Press, 2023, pp. 216-223.
8. Makarov A.N., Makarov E.A. *Informatsionnaya i tsifrovaya ekonomika v kontekste ekonomicheskoy metodologii i teorii* [Information and digital economics in the context of economic methodology and theory]. Kursk: Universitetskaya kniga, 2023, 185 p.
9. Milkina Yu.A., Makarova E.E. *Organizator proizvodstva,* 2021, vol. 29, no. 3, pp. 101-110.
10. Muratova M.N. *Ekonomika i predprinimatel'stvo,* 2023, no. 1 (150), pp. 1236-1239.
11. Muratova M.N. *Ekonomika i predprinimatel'stvo,* 2022, no. 10 (147), pp. 1305-1309.
12. Muratova M.N., Kamchatova E.Yu. *Uchenye zapiski Rossiyskoy akademii predprinimatel'stva,* 2022, vol. 21, no. 3, pp. 62-67.
13. Pashkov N.N., Drozd V.G. *Sovremennye nauchnye issledovaniya i innovatsii,* 2020, no. 1(105), p. 3.
14. Plenary session of the International Congress on Cybersecurity. URL: http://www.kremlin.ru/events/president/news/57957

15. Proskurina Z.B., Makarova E.E. *Ekonomika i predprinimatel'stvo,* 2018, no. 8 (97), pp. 584-589.
16. Syshchikova E.N. *Napravleniya povysheniya effektivnosti proizvodstva na osnove modernizatsii sistemy upravleniya predpriyatiem* [Directions for increasing production efficiency based on modernizing the enterprise management system]. Monograph. Saint-Louis, Missouri, USA: Science and Innovation Center Publishing House, 2017, 216 p. https://doi.org/10.12731/Syshchikova.2017.216
17. Syshchikova E.N. *Teoriya i metody povysheniya effektivnosti sistemy upravleniya na predpriyatii* [Theory and methods of increasing the efficiency of the management system at an enterprise]: monograph. Voronezh: Voronezh State Technical University, 2010, 206 p.
18. Shakin D.N., Bunev E.G., Dotsenko S.M., Il'in A.P., Margolin P.S., Pirumov V.S., Tynyankin S.I. *Informatsionnaya bezopasnost'* [Information Security]. M.: Oruzhie i tekhnologii Publ., 2009, 256 p.
19. Shewhart W.A. Statistical method from the viewpoint of quality control. Washington: The Graduate School, the Department of Agriculture, 1939, p. 155.

ДАННЫЕ ОБ АВТОРАХ

Сыщикова Елена Николаевна, заведующий кафедрой «Экономики и управления недвижимостью», доктор экономических наук, доцент
Российский государственный университет правосудия
ул. Новочеремушкинская, 69, г. Москва, 117418, Российская Федерация
syshhikova.elena@mail.ru

Макарова Екатерина Евгеньевна, доцент кафедры «Экономики и управления недвижимостью», кандидат экономических наук, доцент
Российский государственный университет правосудия
ул. Новочеремушкинская, 69, г. Москва, 117418, Российская Федерация
mak_katusha@mail.ru

Муратова Марина Николаевна, старший преподаватель кафедры «Экономики и управления недвижимостью»
Российский государственный университет правосудия
ул. Новочеремушкинская, 69, г. Москва, 117418, Российская Федерация
5856740@gmail.com

DATA ABOUT THE AUTHORS

Elena N. Syshchikova, Head of the Department of «Economics and Real Estate Management», Doctor of Economics, Associate Professor
Russian State University of Justice
69, Novocheremushkinskaya Str., Moscow, 117418, Russian Federation
syshhikova.elena @mail.ru
SPIN-code: 6017-1081

Ekaterina E. Makarova, Associate Professor «Economy and Property Management», Candidate of Economic Sciences, Associate Professor
Russian State University of Justice
69, Novocheremushkinskaya Str., Moscow, 117418, Russian Federation
mak_katusha@mail.ru
SPIN-code: 2838-5305

Marina N. Muratova, Senior Lecturer «Economy and Property Management»
Russian State University of Justice
69, Novocheremushkinskaya Str., Moscow, 117418, Russian Federation
5856740@gmail.com
SPIN-code: 7019-4558

Поступила 20.02.2024 Received 20.02.2024
После рецензирования 05.05.2024 Revised 05.03.2024
Принята 18.03.2024 Accepted 18.03.2024