УДК 004.056

Оценка состояния безопасности ИТ-инфраструктуры в организации

© Е. Ю. Головина, А. В. Журавлева, Л. И. Татарникова
Иркутский национальный исследовательский технический университет, г. Иркутск, Российская Федерация

Аннотация. Прогресс информационных систем и технологий предлагает жизненно важные преимущества для бизнеса. Эти изменения, безусловно, несут с собой новые угрозы безопасности. В связи с этим, в данной статье обозначена важность аудитов ИТ-безопасности на регулярной основе, позволяющих составить четкую картину среды рисков кибербезопасности организации и подготовиться к таким угрозам как социальная инженерия и фишинговые атаки. Авторами был выявлен ряд основных вопросов, которые раскрываются в результате проведения процедуры аудита, представлена авторская классификация основных видов аудита кибербезопасности, рассмотрены этапы его проведения и приведены примеры действий по повышению безопасности. Проанализирован инструментарий, который рекомендуется применять для проведения внутреннего аудита ИТ-безопасности. Описаны основные причины возникновения проблем при проведении ИТ-аудита инфраструктуры и возможные пути их решения. Проводимые на регулярной основе аудиты и аналитика безопасности для всего спектра функций способствуют повышению уровня информационной безопасности организации.

Ключевые слова: ИТ-инфраструктура, информационная безопасность, оценка кибербезопасности, аудит информационной безопасности, методика аудита ИТ-инфраструктуры, системы менеджмента информационной безопасности

Assessment of the security status of the IT- infrastructure in the organization

© Elena Y. Golovina, Anna V. Zhuravleva, Ludmila I. Tatarnikova
Irkutsk National Research Technical University, Irkutsk, Russian Federation

Abstract. Advances in information systems and technology offer vital business benefits. These changes certainly bring with them new security threats. In this regard, this article outlines the importance of IT security audits on a regular basis in order to get a clear picture of the organization's cybersecurity risk environment and prepare for threats such as social engineering and phishing attacks. The authors identified a number of key issues that are revealed as a result of the audit procedure, presented the author's classification of the main types of cybersecurity audit, considered the stages of the audit, and provided examples of actions to improve security. The toolkit, which is recommended to be used for conducting an internal audit of IT security, has been analyzed. The main causes of problems during the IT infrastructure audit and possible solutions are described. Regular audits and security analytics across the full range of functions help to improve the level of information security of the organization.

Keywords: IT-infrastructure, information security, cybersecurity assessment, information security audit, IT-infrastructure audit methodology, information security management systems

Последнее время наблюдается рост числа киберпреступлений в различных отраслях промышленности по всему миру, тысячи компаний становятся жертвами вредоносных программ, DDoS-атак и тому подобное. Согласно данным аналитических агентств, во время пандемии COVID-19 кибератаки на бизнес увеличились на 300 %, а средняя стоимость утечки данных достигла 4,24 миллиона долларов в 2021 году с 3,86 миллиона долларов в 2020 году. Несмотря на то что большинство регулирующих и руководящих органов прилагают все усилия для предотвращения таких инцидентов, тем не менее очевидно, что ни один бизнес или отрасль не могут быть на 100 % защищены от меняющегося ландшафта угроз. В современных реалиях бизнесу крайне важно проявлять инициативу в борьбе с любыми потенциальными угрозами и атаками и иметь эффективную стратегию кибербезопасности. Это именно то, когда и где аудит ИТ-безопасности может быть полезен. Большое количество угроз можно предотвратить, создав надежную систему защиты от киберпреступлений. Этого можно достичь с помощью эффективного процесса оценки – аудита информационной безопасности, который помогает определить

угрозы, установить меры безопасности и еще больше повысить общую безопасность бизнес-инфраструктуры и бизнес-операций.

Категория понятия «аудит информационной безопасности» еще не устоялась и имеет различные трактовки, но в общем случае его можно описать как процесс оценки, в ходе которого оцениваются установленные в организации методы обеспечения безопасности. Это процесс, который определяет эффективность систем защиты от любых угроз. Аудит информационной безопасности обычно включает сканирование уязвимостей, тестирование на проникновение, оценку сети и многое другое, что помогает определить уровень защищенности организации в ИТ-системах от атак злоумышленников.

Наряду с аудитом безопасности, также актуальна и оценка ИТ-рисков. Несмотря на то что оба процесса включают в себя изучение и оценку рисков безопасности для организации, все же различия между ними есть и связаны они с сроками и масштабами проведения.

Оценка риска часто выполняется в начале ИТ-инициативы, до развертывания инструментов и технологий, с целью определения лучшего их построения. Аудит безопасности проводится в уже существующей ИТ-инфраструктуре и позволяет проверить состояние всех систем и операций компании: оборудования, программного обеспечения, служб, сетей и центров обработки данных через регулярные промежутки времени, с целью постоянного мониторинга и оценки кибербезопасности для устранения известных угроз, другими словами, аудит безопасности как процесс протекает гораздо глубже, чем оценка риска.

Удовлетворяя растущую потребность в инструментах управления ИТ-безопасностью, был разработан ряд стандартов. Общепризнанным в мире в сфере кибербезопасности является стандарт ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements [1]. На сегодня семейство данного стандарта содержит более тридцати документов, регламентирующих различные сегменты системы менеджмента информационной безопасности (СМИБ), от уровня стратегического менеджмента и контроля СМИБ, и заканчивая техническими рекомендациями по применению отдельных программно-технических и организационных мер защиты информации [2].

Другой стандарт аудита ИТ-безопасности, являющийся международным индустриальным стандартом PCI Data Security Standard (PCI DSS), распространяется на организации, работающие с данными платежных карт клиентов, предназначенный для обеспечения защиты данных платежных карт, связанных с транзакциями онлайн-платежей [3, 4]. Так, например, в платежной системе (ПС) «Мир» для обеспечения безопасности данных карт как раз применяется PCI DSS.

Такая методология как FRAP (Facilitated Risk Analysis Process), представляет упрощенный анализ и оценку рисков информационной безопасности, с ориентацией на более критичные активы. В данном процессе участвуют группа экспертов по предмету и фасилитатор. Качественный анализ проводится с использованием методов мозгового штурма.

В отличие от предыдущей, методология OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) основана на методах операционных рисков и безопасности, а не на технологиях, и ориентирована на самоуправляемый подход, означающий, что члены бизнес-подразделений берут на себя ответственность за разработку стратегии безопасности организации в целом.

По мере развития угроз кибербезопасности компании должны адаптировать и переосмыслить свои стратегии безопасности. Это означает переход от традиционных технологий к новым основам кибербезопасности [5]. Одной из таких структур является структура кибербезопасности, представленная стандартами семейства NIST, разработанных Национальным институтом стандартов и технологий. NIST SP 800-39 – является основным и самым высокоуровневым из серии документов фреймворка управления рисками (Risk Management Framework). Стандарты данного семейства взаимосвязаны друг с другом и работают в координации для обеспечения эффективного управления рисками, обеспечивая полное покрытие этих аспектов. Данные структуры, а именно NIST SP 800-39 и NIST 800-37, предназначены для процесса

управления рисками, а NIST SP 800-30 – для их оценки. При этом необходимо отметить, что NIST SP 800-39 нацелен на общий процесс управления рисками, NIST SP 800-37 на структуру управления рисками (RMF) для федеральных информационных систем, а NIST SP 800-30 определяет сам процесс оценки рисков.

NIST Framework предлагает не просто руководство, а скорее он предлагает набор процессов, которые могут помочь организациям измерить зрелость их текущих систем кибербезопасности и управления рисками и определить шаги по их укреплению. Представленная структура NIST включает в себя пять основных функций:

– идентификация – определение рисков кибербезопасности для всех активов компании, включая персонал, системы и информацию;

– защита – внедрение систем для защиты наиболее важных активов;

– обнаружение – обнаружение активных событий кибербезопасности, которые могут представлять угрозу для бизнес-среды;

– ответ – принятие мер против угроз для предотвращения или смягчения ущерба;

– восстановление – восстановление возможностей или служб, поврежденных угрозой.

Эти пять функций являются основой всесторонней и эффективной стратегии кибербезопасности, призванной повысить способность компании противостоять угрозам. Технологии аудита и аналитики безопасности воплощают эти принципы и ориентированы на предоставление данных, расширяющих ваши возможности по оценке, анализу и управлению рисками безопасности. В результате организации все чаще обращаются к аудиту, с целью внедрения и поддержания системы ИТ-безопасности.

Чтобы инфраструктурная инициатива, такая как аудит безопасности, была успешной и эффективной, необходимо выполнение ряда условий:

– понимание и поддержка со стороны высшего руководства организации, так как это поможет гарантировать получение необходимого количества времени и ресурсов;

– выполнение четких и практических рекомендаций по улучшению кибербезопасности;

– проведение аудита на регулярной основе с целью выявления слабых мест и уязвимостей в существующей ИТ-инфраструктуре, проверки средства безопасности, обеспечения соответствия нормативным требованиям.

В результате анализа достаточного количества источников в данной области исследования, авторами был выявлен ряд основных вопросов, которые раскрываются в результате проведения процедуры аудита:

– есть ли слабые места и уязвимости в текущей системе безопасности?

– существуют ли какие-либо посторонние инструменты или процессы, которые не выполняют полезную функцию безопасности?

– готовы ли в организации отразить угрозы безопасности и восстановить бизнес-возможности в случае сбоя системы или утечки данных?

– в случае обнаружения недостатков в системе безопасности, какие конкретные действия может организация предпринять для их устранения?

Необходимо отметить, что приоритизация угроз, выявленных в ходе аудита, является одним из наиболее важных шагов. При этом важно учитывать три основных фактора: потенциальный ущерб от события, вероятность этого события и текущую способность справиться с этим событием. Среднее значение этих трех факторов, как правило, дает оценку риска.

Рассматривая вопросы аудита кибербезопасности, необходимо отметить и другие факторы, которые также следует учитывать:

1. Текущие тенденции кибербезопасности: какой текущий метод выбирают хакеры? Какие угрозы становятся все более популярными, а какие встречаются реже?

2. Тенденции на уровне отрасли: какие типы утечек наиболее распространены в конкретной отрасли?

3. Регулирование и соблюдение: какова организационно-правовая форма организации? Какие данные обрабатываются? Работает ли организация с конфиденциальной финансовой или личной информацией? Кто имеет доступ к различным системам?

Ответы на эти вопросы повлияют на оценку риска, которая присваивается опре-

деленным угрозам, и на ценность, которая придается конкретным активам.

Тщательный аудит также может помочь в соблюдении законов о безопасности данных, регламентированных национальными и международными нормами.

Аудит соответствия обычно проводится сертифицированным аудитором безопасности из соответствующего регулирующего органа или независимого стороннего поставщика. Однако в некоторых случаях персонал компании может провести внутренний аудит, чтобы проверить соответствие компании нормативным требованиям или общий уровень безопасности [6]. Исходя из этого, выделяют внутренний аудит, когда используются собственные ресурсы и сотрудники компании (отдел внутреннего аудита), и внешний аудит, к процессу привлекается сторонняя организация.

Во время аудита безопасности каждая система, которую использует организация, может быть проверена на наличие уязвимостей в следующих областях: сетевые уязвимости (регулярный мониторинг сетевого трафика, включая электронную почту, мгновенные сообщения, файлы и другие сообщения, доступность сети и точки доступа); контроль безопасности (включает в себя оценку того, насколько хорошо организация внедрила политику и процедуры, которые она установила для защиты своей информации и систем); шифрование (проверка наличия в организации средств контроля для управления процессами шифрования данных); программные системы (проверка адекватности работы ПО); возможности управления архитектурой (проверка наличия у руководства ИТ организационных структур и процедур для создания эффективной и контролируемой среды для обработки информации); управление телекоммуникациями (проверка работоспособности телекоммуникационных средства управления как на стороне клиента, так и на стороне сервера, а также в сети, которая их соединяет); обработка информации (подтверждение принятия мер безопасности обработки данных) [7].

Наличие значительного числа областей мониторинга позволило авторам статьи выделить следующие основные виды аудита информационной безопасности, представленные на рис. 1.

Далее выделим основные этапы аудита, включающие сбор и обработку полученной информации, анализ с последующей интерпретацией предложений по повышению уровня защиты ИС. Аудиты безопасности, являясь частью общей стратегии защиты ИТ-систем и данных, состоят из пяти этапов:

1. Определение и согласование цели. В процесс обсуждения того, что должно быть достигнуто с помощью аудита, включаются все заинтересованные стороны.

2. Определение области аудита. Выявляются все активы, подлежащие аудиту, включая компьютерное оборудование, внутреннюю документацию и обработанные данные.

3. Процедура аудита и выявление угроз. Определение потенциальных угроз, связанных с каждым из существующих бизнес-процессов, в том числе физический осмотр центра обработки данных на предмет устойчивости к пожарам, наводнениям и скачкам напряжения в рамках оценки аварийного восстановления.

4. Оценка безопасности и рисков. Анализ рисков возникновения каждой из выявленных угроз и то, какие превентивные меры защиты от них применяются в организации [8].

5. Формирование результатов отчета и определение необходимых элементов управления. Сбор всей документации, связанной с аудитом, в официальный отчет, который можно передать заинтересованным сторонам из руководства или регулирующему органу. Отчет должен включать список любых угроз безопасности и уязвимостей, обнаруженных в системах, а также действия, которые ИТ-специалисты рекомендуют предпринять для их устранения.

Так примеры действий по повышению безопасности могут включать:

– выполнение процедур по исправлению конкретного недостатка безопасности;

– обучение сотрудников соблюдению требований безопасности данных и осведомленности о безопасности;

– внедрение дополнительных инновационных методов обработки конфиденциальных данных и распознавания признаков вредоносных программ и фишинговых атак;

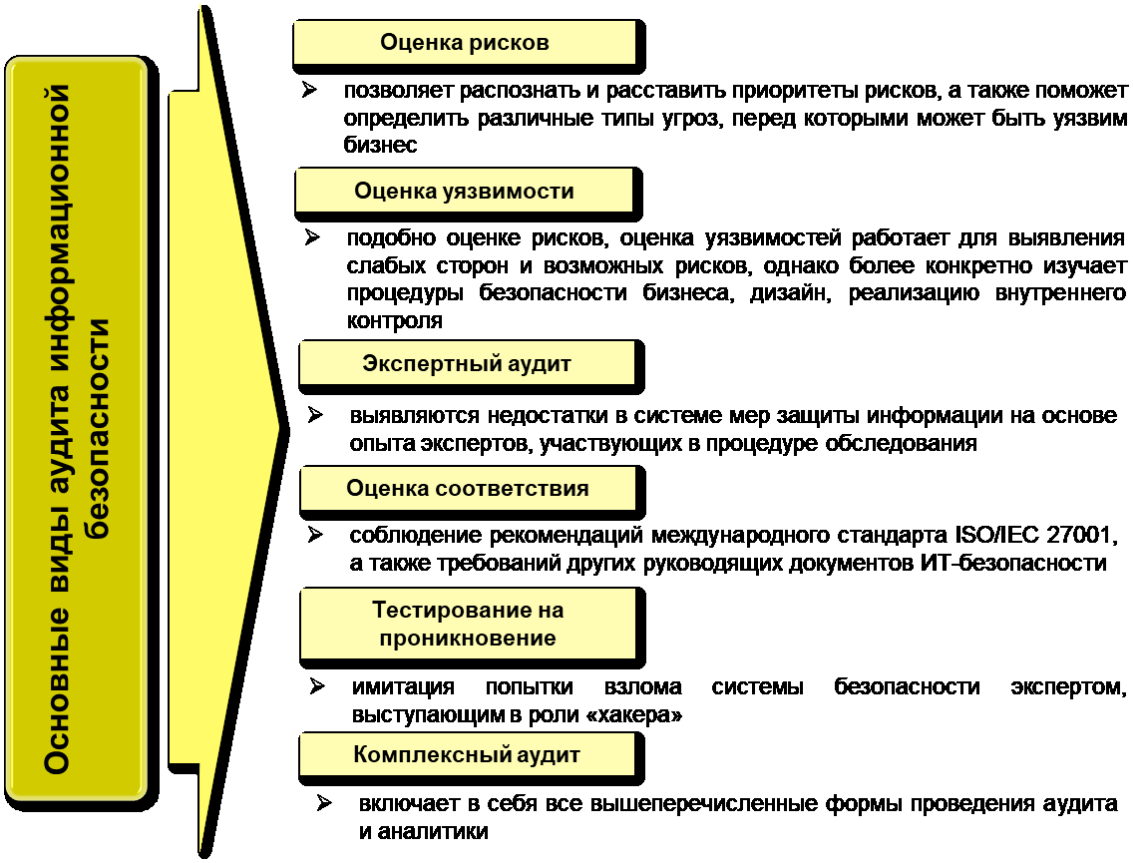

Рис. 1. Авторская классификация видов аудита кибербезопасности

– приобретение новых технологий для защиты существующих систем и регулярного мониторинга имеющейся инфраструктуры на предмет угроз безопасности.

Как правило, рекомендации направлены не на полное устранение всех выявленных рисков, а лишь на их уменьшение до приемлемого уровня. При выборе мер для повышения уровня защиты ИС учитывается одно принципиальное ограничение – стоимость реализации этих мер не должна превышать стоимости защищаемых информационных ресурсов, а также убытков компании от возможного нарушения конфиденциальности, целостности или доступности информации.

Другим немаловажным фактором является необходимость учитывать ряд проблем, которые могут возникнуть при проведении ИТ-аудита инфраструктуры [9]. Авторы выделяют наиболее распространенные среди них, представленные на рис. 2.

Также, прежде чем приступить к процессу аудита безопасности, важно определиться с его видом и сделать правильный выбор набора инструментов [10].

Сегодня на рынке существует ряд автоматизированных методов аудита, оптимизирующих сам процесс и облегчающий соблюдение требований посредством мониторинга, управления и отчетности. Kali Linux – одна из таких ОС, которая настроена и содержит набор инструментов для проведения аудита безопасности. Эту операционную систему можно использовать, установив ее на отдельную машину или загрузив в существующую машину с двойной загрузкой, или на виртуальной машине в облачном сервере.

Рассматриваемый ниже инструментарий логичнее применять для проведения внутреннего аудита ИТ-безопасности, используя собственные ресурсы:

1. Recon Dog (собака-разведчик) – этот инструмент не требует установки и используется как обычный скрипт, с целью выявления точных слабых мест ИТ-инфраструктуры.

2. Nmap – применяется для обнаружения уязвимостей открытых портов и снятия отпечатков пальцев как внутри сети, так и через Интернет.

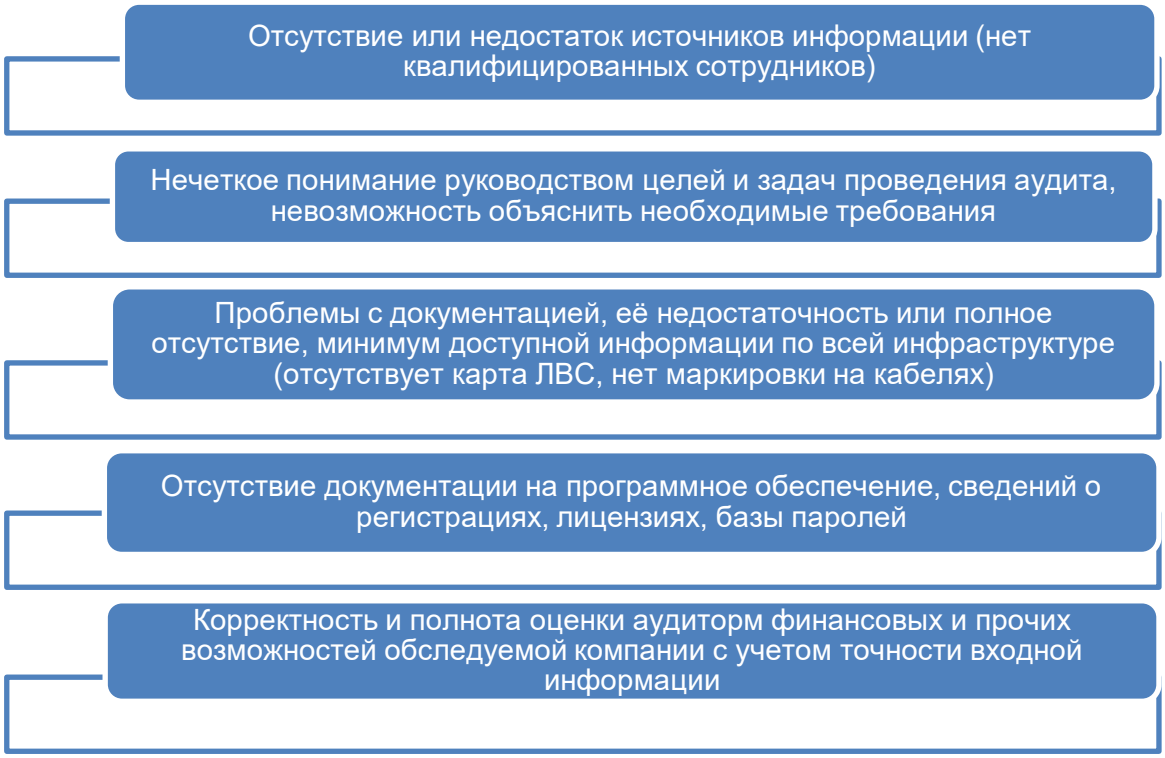

Рис. 2. Ключевые проблемы, возникающие при аудите кибербезопасности

3. Nikto – инструмент для поиска уязвимостей на сервере. Используется для обнаружения всех виды потенциальных неправильных конфигураций сервера.

4. Платформа Metasploit – одна из самых мощных сред эксплуатации, используемых для проведения аудита ИТ-безопасности. Допустим, все потенциальные уязвимости, обнаруженные с помощью Nikto, можно проверить с помощью Metasploit, так как она содержит большое количество эксплойтов.

5. Xsser – применяется для проверки на наличие распространенных уязвимостей веб-инъекций, таких как SQL-инъекция и межсайтовые сценарии.

6. Sqlmap (SQL-карта) – для проверки ошибок SQLi на сайте.

Распространение все более совершенных угроз кибербезопасности требует, чтобы организации придерживались подхода «предполагать компрометацию»: ожидание того, что внутри их ИТ-систем уже есть злоумышленники. Традиционные инструменты безопасности, такие как технологии управления информацией и событиями безопасности (SIEM), и предотвращения потери данных (DLP), не обеспечивают всех функций безопасности. Возможностей этих инструментов самих по себе недостаточно для защиты всей инфраструктуры. Кроме того, без надлежащей настройки и процессов управления данными возникает риск потока ложных предупреждений. Поэтому организации необходимо создать надежную систему безопасности, проводя на регулярной основе аудит и внедряя аналитику безопасности для всего спектра функций: идентификация, защита, обнаружение, реагирование и восстановление. Только в этом случае все вышесказанное будет приносить реальную отдачу и способствовать повышению уровня информационной безопасности компании.

Список источников

1. Головина Е. Ю., Асминкина Т. К., Журавлева А. В., Коробова И. А. Аналитический обзор действующих стандартов системы менеджмента информационно безопасности (СМИБ) // Материалы VIII Всероссийской научно-практической конференции «Экономика инфраструктурных преобразований: проблемы и перспективы развития» (Иркутск, 30 ноября 2021 г.). Иркутск: Изд-во ИРНИТУ, 2021. Вып. 8. 279 с.

2. Прищеп С. Д. Как избежать двойных стандартов в информационной безопасности. [Электронный ресурс]. URL: https://www.iksmedia.ru /articles/5558688-Kak-izbezhat-dvojnyx-standartov-v.html (21.03.2022).
3. Nelli V. Syreyshchikova, Danil Yu. Pimenov, Tadeusz Mikolajczyk, Liviu Moldovan, Information Safety Process Development According to ISO 27001 for an Industrial Enterprise, Procedia Manufacturing. 2019. Vol. 32. P. 278-285. ISSN 2351-9789. DOI: https://doi.org/10.1016/j.promfg.2019.02.215.
4. Козьминых С. И., Козьминых П. С. Аудит информационной безопасности // Вестник Московского университета МВД России. 2016. № 1. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/audit-informatsionnoy-bezopasnosti (17.04.2022).
5. Lontsikh P. A., Safonova O. M., Koksharov A. V., Lontsikh N. P., Golovina E. Y. Remote Audit Improvement Methods in the System-oriented Information and Security Analysis (2021) Proceedings of the 2021 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", T and QM and IS 2021, pp. 178-182. DOI: 10.1109/ITQMIS53292.2021.9642900.
6. Оладько В. С. Аудит информационной безопасности в электронной коммерции // Международный научно-исследовательский журнал. 2015. № 11 (42). Часть 2. С. 76–78.
7. Макаренко С. И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018. № 1. [Электроннный ресурс]. URL: https: // cyberleninka.ru/article/n/audit informatsionnoy-bezopasnosti-osnovnye-etapy-kontseptualnye-osnovy-klassifikatsiya-meropriyatiy (16.04.2022).
8. Шелков А. Б., Шульц В. Л., Кульба В. В. Аудит информационной безопасности автоматизированных систем управления // Тренды и управление. 2014. № 4. С. 319–334.
9. Двойнишников Н. Э., Исламутдинова Д. Ф. Понятие и оценка аудита безопасности информационных систем // Московский экономический журнал. 2019. № 10.
10. Труфанов В. Н. Подход к созданию центров обработки персональных данных в организациях, обеспечивающих защиту государственных информационных ресурсов // Информатизация и связь. 2018. С. 56–62.

Информация об авторах / Information about the Authors

Елена Юрьевна Головина,
кандидат экономических наук,
доцент кафедры экономики и цифровых бизнес-технологий,
Институт экономики, управления и права,
Иркутский национальный исследовательский технический университет,
664074, г. Иркутск, ул. Лермонтова, 83,
Российская Федерация,
elena_uspeh@mail.ru

Elena Y. Golovina
Associate Professor of Economics and Digital Business Technologies Department,
Institute of Economics, Management and Law,
Irkutsk National Research Technical University,
83 Lermontov St., Irkutsk 664074,
Russian Federation,
elena_uspeh@mail.ru

Анна Владимировна Журавлева,
магистрант группы УПКм-20-1,
Институт высоких технологий,
Иркутский национальный исследовательский технический университет,
664074, г. Иркутск, ул. Лермонтова, 83,
Российская Федерация,
anna.zhuravleva22@yandex.ru

Anna V. Zhuravleva,
Undergraduate,
Institute of High Technologies,
Irkutsk National Research Technical University,
83 Lermontov St., Irkutsk 664074,
Russian Federation,
anna.zhuravleva22@yandex.ru

Людмила Ильинична Татарникова,
кандидат физико-математических наук,
доцент кафедры автоматизации и управления,
Институт высоких технологий,
Иркутский национальный исследовательский технический университет,
664074, г. Иркутск, ул. Лермонтова, 83,
Российская Федерация,
tatarnikova_li@mail.ru

Ludmila I. Tatarnikova,
Associate Professor of Automation and Management Department,
Institute of High Technologies,
Irkutsk National Research Technical University,
83 Lermontov St., Irkutsk 664074,
Russian Federation,
tatarnikova_li@mail.ru