УДК 331.1

С. Г. Симонов
ФГБОУ ВО «Тюменский индустриальный университет», Тюмень,
e-mail: mushkam@inbox.ru

ПРЕДПРИНИМАТЕЛЬСКИЕ РИСКИ, СВЯЗАННЫЕ С УДАЛЕННЫМ ФОРМАТОМ РАБОТЫ ПЕРСОНАЛА ПРЕДПРИЯТИЯ

Ключевые слова: социальные риски, информационная безопасность, режим on-line, кибератаки, фишинг, персонал, бизнес-структура, хакеры, мессенджеры, программное обеспечение.

Выяснена социальная природа и основные виды предпринимательских рисков при организации работы сотрудников предприятия в режиме on-line. Дана статистическая оценка киберпреступлений против российского бизнеса. Изучены последствия фишинговых атак на IT-инфраструктуру отечественных предприятий. Рассмотрены причины утечки корпоративных данных и потери бизнеса, связанные с рисками организации удаленной работы персонала. Охарактеризованы финансовые потери предприятий, функционирующих в режиме on-line. Изучены риски возвращения сотрудников бизнес-структуры с релокации к работе в офисе и приведены результаты социологического исследования, в каком формате они предпочитают трудиться в течение рабочей недели. Систематизированы риски несоблюдения корпоративных правил информационной безопасности удаленно занятыми работниками предприятия. Определены наиболее уязвимые элементы корпоративной системы информационной безопасности и предложены некоторые меры по повышению эффективности последней и минимизации основных видов предпринимательских рисков в условиях деятельности сотрудников предприятия в режиме on-line. В статье выявлены наиболее уязвимые места с позиции информационной безопасности тюменских предприятий. Предложены направления минимизации предпринимательских рисков при организации работы персонала в режиме on-line и повышения уровня кибербезопасности средним и малым бизнес-структурам.

S. G. Simonov
Industrial University of Tyumen, Tyumen, e-mail: mushkam@inbox.ru

BUSINESS RISKS ASSOCIATED WITH THE REMOTE FORMAT OF THE COMPANY'S STAFF

Keywords: social risks, information security, on-line mode, cyber attacks, phishing, personnel, business structure, hackers, messengers, software.

The social nature and the main types of entrepreneurial risks in the organization of the work of employees of the enterprise in the on-line mode are clarified. A statistical assessment of cybercrimes against Russian business is given. The consequences of phishing attacks on the IT infrastructure of domestic enterprises have been studied. The reasons for the leakage of corporate data and business losses related to the risks of organizing remote work of personnel are considered. The financial losses of enterprises operating on-line are characterized. The risks of returning employees of a business structure from relocation to work in the office are studied and the results of a sociological study are presented, in which format they prefer to work during the working week. The risks of non-compliance with corporate information security rules by remotely employed employees of the enterprise are systematized. The most vulnerable elements of the corporate information security system are identified and some measures are proposed to improve the effectiveness of the latter and minimize the main types of business risks in the conditions of on-line activity of the company's employees. The article identifies the most vulnerable points from the point of view of information security of Tyumen enterprises. The directions of minimizing entrepreneurial risks in the organization of staff work on-line and increasing the level of cybersecurity for medium and small business structures are proposed.

Введение

Начавшийся еще в ковидный период переход российских предприятий на функционирование в режиме on-line привел к тому, что в настоящее время многие из них продолжают его использовать, находя в «удаленке» определенные преимущества и выгоду. Вместе с тем в условиях удаленной работы все большая часть отечественных бизнес-структур, особенно средних и малых, стала сталкиваться с проблемой обеспечения информационной безопасности, когда границы киберзащиты расширяются далеко за пределы офиса предприятия. Это обусловливает известные предпринимательские риски, ибо поведение персонала предприятия в неожи-

данно изменившейся внешней бизнес-среде становится непредсказуемым и способным привести к утечке важных корпоративных данных, росту числа киберпреступлений, высоким репутационным издержкам и т.д.

Цель: выявить направления снижения предпринимательских рисков при организации работы персонала в режиме on-line и повышения уровня кибербезопасности средним и малым бизнес-структурам.

Материалы и методы исследования

Исследование проблемы предпринимательских рисков и связанного с ними обеспечения информационной безопасности деятельности предприятий, использующих удаленный формат работы сотрудников, реализовано на юге Тюменской области, которая выступает пилотной территорией для федеральной программы «Производительность труда и поддержка занятости». Для сбора эмпирического материала, лежащего в основе настоящей работы, использовались такие методы, как экспертная оценка, анкетирование, анализ вторичных данных.

Первым из названных методов были охвачены две группы экспертов:

- менеджеры высшего и среднего звеньев тюменских предприятий, принимающих участие в отмеченной федеральной программе;

- представители местных органов власти, общественных организаций и научного сообщества региона, напрямую не связанные с бизнес-деятельностью.

Анкетирование, как метод исследования, дал возможность обнаружить у возвращающихся с «удаленки» сотрудников тюменских предприятий проблемы с адаптацией и необходимость первое время поддерживать меры для вхождения в рабочий ритм офиса, а также некоторое снижение мотивации и желание сменить работу.

Анализ вторичных данных предполагал тщательное изучение материалов, которые были получены по данной тематике другими отечественными и зарубежными учеными. С помощью вторичного анализа удалось верифицировать и в известной степени интерпретировать полученные результаты исследования. Кроме того, он дал возможность сопоставить предпринимательские риски при организации работы персонала предприятий в режиме on-line, имеющие место в Тюменской области и других регионах.

Результаты исследования и их обсуждение

Проведенный нами экспресс-анализ литературы по изучаемой проблеме позволил установить наиболее часто встречающиеся виды предпринимательских рисков при организации работы сотрудников предприятий в режиме on-line. Остановимся на них подробнее.

1. Риски роста количества киберпреступлений и фишинговых атак

По данным представителей МВД России, за первые шесть месяцев 2023 года по сравнению с аналогичным периодом 2022 года число киберпреступлений увеличилось почти на треть (на 27,9%), а их раскрываемость – всего лишь на 5,4% [1]. Руководствуясь финансовыми мотивами, хакеры свои атаки направляли, в первую очередь, на промышленные и логистические предприятия, финансовые и медицинские учреждения, а также IT-компании, которые занимаются разработкой программного обеспечения.

При этом 76,3% IT-преступлений в нашей стране совершаются через интернет и около половины из них (45%) – с помощью средств мобильной связи. Что касается географии IT-преступлений, то наибольший их прирост зафиксирован в Ингушетии (в 2,17 раза), Ненецком АО (в 2,15 раза), Томской (+88,8%), Ярославской (+77,3%), Липецкой (+66,1%) областях, Ямало-Ненецком АО (+64,8%), Мордовии (+59,3%), Новгородской (+58,2%), Белгородской (+57,4%) и Тульской (+57,2%) областях. В то же время число зарегистрированных в сфере IT преступлений сократилось в Чечне (-52,9%), Дагестане (-23%), Туве (-22%), Адыгее (-9,5%) и Подмосковье (-0,3%) [2].

Сотрудники предприятия, занятые в удаленном формате, зачастую становятся жертвами фишинга. Хакеры его применяют для кражи конфиденциальной корпоративной информации, банковских счетов, паролей, номеров карт и др. Сегодня фишинговая атака представляет собой выдачу фейковых сайтов, имитирующих интернет-страницы популярных интернет-магазинов, социальных сетей, стриминговых сервисов и т.п. Расчет делается на то, что пользователь не заметит подделки и укажет на странице конфиденциальную информацию о предприятии, корпоративные или личные данные. Кроме того, хакеры могут сделать недоступным на время

шлюз удалённого доступа, а затем, представившись службой технической поддержки бизнес-структуры, сделать вид, что решают проблему конкретного пользователя, попутно выманив у него учётные данные.

Главная сложность борьбы с фишингом заключается в том, что не существует программного обеспечения, которое защитило бы предприятие и его работников, особенно в условиях удаленной работы, поскольку сайты-фейки трудно отличить от оригиналов. Все зависит от персонала – насколько он будут внимателен и компетентен для распознания фейка. В РФ число фишинговых атак растет из года в год. Чаще всего с их помощью подделываются следующие *ресурсы*: онлайн-сервисы (39,6%); почтовые сервисы (15,6%); финансовые учреждения (15%); облачные хранилища (14,5%); платежные сервисы (6,6%); букмекерские конторы (2,2%). В первую очередь фишинговые атаки используются для получения доступа к инфраструктуре предприятия, далее в ход идут другие способы взлома. Согласно данным разработчика решений по предотвращению и расследованию киберпреступлений Group-IB, около 70% всех целенаправленных атак на отечественный бизнес начинаются с фишинга. Получив с его помощью доступ хотя бы к одному корпоративному компьютеру, хакеры получают возможность закрепиться в сети предприятия и получить контроль над всей его инфраструктурой [3].

2. Риски утечки корпоративных данных

В научной литературе, посвященной кибербезопасности, утечка корпоративных данных при организации работы сотрудников в удаленном доступе рассматривается как инцидент, в результате которого произошло неправомерное раскрытие конфиденциальной информации. К сожалению, работающий на взломанных ресурсах в режиме on-line персонал не спешит ставить в известность руководство предприятия, как именно это произошло. Обычно основной причиной являются уязвимости в прикладном программном обеспечении, через которые становится возможным доступ к данным аутентификации. Не редки ситуации, когда должным образом не защищен удаленный доступ на сами серверы. Хакеры представляются ИБ-специалистами известных IT-компаний, предлагая загрузить приложение, которое якобы будет искать уязвимости. На самом деле, устанавливая программное обеспечение, сотрудники предприятия, работающие в уделенном формате, дают им право удалённого доступа к своему устройству. Чаще всего хакеры связываются с потенциальными жертвами через популярные мессенджеры, иногда – через телефонную связь.

Добавим, что утечки корпоративных данных могут явиться также следствием действий инсайдеров. Дело в том, что разработчики программного обеспечения зачастую не тестируют его должным образом и не применяют практики безопасной разработки. Последнее, в свою очередь делает утечки конфиденциальных данных предприятия возможными [4].

Отметим, что специально разгласить конфиденциальные корпоративные данные могут как «свои» люди (персонал предприятия, подрядчики, клиенты, партнеры), так и хакеры, кибермошенники. На наш взгляд, это проистекает из-за недостаточной защищенности информационной базы бизнес-структуры, отсутствия регулярного пересмотра системы ее защиты, неустранения уязвимостей, избыточного хранения корпоративных данных и неорганизованности порядка их обработки, в результате чего они могут попасть не тем субъектам.

3. Риски, следствием которых являются потери бизнес-структуры

Так как корпоративные данные могут быть самыми разными, то и последствия их потери предприятием, являющиеся результатом предпринимательских рисков при организации работы сотрудников в режиме on-line, тоже весьма дифференцированны. Условно их можно разделить на прямые и косвенные.

К *прямым* потерям предприятия относят:

- компенсации пострадавшим субъектам хозяйствования;
- штрафы от регулирующих органов в лице суда или Роскомнадзора;
- затраты предприятия на проведение расследования инцидента и степени его тяжести, определение виновных лиц;
- восстановление правомерного порядка обработки корпоративных данных, установление нового порядка, закупка более надежного информационного оборудования;
- расходы, связанные с невозможностью исполнения обязательств и вытекающими отсюда санкциями (расторжение договоров и контрактов с субъектами, кого «задела» утечка, выплата договорных неустоек и штрафов).

Косвенные потери предприятия включают:

- уход части потенциальных клиентов предприятия и контрагентов;
- снижение уровня конкурентоспособности предприятия на рынке;
- уменьшение стоимости активов предприятия (акций и иных ценных бумаг, нематериальных активов и др.);
- определенный удар по репутации предприятия;
- рост затрат на поддержание имиджа бизнес-структуры и рекламу для восстановления ее позиций на рынке;
- дополнительное, не всегда выгодное предприятию внимание со стороны регулирующих органов (правоохранительных, судебных, надзирательных, местных органов власти) [5].

По результатам ежегодного исследования «Cost of a Data Breach Report», проведенного Ponemon Institute при спонсорской и аналитической поддержке IBM Security, были выявлены следующие тенденции размера финансовых потерь предприятий, функционирующих в удаленном формате:

а) переход на работу персонала предприятия в режиме on-line увеличивает размеры финансовых потерь от утечек данных в среднем на один миллион долларов США, чем в ситуациях, в которых дистанционный фактор не задействован ($4,96 млн против $3,89 млн);

б) в отраслевом разрезе рост финансовых потерь предприятий от утечек корпоративных данных особо наблюдается в здравоохранении, розничной торговле, гностичном и ресторанном бизнесе, отраслях, производящих потребительские товары. Самые дорогостоящие утечки корпоративной информации имеют место в здравоохранении: $9,23 млн. на каждый случай в 2021 году, что на $2 млн. больше, чем в 2020 году;

в) компрометация учетных записей приводит к краже корпоративных данных, а причиной большей части вытекающих отсюда потерь является доступ с помощью украденных учетных данных;

г) к современным инструментам, помогающим снизить убытки, относятся применение искусственного интеллекта, ИБ-аналитика и шифрование, которые доказали свою эффективность в плане уменьшения финансовых потерь из-за утечек корпоративных данных. Экономия составляет от $1,25 млн. до $1,49 млн. по сравнению с предприятиями, где данные инструменты практически не используются. Что касается утечек корпоративных данных, находящихся в облаке, то предприятиям, применяющим гибридные облака, они обходятся дешевле ($3,61 млн.), чем тем, кто использует только публичное облако ($4,80 млн.) или только частное облако ($4,55 млн.) [6].

4. Риски возвращения персонала бизнес-структуры с релокации к офисной работе

Результаты наших исследований и исследований других ученых свидетельствуют, что психологически бывает весьма непросто вернуться после режима on-line, к которому привык и который удобен многим сотрудникам предприятия, к прежнему офисному.

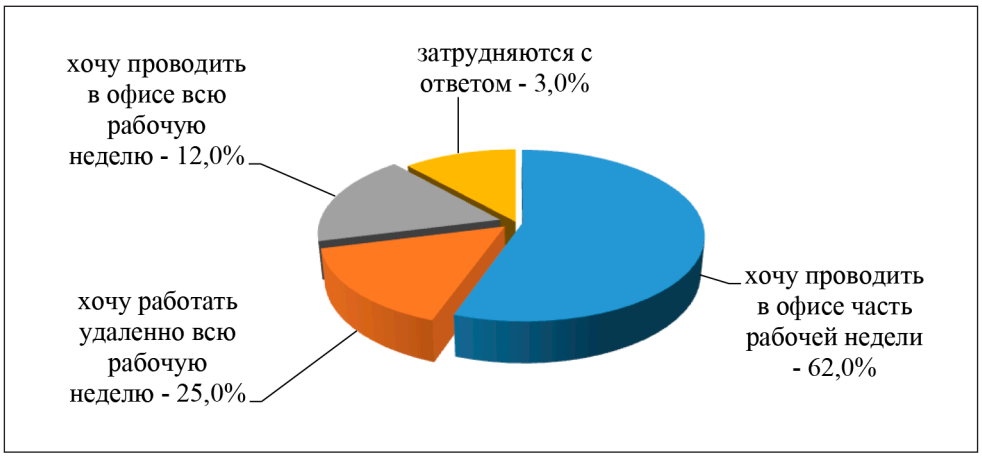

Рис. 1. Результаты ответов на вопрос: «В каком формате Вы хотели бы работать на своем предприятии?»

Например, по завершению в России ковидного периода, в течение которого большинство бизнес-структур функционировало в удаленном формате, у значительной части персонала при возвращении в офис обнаружились проблемы адаптации, потребовался комплекс поддерживающих мер для вхождения в рабочий ритм, имели место невысокая мотивация и желание сменить работу [7,8].

В известной мере это коррелирует с результатами нашего социологического исследования, которое было проведено в 2023 году и в котором приняли участие около 400 сотрудников тюменских предприятий, имеющих опыт работы в режиме on-line (рис. 1).

5. Риски несоблюдения корпоративных правил информационной безопасности персоналом предприятия при организации удаленной работы

Согласно статистике, 52% персонала предприятия, работающего в режиме on-line, не соблюдают правила информационной безопасности [9]. Очевидно, что от корпоративного менеджмента требуется спланировать бизнес-деятельность таким образом, чтобы получить преимущества от новой реальности и удаленного формата деятельности своих сотрудников. В противном случае ошибки в планировании могут привести к ряду *производных* предпринимательских рисков.

Риски несанкционированного доступа к программному обеспечению. К сожалению, реальность такова, что сегодня у многих предприятий отсутствует чёткая политика самого удалённого доступа. Функционируя в режиме on-line, они просто открывают доступ к своей корпоративной системе в надежде на авось, рассчитывая, что всё будет в порядке. Вместе с тем современная бизнес-практика такова, что без грамотной политики удалённого доступа любая уязвимость может повлечь взлом IT-инфраструктуры предприятия. Причем, в самом содержании данной политики должны быть четко и подробно прописаны все необходимые положения, что даст возможность, по нашему мнению, минимизировать для предприятия риски информационного характера.

Риски перезагрузки системы удаленного обновления оборудования и модернизации софта предприятия. При организации работы персонала предприятия в режиме on-line корпоративное оборудование с настроенными инструментами защиты переустанавливается из офисов в жилье сотрудников. При этом часто предприятию не удаётся рассчитать технические мощности оборудования, призванного выдержать нагрузку при подключении всех «удаленщиков». Возникают определенные предпринимательские риски, устранение которых требует регулярного обновления программного обеспечения, модернизации софта, оптимальной загрузки технических мощностей оборудования.

Симптоматично, что сегодня в нашей стране имеется всего лишь несколько бизнес-структур, уже разработавших системы удалённого обновления оборудования и модернизации софта и благодаря этому существенно повысивших уровень собственной информационной безопасности. Ряд предприятий также продвигаются в этом направлении, планируя у себя внедрение той же двухфакторной аутентификации [10] или NAC [11].

Риски использования корпоративного оборудования в собственных целях персоналом предприятия. Часто работники предприятия, используя в режиме on-line корпоративное программное обеспечение, устанавливают на нем личные приложения и игры. Такое «скачивание» из непроверенных источников может привести к попаданию в корпоративную сеть «вредоноса». В результате бизнес-структуре приходится внепланово проводить проверку всех устройств на наличие угроз и уязвимостей информационного характера. Заметим, что этого бы не потребовалось, если бы менеджмент предприятия своевременно установил управляющее программное обеспечение.

Риски допуска к корпоративному оборудованию третьих лиц из числа домочадцев «удаленщика»-сотрудника предприятия. В условиях удаленной работы корпоративное оборудование становится не только рабочим инструментом для работника предприятия, но и предметом досуга для членов его семьи, имеющих, как правило, свой гаджет. При этом система защиты просто отключается, или же в лучшем случае создаётся новая учётная запись. Отсюда, учётные данные сотрудника-«удаленщика» становятся достоянием его домочадцев со всеми вытекающими отсюда негативными для предприятия последствиями. После отмены режима on-line и возвращения персонала в офисы большинство учётных записей можно считать скомпрометированными, что потребует скрупулезной и продолжительной по времени процедуры замены имеющихся корпоративных данных на новые.

Рис. 2. Результаты ответов на вопрос: «Какие элементы системы информационной безопасности предприятия являются, на Ваш взгляд, наиболее уязвимыми?»

Риски решения корпоративных задач на личных устройствах персонала предприятия у себя дома в период удаленного формата работы. Подобные риски возникают в ситуациях, когда сотрудники бизнес-структуры, находясь в режиме on-line, вообще не прибегают к корпоративному оборудованию. Они работают со своего домашнего телефона или на своем устройстве, используют личные USB-Flash и другие накопители, что для них привычнее и удобнее. В результате для предприятия возникает риск обнаружения в своей корпоративной сети новых устройств, которые могут являться источником заражения вредоносным программным обеспечением. Для выяснения всех обстоятельств и последствий этого необходимо запустить трудоемкий и дорогостоящий процесс сканирования сети.

Для полноты исследования основных видов предпринимательских рисков при организации работы персонала предприятий в удаленном формате была предпринята попытка выяснить, какие элементы корпоративной системы информационной безопасности являются наиболее уязвимыми. Для этого мы предложили менеджерам высшего и среднего звеньев бизнес-структур юга Тюменской области, а также представителям местных органов власти, общественных организаций и научного сообщества региона ответить на вопрос «Какие элементы системы информационной безопасности предприятия являются, на Ваш взгляд, наиболее уязвимыми?» (рис. 2).

Выводы

Исследованием установлено, что наиболее уязвимыми с позиции информационной безопасности тюменских предприятий, в первую очередь, выступают сайты и мобильные приложения, персонал, удаленный доступ и корпоративная почта. Именно им бизнес должен уделять первоочередное внимание для повышения эффективности корпоративной системы информационной безопасности в целом.

Известные надежды на улучшение работы данной системы и, соответственно, локализацию предпринимательских рисков при организации работы сотрудников предприятий в режиме on-line ученые и специалисты возлагают на само государство в лице одного из высших органов законодательной власти страны. Принятый недавно Госдумой законопроект об уголовной ответственности за кражи и утечки корпоративных и персональных данных влечет за собой внесение соответствующих изменений как в Уголовной Кодекс, так и в Кодекс РФ об административных правонарушениях, предусматривающих оборотные штрафы для бизнес-структур, допустивших потерю конфиденциальной корпоративной информации.

Поддержал данный законопроект и Госкомнадзор в лице его замглавы М. Вагнера, справедливо считающего, что наказывать необходимо не только тех, кто крадёт и продает корпоративные и персональные данные, но и тех, кто использует их в своих корыстных целях [12]. Следовательно, под

уголовную ответственность должны попадать операторы, обогащающие свои базы данных слитыми сведениями.

При всей значимости поддержки со стороны государства и участии его органов в решении рассматриваемой проблемы следует иметь в виду, что это в большей мере касается крупного бизнеса. Последний в известной степени адаптировался к новым вызовам кибербезопасности, чего не скажешь о многочисленных средних и малых субъектах хозяйствования, так и не оправившихся от постковидных ограничений и опосредованного влияния экономических санкций Запада.

В деле минимизации предпринимательских рисков при организации работы персонала в режиме on-line и повышения уровня кибербезопасности предприятия в целом средним и малым бизнес-структурам надо полагаться, в первую очередь, на самих себя. Учитывая имманентную им ограниченность ресурсов, предложим ряд доступных шагов на пути к решению настоящей проблемы:

- разработать концепцию удалённого доступа к программному обеспечению, в которой подробно расписать все необходимые положения с привязкой к конкретному предприятию;

- выбрать и внедрить конкретное программное обеспечение, реализующее удалённый доступ, не забыв настроить правила межсетевого экранирования и выделить необходимые сетевые сегменты;

- организовать контроль утечек корпоративных данных, антивирусной защиты, контроль «здоровья» компьютеров пользователей, которые подключаются к IT-инфраструктуре предприятия;

- активнее применять аутстаффинг, то есть одалживать у других бизнес-структур ИБ-специалистов, имеющих опыт работы в удаленном формате;

- больше уделять внимания мониторингу событий, используя SIEM, SOC и другие инструменты для выявления слабых мест корпоративной системы информационной безопасности и отражения кибератак;

- в долгосрочной перспективе вместе с другими средними и малыми бизнес-структурами привлекать технологии искусственного интеллекта при создании корпоративной системы информационной безопасности.

Библиографический список

1. Волк И. В России за полгода почти на 30% выросло число киберпреступлений. URL: https://tass.ru/obschestvo/18322395 (дата обращения: 20.12.2023).

2. Васильева Н. Ингушетия стала регионом с самым большим приростом киберпреступлений. URL: https://www.pnp.ru/social/chislo-kiberprestupleniy-v-rossii-v-yanvare-mae-vyroslo-pochti-na-28.html (дата обращения: 23.12.2023).

3. Марков Д. Что такое фишинг: как не стать жертвой хакеров. URL: https://trends.rbc.ru/trends/industry/602e9fe79a7947a4bd611504 (дата обращения: 07.11.2023).

4. Литвинов Р. Мошенники обманывают граждан, предлагая установить защитное ПО. URL: https://infobezopasnost.ru/blog/news/ (дата обращения: 10.11.2023).

5. Полунин С., Царев Е. Прямые и косвенные потери от утечек персональных данных. Мнения экспертов. URL: https://infobezopasnost.ru/blog/articles/ (дата обращения: 07.11.2023).

6. Потери от утечки данных. URL: //https://www.tadviser.ru/index.php (дата обращения: 10.12.2023).

7. Симонов С.Г. Развитие регионального бизнес-сообщества в период пандемии COVID-19: корректировка или смена парадигмы? // Известия вузов. Социология. Экономика. Политика. 2021. № 1. С. 98-114.

8. Симонов С.Г., Хаматханова М.А. Проблемы этнического предпринимательства в период COVID-19? // Научные исследования и разработки. Экономика. 2022. № 1 (55). С. 44-50.

9. Сотрудники возвращаются в офисы вместе с проблемами безопасности. URL: https://infobezopasnost.ru/blog/articles/ (дата обращения: 11.12.2023).

10. Ковалева И. Двухфакторная аутентификация: защищаемся от взлома в соцсетях и сервисах. URL: https://www.unisender.com/ru/blog/sovety/ (дата обращения: 06.12.2023).

11. Что такое контроль доступа к сети (NAC) 802.1X? URL: https:www.juniper.net/ru/ru/research-topics/what-is-802-1x-network-access-control.html (дата обращения: 24.12.2023).

12. Вагнер М. Госкомнадзор поддерживает введение уголовной ответственности за использование утекших данных. URL: https://tass.ru/politika/18047109 (дата обращения: 17.12.2023).