УДК 394:314.15
DOI: 10.31660/1993-1824-2024-1-116-133

Социальные риски при организации работы персонала бизнес-структур в режиме online

С. Г. Симонов*, О. Н. Кузяков

Тюменский индустриальный университет, Тюмень, Россия
**simonovsg@tyuiu.ru*

Аннотация. Статья посвящена проблеме корпоративной информационной безопасности в таком ее аспекте, как выявление, идентификация и минимизация социальных рисков при организации работы персонала бизнес-структуры в режиме online. За ее основу взяты эмпирический материал по результатам авторского исследования различных вопросов возникающих социальных рисков и связанного с ними обеспечения информационной безопасности деятельности компаний, использующих удаленный формат работы сотрудников. Исследование реализовано на юге Тюменской области, пилотной территории для федеральной программы «Производительность труда и поддержка занятости», и проведено с применением таких методов, как экспертная оценка, анкетирование, анализ вторичных данных. Приведены статистические данные прироста IT-преступлений за последние годы в разрезе регионов страны и статистические расчеты удельных весов корпоративных сотрудников в зависимости от формата, в котором они хотели бы работать в своей компании. В работе описываются основные результаты исследования: выяснена социальная природа предпринимательских рисков, связанных с удаленным форматом работы персонала; выявлены пять основных видов социальных рисков при организации работы сотрудников компаний в режиме online; дана статистическая оценка киберпреступлений против отечественных компаний; проанализированы последствия фишинговых атак на IT-инфраструктуру российских бизнес-структур; рассмотрены причины утечки корпоративных данных и потери бизнеса, связанные с рисками организации удаленной работы персонала; охарактеризованы финансовые потери компаний, функционирующих в режиме online; изучены риски возвращения сотрудников бизнес-структуры с релокации к офисной работе и приведены результаты социологического исследования, в каком формате они предпочитают трудиться в течение рабочей недели; обоснованы и систематизированы риски несоблюдения корпоративных правил информационной безопасности удаленно занятыми сотрудниками компании; указаны наиболее уязвимые звенья корпоративной системы информационной безопасности. Приводится мнение авторов статьи о роли и месте государственных органов в решении проблемы корпоративной информационной безопасности в таком ее аспекте, как выявление, идентификация и минимизация социальных рисков при организации работы персонала бизнес-структуры в режиме online. В заключительном разделе статьи даны интерпретация и применение полученных результатов, описана польза проведенного исследования для научного сообщества. Обоснована позиция авторов о том, что при всей важности поддержки и участия государственных органов в решении данной проблемы следует иметь в виду, что они устраняют лишь социально-экономические последствия, а не причины.

Ключевые слова: социальные риски, информационная безопасность, кибератака, фишинг, персонал, бизнес-структура, хакеры, мессенджеры, программное обеспечение

Для цитирования: Симонов, С. Г. Социальные риски при организации работы персонала бизнес-структур в режиме online / С. Г. Симонов, О. Н. Кузяков. – DOI 10.31660/1993-1824-2024-1-116-133 // Известия высших учебных заведений. Социология. Экономика. Политика. – 2024. – № 1. – С. 116–133.

Social risks in the organization of the work of the personnel of business structures in online mode

Sergey G. Simonov*, Oleg N. Kuzyakov

Industrial University of Tyumen, Tyumen, Russia
**simonovsg@tyuiu.ru*

Abstract. The article is devoted to the problem of corporate information security in such an aspect as the identification, identification and minimization of social risks in the organization of the work of the staff of a business structure in online mode. It is based on empirical material based on the results of the author's research on various issues of emerging social risks and related information security of companies using the remote format of employee work, implemented in the south of Tyumen region, which is a pilot territory for the federal program "Labor Productivity and employment support". The study was conducted using such methods as expert assessment, questionnaires, and analysis of secondary data. Statistical data on the increase in IT crimes in recent years by regions of the country and statistical calculations of the specific weights of corporate employees, depending on the format in which they would like to work in their company, are presented. The article describes the main results of the study: the social nature of entrepreneurial risks associated with the remote format of staff work is clarified; five main types of social risks are identified when organizing the work of company employees online; a statistical assessment of cybercrimes against domestic companies is given; the consequences of phishing attacks on the IT infrastructure of Russian business structures are analyzed; the causes of corporate data leakage and business losses associated with the risks of organizing remote work of personnel are considered; financial losses of companies operating online are characterized; the risks of returning employees of a business structure from relocation to office work 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 company are substantiated and systematized; the most vulnerable links of the corporate information security system are indicated. The opinion of the authors of the article on the role and place of government agencies in solving the problem of corporate information security in such an aspect as the identification, identification and minimization of social risks in the organization of the work of the staff of a business structure in online mode is given. In the final section of the article the interpretation and application of the results obtained are given, and the benefits of the conducted research for the scientific community are described. The authors' position is substantiated that, despite the importance of the support and participation of state bodies in solving this problem, it should be borne in mind that they eliminate only the socio-economic consequences, not the causes.

Keywords: social risks, information security, online mode, cyber attacks, phishing, personnel, business structure, hackers, messengers, software

For citation: Simonov, S. G., & Kuzyakov, O. N. (2024). Social risks in the organization of the work of the personnel of business structures in online mode. Proceedings of Higher Educational Institutions. Sociology. Economics. Politics, (1), pp. 116-133. (In Russian). DOI: 10.31660/1993-1824-2024-1-116-133

Введение

В условиях удаленной работы многие отечественные бизнес-структуры вынуждены решать проблему обеспечения информационной безопасности в режиме online, при котором границы киберзащиты расширяются далеко за пределы офиса. Это обусловливает известные социальные риски, поскольку поведение персонала бизнес-структуры в неожиданно изменившейся внешней хозяйственной среде часто бывает непредсказуемым и способно привести к утечке важных корпоративных данных, росту количества киберпреступлений, репутационным издержкам и др.

В настоящее время многими учеными и специалистами понятие социального риска рассматривается как вероятность, потенциальная возможность возникновения негативных последствий, связанных с социальными проблемами и вызванных недостаточным или неэффективным функционированием социальных институтов, политик и программ [1–3]. В широком смысле социальные риски можно рассматривать как целенаправленные действия субъектов, совершаемые в условиях неопределенности результатов. Главной отличительной чертой такого рода рисков является их социальное происхождение: они связаны с угрозами нормальному функционированию субъектов (отдельного работника, персонала компании, населения региона и пр.) ввиду нарушений со-

циально значимых элементов, то есть отклонения от социальной нормы фундаментальных параметров их положения во внешней и внутренней хозяйственной среде.

Следует сказать, что до определенного времени категория «социальные риски» признавалась научным сообществом как устоявшееся, достаточно изученное понятие. Однако с усложнением жизни современного социума, появлением новых обстоятельств и на их основе новых общественных отношений возникла объективная необходимость в дальнейшем исследовании данного феномена. Результатом последнего явилось разделение социальных рисков на традиционные (классические) и новые (современные) социальные риски.

Первые из них ученые связывают с высоким уровнем технологической и региональной безработицы, угрозой попадания значительной части населения за черту бедности, учащением случаев нарушения прав человека, большой дифференциацией в доходах людей и компаний, ведущей к конфликтам и социальной напряженности, и др.

Новые социальные риски в известной мере можно рассматривать как естественную реакцию на современные вызовы реалиям сегодняшнего российского общества.

В числе последних следующие:

- пандемии в форме глобальных эпидемий, такие как COVID-19, способные привести к тяжелым последствиям для здоровья населения и для экономики страны, приостановке транспортных систем и потоков, массовому сокращению средних и малых бизнес-структур и т. д.;
- участившиеся случаи экстремизма и терроризма, которые вызывают панику и страх у населения, отечественных предпринимателей и персонала компаний, а также могут привести к разрушению производственной и социально-бытовой инфраструктуры, потере большей части активов и др.;
- демографический кризис, нашедший свое выражение в снижении рождаемости, увеличении смертности и старении российского населения, что обусловливает сокращение рабочей силы, ухудшение ее качества, увеличение бремени налогов на трудоспособное население;
- возникновение проблемы кибербезопасности на фоне развития в стране рынка IT-услуг (рост киберпреступлений, фишинговых атак на бизнес и население, утечки корпоративных и персональных данных, компьютерное мошенничество и т. п.);
- набирающее обороты распространение фейковой информации в предпринимательской и обывательской среде, приводящее на микроуровне к неэффективным хозяйственным решениям, ошибкам в управлении бизнес-процессами, ухудшении морально-психологического климата в трудовом коллективе и ложным потребительским ожиданиям, а на макроуровне — к общей экономической нестабильности и снижению качества жизни населения в стране и ее регионах.

Актуализация выявления и анализа новых социальных рисков, а также путей минимизации их последствий не вызывает сомнения. Однако в рамках одной статьи сделать это не представляется возможным, в силу чего акцент был сделан на последних из указанных видов социальных рисков.

Методы исследования

Исследование проблемы социальных рисков и связанного с ними обеспечения информационной безопасности деятельности бизнес-структур, использующих удаленный формат ра-

боты 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.

Так, первым из них были охвачены две группы экспертов:

- менеджеры высшего и среднего звеньев тюменских компаний, принимающих участие в отмеченной федеральной программе;
- представители местных органов власти, общественных организаций и научного сообщества региона, напрямую не связанные с бизнес-деятельностью.

Такой метод исследования, как анкетирование, позволил обнаружить у возвращающихся с «удаленки» сотрудников тюменских бизнес-структур проблемы с адаптацией и необходимость на первых порах в поддерживающих мерах 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 социальные риски при организации работы персонала бизнес-структур в режиме online, имеющие место в Тюменской области и других регионах. В качестве гипотезы постановки исследуемой проблемы нами предложен алгоритм превентивных шагов по созданию корпоративной системы информационной безопасности персонала при удаленном формате работы (рис. 1).

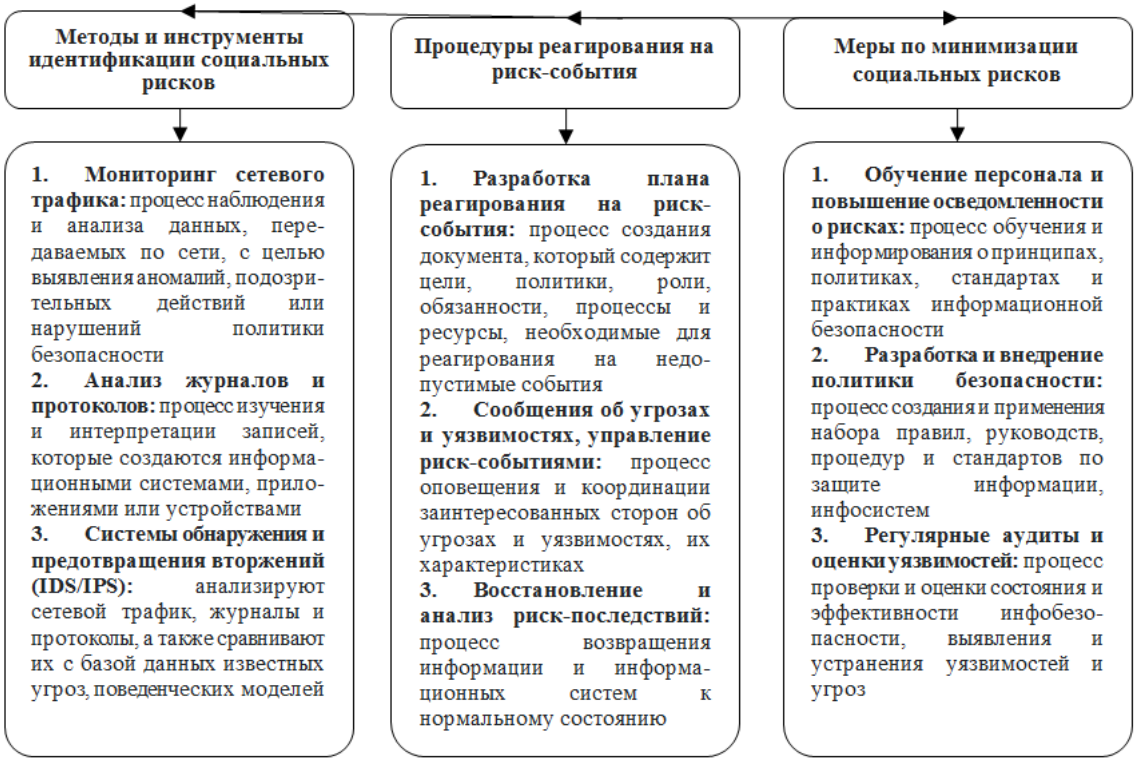

Рис. 1. ***Алгоритм превентивных шагов по созданию корпоративной системы корпоративной информационной безопасности персонала при удаленном формате работы***

Результаты и обсуждение

Шаг 1. Методы и инструменты идентификации социальных рисков.

Обнаружение, регистрация и классификация социальных рисков является начальным и наиболее важным шагом на пути решения поставленной проблемы, от которого зависит, по нашему мнению, 70–75 % конечного успеха. Для этого используются следующие методы и инструменты.

- Мониторинг сетевого трафика, представляющий собой процесс наблюдения и анализа данных, передаваемых по сети, с целью выявления аномалий, подозрительных действий или нарушений политики безопасности. Подобный мониторинг осуществляется с помощью специализированного программного обеспечения или оборудования (снифферов, прокси-серверов, межсетевых экранов и др.).
- Экспресс-анализ журналов и протоколов, который можно рассматривать как процесс изучения и интерпретации записей, создаваемых информационными системами, приложениями или устройствами при выполнении различных операций, событий или действий. Он позволяет выявить рисковые события, такие как неудачные попытки входа, несанкционированный доступ, изменение или удаление корпоративных или персональных данных, нарушение правил доступа и пр.
- Системы обнаружения и предотвращения вторжений (IDS/IPS) в виде программных или аппаратных решений, которые автоматически «мониторят» сетевой трафик, журналы и протоколы, сравнивают их с базой данных известных угроз, уязвимостей или поведенческих моделей. Системы обнаружения вторжений (IDS) предназначены для оповещения менеджмента компании о риск-событиях, блокировки и приостановки последних. Отметим, что системы IDS/IPS могут быть развернуты на разных уровнях сети (например, таких как хост, сетевой уровень, прикладной уровень).

Основные виды рисков при организации работы персонала тюменских компаний в режиме online

№ п/п	Наименование видов рисков при организации работы персонала компаний в режиме online	Ранг значимости видов рисков при организации работы персонала компаний в режиме online
1	Риски фишинговых атак	I
2	Риски роста количества киберпреступлений	II
3	Риски утечки корпоративных данных	III
4	Риски, следствием которых являются потери компании	IV
5	Риски возвращения персонала бизнес-структуры с релокации к офисной работе	V
6	Риски несоблюдения корпоративных правил информационной безопасности сотрудниками компании при организации удаленной работы	VI

Изучение литературы по исследуемой проблеме дало возможность выявить пять основных видов социальных рисков при организации работы персонала компаний в

режиме online: риски роста количества киберпреступлений и фишинговых атак; риски утечки корпоративных данных; риски, следствием которых являются потери бизнес-структуры; риски возвращения персонала бизнес-структуры с релокации к офисной работе; риски несоблюдения корпоративных правил информационной безопасности сотрудниками компании при организации удаленной работы. Используя метод экспертной оценки, нам удалось установить ранг их значимости при организации работы персонала бизнес-структур г. Тюмени в режиме online (таблица).

Риски роста количества киберпреступлений и фишинговых атак

Как заявила официальный представитель МВД И. Волк, за первое полугодие 2023 года по сравнению с аналогичным периодом 2022 года количество киберпреступлений выросло на 27,9 %, в то время как их раскрываемость — лишь на 5,4 % [4].

За период январь–май 2023 года против отечественных компаний совершено 261 тысяча преступлений. При этом киберпреступники имеют финансовые мотивы, в связи с чем они выбирали предпринимателей, готовых платить за сохранность своих корпоративных данных. Атаки чаще всего приходились на промышленные, логистические, финансовые и медицинские компании, а также IT-компании, занимающиеся разработкой программного обеспечения.

Для получения доступа к внутренним сетям компании киберпреступники использовали уязвимости в устаревших версиях Bitrix, Confluence и Webmin на серверах под управлением Linux. Далее загружалось и закреплялось в системе собственное вредоносное программное обеспечение для получения доступа к корпоративным данным. Причем киберпреступники не шифруют данные, а анализируют их вручную и копируют важную бизнес-информацию. И только после получения конфиденциальных данных о деятельности бизнес-структуры начинается привычный ее шантаж.

Более чем три четверти (76,3 %), или 199,2 тысячи, преступлений в РФ совершается через интернет, почти половина из них (45 %), или 117,5 тысячи, — с помощью средств мобильной связи. Симптоматично, что это количество за первые пять месяцев 2023 года увеличилось на 51 % по сравнению с тем же периодом 2022 года. В региональном разрезе наибольший прирост IT-преступлений 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 %) [5].

Работающие в режиме online сотрудники бизнес-структуры могут легко стать жертвами фишинга. Преступники могут, например, сделать недоступным на время шлюз удаленного доступа, а затем, представившись службой технической поддержки компании, сделать вид, что решают проблему конкретного пользователя, попутно выманив у него учетные данные. Фишинг применяется для кражи конфиденциальной корпоративной информации, банковских счетов, паролей, номеров карт и т. п.

Чаще всего фишинговая атака представляет собой выдачу фейковых сайтов, которые имитируют интернет-страницы популярных компаний (соцсетей, интернет-

магазинов, стриминговых сервисов и др.). Расчет делается на то, что пользователь не заметит подделки и укажет на странице конфиденциальную информацию о компании, корпоративные или личные данные.

Основная проблема, связанная с фишингом, состоит в том, что не существует программного обеспечения, которое защитило бы бизнес-структуру и ее персонал, особенно в условиях удаленной работы, поскольку сайты-фейки трудно отличить от оригиналов. Все зависит от сотрудников бизнес-структуры — насколько они будут внимательны, компетентны для распознания фейка.

В нашей стране количество 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 компании, далее в ход идут другие способы взлома. По данным разработчика решений по предотвращению и расследованию киберпреступлений Group-IB, около 70 % всех целенаправленных атак на российский бизнес начинаются с фишинга. Получив с его помощью доступ хотя бы к одному корпоративному компьютеру, киберпреступники способны закрепиться в сети компании и получить контроль над всей ее инфраструктурой [6].

Риски утечки корпоративных данных

В научной литературе утечка корпоративных данных при организации работы персонала в режиме online рассматривается как инцидент, в результате которого произошло неправомерное раскрытие конфиденциальной информации. К сожалению, работающие на «удаленке» сотрудники взломанных ресурсов не спешат делиться с руководством бизнес-структуры информацией о том, как именно это произошло. Чаще всего 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. Кибермошенники представляются специалистами по информационной или компьютерной безопасности (ИБ-специалистами) известных IT-компаний и предлагают загрузить приложение, которое якобы будет искать уязвимости. На самом деле, устанавливая программное обеспечение, сотрудники бизнес-структуры, работающие в режиме online, дают им право удаленного доступа к своему устройству. Чаще всего кибермошенники связываются с потенциальными жертвами через популярные мессенджеры, иногда — через телефонную связь.

Кроме того, утечки корпоративных данных могут явиться следствием действий инсайдеров. Дело в том, что разработчики программного обеспечения зачастую не тестируют его должным образом и не применяют практики безопасной разработки, а это в свою очередь также делает утечки возможными [7].

Отметим, что в современной теории информационной безопасности бизнеса причины утечек корпоративных данных делят на два вида:

- случайные ошибки персонала бизнес-структуры, которые могут произойти из-за человеческого фактора (например, сотрудник перепутал адреса электронной по-

чты клиентов и направил данные не тому, по ошибке предоставил общий доступ к документу с конфиденциальными корпоративными данными и т. п.);

- намеренные действия кибермошенников, решивших нажиться на украденной базе данных.

Таким образом, специально разгласить конфиденциальные корпоративные данные могут как «свои» люди (персонал бизнес-структуры, подрядчики, клиенты, партнеры), так и кибермошенники и хакеры. Это, по нашему мнению, происходит из-за недостаточной защищенности информационной базы компании, отсутствия регулярного пересмотра системы ее защиты, неустранения уязвимости, избыточного хранения корпоративных данных и неорганизованности порядка их обработки, в результате чего они могут попасть не тем субъектам.

Риски, следствием которых являются потери бизнес-структуры

Поскольку корпоративные данные могут быть самыми разными, то и последствия их потери бизнес-структурой, являющейся результатом социальных рисков при организации работы персонала в режиме online, тоже весьма дифференцированны. Условно их можно разделить на прямые и косвенные. К первым, на наш взгляд, относятся следующие:

- компенсации пострадавшим хозяйствующим субъектам;
- штрафы от регулирующих органов (например, суда или Роскомнадзора);
- затраты бизнес-структуры 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 бизнес-структуры включают следующие:

- уход части потенциальных клиентов компании и контрагентов;
- снижение уровня конкурентоспособности бизнес-структуры на рынке;
- уменьшение стоимости активов бизнес-структуры (акций и других ценных бумаг, нематериальных активов и т. п.);
- определенный удар по репутации компании;
- рост затрат на поддержание имиджа и рекламу для восстановления позиций на рынке;
- дополнительное, не всегда выгодное компании внимание со стороны регулирующих органов (правоохранительных, судебных, надзирательных, органов власти на местах) [8].

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 компаний, функционирующих в режиме online .

1. Переход на удаленную работу персонала компании 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).

2. В отраслевом разрезе рост финансовых потерь компаний от утечек корпоративных данных особо наблюдается в здравоохранении, розничной торговле, гостиничном и ресторанном бизнесах, а также в отраслях, производящих потребительские товары. Самые дорогостоящие утечки корпоративной информации — в здравоохранении: $9,23 млн на каждый случай в 2021 году, что на $2 млн больше, чем в 2020 году.

3. Компрометация учетных записей приводит к краже корпоративных данных. Причиной большей части потерь является доступ с помощью украденных учетных данных.

4. Современные инструменты помогают снизить убытки. Речь идет о применении искусственного интеллекта, ИБ-аналитики и шифрования, доказавших свою эффективность в плане уменьшения финансовых потерь, связанных с утечками данных компании. Экономия составляет от $1,25 млн до $1,49 млн по сравнению с бизнес-структурами, где данные инструменты практически не используются. Что касается утечек корпоративных данных, находящихся в облаке, то компаниям, 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) [9].

Риски возвращения персонала бизнес-структуры с релокации к офисной работе

Как показали наши исследования и исследования других ученых, психологически вернуться с удаленного формата работы, к которому привык и который во многом удобен персоналу компании, к прежнему офисному часто бывает весьма непросто. Например, по завершению в нашей стране периода пандемии коронавируса, в течение которого большинство компаний функционировало в режиме online, у многих сотрудников при возвращении в офис обнаружились проблемы адаптации и потребовались на первое время поддерживающие меры для вхождения в рабочий ритм, а также обнаружились невысокая мотивация и желание сменить эту работу [10; 11].

В значительной степени это коррелирует с результатами нашего социологического исследования, которое было проведено в 2023 году и в котором приняли участие около 400 сотрудников тюменских бизнес-структур, имеющих опыт работы в удаленном формате (рис. 2).

Как показало исследование, почти 2/3 опрошенных сотрудников тюменских компаний, которые имеют опыт за период пандемии коронавируса работы в режиме online, предпочитают проводить в офисе только часть рабочей недели. По их мнению, выполнение своих прямых трудовых обязанностей, например, дома в течение 2–3 дней рабочей недели нисколько не сказывается на производительности и качестве труда. В то же время данная группа респондентов считает, что находиться определенную часть рабочей недели непосредственно в офисе компании необходимо и даже полезно, объясняя это стремлением быть постоянно в курсе дел компании, осуществлять живой контакт с корпоративным руководством (особенно если сотрудник включен в кадровый резерв), владеть внутренней информацией, которую невозможно получить в удаленном формате.

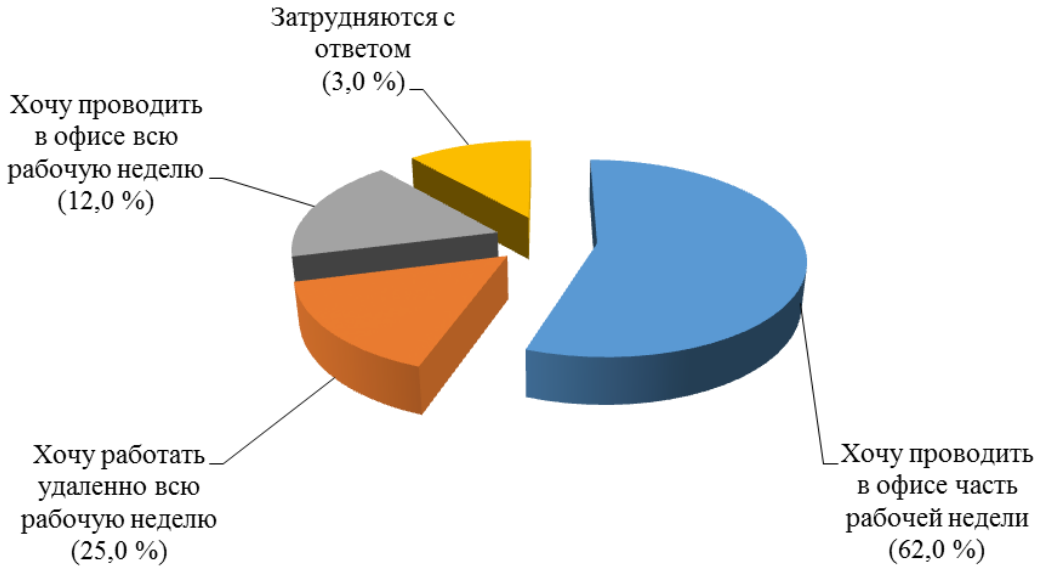

Рис. 2. ***Результаты ответов на вопрос: «В каком формате Вы хотели бы работать в Вашей компании?»***

Четверть опрошенного персонала тюменских бизнес-структур (25,0 %) выразили желание работать в режиме online всю рабочую неделю. Из беседы с этой группой опрошенных сотрудников выяснилось следующее:

- Значительная ее часть перешагнула 50-летний рубеж, не строит иллюзий относительно своего карьерного роста, семейные ценности и интересы явно доминируют над корпоративными. Вместе с тем она держится за свое рабочее место и дорожит им, осознавая высокие риски смены компании.
- Другая ее часть (возрастной диапазон 40–50 лет) полагает, что знает о своей работе все и способна выполнять ее качественно и, главное, быстро, в силу чего не видит смысла в офисном пребывании. Здесь важным мотивом является потенциальная возможность подработки в другом месте в границах традиционной пятидневки.
- Третью часть данной группы образует в основном молодой персонал не старше 30 лет. Она весьма неоднородна, поскольку сюда входят те, кто осознанно пришел временно, переждать, пока найдется более «доходное» место, кого коллектив не принял и не видит в «своей команде», кому нужна просто запись в трудовой книжке или не хватает амбиций и т. д.

Риски несоблюдения корпоративных правил информационной безопасности сотрудниками компании при организации удаленной работы

Как свидетельствует статистика, более половины персонала компании (52 %), работающего в режиме online, не соблюдают правила информационной безопасности [12]. В связи с этим от корпоративного менеджмента требуется спланировать бизнес-деятельность таким образом, чтобы получить преимущества от новой реальности и удаленного формата работы своих сотрудников. В противном случае ошибки в планировании могут привести к целому ряду следующих социальных рисков.

Риски несанкционированного доступа к программному обеспечению. В настоящее время во многих компаниях нет четкой политики самого удаленного доступа. Работая в режиме online, они просто открывают какой-то доступ к своей корпоративной системе, рассчитывая, что все будет в порядке. Вместе с тем в реальной бизнес-практике без грамотной политики удаленного доступа любая уязвимость может повлечь взлом IT-инфраструктуры компании [13]. Причем в данной политике должны быть подробно расписаны все необходимые положения, что позволит, на наш взгляд, минимизировать для бизнес-структуры риски информационного характера.

Риски перезагрузки системы удаленного обновления оборудования и модернизации софта бизнес-структуры. При организации удаленной работы персонала компании корпоративное оборудование с настроенными инструментами защиты переустанавливается из офисов в жилье сотрудников. При этом зачастую компании не удается рассчитать технические мощности оборудования, которое должно будет выдержать нагрузку при подключении всех «удаленщиков». Возникают определенные риски, устранение которых требует регулярного обновления программного обеспечения, модернизации софта, оптимальной загрузки технических мощностей оборудования.

Добавим, что сегодня в России имеется всего лишь несколько компаний, которые разработали системы удаленного обновления оборудования и модернизации софта, тем самым серьезно повысив уровень собственной информационной безопасности. Ряд компаний также продвигаются в этом направлении, планируя у себя внедрение той же двухфакторной аутентификации [14] или контроля доступа к сети (Network Fccess Control — NAC) [15].

Риски использования корпоративного оборудования в собственных целях сотрудниками компании. Часто персонал бизнес-структуры, используя в режиме online корпоративное программное обеспечение, устанавливает на нем личные приложения и игры. Такое «скачивание» из непроверенных источников — прямой путь попадания в корпоративную сеть «вредоноса». В результате компании приходится внепланово проводить проверку всех устройств на наличие угроз и уязвимостей информационного характера. Заметим, что этого бы не потребовалось, если бы менеджмент компании своевременно установил управляющее программное обеспечение.

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

Риски решения корпоративных задач на личных устройствах сотрудников бизнес-структур у себя дома в период удаленного формата работы. Подобные риски

возникают в ситуациях, когда сотрудники, находясь в режиме online, 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 компании 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 процесс сканирования сети.

Шаг 2. Процедуры реагирования на риск-события.

Чтобы эффективно справиться с риск-событиями, необходимо иметь четкие и согласованные процедуры реагирования, которые определяют, как действовать в случае обнаружения, управления и восстановления после превращения потенциальной угрозы или уязвимости в реальную. Процедуры реагирования на риск-события включают в себя следующие процессы:

- Процесс создания документа, который содержит цели, политики, роли, обязанности, процессы и ресурсы, необходимые для реагирования на риск-события, заканчивающийся составлением плана реагирования. Он должен быть разработан заранее, с учетом различных сценариев, угроз, уязвимостей, а также регулярно обновляться и тестироваться.
- Процесс оповещения и координации заинтересованных сторон (руководство компании, ее персонал, клиенты, партнеры, поставщики, правоохранительные органы и др.) о риск-событиях и их характеристиках, таких как время, место, источник, цель, вектор, эффект и т. д. Подобные сообщения также включают в себя анализ, оценку, приоритеты, назначение, исполнение и контроль действий, направленных на устранение риск-событий и их последствий.
- Процесс возвращения информации и информационных систем к нормальному состоянию после риск-событий, выяснения причин и ранга их значимости, хода и результатов превращения потенциальных угроз или уязвимостей в реальные. Кроме этого, сюда относится разработка рекомендаций и выводов, направленных на предотвращение реализации угроз и уязвимостей и снижение рисковой вероятности в будущем.

Шаг 3. Превентивные меры по минимизации социальных рисков.

Для предотвращения или снижения вероятности наступления риск-события важно принимать превентивные меры по минимизации его последствий и повышению уровня информационной безопасности в целом. Данные меры включают в себя следующие действия:

- Процесс обучения и информирования персонала компании, ее клиентов и бизнес-партнеров о принципах, политике, стандартах и практиках информационной безопасности, о типах, методах и последствиях риск-событий и др. Обучение сотрудников и повышение осведомленности о социальных рисках может быть осуществлено с помощью различных форм и методов (лекций, семинаров, вебинаров, тренингов, брошюр, плакатов, электронных писем и т. п.).

- Процесс создания и внедрения политики безопасности, применения набора правил, руководств, процедур и стандартов, которые определяют, как информация и информационные системы должны быть защищены, использованы, управляемы и поддерживаемы. Такая политика призвана быть основанной на анализе социальных рисков, согласованной с бизнес-целями и требованиями, а также соблюдаться всеми заинтересованными сторонами. Она должна быть документирована, распространена, контролируема, периодически пересматриваться и обновляться.
- Процесс проверки состояния и оценки эффективности информационной безопасности, выявления и устранения угроз и уязвимостей, нарушений в информационных системах. Регулярные аудиты риск-событий, их последствий могут быть проведены компанией с помощью как своих специалистов, так и аутстаффинга с широким применением самых разнообразных методик и инструментов (например, тестирования, сканирования, наблюдения, интервью, анкетирования и пр.).

Заявленный социологический инструментарий в рамках проводимого исследования был использован для выяснения, какие звенья корпоративной системы информационной безопасности являются наиболее уязвимыми. Для этого нами было предложено менеджерам высшего и среднего звеньев компаний юга Тюменской области, а также представителям местных органов власти, общественных организаций и научного сообщества региона ответить на вопрос «Какие звенья компании являются, по Вашему мнению, наиболее уязвимыми с точки зрения информационной безопасности?» (рис. 3).

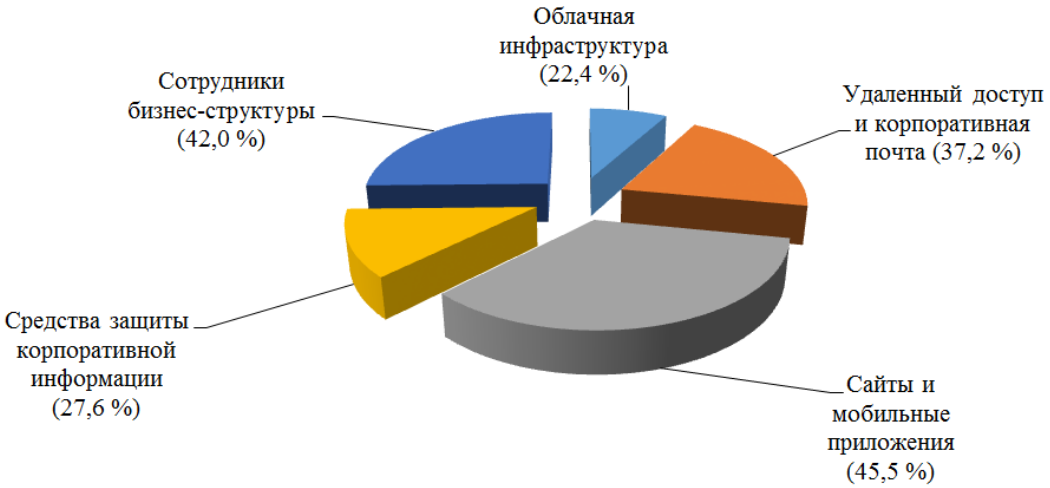

Рис. 3. ***Результаты ответов на вопрос: «Какие звенья компании являются, по Вашему мнению, наиболее уязвимыми с точки зрения информационной безопасности?»***

Как выяснилось, «болевыми точками» с позиции информационной безопасности тюменских компаний в первую очередь выступают сайты и мобильные приложения, персонал, удаленный доступ и корпоративная почта. Очевидно, что именно этим уязвимостям бизнес должен уделять особое внимание для повышения эффективности корпоративной системы информационной безопасности в целом.

Нельзя не отметить, что определенные надежды на улучшение работы данной системы и, соответственно, локализацию социальных рисков при организации работы персонала компаний в режиме online ученые и специалисты возлагают на само государство в лице Государственной Думы РФ. Принятый недавно Госдумой законопроект об уголовной ответственности за кражи и утечки корпоративных и персональных данных влечет за собой внесение соответствующих изменений не только в Уголовный кодекс (УК), но и в Кодекс РФ об административных правонарушениях (КоАП), предусматривающих оборотные штрафы для компаний, допустивших потерю конфиденциальной информации.

В поддержку данного законопроекта выступил М. Вагнер — представитель другого органа государства в лице заместителя руководителя Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Госкомнадзора). Однако при этом он считает, что наказывать необходимо не только тех, кто крадет и продает корпоративные и персональные данные, но и тех, кто использует их в своих целях [16]. Таким образом, под уголовную ответственность должны попадать операторы, обогащающие свои базы данных слитыми сведениями.

Выводы

При всей важности поддержки и участия государственных органов в решении данной проблемы следует иметь в виду, что они устраняют лишь социально-экономические последствия, а не причины. Такое устранение в большей мере касается крупного бизнеса, в известной мере адаптировавшегося к новым вызовам кибербезопасности, а не многочисленных хозяйствующих субъектов среднего и малого форматов, не полностью оправившихся от ковидных ограничений и опосредованного влияния западных экономических санкций.

В деле минимизации социальных рисков при организации работы персонала в режиме online 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 к выше отмеченному некоторые дополнительные рекомендации на пути к решению настоящей проблемы:

- разработать концепцию удаленного доступа к программному обеспечению, в которой подробно расписать все необходимые положения с привязкой к конкретному предприятию;
- выбрать и внедрить конкретное программное обеспечение, реализующее удаленный 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 Security infor and event management (SIEM), Security operation center (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.

Список источников

1. Осипова, П. А. Социальные риски : понятие, признаки, виды и основные проблемные аспекты / П. А. Осипова. – Текст : электронный // Материалы всероссийской научной интернет-конференции «Актуальные проблемы трудового права и права социального обеспечения» (2023). – URL: https://conf.siblu.ru/socialnye-riski-ponyatie-priznaki-vidy-i-osnovnye-problemnye-aspekty (дата обращения: 10.04.2023).
2. Федорова, М. Ю. Нетипичные наднациональные формы социального обеспечения / М. Ю. Федорова. – Текст : непосредственный // Российский юридический журнал. – 2012. – № 3 (84). – С. 188–198.
3. Захаров, М. Л. Право социального обеспечения / М. Л. Захаров, Э. Г. Тучкова. – Москва : Волтерс Клувер. – 2004. – 560 с. – Текст : непосредственный.
4. В России за полгода почти на 30 % выросло число киберпреступлений. – Текст : электронный // Информационное агентство ТАСС : сайт. – 2023. – 20 июля. – URL: https://tass.ru/obschestvo/18322395 (дата обращения: 20.07.2023).
5. Васильева, Н. Ингушетия стала регионом с самым большим приростом киберпреступлений / Н. Васильева. – Текст : электронный // Парламенсткая газета. – 2023. – 23 июня. – URL: https://www.pnp.ru/social/chislo-kiberprestupleniy-v-rossii-v-yanvare-mae-vyroslo-pochti-na-28.html (дата обращения: 23.06.2023).
6. Марков, Д. Что такое фишинг : как не стать жертвой хакеров / Д. Марков. – Текст : электронный // РБК : сайт. – 2023. – 07 фев. – URL: https://trends.rbc.ru/trends/industry/602e9fe79a7947a4bd611504 (дата обращения: 07.02.2023).
7. Литвинов, Р. Мошенники обманывают граждан, предлагая установить защитное ПО / Р. Литвинов. – Текст : электронный // Инфобезопасность : сайт. – 2023. – 10 авг. – URL: https://infobezopasnost.ru/blog/news/moshenniki-obmanyvayut-grazhdan-predlagaya-ustanovit-zashhitnoe-po/ (дата обращения: 10.08.2023).
8. Полунин, С. Прямые и косвенные потери от утечек персональных данных. Мнения экспертов / С. Полунин, Е. Царев. – Текст : электронный // Инфобезопасность : сайт. – 2023. – 07 авг. – URL: https://infobezopasnost.ru/blog/articles/pryamye-i-kosvennye-poteri-ot-utechek-personalnyh-dannyh-mneniya-ekspertov/ (дата обращения: 07.08.2023).

9. Потери от утечек данных. – Текст : электронный // TAdviser : сайт. – 2022. – 10 мая. – URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D0%BE%D1%82%D0%B5%D1%80%D0%B8_%D0%BE%D1%82_%D1%83%D1%82%D0%B5%D1%87%D0%B5%D0%BA_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85 (дата обращения: 10.05.2022).

10. Симонов, С. Г. Развитие регионального бизнес-сообщества в период пандемии COVID-19 : корректировка или смена парадигмы? / С. Г. Симонов. – Текст : непосредственный // Известия вузов. Социология. Экономика. Политика. – 2021. – № 1. – С. 97–114.

11. Симонов, С. Г. Проблемы этнического предпринимательства в период COVID-19 / С. Г. Симонов, М. А. Хаматханова. – DOI 10.12737/2587-9111-2022-10-1-44-49. – Текст : непосредственный // Научные исследования и разработки. Экономика. – 2022. – Т. 10, № 1 (55). – С. 44–49.

12. Литвинов, Р. Сотрудники возвращаются в офисы вместе с проблемами безопасности / Р. Литвинов. – Текст : электронный // Инфобезопасность : сайт. – 2023. – 11 авг. – URL: https://infobezopasnost.ru/blog/articles/sotrudniki-vozvrashhayutsya-v-ofisy-vmeste-s-problemami-bezopasnosti/ (дата обращения: 11.08.2023).

13. Кузяков, О. Н. Исследование угроз информационной безопасности автоматизированной системы диагностики патологий легких при лимфоме / О. Н. Кузяков, С. А. Сорокина, Е. А. Шутова. – Текст : непосредственный // Материалы Международной научно-практической конференции им. Д. И. Менделеева. – Тюмень : ТИУ, 2023. – С. 370–372.

14. Ковалева, И. Двухфакторная аутентификация : защищаемся от взлома в соцсетях и сервисах / И. Ковалева. – Текст : электронный // Unisender : сайт. – 2022. – 06 апр. – URL: https://www.unisender.com/ru/blog/chto-takoe-dvuhfaktornaya-autentifikaciya/ (дата обращения: 06.04.2022).

15. What is 802.1X Network Access Control (NAC)? – Text : electronic // Juniper networks : website. – URL: https:www.juniper.net/ru/ru/research-topics/what-is-802-1x-network-access-control.html

16. РКН поддержал введение уголовной ответственности за использование утекших данных. – Текст : электронный // Информационное агентство ТАСС : сайт. – 2023. – 17 июня. – URL: https://tass.ru/politika/18047109 (дата обращения: 17.06.2023).

References

1. Osipova, P. A. (2023). Sotsial'nye riski: ponyatie, priznaki, vidy i osnovnye problemnye aspekty. Materialy vserossiyskoy nauchnoy internet-konferentsii "Aktual'nye problemy trudovogo prava i prava sotsial'nogo obespecheniya" (2023). (In Russian). Available at: https://conf.siblu.ru/socialnye-riski-ponyatie-priznaki-vidy-i-osnovnye-problemnye-aspekty

2. Fedorova, M. Yu. (2012). Non-typical supranational forms of social security. Russian juridical journal, (3(84)), pp. 188-198. (In Russian).

3. Zakharov, M. L., & Tuchkova, E. G. (2004). Pravo social'nogo obespecheniya. Moscow, Volters Kluwer Publ., 560 p. (In Russian).

4. V Rossii za polgoda pochti na 30 % vyroslo chislo kiberprestupleniy. (2023) (In Russian). Available at: https://tass.ru/obschestvo/18322395

5. Vasil'eva, N. (2023). Ingushetiya stala regionom s samym bol'shim prirostom kiberprestupleniy. Parlamenstkaya gazeta. (In Russian). Available at: https://www.pnp.ru/social/chislo-kiberprestupleniy-v-rossii-v-yanvare-mae-vyroslo-pochti-na-28.html

6. Markov, D. (2023). Chto takoe fishing: kak ne stat' zhertvoy khakerov. (In Russian). Available at: https://trends.rbc.ru/trends/industry/602e9fe79a7947a4bd611504

7. Litvinov, R. (2023). Moshenniki obmanyvayut grazhdan, predlagaya ustanovit' zashchitnoe PO. (In Russian). Available at: https://infobezopasnost.ru/blog/news/moshenniki-obmanyvayut-grazhdan-predlagaya-ustanovit-zashhitnoe-po/

8. Polunin, S., & Tsarev, E. (2023). Pryamye i kosvennye poteri ot utechek personal'nykh dannykh. Mneniya ekspertov. (In Russian). Available at: https://infobezopasnost.ru/blog/articles/pryamye-i-kosvennye-poteri-ot-utechek-personalnyh-dannyh-mneniya-ekspertov/

9. Poteri ot utechek dannykh. (2022). (In Russian). Available at: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9F%D0%BE%D1%82%D0%B5%D1%80%D0%B8_%D0%BE%D1%82_%D1%83%D1%82%D0%B5%D1%87%D0%B5%D0%BA_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85

10. Simonov, S. G. (2021). Development of the regional business community during the COVID-19 pandemic: adjustment or change of the paradigm? Proceedings of Higher Educational Institutions. Sociology. Economics. Politics, (1), pp. 97-114. (In Russian).

11. Simonov, S. G., & Hamathanova, M. A. (2022). Problems of ethnic entrepreneurship in the period of COVID-19. Scientific research and development. Economics, 10(1(55)), pp. 44-50. (In Russian). DOI: 10.12737/2587-9111-2022-10-1-44-49

12. Litvinov, R. (2023). Sotrudniki vozvrashchayutsya v ofisy vmeste s problemami bezopasnosti. (In Russian). Available at: https://infobezopasnost.ru/blog/articles/sotrudniki-vozvrashhayutsya-v-ofisy-vmeste-s-problemami-bezopasnosti/

13. Kuzyakov, O. N., Sorokina, S. A., & Shutova, E. A. (2023). Issledovanie ugroz informatsionnoy bezopasnosti avto-matizirovannoy sistemy diagnostiki patologiy legkikh pri limfome. Materialy Mezhdunarodnoy nauchno-prakticheskoy konferentsii im. D. I. Mendeleeva. Tyumen, Industrial University of Tyumen Publ., pp. 370-372. (In Russian).

14. Kovaleva, I. (2022). Dvukhfaktornaya autentifikatsiya: zashchishchaemsya ot vzloma v sotssetyakh i servisakh. (In Russian). Available at: https://www.unisender.com/ru/blog/chto-takoe-dvuhfaktornaya-autentifikaciya/

15. What is 802.1X Network Access Control (NAC)? (In English). Available at: https:www.juniper.net/ru/ru/research-topics/what-is-802-1x-network-access-control.html

16. RKN podderzhal vvedenie ugolovnoy otvetstvennosti za ispol'zovanie utekshikh dannykh. (2023). (In Russian). Available at: https://tass.ru/politika/18047109

Информация об авторах / Information about the authors

Симонов Сергей Геннадьевич, доктор социологических наук, кандидат экономических наук, профессор кафедры экономики и организации производства, Тюменский индустриальный университет, г. Тюмень, simonovsg@tyuiu.ru

Кузяков Олег Николаевич, доктор технических наук, профессор, заведующий кафедрой кибернетических систем, Тюменский индустриальный университет, г. Тюмень

Sergey G. Simonov, Doctor of Sociology, Candidate of Economics, Professor at the Department of Economics and Organization of Production, Industrial University of Tyumen, simonovsg@tyuiu.ru

Oleg N. Kuzyakov, Doctor of Engineering, Professor, Head of the Department of Cybernetic Systems, Industrial University of Tyumen

Статья поступила в редакцию 08.02.2024; одобрена после рецензирования 27.02.2024; принята к публикации 07.03.2024.
The article was submitted 08.02.2024; approved after reviewing 27.02.2024; accepted for publication 07.03.2024.