DOI: 10.18137/RNU.V9187.24.02.P.142 УДК 004.056.5

С.А. Никитин

УДАЛЕННАЯ РАБОТА: ВЫЗОВЫ И IT-РЕШЕНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ

Аннотация. Проведен анализ вызовов информационной безопасности и IT-решений для обеспечения безопасности данных в контексте удаленной работы. Обзор научной литературы позволил выявить ключевые угрозы безопасности данных в условиях удаленной работы, а также представить для этого информационно-технологические решения. Обозначены перспективы развития IT-решений для обеспечения безопасности данных, даны авторские рекомендации по оптимизации управления безопасностью данных в контексте удаленной работы.

Ключевые слова: информационные технологии, безопасность данных, удаленная работа, дистанционный формат, IT-решения, управленческие решения.

S.A. Nikitin

REMOTE WORK: CHALLENGES AND IT SOLUTIONS FOR DATA SECURITY

Abstract. The article analyzes information security challenges and IT solutions to ensure data security in the context of remote work is carried out. The literature review made it possible to identify key threats to data security in remote work conditions, as well as to present information technology solutions to ensure data security. In conclusion, the prospects for the development of IT solutions for data security in terms of remote work are outlined, and the author's recommendations are also given to promote the optimization of data security management in the context of remote work.

Keywords: information technology, data security, remote work, distance format, IT solutions, management solutions.

Введение

До пандемии Covid-19 удаленная работа не была особенно распространенной практикой и была скорее привилегией немногих [1]. Пандемия Covid-19 изменила ситуацию, когда была осознана необходимость внедрения удаленной работы для сотрудников во всем мире и признания дистанционного формата «глобальной лабораторией удаленной работы» [2]. После массового карантина множество организаций столкнулись с необходимостью осуществления перехода на дистанционный формат работы, что привело к возникновению специфических трудностей и возможностей и для сотрудников, и для компаний. Так, с одной стороны, удаленная работа в условиях пандемии сэкономила финансовые ресурсы сотрудников и предприятий, привела к повышению удовлетворенности работой, производительности компаний и новым возможностям трудоустройства [3], с другой – переход на удаленные информационные технологии открыл множество возможностей для киберинцидентов и атак, число которых значительно возросло [4], поскольку удаленная рабочая среда создает весьма привлекательные возможности для киберпреступников [5].

После резкого перехода на удаленную работу в 2020–2021 гг. прошло уже достаточно много времени, и, несмотря на все преимущества удаленной работы, сегодня многие ком-

Никитин Семён Анатольевич
заместитель генерального директора по информационным технологиям и коммуникациям, ООО «ДАДА Креатив», Москва. Сфера научных интересов: информационные технологии. Электронный адрес: snikitin@dada.llc

пании возвращают своих сотрудников в офисы, проводя соответствующую политику [6]. Вместе с тем рабочее место после COVID неизбежно будет сильно отличаться от того, каким оно было раньше [7; 8], в связи с чем удаленная работа как способ организации труда, особенно учитывая нынешний рост цифровых технологий, едва ли исчезнет в постковидном мире [9].

Серьезная угроза кибербезопасности, создаваемая удаленной работой и участием предприятий в программах цифровой трансформации, привела к тому, что многие специалисты по IT-безопасности внесли изменения в инфраструктуру. Можно предположить, что быстрый рост количества выданных цифровых сертификатов для облачных приложений и корпоративной аутентификации связан с тем, что организации создали инфраструктуру для удаленной работы и расширили цифровые возможности в начале 2020 года. Это позволило некоторым предприятиям быстро перейти к цифровому стилю работы, однако другие организации внедрили быстрые исправления и временные меры, отвечающие требованиям времени [10].

Основные угрозы безопасности данных в условиях удаленной работы

Угрозы безопасности данных и проблемы киберзащиты обусловливают необходимость исследования вызовов и IT-решений в области обеспечения безопасности данных.

Прежде всего, крайне маловероятно, что все компании смогут предоставить своим сотрудникам рабочий компьютер (то есть портативное устройство, принадлежащее компании, с прямым доступом к серверу и степенью киберзащиты, равной уровню компьютерной защиты) для использования на дому. Таким образом, некоторые сотрудники используют свои личные устройства для удаленного доступа к серверу, а также частные сети Wi-Fi. Эти персональные конечные точки (ноутбуки, планшеты, компьютеры) и домашние беспроводные соединения являются потенциальными точками входа для киберпреступников. Использование личных устройств для работы (феномен, известный как “bring your own device”), при котором работодатели как контролеры данных несут ответственность за любые персональные данные, обрабатываемые на личных устройствах в рабочих целях, создает определенные проблемы с соблюдением требований по защите данных [11], при этом такой формат в настоящее время все чаще используется в условиях удаленной работы.

Кроме того, как правило, персональные устройства имеют более низкую степень кибербезопасности, так как сотрудники, не работающие непосредственно с системой безопасности данных, редко полностью осведомлены о киберугрозах, с которыми они могут столкнуться. Также многие сотрудники не осведомлены о том, какие протоколы безопасности установлены на их устройствах, насколько эффективна их антивирусная поддержка, ограничивающая Wi-Fi, и др. [12].

Кроме того, сотрудники под давлением рабочих задач могут начать загружать файлы компании на свои персональные компьютеры, а не в облако, чтобы иметь возможность

продолжать работать, если удаленный доступ прерван или замедлен. Более того, с учетом «домашних отвлекающих факторов» (например, детей, домашних животных и др.) безопасность данных не находится в центре внимания сотрудников. В таких условиях сотрудники могут допустить халатность и не уделить должного внимания мерам защиты от кибератак, особенно если они не прошли должную подготовку в области кибербезопасности. Неудивительно, что фишинговые атаки, которые используют электронную почту или текстовые сообщения для того, чтобы обманом заставить людей предоставить им личную информацию, становятся все более распространенными, поскольку киберпреступники эксплуатируют страхи людей и потребность в информации [13]. Если сотрудник стал жертвой фишинга, контроль компании над его данными может быть нарушен, следовательно, компания может нести юридическую ответственность за утечку данных. Иными словами, различные приложения и устройства, используемые для удаленной работы (инструменты для обмена файлами и совместной работы (например, Zoom), многочисленные персональные устройства, подключающиеся к сети, более высокий трафик электронной почты, облачные решения и др.) могут привести к утечке данных, а также к потере и краже данных, что оборачивается огромными финансовыми и репутационными потерями компаний [14].

Неблагоприятные последствия перехода на удаленный формат работы также включают в себя социальную и профессиональную изоляцию, предполагаемые угрозы для профессионального развития, продолжительное рабочее время в режиме «всегда на связи», повышенное эмоциональное истощение, ограниченный контроль со стороны линейных руководителей, больший когнитивный стресс, перегрузки и ухудшение здоровья опорно-двигательного аппарата [14].

Систематический обзор литературы, проведенный португальскими учеными [15], позволил выявить многие проблемы, встречающиеся в контексте удаленной работы:

- коммуникационные проблемы;
- проблемы управления;
- проблемы прозрачности;
- технологические проблемы;
- проблемы поддержания сплоченности команды;
- проблемы обучения;
- безличная среда;
- неэффективное использование информационно-коммуникационных технологий;
- проблемы с производительностью;
- проблемы безопасности;
- баланс между формальным и неформальным общением и документацией;
- отсутствие посещаемости работы.

Исследования по теме безопасности данных при удаленной работе

В научной литературе встречается множество исследований по теме безопасности данных при удаленной работе. Можно выделить основные из них, которые были опубликованы в 2021–2024 гг. (см. Таблицу).

В целом можно сделать вывод, что современные ученые не имеют единой точки зрения на природу угроз безопасности данных.

Таблица

Обзор исследований по теме безопасности данных при удаленной работе

Источник	Метод / локация / выборка (чел.)	Ключевые выводы исследования
[4]	Кейс-стади / Хорватия / —	Хорватия хранит полное молчание об угрозах кибербезопасности, связанных с пандемией; компании были вынуждены искать собственные способы реагирования на возросшие киберугрозы
[16]	Опрос / Южная Корея / 411	Производительность и гибкость работы оказывают существенное опосредующее влияние на намерение продолжать использовать формат удаленной работы
[17]	Опрос / США / 203	Вопреки широко распространенным представлениям об удаленной работе, результаты показывают, что удаленная работа положительно связана с осведомленностью о кибербезопасности и принятием необходимых мер предосторожности
[18]	Обзор литературы / — / —	Наиболее распространенной причиной утечки данных являются человеческие ошибки, а именно фишинговые атаки и халатность сотрудников
[2]	Опрос и качественный анализ / Китай / 244	Переход на удаленную работу после карантина объясняется тремя основными переменными: поведенческим намерением, поведенческим ожиданием и способствующими условиями
[19]	Обзор литературы / — / —	Недостаток обучения по безопасности дистанционной работы, стресс, неразборчивое применение технологий и наличие ненадежных лиц в местах удаленной работы могут увеличивать киберриски. Одновременно с этим попытки организаций контролировать эти риски часто приводят к нарушению конфиденциальности сотрудников через интенсивное использование технологий мониторинга
[20]	Смешанная стратегия / международное исследование / 130	Несмотря на то, что большинство организаций имеют стратегии по обеспечению соблюдения требований кибербезопасности для своих удаленных сотрудников, более половины опрошенных не знают об этом или не имеют подготовки, необходимой для соблюдения данных требований
[21]	Смешанная стратегия / международное исследование / 313	Работодатели и менеджеры по информационной безопасности, вероятно, продолжат уделять повышенное внимание ограничению рисков, связанных с человеческим фактором, который стал более многогранным во время пандемии Covid-19, учитывая психоэмоциональные проблемы удаленной работы, с которыми сталкивается большая часть работников
[22]	Кейс-стади / — / —	Распространенность беспроводной локальной сети во время пандемии Covid-19 не оказала существенного влияния на безопасность данных
[23]	Обзор литературы / — / —	Компаниям недостаточно существующих IT-решений, и они продолжают страдать от угроз безопасности из-за растущего списка уязвимостей безопасности

Источник: составлено автором на основе литературы, указанной в таблице.

В связи с этим целесообразно привести обзор основных IT-решений для обеспечения безопасности данных.

Обзор основных IT-решений для обеспечения безопасности данных

Наиболее очевидным способом защитить данные между удаленными сотрудниками и основными системами является ***VPN***. В «идеальном» мире организации использовали бы сетевую систему с нулевым уровнем доверия. Однако это достаточно трудно реализовать, особенно в ответ на кризисные явления (такие, как, например, пандемия), поскольку внедрение должно быть поэтапным, что предполагает пилотные проекты и доработки в безопасной среде перед развертыванием. Однако если организация еще не приняла концепции привилегированного доступа и наименьших привилегий или по-прежнему использует общие учетные записи для доступа, то нулевое доверие, вероятно, не сработает. Организации должны обеспечить сотрудникам современные средства защиты на любых устройствах, такие как средства проверки на вирусы, брандмауэры и шифрование устройств.

Еще одним важным для организаций способом снижения рисков является внедрение ***системы управления мобильными устройствами*** (далее – MDM). Например, существуют такие опции MDM, которые позволяют нескольким пользователям, использующим одно и то же устройство, полностью контролировать VPN, возможности очистки устройств и настройки политик защиты корпоративных данных. Они также позволяют разделять личные и корпоративные данные, что может оказаться полезной функцией в сложных средах личных устройств сотрудников. Компании также могут выбирать между интеллектуальным анализом данных, традиционными моделями Active Directory или групповой политикой.

Кроме того, существуют продукты сторонних производителей, которые могут помочь предприятиям установить меньшие границы для обеспечения соответствия требованиям и сосредоточиться на них, а не на всей сети в целом. Например, некоторые IT-решения позволяют изолировать конфиденциальную личную информацию от конфиденциальной корпоративной информации, то есть данные компании никогда не хранятся на мобильном устройстве. Это важно для отдельных лиц и компаний, если возникают юридические проблемы. Это также снижает затраты и упрощает управление устройствами. Также важны «белые» и «черные» списки приложений. Компаниям также следует использовать IT-сервисы, помогающие контролировать устройства, используемые сотрудниками. Компании, в которых действуют программы контроля личных устройств сотрудников, могут разрешить администраторам выполнять выборочную очистку устройств и данных приложений, не очищая все устройство целиком. Кроме того, когда требуется полная очистка, политика может принудительно выполнить очистку защищенной цифровой карты (SD), а также при необходимости – внутренней памяти устройства. Администраторы также могут настраивать настройки Wi-Fi для каждого устройства с помощью политик приложений, позволяя им настроить их один раз и отправлять на все управляемые устройства одновременно.

Контейнеризация – еще один способ разделения корпоративных и личных данных на устройстве сотрудника, что предполагает разделение корпоративных мобильных приложений и связанных с ними данных на «контейнеры» на мобильном устройстве, создавая четкое разделение в отношении того, что подпадает под действие корпоративных политик безопасности, таких как удаление данных. Наконец, есть также возможность создать портал контролируемых приложений с нуля [24].

Также можно выделить следующие IT-решения.

• ***Многофакторная аутентификация.*** Является одним из наиболее важных структурных компонентов более широких и безопасных киберсистем. Аутентификация обычно основана на концептуальном пароле, текстовом или ином. Обычно подразделяется на аутентификацию по факторам. Эти факторы, как правило, включают в себя:

a) то, что знает пользователь, например, PIN-код или буквенно-цифровой пароль;

b) то, что есть у пользователя, например ключ-карта или файл;

c) то, что является частью пользователя, например биометрическая информация (обычно отпечатки пальцев; реже – распознавание радужной оболочки глаза);

d) то, что делает пользователь, например, рисует подпись или узор [25].

• ***Аутентификация на основе биометрии.*** Сегодня всё чаще предлагаются биометрические ключи, основанные на физиологических и поведенческих характеристиках людей, таких как отпечатки пальцев, лица, радужная оболочка глаз, геометрия руки, отпечатки ладоней и др. Можно выделить следующие преимущества биометрических ключей: их невозможно потерять или забыть; их очень сложно скопировать или передать; их чрезвычайно сложно подделать или распространить; их нелегко угадать; чьи-то биометрические данные взломать сложнее, чем у других [26].

• ***Шифрование данных.*** Риск утечки данных возрастает с увеличением расстояния между пользователем и местоположением хранения его информации, что угрожает конфиденциальности. Применение традиционных методов шифрования при передаче данных поставщикам облачных услуг помогает минимизировать подобные угрозы [27].

• ***Облачные решения и регулярное обновление.*** Облачные вычисления обеспечивают масштабируемость, регулярные обновления программного и аппаратного обеспечения, эффективное использование сетевых ресурсов и улучшенные меры безопасности. Эти преимущества подчеркивают значительный потенциал облачных технологий, открывая новые возможности для различных отраслей [27].

Создание безопасной удаленной рабочей среды требует комплексного подхода, включающего не только защиту данных, но и реализацию дополнительных мер безопасности. Так, важно обеспечить защиту инфраструктуры, включая установку надежных протоколов безопасности и VPN-соединений на всех рабочих устройствах. Компаниям также необходимо защитить свои сети от киберугроз, используя программное обеспечение для постоянного мониторинга угроз. Сотрудников следует стимулировать к обращению за помощью к ИТ-поддержке, чтобы избежать самостоятельного решения технических проблем, что повышает риски. Наконец, использование коммуникационных средств должно соответствовать стандартам безопасности для обеспечения безопасного общения [18].

С увеличением зависимости от удаленных бизнес-процессов важность надежных IT-решений для защиты информации продолжает усиливаться. Интеграция современных цифровых технологий стала ключевой составляющей стратегий укрепления информационной безопасности в компаниях. Однако существует потребность в более гибкой адаптации и развитии этих технологий для эффективного реагирования на динамично меняющиеся киберугрозы. Так, значительный прогресс в области искусственного интеллекта и машинного обучения предоставляет возможности для создания более адаптивных и интеллектуальных систем защиты данных . Эти технологии и системы могут предсказывать потенциальные угрозы и автоматически адаптироваться к новым условиям безопасности, тем самым повышая эффективность обеспечения конфиденциальности и целостности

данных в рамках удаленной работы. Следовательно, перспективы развития IT-решений для обеспечения безопасности данных остаются многообещающими и требуют постоянного обновления знаний и адаптации технологий к текущим вызовам в области кибербезопасности.

В заключение, основываясь на анализе научной литературы, дадим некоторые рекомендации по оптимизации управления безопасностью данных в контексте удаленной работы.

Заключение

Во-первых, целесообразно построить комплексную технологическую систему безопасности данных, включая следующие меры:

• создание системы защиты безопасности, охватывающей полный жизненный цикл сбора, передачи, хранения, обработки, совместного использования и уничтожения данных;

• введение современных механизмов защиты конфиденциальности, таких как аутентификация личности пользователя и рабочего места, детальный контроль доступа, аудит безопасности операций с данными и снижение чувствительности данных, для предотвращения несанкционированного доступа и утечки данных;

• общее планирование, а также активные усилия по исследованию и разработке общих и специализированных стандартов безопасности для разработки стандартной системы, связанной с безопасностью данных.

Во-вторых, целесообразно повысить способность руководства предотвращать и устранять риски кибербезопасности. Для комплексного устранения рисков кибербезопасности должны быть предприняты действия, касающиеся двух сторон – социальных субъектов и объектных систем, включая следующие меры:

• главные органы управления должны играть свою роль в пресечении незаконных и преступных действий, которые ставят под угрозу кибербезопасность, строго наказывать за неисполнение обязанностей и нарушения, а также предотвращать и устранять риски кибербезопасности посредством строгого контроля за исполнением закона;

• целесообразно использовать общую эффективность существующих систем оценки безопасности, оценки рисков и секретной защиты, а также повысить способность обнаруживать скрытые опасности в продуктах и системах информационных технологий;

• руководству компаний целесообразно подробнее изучать новые модели и IT-решения, основанные на технологии блокчейн, безопасных многосторонних вычислениях и др., что должно способствовать ускорению создания механизмов интеграции и соединения безопасности данных между объектами данных.

В-третьих, целесообразно улучшить системы поддержки управления безопасностью данных. В этом плане можно рекомендовать использовать следующие меры:

• усилить государственную поддержку для бизнеса. Этому может способствовать национальная стратегия защиты безопасности данных, позволяющая позиционировать безопасность данных и укреплять координацию стратегии данных с высоты национальной безопасности и национальных стратегических ресурсов;

• создать систему управления талантами, которая адаптируется к особенностям безопасности данных, что позволит преодолеть институциональные границы и обеспечить упорядоченное и эффективное перемещение талантов;

• углубить классификацию данных. Так, система классификации данных должна начинаться с повышения эффективности надзора и включать различные нормативные меры и законодательные требования для данных разных типов и классов.

Таким образом, обеспечение безопасности данных в контексте удаленной работы сегодня сопряжено со множеством вызовов, с которыми возможно справиться, только если агрегировать современные IT-решения в единый комплекс управленческих решений.

Литература / References

1. Kossek E.E., Lautsch B.A. (2018). Work-life flexibility for whom? Occupational status and work-life inequality in upper, middle, and lower level jobs. *Academy of Management Annals*. Vol. 12. No. 1. Pp. 5–36. DOI: https://doi.org/10.5465/annals.2016.0059
2. Sahut J.M., Lissillour R. (2023). The adoption of remote work platforms after the Covid-19 lockdown: New approach, new evidence. *Journal of business research*. Vol. 154. Art. ID 113345. Pp. 1–14. DOI: https://doi.org/10.1016/j.jbusres.2022.113345
3. Kähkönen T. (2023) Remote work during the COVID-19 pandemic: Identification of working life impacts, employees' data protection abilities and trust outcomes. *Journal of Organizational Change Management*. Vol. 36. No. 3. Pp. 472–492. DOI: https://doi.org/10.1108/JOCM-06-2022-0179
4. Škiljić A. (2020). Cybersecurity and remote working: Croatia's (non-) response to increased cyber threats. *International Cybersecurity Law Review*. No. 1. Pp. 51–61. DOI: https://doi.org/10.1365/s43439-020-00014-3
5. Ahmad T. (2020). Corona virus (covid-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity. *SSRN Electronic Journal.* Pp. 1–4. DOI: https://dx.doi.org/10.2139/ssrn.3568830
6. Flynn S., Ghent A.C., Nair V. (2024). Determinants and Consequences of Return to Office Policies. *SSRN Electronic Journal.* Pp. 1–49. DOI: https://dx.doi.org/10.2139/ssrn.4757876
7. Cooke F.L., Dickmann M., Parry E. (2020). IJHRM after 30 years: Taking stock in times of COVID-19 and looking towards the future of HR research. *The International Journal of Human Resource Management*. Vol. 32. No. 1. Pp. 1–23. DOI: https://doi.org/10.1080/09585192.2020.1833070
8. Maharani A. (2024). Back to Work or Remote Work: Trends and Challenges. In: Endress T., Badir Y.F. (Eds) *Business and Management in Asia: Disruption and Change*. Singapore : Springer. Pp. 139–150. DOI: https://doi.org/10.1007/978-981-99-9371-0_9
9. McPhail R., Chan X.W., May R., Wilkinson A. (2024). Post-COVID remote working and its impact on people, productivity, and the planet: An exploratory scoping review. *The International Journal of Human Resource Management*. Vol. 35. No. 1. Pp. 154–182. DOI: https://doi.org/10.1080/09585192.2023.2221385
10. Grimm J. (2021). Securing the remote workforce in the new normal. *Computer Fraud & Security*. No. 2. Pp. 8–11. DOI: https://doi.org/10.1016/S1361-3723(21)00018-X
11. Kaufman E., Lovich D., Bailey A., Messenböck R., Schuler F., Shroff A. (2020). *Remote Work Works – Where Do We Go from Here*. Boston Consulting Group. 8 p. URL: https://www.projecttimes.com/wp-content/uploads/attachments/bcg-remote-work-works-where-do-we-go-from-here-aug-2020-1.pdf (accessed 23.02.2024).
12. Chigada J., Madzinga R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*. Vol. 23. No. 1. Art. ID a1277. DOI: https://doi.org/10.4102/sajim.v23i1.1277
13. Ahmad W., Rasool A., Javed A.R., Baker T., Jalil Z. (2021). Cyber security in IOT-based cloud computing: A comprehensive survey. *Electronics*. Vol. 11. No. 1. Art. ID 16. Pp. 1–34. DOI: https://doi.org/10.3390/electronics11010016

14. Babapour M., Hultberg A., Bozic Y.N. (2021). Post-pandemic office work: Perceived challenges and opportunities for a sustainable work environment. *Sustainability*. Vol. 14. No. 1. Art. no. 294. Pp. 1–20. DOI: https://doi.org/10.3390/su14010294
15. Ferreira R., Pereira R., Bianchi I.S., da Silva M.M. (2021). Decision factors for remote work adoption: Advantages, disadvantages, driving forces and challenges. *Journal of Open Innovation: Technology, Market, and Complexity*. Vol. 7. No. 1. Pp. 1–23. DOI: https://doi.org/10.3390/joitmc7010070
16. Yang H. (2024) The Utility of Remote Work Solutions Post-Pandemic Era: Mediating Effects of Productivity and Work Flexibility. *SSRN Electronic Journal.* Pp. 1–25. DOI: https://dx.doi.org/10.2139/ssrn.4745244
17. Nwankpa J.K., Datta P.M. (2023). Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers. *Computers & Security*. Vol. 130. Pp. 103266–103266. DOI: 10.1016/j.cose.2023.103266
18. Bandari V. (2023). Enterprise data security measures: A comparative review of effectiveness and risks across different industries and organization types. *International Journal of Business Intelligence and Big Data Analytics*. Vol. 6. No. 1. Pp. 1–11. DOI: https://hcommons.org/deposits/item/hc:51451
19. Nurse J.R., Williams N., Collins E., Panteli N., Blythe J., Koppelman B. (2021). Remote working pre-and post-COVID-19: An analysis of new threats and risks to security and privacy. In: Stephanidis, C., Antona, M., Ntoa, S. (Eds) HCI International 2021 – Posters. HCII 2021. Communications in Computer and Information Science. Vol. 1421. Springer, Cham. Pp. 583–590. DOI: https://doi.org/10.1007/978-3-030-78645-8_74
20. Nyarko D.A., Fong R.C.W. (2023). Cyber security compliance among remote workers. In: In: Jahankhani H. (Ed) *Cybersecurity in the Age of Smart Societies. Advanced Sciences and Technologies for Security Applications*. Springer, Cham. Pp. 343–369. DOI: https://doi.org/10.1007/978-3-031-20160-8_18
21. Atstāja L., Rūtītis D., Deruma S., Aksjoņenko E. (2021). Cyber security risks and challenges in remote work under the covid-19 pandemic. In: Ozsahin M. (Ed.) *New Strategic, Social and Economic Challenges in the Age of Society 5.0 Implications for Sustainability.* Vol. 121. Pp. 12–22. European Proceedings of Social and Behavioural Sciences. European Publisher. DOI: https://doi.org/10.15405/epsbs.2021.12.04.2
22. Lindroos S., Hakkala A., Virtanen S. (2022). The COVID-19 pandemic and remote working did not improve WLAN security. *Procedia Computer Science*. Vol. 201. Pp. 158–165. DOI: https://doi.org/10.1016/j.procs.2022.03.023
23. Hijji M., Alam G. (2022). Cybersecurity Awareness and Training (CAT) framework for remote working employees. *Sensors*. Vol. 22. No. 22. Art. ID 8663. DOI: https://doi.org/10.3390/s22228663
24. Curran K. (2020). Cyber security and the remote workforce. *Computer Fraud & Security*. 2020. No. 6. Pp. 11–12. DOI: https://doi.org/10.1016/S1361-3723(20)30063-4
25. Obaidat M., Brown J., Obeidat S., Rawashdeh M. (2020). A hybrid dynamic encryption scheme for multi-factor verification: A novel paradigm for remote authentication. *Sensors*. 20. No. 15. Art. ID 4212. DOI: https://doi.org/10.3390/s20154212
26. Li C.T., Hwang M.S. (2010). An efficient biometrics-based remote user authentication scheme using smart cards. *Journal of Network and Computer Applications*. Vol. 33. No. 1. Pp. 1–5. DOI: https://doi.org/10.1016/j.jnca.2009.08.001
27. Seth B., Dalal S., Jaglan V., Le D.N., Mohan S., Srivastava G. (2022). Integrating encryption techniques for secure data storage in the cloud. *Transactions on Emerging Telecommunications Technologies*. Vol. 33. No. 4. Art. ID e4108. DOI: https://doi.org/10.1002/ett.4108