УДК 004.056

А. А. Бутин[1], А. С. Сафронов[1]

[1] Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ДИСТАНЦИОННОГО РЕЖИМА РАБОТЫ ОРГАНИЗАЦИИ

Аннотация. В данной статье рассматриваются вопросы обеспечения информационной безопасности в условиях дистанционного режима работы организации. Также, освещены причины возникновения потребности в дистанционном режиме работы организации, риски, связанные с использованием дистанционного режима работы организации, а также способы перехода на дистанционный режим работы организации с соблюдением требований информационной безопасности. Приведена аналитика атак на различные предприятия в отношении информационной безопасности, а также рассмотрены способы распространения вредоносного программного обеспечения на предприятиях. В заключение, рассмотрены основные рекомендации по соблюдению цифровой гигиены, а также обозначен основной источник угроз информационной безопасности на предприятии. Особое внимание уделено мерам защиты от различных хакерских атак, контролю доступа к защищаемой информации и использованию надежных и проверенных средств связи и средств обеспечения информационной безопасности на предприятии. Рекомендации, приведенные в данной статье, будут полезны как специалистам, работающим в области информационной безопасности, так и руководителям компаний, которые планируют переход на дистанционный режим работы или внедрение дистанционного режима работы параллельно с очным режимом работы, а также в качестве учебного пособия для использования и учебных организациях, специализирующихся на информационной безопасности

Ключевые слова: информационная безопасность, дистанционный режим работы, угроза информационной безопасности, риск информационной безопасности, киберпреступление, рекомендации по информационной безопасности.

A. A. Butin[1], A. S. Safronov[1]

[1]Irkutsk State Transport University, Irkutsk, Russian Federation

DEVELOPMENT OF RECOMMENDATIONS FOR ENSURING INFORMATION SECURITY IN THE CONDITIONS OF REMOTE OPERATION OF THE ORGANIZATION

Abstract. This article discusses the issues of ensuring information security in the conditions of the remote operation of the organization. Also, the reasons for the need for a remote mode of operation of the organization, the risks associated with using the remote mode of operation of the organization, as well as ways to switch to a remote mode of operation of the organization in compliance with information security requirements are highlighted. The analysis of attacks on various enterprises in relation to information security is presented, as well as the ways of spreading malicious software in enterprises are considered. In conclusion, the main recommendations on the observance of digital hygiene are considered, as well as the main source of threats to information security in the enterprise is identified. Special attention is paid to protection measures against various hacker attacks, access control to protected information and the use of reliable and proven means of communication and information security at the enterprise. The recommendations given in this article will be useful both to specialists working in the field of information security and to heads of companies who plan to switch to a remote mode of operation or implement a remote mode of operation in parallel with full-time work, as well as as a training tool for use by educational organizations specializing in information security.

Keywords: information security, remote work, information security threat, information security risk, cybercrime, information security recommendations.

В 2020 году мир столкнулся с коронавирусной инфекцией [1]. Несмотря на большое количество проблем в самых разных сферах деятельности, не менее острым вопрос стоял и в организации работы сотрудников практически всех предприятий – от мировых, до небольших в масштабах города или даже района [2]. Дистанционный режим работы стал спасением для многих организаций и экономики в целом [3]. Большую часть работ можно вынести за пределы здания и работать, не выходя из дома, выполняя свои должностные обязанности ничем не хуже, чем на рабочем месте. Однако, многие из организаций, перешедших на дистанционный

режим работы, столкнулись с проблемами информационной безопасности [4]. Цель данной статьи – показать важность правильной подготовки к дистанционному режиму работы организации и разработать список рекомендаций по обеспечению информационной безопасности в условиях дистанционного режима работы организации, который можно будет использовать как для построения системы информационной безопасности с нуля, так и для улучшения уже существующей системы.

Так как организовать работу нужно было в кратчайшие сроки – многие забыли о безопасности в сети и организовали работу «как попало». В результате чего количество инцидентов информационной безопасности в 2020 году увеличилось на 51% по сравнению с 2019 годом (рис. 1). 86% всех атак были направлены на организации. Больше всего злоумышленников интересовали государственные и медицинские учреждения, а также промышленные организации [5].

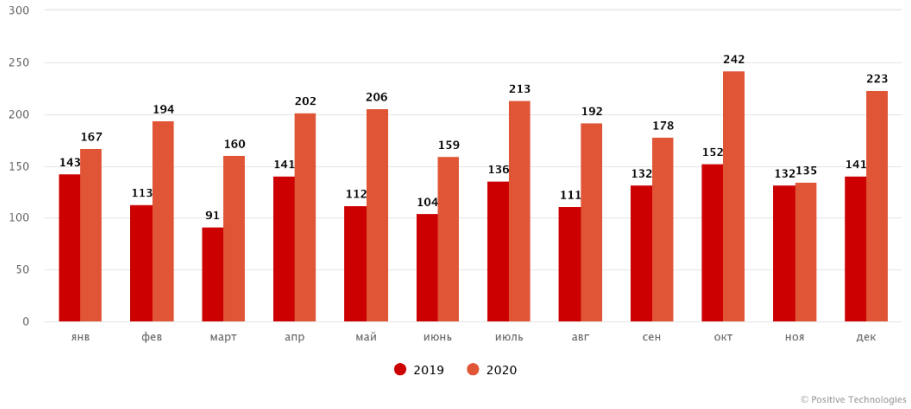

Рис. 1. Рост числа атак на фоне пандемии

В атаках на организации основными векторами доставки вредоносного программного обеспечения (ВПО) остаются электронная почта (71%) и компрометация компьютеров, серверов и сетевого оборудования (24%) [5] (рис. 2).

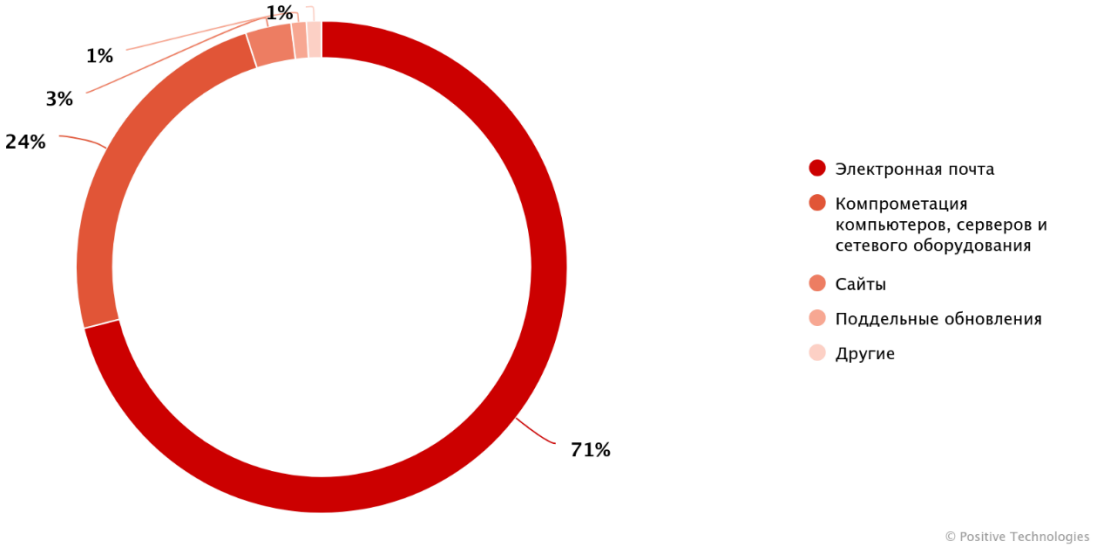

Рис. 2. Способы распространения ВПО в атаках на организации

Количество атак на промышленность увеличилось почти в два раза по сравнению с 2019 годом: прирост составил 91% [5] (рис. 3).

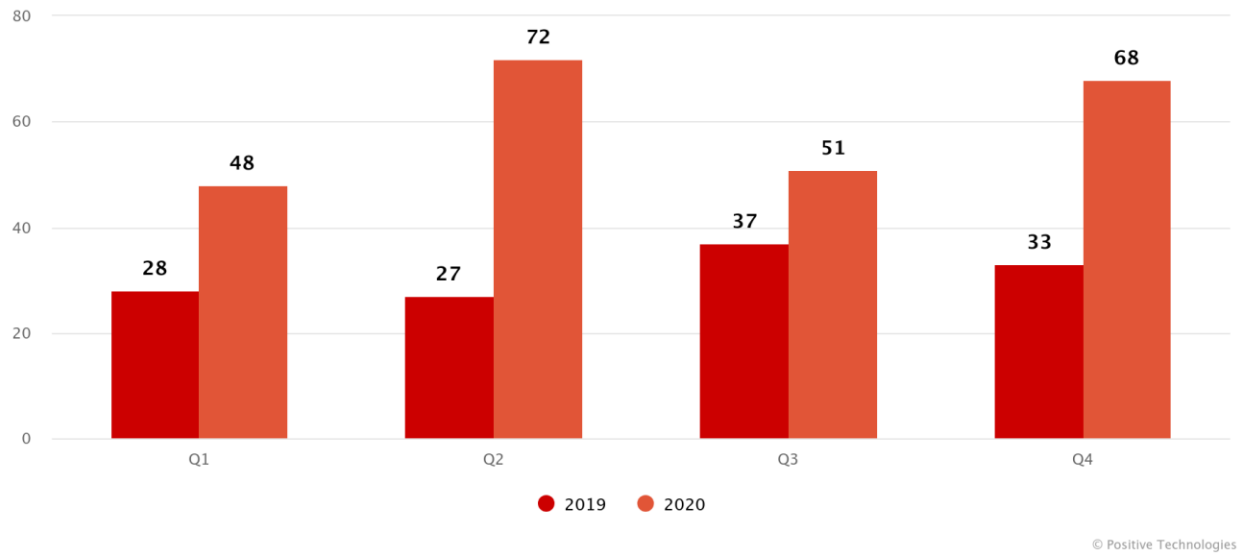

Рис. 3. Количество атак на промышленность

Все приведенные примеры показывают, что при внезапной смене обстановки злоумышленники адаптируются к ней гораздо быстрее, чем те, кто защищается [6]. Также, можно сделать выводы о том, что за период пандемии злоумышленники стали пользоваться удобствами дистанционного режима работы в своих целях [7]. Использование вредоносного программного обеспечения, социальная инженерия, вредоносные письма и поиск уязвимостей в программном обеспечении, которое обеспечивает дистанционный режим работы или безопасность такого режима – это все перспективные направления для злоумышленников, которые были бы менее доступны в очном режиме работы.

Использование дистанционного режима работы может быть связано не только с пандемией и глобальными проблемами [8]. Наоборот, это открыло для предприятий новые возможности. Например, если сотрудник чувствует себя неважно, то вместо походов в больницу для оформления больничного на пару дней, он может находиться дома и продолжать работу дистанционно [9]. Конечно, это не относится к случаям тяжелой болезни и серьезного недомогания. В такой ситуации необходимо обратиться в медучреждение и брать больничный. С другой стороны, организации могут расширить штат сотрудников, не ограничиваясь своим физическим расположением [10]. Безусловно, есть работа, которая требует непосредственного участия сотрудника в рабочем процессе. Однако, с развитием ИТ-инфраструктуры, рабочих мест для удаленных сотрудников становится все больше. Таким же образом поступают и некоторые образовательные организации. Уже сейчас есть большое количество образовательных платформ, которые предоставляют возможность пройти онлайн-курсы и получить образование в перспективных направлениях [11].

Анализ полученного за время пандемии опыта в совокупности с современными технологиями и темпами развития ИТ-индустрии может помочь выстроить грамотную политику безопасности в отношении дистанционного режима работы на предприятии.

Рассмотрим три метода по обеспечению информационной безопасности для дистанционного режима работы.

Первый метод заключается в самостоятельном подборе решений, программ и компонентов, обеспечивающих информационную безопасность на предприятии. Организация, используя знания и умения своих штатных сотрудников, находит необходимое программное обеспечение, настраивает его для работы в соответствии с принятой политикой информационной безопасности. Такой метод напрямую зависит от компетенций самих сотрудников. Самостоятельный подбор решений, настройка и установка программного обеспечения без необходимых знаний может быть произведена некорректно и не в полном объеме, что может привести к негативным последствиям как для ответственных сотрудников, так и для организации в целом. Действовать, используя такой метод, стоит на свой страх и риск.

Второй метод противоположен первому. В данном случае привлекается сторонняя организация, которая или использует уже готовое решение, если оно удовлетворяет требованиям политики безопасности организации, или подготавливает новое уникальное решение специально для организации. Этот метод хорош тем, что организацией информационной безопасности на предприятии занимаются специалисты в области информационной безопасности. Однако, нужно быть уверенным в выборе организации, иначе можно потерять не только деньги и время, но и стать жертвой киберпреступников. В настоящее время на рынке есть множество организаций, предлагающих свои услуги в области информационной безопасности, что позволяет выбрать решение, которое устроит любой бюджет и любые требования [12].

Третий метод — это нечто среднее между первым и вторым. В открытых источниках, в том числе и официальных, есть большое количество информации о том, как правильно и корректно настроить программное обеспечение, подобрать те или иные решения для правильной организации информационной безопасности и построения системы обеспечения информационной безопасности. У официальных вендоров программного обеспечения есть примеры различных решений для тех или иных организаций, которые так же могут подходить и для вашего предприятия [13]. То есть, данный метод заключается в том, что решение не придумывается самостоятельно, а выбирается уже готовое из открытых источников. Но настройка и установка программ и компонентов производится уже собственными силами. Минусами такого метода является то, что для вашего предприятия в открытых источниках может не быть подходящего решения, а также недостаточные компетенции сотрудников предприятия. Некорректная установка или настройка программного обеспечения может привести к реализации угроз информационной безопасности на предприятии. Такой метод позволит сэкономить на подборе решения для вашего предприятия, но в то же время влечет за собой дополнительные риски, которые могут стать угрозой для вашей организации.

Несмотря на то, насколько грамотно и хорошо выстроена система обеспечения информационной безопасности на вашем предприятии, сотруднику необходимо соблюдать правила цифровой гигиены. Рассматривая предыдущие работы в совокупности с полученной информацией, сформирован следующий список рекомендаций по соблюдению цифровой гигиены [14]:

- без необходимости не хранить и не открывать на домашнем компьютере рабочие документы;
- во избежание взлома роутера, заменить пароль на более сложный;
- не открывать подозрительные электронные письма и тем более вложения из таких писем;
- использовать только разрешенные каналы связи;
- настроить двухфакторную аутентификацию в электронной почте, мессенджерах и при удаленном доступе через VPN;
- установить сложные пароли везде, где это возможно;
- не хранить пароли ни на рабочем, ни на домашнем компьютере;
- очищать остаточную информацию из браузера после работы;
- соблюдать все рекомендации ИТ-специалистов при работе.

Данные правила помогут соблюдать информационную безопасность при работе как при дистанционном режиме работы, так и при работе непосредственно на рабочем месте и не создавать дополнительных угроз информационной безопасности.

Самым главным источником угроз информационной безопасности был и по сей день остается человеческий фактор. По данным Positive Technologies в 3 квартале 2022 года в 93% атак был задействован человеческий фактор [15]. Из этого можно сделать вывод – насколько бы не была проработанной ваша система обеспечения информационной безопасности, необходимо также уделять большое внимание обучению сотрудников и контролю за ними, так как именно они являются наибольшей угрозой любой системы информационной безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Dating first cases of COVID-19 | PLOS Pathogens [Электронный ресурс]. – URL:https://journals.plos.org/plospathogens/article?id=10.1371/journal.ppat.1009620. (Дата обращения: 20.01.2024).
2. Симагаева, Т. В. Удаленная работа в условиях пандемии COVID-19 / Т. В. Симагаева. — Текст: непосредственный // Молодой ученый. — 2021. — № 15 (357). — С. 101-103. — URL: https://moluch.ru/archive/357/79964/. (дата обращения: 20.01.2024).
3. COVID-19 и культура удаленной работы. Автор Уварова Елена (46688). (hrtime.ru) [Электронный ресурс]. – URL:https://hrtime.ru/material/covid-19-i-kultura-udalennoy-raboty-46688/. (дата обращения: 20.01.2024).
4. Какое влияние оказал COVID-19 на кибербезопасность? (securitylab.ru) [Электронный ресурс]. – URL:https://www.securitylab.ru/blog/company/bitdefender/348975.php. (дата обращения: 20.01.2024).
5. Актуальные киберугрозы: итоги 2020 года (ptsecurity.com) [Электронный ресурс]. – URL:https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/. (Дата обращения: 20.01.2024).
6. Пандемия COVID-19 привела к пандемии кибератак: аналитическая записка - Innostage (innostage-group.ru) [Электронный ресурс]. – URL:https://innostage-group.ru/press/blog/analytics/pandemiya-kiberatak/?ysclid=lxbp6g5d73129071990. (Дата обращения: 20.01.2024).
7. Как киберпреступники наживаются на пандемии COVID-19 — ТОП-7 способов (anti-malware.ru) [Электронный ресурс]. – URL:https://www.anti-malware.ru/analytics/Threats_Analysis/How-Cybercrooks-use-COVID-pandemic-top-7. (Дата обращения: 20.01.2024).
8. Доля работающих удаленно сотрудников растет по всему миру - Inc. Russia (incrussia.ru) [Электронный ресурс]. – URL:https://incrussia.ru/news/dolya-rabotayushchikh-udalenno-sotrudnikov-prodolzhaet-rasti-po-vsemu-miru/. (Дата обращения: 20.01.2024).
9. Депутаты хотят дать работникам право переходить на дистанционную работу на время болезни - Российская газета (rg.ru) [Электронный ресурс]. – URL:https://rg.ru/2024/01/11/deputaty-hotiat-dat-rabotnikam-pravo-perehodit-na-distancionnuiu-rabotu-na-vremia-bolezni.html?ysclid=lxbpk666um1727553. (Дата обращения: 20.01.2024).
10. Никогда не будут прежними: как компании трансформируются на удаленке | РБК Тренды (rbc.ru) [Электронный ресурс]. – URL:https://trends.rbc.ru/trends/industry/cmrm/5fbb8a049a7947769d3f9aed. (Дата обращения: 20.01.2024).
11. Открытое образование - Главная страница (openedu.ru) [Электронный ресурс]. – URL:https://openedu.ru/?ysclid=lxbpniyu35159628639. (Дата обращения: 20.01.2024).
12. Секрет- Сервис | (secrets.ru) [Электронный ресурс]. – URL: https://www.secrets.ru/?ysclid=lxbpqbvudq210881948. (Дата обращения: 20.01.2024).
13. Готовые решения для «удаленки» даже для убежденных консерваторов (business-gazeta.ru) [Электронный ресурс]. – URL: https://www.business-gazeta.ru/article/482960?ysclid=lxbpu4dp3j130832532. (Дата обращения: 20.01.2024).
14. Бутин А.А., Василевская А.Н. Обзор основных рекомендаций по предупреждению инцидентов информационной безопасности в условиях удаленной работы и режима самоизоляции // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2020. – №2(7). – С. 39-45 – DOI: 10.26731/2658-3704.2020.2(7).39-45 – Режим доступа: http://ismm-irgups.ru/toma/27-2020, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 20.01.2024)
15. Актуальные киберугрозы: III квартал 2022 года (ptsecurity.com) [Электронный ресурс]. – ULR:https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q3/?sphrase_id=295071. (Дата обращения: 20.01.2024)

REFERENCES

1. Dating first cases of COVID-19 | PLOS Pathogens [Electronic resource]. – URL:https://journals.plos.org/plospathogens/article?id=10.1371/journal.ppat.1009620. (Date of application: 01/20/2024).

2. Simagaeva, T. V. Remote work in the context of the COVID-19 pandemic / T. V. Simagaeva. — Text: direct // Young scientist. — 2021. — № 15 (357). — Pp. 101-103. — URL: https://moluch.ru/archive/357/79964 /. (date of application: 01/20/2024).

3. COVID-19 and the culture of remote work. The author is Elena Uvarova (46688). (hrtime.ru) [Electronic resource]. – URL:https://hrtime.ru/material/covid-19-i-kultura-udalennoy-raboty-46688/. (accessed: 01/20/2024).

4. What impact has COVID-19 had on cybersecurity? (securitylab.ru) [Electronic resource]. – URL:https://www.securitylab.ru/blog/company/bitdefender/348975.php . (date of issue: 01/20/2024).

5. Current cyber threats: the results of 2020 (ptsecurity.com) [Electronic resource]. – URL:https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/. (Accessed: 01/20/2024).

6. The COVID-19 pandemic led to a pandemic of cyber attacks: analytical note - Innostage (innostage-group.ru) [Electronic resource]. – URL:https://innostage-group.ru/press/blog/analytics/pandemiya-kiberatak/?ysclid=lxbp6g5d73129071990. (Date of issue: 01/20/2024).

7. How cybercriminals profit from the COVID-19 pandemic — TOP 7 ways (anti-malware.ru) [Electronic resource]. – URL:https://www.anti-malware.ru/analytics/Threats_Analysis/How-Cybercrooks-use-COVID-pandemic-top-7. (Date of issue: 01/20/2024).

8. The share of employees working remotely is growing worldwide - Inc. Russia (incrussia.ru) [Electronic resource]. – URL:https://incrussia.ru/news/dolya-rabotayushchikh-udalenno-sotrudnikov-prodolzhaet-rasti-po-vsemu-miru/. (Date of application: 01/20/2024).

9. Deputies want to give employees the right to switch to remote work during illness - Rossiyskaya Gazeta (rg.ru) [Electronic resource]. – URL:https://rg.ru/2024/01/11/deputaty-hotiat-dat-rabotnikam-pravo-perehodit-na-distancionnuiu-rabotu-na-vremia-bolezni.html?ysclid=lxbpk666um1727553. (Accessed: 01/20/2024).

10. They will never be the same: how companies transform on the remote | RBC Trends (rbc.ru) [Electronic resource]. – URL:https://trends.rbc.ru/trends/industry/cmrm/5fbb8a049a7947769d3f9aed. (Date of application: 01/20/2024).

11. Open Education - Home page (openedu.ru) [Electronic resource]. – URL:https://openedu.ru/?ysclid=lxbpniyu35159628639. (Date of application: 01/20/2024).

12. Secret Service | (secrets.ru) [Electronic resource]. – URL: https://www.secrets.ru/?ysclid=lxbpqbvudq210881948. (Date of application: 01/20/2024).

13. Ready-made solutions for "remote" even for convinced conservatives (business-gazeta.ru) [Electronic resource]. – URL: https://www.business-gazeta.ru/article/482960?ysclid=lxbpu4dp3j130832532. (Date of application: 01/20/2024).

14. Butin A.A., Vasilevskaia A.N. Overview of basic recommendations for preventing information security incidents under remote work and self-isolation mode // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2020. No. 2(7). P. 39-45. DOI: 10.26731/2658-3704.2020.2(7).39-45 [Accessed 20/01/24]

15. Current cyber threats: The third quarter of 2022 (ptsecurity.com) [Electronic resource]. – ULR:https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q3/?sphrase_id=295071 (Date of the operation: 01.01.2024)

Информация об авторах

А*лександр Алексеевич Бутин* – к. ф.-м. н., доцент, доцент кафедры «кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск

Андрей Сергеевич Сафронов – студент, Иркутский государственный университет путей сообщения, г. Иркутск

Authors

Aleksander Alekseevich Butin, Candidate of Physico-Mathematical Sciences, Doctor, Associate Professor, the Subdepartment of Information systems and information security, Irkutsk State Transport University, Irkutsk

Andrey Sergeevich Safronov, student, Irkutsk State Transport University, Irkutsk

Для цитирования

Бутин А. А., Сафронов А. С. Разработка рекомендаций по обеспечению информационной безопасности в условиях дистанционного режима работы организации // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2024. – №2. – С. 52-58. – Режим доступа: http://ismm-irgups.ru/toma/222-2024.

For citations

Butin A. A., Safronov A. S. Development of recommendations for ensuring information security in the conditions of remote operation of the organization // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2024. No. 2. P. 52-58.