Современные инновации, системы и технологии // Modern Innovations, Systems and Technologies
2023; 3(2)
https://www.oajmist.com

УДК: 002.056.5
DOI: https://doi.org/10.47813/2782-2818-2023-3-2-0234-0242
EDN: JHHRLC

Обеспечение безопасности конфиденциальной информации компании при удаленном доступе сотрудника

С. А. Нуриев[1], И. Н. Карцан[1,2]

[1]ФГБУН ФИЦ «Морской гидрофизический институт РАН», Севастополь, Россия
[2]ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева», Красноярск, Россия

Аннотация. Быстрый рост удаленной работы привел к появлению новых проблем и вопросов, связанных с безопасностью и конфиденциальностью информации компании. Поскольку сотрудники получают доступ к конфиденциальным данным из различных мест и с различных устройств, обеспечение защиты конфиденциальной информации стало важнейшим приоритетом для организаций. В этой статье рассматриваются проблемы, связанные с безопасным доступом к конфиденциальной информации компании в среде удаленной работы, а также возможные решения и лучшие практики. Первая проблема заключается в установлении безопасного соединения между удаленными сотрудниками и сетью компании. Виртуальные частные сети стали широко распространенным решением для шифрования передачи данных и обеспечения безопасного удаленного доступа. Однако организации должны тщательно настраивать и поддерживать свою инфраструктуру для уменьшения уязвимостей и защиты от несанкционированного доступа. Другая важная проблема связана с аутентификацией и авторизацией пользователей. Традиционные механизмы аутентификации на основе паролей становятся все более уязвимыми для сложных атак, что приводит к необходимости внедрения методов многофакторной аутентификации. Многофакторная аутентификация объединяет несколько факторов, таких как пароли, биометрические данные и маркеры безопасности, для усиления контроля доступа и проверки личности удаленных сотрудников. Шифрование данных играет решающую роль в защите конфиденциальной информации во время транспортировки и хранения. Передовые алгоритмы шифрования и надежные системы управления ключами необходимы для предотвращения несанкционированного доступа к конфиденциальным данным. Кроме того, организации должны внедрять строгие политики безопасности, такие как регулярная смена паролей и протоколы классификации данных, для дальнейшего усиления защиты данных. Кроме того, обучение и информирование сотрудников являются важнейшими компонентами комплексной стратегии безопасности. Организациям следует регулярно проводить обучение безопасным методам удаленной работы, подчеркивая важность надежных паролей, безопасных сетей Wi-Fi и защиты от фишинга. Решая проблемы, связанные с безопасным доступом к конфиденциальной информации компании в среде удаленной работы, и внедряя соответствующие решения и передовые методы, организации могут значительно повысить уровень информационной безопасности и защитить конфиденциальные данные от несанкционированного доступа.

Ключевые слова: удаленная работа, безопасный доступ, конфиденциальная информация, шифрование данных, многофакторная аутентификация, VPN, мониторинг и аудит, обучение

Благодарности: Работа выполнена в рамках государственного задания по теме № FNNN-2021-0005.

Для цитирования: Нуриев, С. А., & Карцан, И. Н. (2023). Обеспечение безопасности конфиденциальной информации компании при удаленном доступе сотрудника. Современные инновации, системы и технологии - Modern Innovations, Systems and Technologies, 3(2), 0234–0242. https://doi.org/10.47813/2782-2818-2023-3-2-0234-0242

Ensuring the security of confidential company information during remote access of an employee

S. A. Nuriev[1], I.N. Kartsan[1,2]

[1]FSBUN FIC "Marine Hydrophysical Institute of the Russian Academy of Sciences", Sevastopol, Russia
[2]FSBEI HE "Siberian State University of Science and Technology named after Academician M.F. Reshetnev", Krasnoyarsk, Russia

Abstract. The rapid growth of remote work has introduced new challenges and concerns regarding the security and confidentiality of company information. With employees accessing sensitive data from various locations and devices, ensuring the protection of confidential information has become a critical priority for organizations. This article examines the challenges associated with secure access to confidential company information in a remote work environment and explores potential solutions and best practices. The first challenge lies in establishing a secure connection between remote employees and the company's network. Virtual Private Networks (VPNs) have emerged as a widely adopted solution for encrypting data transmissions and providing secure remote access. However, organizations must carefully configure and maintain their VPN infrastructure to mitigate vulnerabilities and protect against unauthorized access. Another critical challenge involves user authentication and authorization. Traditional password-based authentication mechanisms are increasingly vulnerable to sophisticated attacks, necessitating the adoption of multi-factor authentication (MFA) techniques. MFA combines multiple factors, such as passwords, biometrics, and security tokens, to strengthen access controls and verify the identities of remote employees. Data encryption plays a crucial role in safeguarding confidential information during transit and storage. Advanced encryption algorithms and robust key management systems are essential to prevent unauthorized access to sensitive data. Additionally, organizations should enforce strong security policies, such as regular password changes and data classification protocols, to further enhance data protection. Moreover, employee education and awareness are critical components of a comprehensive security strategy. Organizations should provide regular training on secure remote work practices, emphasizing the importance of strong passwords, secure Wi-Fi networks, and phishing prevention. By addressing the challenges associated with secure access to confidential company information in a remote work environment and implementing appropriate solutions and best practices, organizations can significantly enhance their information security posture and protect sensitive data from unauthorized access.

Keywords: remote work, secure access, confidential information, data encryption, multi-factor authentication, VPN, monitoring and auditing, employee education

Acknowledgements: This study was supported by the Russian Federation State Task № FNNN-2021-0005.

For citation: Nuriev, S. A., & Kartsan, I. N. (2023). Ensuring the security of confidential company information during remote access of an employee. Modern Innovations, Systems and Technologies, 3(2), 0234–0242. https://doi.org/10.47813/2782-2818-2023-3-2-0234-0242

ВВЕДЕНИЕ

Современные реалии бизнеса требуют от компаний перехода на удаленную работу, что ставит вопрос обеспечения безопасности конфиденциальной информации компании при удаленном доступе сотрудника на первый план [1-4]. Необходимость защиты конфиденциальной информации усилилась еще больше в последнее время, поскольку появилось еще больше угроз безопасности. Соответственно, компании вынуждены регулярно улучшать меры защиты.

Кроме уже привычных мер безопасности, таких как использование защищенных соединений с помощью VPN или других средств шифрования, установка и использование антивирусного программного обеспечения на устройствах сотрудников, а также ограничение доступа к конфиденциальной информации только для уполномоченных сотрудников, существуют и другие способы обеспечения безопасности при удаленном доступе сотрудника. Один из таких способов - обучение сотрудников основам информационной безопасности.

Это позволит им лучше понимать угрозы, с которыми они могут столкнуться при удаленной работе, а также научит правильно обращаться с конфиденциальной информацией.

МЕТОДЫ

В качестве метода обеспечения безопасности при удаленном доступе сотрудника используется двухфакторная аутентификация [5-7]. Это обеспечивает дополнительный уровень безопасности, требуя от сотрудников ввода не только пароля, но и дополнительного кода, который может быть отправлен им на мобильный телефон или другое устройство.

Также можно использовать системы мониторинга безопасности, которые могут оповещать о любых подозрительных действиях сотрудников при удаленном доступе [6, 8-10]. Это позволяет быстро обнаруживать и реагировать на возможные угрозы безопасности.

Наконец, важно регулярно обновлять программное обеспечение и выполнять резервное копирование данных, чтобы минимизировать риски потери информации в случае атаки или сбоя системы [11-13].

РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

Важно понимать, что обеспечение безопасности информации — это непрерывный процесс, который требует постоянного внимания. Кроме проведения регулярных проверок на наличие утечек и несанкционированных действий, существует множество других действий, которые могут быть предприняты для обеспечения безопасности информации.

Например, можно установить систему контроля доступа, которая позволит определять, кто имеет доступ к конфиденциальной информации и контролировать их действия. Также можно организовать обучение сотрудников по вопросам информационной безопасности, чтобы они могли более эффективно защищать информацию, с которой работают.

Кроме того, следует проводить аудит информационной безопасности с использованием современных инструментов, которые позволяют выявлять уязвимости и определять необходимые меры по их устранению. Кроме того, рекомендуется создать регламент по обеспечению безопасности информации, в котором будет определено, кто и каким образом должен обеспечивать безопасность информации в компании.

Таким образом, предпринимаемые меры по обеспечению безопасности информации должны быть комплексными и непрерывными, и должны включать в себя не только проверки на утечки и несанкционированные действия, но и множество других действий, направленных на защиту конфиденциальной информации.

Важным аспектом является также обучение сотрудников правилам безопасности и контроль за их соблюдением. Для того, чтобы повысить эффективность обучения, можно внедрить систему промежуточной аттестации, которая позволит оценить уровень знаний сотрудников и выявить пробелы в информированности. Кроме того,

сотрудники могут получить дополнительные знания и навыки на тренингах, конференциях и обучающих курсах по вопросам информационной безопасности. Это поможет им не только глубже понимать принципы безопасности, но и быть готовыми к решению нестандартных ситуаций.

Внутренние правила и инструкции по обеспечению безопасности информации также являются важным элементом в этом процессе. Они помогают сотрудникам быстрее ориентироваться в правилах и требованиях, что позволяет им лучше справляться со своими обязанностями и уменьшает вероятность нарушений. Кроме того, методы социальной инженерии могут быть использованы для проверки готовности сотрудников к действиям в нестандартной ситуации, что помогает лучше понимать уровень подготовки персонала и выявлять потенциальные слабые места в системе безопасности.

Важно понимать, что план действий в случае нарушения безопасности информации является неотъемлемой частью общей стратегии информационной безопасности компании. Его разработка должна быть комплексной и охватывать не только шаги по ликвидации угрозы безопасности, но и процедуры предотвращения подобных инцидентов [14]. В рамках такого плана необходимо проводить анализ причин и последствий инцидента, чтобы предотвратить возникновение подобных ситуаций в будущем. Кроме того, важно уведомлять компетентные органы и руководство компании в случае нарушения безопасности информации. Для того, чтобы быть максимально готовыми к возможным угрозам, следует проводить регулярные тренировки по выполнению действий по плану. Это поможет сформировать практические навыки у сотрудников и научить их реагировать на инциденты быстро и эффективно.

Для обеспечения безопасности конфиденциальной информации компании при удаленном доступе сотрудника необходимо принимать регулярные меры по мониторингу и обновлению мер защиты [15]. Это включает в себя внедрение современных технологий безопасности, проведение обучения сотрудников в области информационной безопасности, регулярные проверки уязвимостей и разработку плана

действий в случае нарушения безопасности информации. Дополнительными мерами могут стать ограничение доступа к конфиденциальной информации только необходимым сотрудникам, установка системы мониторинга доступа и шифрование конфиденциальной информации.

Важно помнить, что безопасность информации — это ответственность каждого сотрудника компании, а не только IT-отдела. Поэтому необходимо обучать всех сотрудников правилам безопасности, чтобы они понимали, какие методы и технологии используются для защиты конфиденциальных данных компании. Кроме того, важно проводить регулярные тренинги и тестирования, чтобы убедиться в том, что сотрудники действительно понимают и соблюдают правила безопасности. Это позволит улучшить общий уровень безопасности компании и защитить ее от потенциальных угроз.

ЗАКЛЮЧЕНИЕ

Сегодняшнее время характеризуется как эпоха цифровой революции, где информационные технологии играют ключевую роль в бизнесе. В связи с этим, безопасность стала одной из важнейших задач для любой компании. Сегодня компании должны принимать все возможные меры для защиты конфиденциальной информации, но только этого недостаточно. Необходимо также следить за соответствием последним стандартам безопасности и регулярно совершенствовать меры защиты. Компании также должны учитывать внутренние и внешние угрозы, такие как хакерские атаки, вирусы и несанкционированный доступ к информации, и принимать меры для предотвращения их возникновения. Все эти факторы существенно влияют на безопасность и стабильность компании, поэтому необходимо уделять им должное внимание.

СПИСОК ЛИТЕРАТУРЫ

[1] Сухостат В. В. Теория информационной безопасности и методология защиты информации. СПб: Университет ИТМО; 2018.

[2] Хорев А. А. Организация защиты информации от утечки по техническим каналам. М.: МО РФ; 2017. 316.

[3] Мухаметьянова А. Р. Особенности защиты информации на предприятии от утечки по техническим каналам. Уфа: Башкирский гос. ун-т; 2019. 56.

[4] Нуриев С. А., Карцан И. Н. Роль пространственной киберинфраструктуры в геоинформационных системах. E3S Web of Conferences. 2023; 389: 04023. doi.org/10.1051/e3sconf/202338904023

[5] Карцан И. Н., Контылева, Е. А. Глубокий интернет вещей. Современные инновации, системы и технологии. 2023; 3(2): 0201-0212. https://doi.org/10.47813/2782-2818-2023-3-2-0201-0212

[6] Maddox A., Barratt M.J., Allen M., Lenton S. Constructive activism in the dark Web: Cryptomarkets and illicit drugs in the digital demimonde. Inf., Commun. Soc. 2016; 19(1): 111-126.

[7] Аверьянов В.С., Каричев А.А., Карцан И.Н. Об атаках с явным исходом динамических переменных и криптостойкости ключей безопасности квантовых систем. Математические методы в технологиях и технике. 2022; 12(1): 29-34.

[8] Жуков А.О., Карцан И.Н., Аверьянов В.С. Кибербезопасность Арктической зоны. Информационные и телекоммуникационные технологии. 2021; 51: 9-13.

[9] Mishra P., Pilli E.S., Varadharajan V., Tupakula U. Intrusion detection techniques in cloud environment: A survey. J. Netw. Comput. Appl. 2017; 77: 18-47.

[10] Chang D., Ghosh M., Sanadhya S.K., Singh M., White D.R. FbHash: A new similarity hashing scheme for digital forensics. Digit. Invest. 2019; 29: S113-S123.

[11] Ahmed M., Mahmood A.N., Islam M.R. A survey of anomaly detection techniques in financial domain. Future Gener. Comput. Syst. 2016; 55: 278-288.

[12] Жукова Е.С., Карцан И.Н. Обеспечение конфиденциальности информации в центре управления полетами. Вестник Сибирского государственного аэрокосмического университета им. академика М.Ф. Решетнева. 2009; 3(24): 93-97.

[13] Карцан Р.В., Жукова Е.С., Карцан И.Н. Универсальное программное обеспечение по типу «Каркас». Актуальные проблемы авиации и космонавтики. 2012; 1(8): 356-357.

[14] Карцан Р.В., Карцан И.Н. Дактилоскопия биометрический метод идентификации на режимном предприятии. Актуальные проблемы авиации и космонавтики. 2013; 1(9): 405-406.

[15] Гурьянов К.В., Шатило Я.С. Организация противодействия распространению наркотиков через интернет. Антинаркотическая безопасность. 2016; 1(6): 101-108.

REFERENCES

[1] Suhostat V. V. Teoriya informacionnoj bezopasnosti i metodologiya zashchity informacii. SPb: Universitet ITMO; 2018.

[2] Horev A. A. Organizaciya zashchity informacii ot utechki po tekhnicheskim kanalam. M.: MO RF; 2017. 316.

[3] Muhamet'yanova A. R. Osobennosti zashchity informacii na predpriyatii ot utechki po tekhnicheskim kanalam. Ufa: Bashkirskij gos. un-t; 2019. 56.

[4] Nuriev S. A., Karcan I. N. Rol' prostranstvennoj kiberinfrastruktury v geoinformacionnyh sistemah. E3S Web of Conferences. 2023; 389: 04023. doi.org/10.1051/e3sconf/202338904023

[5] Karcan I. N., Kontyleva, E. A. Glubokij internet veshchej. Sovremennye innovacii, sistemy i tekhnologii. 2023; 3(2): 0201-0212. https://doi.org/10.47813/2782-2818-2023-3-2-0201-0212

[6] Maddox A., Barratt M.J., Allen M., Lenton S. Constructive activism in the dark Web: Cryptomarkets and illicit drugs in the digital demimonde. Inf., Commun. Soc. 2016; 19(1): 111-126.

[7] Aver'yanov V.S., Karichev A.A., Karcan I.N. Ob atakah s yavnym iskhodom dinamicheskih peremennyh i kriptostojkosti klyuchej bezopasnosti kvantovyh sistem. Matematicheskie metody v tekhnologiyah i tekhnike. 2022; 12(1): 29-34.

[8] Zhukov A.O., Karcan I.N., Aver'yanov V.S. Kiberbezopasnost' Arkticheskoj zony. Informacionnye i telekommunikacionnye tekhnologii. 2021; 51: 9-13.

[9] Mishra P., Pilli E.S., Varadharajan V., Tupakula U. Intrusion detection techniques in

cloud environment: A survey. J. Netw. Comput. Appl. 2017; 77: 18-47.

[10] Chang D., Ghosh M., Sanadhya S.K., Singh M., White D.R. FbHash: A new similarity hashing scheme for digital forensics. Digit. Invest. 2019; 29: S113-S123.

[11] Ahmed M., Mahmood A.N., Islam M.R. A survey of anomaly detection techniques in financial domain. Future Gener. Comput. Syst. 2016; 55: 278-288.

[12] ZHukova E.S., Karcan I.N. Obespechenie konfidencial'nosti informacii v centre upravleniya poletami. Vestnik Sibirskogo gosudarstvennogo aerokosmicheskogo universiteta im. akademika M.F. Reshetneva. 2009; 3(24): 93-97.

[13] Karcan R.V., Zhukova E.S., Karcan I.N. Universal'noe programmnoe obespechenie po tipu «Karkas». Aktual'nye problemy aviacii i kosmonavtiki. 2012; 1(8): 356-357.

[14] Karcan R.V., Karcan I.N. Daktiloskopiya biometricheskij metod identifikacii na rezhimnom predpriyatii. Aktual'nye problemy aviacii i kosmonavtiki. 2013; 1(9): 405-406.

[15] Gur'yanov K.V., SHatilo YA.S. Organizaciya protivodejstviya rasprostraneniyu narkotikov cherez internet. Antinarkoticheskaya bezopasnost'. 2016; 1(6): 101-108.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Нуриев Сури Айкович, старший инженер, ФГБУН ФИЦ «Морской гидрофизический институт РАН», Севастополь, Россия
e-mail: surinuriev@gmail.com

Карцан Игорь Николаевич, доктор технических наук, доцент, ведущий научный сотрудник Морского гидрофизического института РАН, Севастополь, Россия
e-mail: kartsan2003@mail.ru
ORCID: 0000-0003-1833-4036

Suri Nuriev, Senior Engineer, Marine Hydrophysical Institute of the Russian Academy of Sciences, Sevastopol, Russia
e-mail: surinuriev@gmail.com

Igor Kartsan, Dr. Sc., Docent, Leading Researcher, Marine Hydrophysical Institute, Russian Academy of Sciences, Sevastopol, Russia
e-mail: kartsn2003@mail.ru

Статья поступила в редакцию 30.05.2023; одобрена после рецензирования 13.06.2023; принята к публикации 19.06.2023.

The article was submitted 30.05.2023; approved after reviewing 13.06.2023; accepted for publication 19.06.2023.