УДК 004.056:004.77

ІНФОРМАЦІЙНА БЕЗПЕКА ВІДДАЛЕНОЇ РОБОТИ

Щербак В.О., Колобилін І.О.
Науковий керівник – к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки, каф. КРіСТЗІ,
м. Харків, Україна
e-mail: valeriia.shcherbak@nure.ua

Many companies have started to actively use remote working mode in the last few years. Employees of literally all office ranks are working remotely now, so personal computers are usually used for work, at least as a tool to connect to a remote desktop on a company PC, and most often the personal PC completely replaces the work PC. In this connection, certain questions regarding information security arise.

Для роботодавця та працівника плюси віддаленої роботи очевидні та зрозумілі. Їх немає сенсу перераховувати та обговорювати. Для інформаційної безпеки плюсів практично немає. До ризиків та уразливостей в офісному просторі додаються ризики, пов'язані з фізичною безпекою конфіденційних документів, фізичних ключових носіїв та ін., оскільки тепер доступ до конфіденційної інформації компанії може отримати не випадковий колега, а буквально будь-яка стороння людина.

Нові ризики.

Як правило, компанія намагається тримати контрольований контур закритим і забезпечувати підключення у внутрішню мережу через виділене захищене з'єднання або віртуальний термінальний сервер тощо. Тобто користувач в першу чергу не повинен працювати у своєму особистому середовищі, змішуючи робочі документи та файли зі звичайного життя.

При віддаленому підключенні до свого робочого ПК варто пам'ятати про забезпечення заходів інформаційної безпеки не тільки на робочому ПК, але й на тих пристроях, з яких ви здійснюєте віддалений доступ до корпоративних ресурсів. У цьому можуть допомогти наступні заходи для налаштування віддаленого робочого місця працівників, ПК чи ноутбука:

1. Використання ліцензійного програмного забезпечення.
2. Наявність антивірусного програмного забезпечення з актуальними антивірусними базами.
3. Встановлення всіх актуальних оновлень для операційної системи.
4. Оновлення програмного забезпечення роутера та встановлення складного пароля для доступу до нього.
5. Розділення облікових записів користувачів на одному ПК.
6. Використання міжмережевого екрану (брандмауера або файрвола).
7. Обмеження використання функції збереження паролів у браузерах та інших консолях.
8. Увімкнення автоматичного блокування ПК, якщо користувач неак-

тивний протягом тривалого часу.

В ідеалі, звичайно, варто не розраховувати на те, що дистанційний співробітник буде все це застосовувати самостійно, а підготувати для нього ПК або персональний ноутбук, який налаштують для віддаленого підключення відповідно до політики безпеки. Як мінімум, це необхідно зробити для найкритичніших кадрів.

Запобіжні заходи. Що має бути заборонено:

1. Зберігати інформацію про обмежений доступ на домашньому ПК та інших пристроях, що не належать до корпоративних.

2. Допускати до пристрою третіх осіб під час запущеної сесії віддаленого підключення.

3. Використовувати громадські мережі Wi-Fi та інші незнайомі мережі для підключення віддаленого доступу (рекомендовано).

4. Зберігати знімки екрана з робочою інформацією у відкритому доступі або на власному пристрої.

5. Після завершення роботи залишати запущену сесію віддаленого підключення.

Додаткові рекомендації.

1. Використання двофакторної аутентифікації з організацією безпечного з'єднання працівника зі свого робочого ПК.

2. Для забезпечення комунікації з колегами та партнерами компанії при встановленні Teams та / або Skype for Business на домашній ПК або мобільні пристрої iOS / Android варто пам'ятати про те, що дистрибутиви програм необхідно завантажувати тільки з офіційних сайтів їх виробників. В ідеалі перевірений дистрибутив має надати сам роботодавець – через IT-відділ або відділ ІБ.

3. З метою забезпечення безпечної роботи з домашнього ПК та інших пристроїв, з яких здійснюється віддалений доступ до корпоративних ресурсів, використовувати антивірусне програмне забезпечення великих постачальників цього софту (Eset, McAfee, Symantec). Зрозуміло, такі антивіруси коштують чимало. Але практично кожен постачальник антивірусного софту має безкоштовні версії ПЗ, які можуть забезпечити базовий рівень захисту пристроїв. Для максимального рівня захисту рекомендується використовувати ті продукти, які забезпечують комплексну безпеку пристроїв, але вони є платними. Проте постачальники софту надають тимчасову можливість використання пробних версій цих продуктів. У налаштуваннях антивірусного програмного забезпечення повинна бути включена функція щоденного оновлення антивірусних баз.

4. Для забезпечення безпеки домашньої мережі за допомогою роутера Wi-Fi рекомендується регулярно змінювати паролі для Wi-Fi та консолі адміністратора, а також оновлювати прошивку пристрою.

5. Якщо видається сертифікат для віддаленого підключення, завжди потрібно використовувати його, а не авторизацію формату «логін та па-

роль».

6. Якщо домашнім комп'ютером, з якого співробітник підключається до робітника, користуються й інші члени сім'ї, необхідно створити для них окремі облікові записи (або створити один окремий обліковий запис під роботу).

7. Постійна освітянська робота з персоналом, оскільки саме від дій співробітників залежать ризики реалізації близько 80% загроз інформаційній безпеці.

Список використаних джерел

1. The Cyber Security Risks of Remote Work: Safeguarding Your Home Office. URL: https://www.itgovernance.co.uk/blog/the-cyber-security-risks-of-working-from-home (дата звернення: 20.12.2023).

2. Cyber Security Risks in Remote Work. URL: https://cyberone.security/cyber-security-risks-in-remote-work/ (дата звернення: 20.12.2023).

3. Kamal A. H. A., Yen C. C. Y., Ping M. H., Zahra, F. Cybersecurity issues and challenges duringCOVID-19 pandemic. Preprints, 2020. doi:10.20944 / preprints 202009.0249.v1

4. User’s Guide to Telework and Bring Your Own Device (BYOD) Security. NIST (July 2016). URL: https://nvlpubs.nist.gov/nistpubs/Special Publications/NIST.SP.800-114r1.pdf (дата звернення: 20.12.2023).

5. Future of Secure Remote Work Report. URL: https://www.cisco.com/c/en/us/products/security/future-secure-remote-work-report.html#download_report (дата звернення: 20.12.2023).

6. Hou H. C., Remoy H., Jylha T., Putte, H. V. A study on office workplace modification during the COVID-19 pandemic in The Netherlands. Journal of Corporate Real Estate, 2021. № 23 (3). P. 186-202.

7. Довбня А. А. Дослідження безпеки хмарних сервісів / А. А. Довбня, Д. Ю. Горелов // Радіоелектроніка та молодь в XXI столітті : матеріали 26-го Міжнародного молодіжного форуму, 24-25 листопада 2022 р. – Харків : ХНУРЕ, 2022. – Т. 3. – С. 96–99.