КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (17), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.17.159166

Пазиніна Ірина Сергіївна
Науковий співробітник
Військова частина А1906, Київ, Україна
ORCID: 0000-0002-0854-5393
Litvinchuk.irina94@gmail.com

Корчомний Руслан Олександрович
Науковий співробітник
Військова частина А1906, Київ, Україна
ORCID:0000-0002-2457-6675
Rra30@ukr.net

РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗНИЖЕННЯ КІБЕРЗАГРОЗ НА ЧАС ВІДДАЛЕНОЇ РОБОТИ З ТОЧКИ ЗОРУ КІБЕРБЕЗПЕКИ

Анотація. Вже декілька років поспіль українські організації (спочатку через пандемію Covid-19 і її наслідки, а тепер і військові дії) та і загалом світові, вимушено переводять працівників на більш оптимальний формат роботи – це віддалена робота (робота вдома). За статистикою, така практика виявила свій позитивний бік в плані більшої продуктивності праці (менша трата часу на пересування містом, комфортні домашні умови і таке інше), однак з точки зору кібербезпеки виявилось збільшення випадків кібернетичних загроз (далі - кіберзагрози) та активації кіберзлочинців.
Віддалений режим роботи означає повний або частковий перехід на використання працівниками особистих пристроїв.Для налаштування віддаленої роботи працівників потрібна чітка підготовленість інформаційних систем в середині організації, тому служби інформаційної безпеки (далі - ІБ) та інформаційних технологій (далі – ІТ) повинні забезпечити безпеку і неперервність бізнес-процесів організації. Оскільки віддалена робота пов'язана з великим ризиком виникнення кіберзагроз і втручання кіберзлочинців.
Кібернетичні загрози (кіберзагрози) – наявні й/або потенційно можливі явища та чинники, що створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства й держави, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [1].
Формування й ефективна реалізація кібербезпеки, в рамках якої розробляється комплекс рекомендацій та заходів щодо прогнозування і протидії кіберзагрозам, є необхідною умовою безпечного та безперервного функціонування організації.

Ключові слова: кіберзагроза; кібербезпека; віддалена робота; служби ІТ та ІБ; кіберзлочинці.

ВСТУП

Постановка проблеми. У всьому світі багато організацій переходять на віддалену роботу. Сучасні технології зробили величезний крок вперед і дозволяють безперешкодно перевести цілу компанію на віддалену роботу (онлайн-наради, робота в хмарному сховищі, надсилання документів, відео-конференції та багато іншого).

Та чим більше організацій переходять в режим віддаленої роботи, тим більше кіберзлочинців і кіберзагроз націлено на незахищеність віддаленого робочого місця працівника, що несе за собою великі втрати для організації. Однак основні критерії залишились незмінними: цілісність, доступність, конфіденційність інформації. Оскільки керівник організації першочергово зацікавлений у чіткій роботі працівника і дотримання вказаних критеріїв безпеки інформації, він повинен спільно з службами ІТ та ІБ надати працівнику можливість працювати безпечно на будь-якому пристрої у будь-якому місці.

Використання лише антивірусного програмного забезпечення чи наприклад використання політики паролів не є повною гарантією захисту від кібератак. Антивірус не є панацеєю від усіх видів вірусів, а зачасту завантажене неліцензоване антивірусне програмне забезпечення, тим паче, не гарантує коректної роботи. У кіберзлочинців є безліч методів та способів, як легко зламати паролі, викрасти, вгадати чи підібрати потрібну комбінацію, варто працівникові знехтувати одним з правил парольної політики. Лише використовуючи розроблений комплекс рекомендацій, які можна вписати в стратегію кібербезпеки щодо зниження кіберзагроз при віддаленій роботі, можна уникнути значних втрат для організації.

Аналіз останніх досліджень і публікацій. У своєму дослідженні компанія Microsoft IT Cloud Security Survey провела аналітичну компанію IDC у країнах Центральної та Східної Європи (Польща, Чехія, Греція, Угорщина, Румунія та інші країни східноєвропейського регіону) та дійшла висновку, що бізнес наразі не готовий повною мірою відповісти на нові виклики у сфері інформаційної безпеки: більш ніж половина компаній (58%) не мають комплексної стратегії кібербезпеки. Такі дані опубліковані в статті видання Укрінформу.

Так, 79% респондентів назвали безпечний віддалений доступ до корпоративних мереж своєю ключовою необхідністю, якій слід приділяти найбільше уваги.

Згідно з даними дослідження, лише 42% компаній в Центральній та Східній Європі розробили комплексну стратегію безпеки, при цьому більшість респондентів (86%) заявили, що задоволені рівнем кібербезпеки своєї організації. Це може свідчити про те, що деякі компанії мають оманливе відчуття безпеки.

За словами Андрія Савчука, керівника відділу корпоративної безпеки, відповідності вимогам та ідентифікації Microsoft в Центральній та Східній Європі, "бізнес повинен використовувати модель Zero Trust (нульової довіри), за якої кожен користувач, який запитує будь-який доступ, повинен пройти строгу аутентифікацію, авторизацію з урахуванням обмежень політик, та перевірку на аномалії — лише після цього може бути наданий відповідний доступ. Для запобігання вторгненням перевіряється все — від посвідчень користувачів до середовища розміщення додатків".

Для зниження ризиків, пов'язаних із забезпеченням безпеки віддалених співробітників, керівники компаній повинні підтримувати своїх працівників: як шляхом підвищення рівня кібергігієни, так і надаючи інструменти, котрі знижують ризики, при цьому дозволяючи їм лишатися продуктивними [2].

Підсумовуючи дане дослідження варто звернути увагу на заклик до необхідності створення будь-то стратегії кібербезпеки, будь-то порядку необхідних дій та заходів безпеки.

Також своїм поглядом на виклики, що постають перед компаніями усього світу в нових умовах поділась визнана у світі лідерка з кіберзахисту - Емілі Моссбург. Основні три напрями, на яких вона акцентує увагу - це адаптація до віддаленої роботи, підвищення кіберобізнаності серед працівників, прийняття «кіберреальності».

1. Адаптація до віддаленої роботи

Ключовим елементом кібербезпеки є кінцеві точки. Це пристрої користувачів, приєднані до мережі компанії, кожен з яких може бути використаним для розкриття даних організації. Якщо проаналізувати типові офісні конфігурації, виявиться, що кінцеві точки досить легко відстежити – це комп’ютери, мобільні пристрої, сервери, смарт-пристрої тощо. З усіма цими пристроями під одним дахом та за допомогою ІТ відділів в офісі організації можуть забезпечити належні практики щодо кіберзахисту, залишаючись поза ризиками.

ISSN 2663 - 4023

Але зі збільшенням кількості віддалених робітників збільшується кількість кінцевих точок, і тим складнішим повинен бути підхід до безпеки. Багато компаній навіть не підозрюють, які пристрої підключені до їхніх систем. Великий ризик для компанії становить і те, що деякі працівники не розуміють природу кіберзагроз й не усвідомлюють, що певні їхні дії можуть створити одну з них.

У міру того, як компанії пристосовуються до цього безпрецедентного виклику, їхні керівники повинні відповісти на три основні питання:

- чи може компанія виявляти та реагувати на кіберзагрози, а також відновлюватися після кіберінцидентів, і як кожна з цих здатностей змінюється щодо загроз, пов'язаних з віддаленою роботою;
- які активи є критичними для компанії;
- чи є в компанії культура кіберзахисту і чи навчені співробітники розпізнавати кіберінциденти й запобігати їм незалежно від їхнього робочого місця.

2. Підвищення рівня кіберобізнаності серед працівників

Багато організацій мають політики безпеки та можливості керувати популярними загрозами, тому більшість піде простим шляхом підтримки вже наявних систем. Однак цього може бути недостатньо.

Один клік працівника може становити загрозу для даних усієї компанії, тому організаціям вкрай необхідно переоцінити всі існуючі кінцеві точки на предмет вразливостей. Також належним чином повинні бути захищені всі нещодавно прийняті хмарні рішення та інструменти для відеоконференцій. Без ефективного контролю безпеки кіберзлочинці можуть приєднуватися до ділових зустрічей та/чи мати доступ до конфіденційної інформації, що зберігається у хмарних сервісах.

Ключовим фактором успішної віддаленої роботи є розуміння працівників їхньої ролі у забезпеченні кібербезпеки. Особиста відповідальність та обізнаність – важливі складники програми кіберризиків. Щоб мати можливість швидше і стійкіше реагувати на кібератаки, необхідно:

- розробити й застосовувати план реагування на кіберінциденти для навчання і тренування працівників;
- підвищити обізнаність працівників про кіберзагрози від фішинг-кампаній в електронних листах, де можуть вимагати гроші;
- вимкнути непідтверджені персональні пристрої з корпоративних мереж і переконатися, що програмне забезпечення корпоративного захисту встановлено на затверджених пристроях до їх підключення у мережу.

3. Прийняття «кіберреальності»

Оскільки мільйони співробітників працюють з дому, керівники підприємств хочуть зосередитися виключно на підтримці операційної спроможності та функціональності за будь-яку ціну. Однак, якщо кібербезпека не буде вбудована у їхні плани, організації можуть бути серйозно скомпрометовані в короткостроковій перспективі й мають ризик не встояти у світі, де всі готові до нових викликів чи можливостей. Зараз організаціям як ніколи важливо зрозуміти, що кібертехнології скрізь, тому треба розглядати їх як ланцюг, що об'єднує їх організацію, клієнтів, постачальників та громади, дозволяючи інтегрувати кібераспекти у стратегічні рішення, які організації приймають щодня.

Організації, для яких кібербезпека є одним із пріоритетів, будують для себе хороший фундамент на місяці й навіть роки вперед [3].

Отже, у своєму коментарі Емілі Моссбург, дала чітке уявлення картини реальності стосовно забезпечення кібербезпеки у будь-якій організації, що наразі зіткнулися з новими випробуванням – віддаленою роботою працівників. Вона надала

досить загальні але чіткі рекомендації, які варто звернути увагу при організації для працівника віддаленого доступу.

Мета статті. Виходячи з наведеного вище, метою статті є розробити рекомендації щодо зниження кіберзагроз на час віддаленої роботи з точки зору кібербезпеки, опираючись на практику світових організацій з кіберзахисту та світових лідерів у цій галузі, аналізуючи основні фактори виникнення кіберзагроз.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Наскільки поняття "робочого місця" стало досить розмитим, настільки ж поняття небезпеки стало досить чітке: від невизначених сценаріїв підключення, безкінечного потоку трафіку, фішингу, стороннього програмного забезпечення (з усіма наслідками від їх неконтрольованого використання), соціальна інженерія, незахищені мережі – все це, як часто буває, залишається поза зоною системи контролю і моніторингу доступу та інших безпекових систем.

Компанія Check Point Software Technologies оприлюднила результати нового дослідження, в якому показала основні пріоритети та проблеми кібербезпеки організацій до 2023 року, а також основні зміни в їх стратегіях кібербезпеки, що виникли через пандемію. Опитування було проведено компанією Dimensional Research для Check Point і охопило 613 IT та ІБ-фахівців по всьому світу.

Ключові висновки опитування:

Основні проблеми безпеки у 2021 році:

- Забезпечення безпеки працівників, які працюють віддалено - це відзначили 47% респондентів;
- Захист від фішингу та атак з використанням соціальної інженерії - 42%;
- Надання безпечного віддаленого доступу - 41%;
- Захист хмарних додатків та інфраструктури - 39%.

Ключові завдання безпеки на наступні два роки:

- Забезпечення віддаленої роботи - 61% респондентів;
- Безпека кінцевих точок і мобільних пристроїв - 59%;
- Захист публічних і гібридних хмар — 52%.

Нова реальність: 50% всіх респондентів вважають, що їх підхід до безпеки не повернеться до колишніх норм; 29% заявили, що в якийсь момент в майбутньому очікують повернення до тих норм, які були до Covid-19.

Зміни в стратегіях безпеки у 2020 році:

- 95% респондентів заявили, що їх стратегії змінилися в другій половині року. При цьому найбільшою зміною стала можливість масової віддаленої роботи - про це розповіли 67% опитаних;
- 39% відзначили, що тепер для співробітників проводиться навчання базовим правилам кібербезпеки;
- 37% розповіли, що поліпшили мережеву безпеку і запобігання загрозам;
- 37% заявили, що розширили безпеку кінцевих точок і мобільних пристроїв;
- 31% відзначили швидке впровадження хмарних технологій;
- 27% заявили, що вони прискорили поточні IT-проєкти протягом року - для більшості заходи, вжиті через пандемію, включали незаплановане переосмислення бізнес-моделі [4].

Наведена вище, статистика опитування показує на скільки є підготовлені організації до «безпечного» переведення на віддалену роботу працівників, з якими труднощами

забезпечення безпеки довелося зіштовхнутися та дала можливість виявити найбільш вразливі точки для реалізації кіберзагроз.

Розгляньмо деякі з основних факторів виникнення кіберзагроз, для подальшої розробки рекомендацій щодо їх мінімалізації або ж повного усунення:

- **Мережеві ризики.** Для віддаленого доступу до ресурсів компанії працівники зазвичай використовують різні комбінації захищених та незахищених, проводових чи безпроводових і, власне, приватних або публічних мереж. Це забезпечує численні можливості входу для хакерів та кіберзлочинців – компанії просто не можуть захистити кожну мережу, яку використовують працівники.
- **Використання персональних пристроїв у робочих цілях.** У цій ситуації існує високий ризик того, що особисте використання програмних продуктів та інших ресурсів може відкрити злочинцям доступ до ресурсів компанії. Зазвичай компанії не мають контролю над застосунками та програмами, що встановлені на персональних пристроях разом із корпоративними застосунками.
- **Соціальна інженерія.** Хакери добре знають, як використати психологічні особливості людини, та можуть тонко маніпулювати працівниками, які працюють поза колективним офісним середовищем. При віддаленій роботі також виникає загроза того, що працівник не в змозі буде скористатися такими простими практиками захисту від соціальної інженерії, як перевірка підозрілого повідомлення разом з колегою поруч [5].
- **Парольна політика.** Частіше за усе, працівники нехтують правилами парольної політики, що в свою чергу надає великі можливості кіберзлочинцям для проникнення до усіх даних організації. За аналізом даних близько 80% від усіх кібератак пов’язані саме зі слабкими паролями.

Отже, поєднуючи чітку статистику та аналіз основних факторів виникнення кіберзагроз, можна запропонувати для зниження ризику виникнення кіберзагроз наступне:

1. Забезпечення працівників пристроями, які є власністю організації. За можливості компанія може надати працівникові власні пристрої (ноутбуки та телефони) для робочих цілей, що контролюються компанією. Це доречно в будь-якому випадку, але для роботи з конфіденційною інформацією чи персональними даними є у пріоритеті.

Альтернативне рішення: якщо працівник використовує власний пристрій, можна попросити зареєструвати пристрій в корпоративній системі контролю - Mobile Device Management system.

2. Впровадження заходів безпеки кінцевих точок - програмне забезпечення для захисту кінцевих точок (включають засоби для захисту від фішингу), включно з антивірусом. Необхідно ввести інвентаризаційний контроль та оновлення програмного забезпечення.

Альтернативне рішення: шифрування пристроїв як введення додаткового захисту (ефективне при загрозі втрати, викрадення).

3. Ініціалізація VPN-з’єднання може усунути значну кількість ризиків, уможливлюючи безпечне передання інформації шифрованим каналом зв’язку. Використання VPN є недорогим і може бути досить легко впроваджене в компанії. Більш практичним способом може бути підключення персональних пристроїв безпосередньо до широкосмугового модему або маршрутизатора, замість використання Wi-Fi [5].

Альтернативне рішення: Створення віртуального робочого столу (VDI), яке дозволяє розділенню робочого простору з пристроєм із якого здійснюється підключення до мережі.

4. Постійне навчання співробітників щодо можливих ризиків та загроз і способів їх уникнення.
5. Виконання парольної політики та багатофакторної автентифікації. Стійкий пароль та вимога його зміни декілька разів на квартал. Багатофакторна автентифікації стане додатковою ланкою в захисті і унеможливить доступ кіберзлочинця до інформації, навіть якщо викраде пароль.
6. Звернути увагу на готові рішення з забезпечення безпеки для віддаленої роботи. Великі корпорації ІТ програм пропонують безліч нових можливостей.
7. Встановлення ліцензованого, перевіреного та комплексного антивірусного програмного забезпечення забезпечує захист від відомих вірусі і попереджує від майбутніх вірусів автоматично оновлюючись.
8. Усвідомлення відповідальності за захист інформації організації. Повинно бути встановлене письмове документальне свідчення відповідальності працівника перед організацією.
9. Підбір кваліфікованих кадрів ІБ та ІБ служб.

Альтернативне рішення: за неможливості створення ІБ та ІТ служб є можливість звернення до Центру моніторингу інформаційної безпеки, які можуть здійснювати контроль у режимі реального часу.

10. Для віддаленої роботи організації частіше переводять свої активи у хмарні рішення, тому для попередження загроз стало актуальним використання система виявлення та знешкодження загроз або XDR. Така система дозволяє моніторити дані на рівні хмар, а також додатків і кінцевих пристроїв, здійснюючи пошук і аналітику для запобігання потенційним загрозам.
11. Впровадження повної або часткової моделі Zero Trust (нульової довіри) з особистими пристроями.

Віддалений доступ працівників компанії до інформації компанії (та загалом її інфраструктури) - це важливе питання якісного налаштування кібербезпеки і впровадження частини або всіх рекомендацій, здатних контролювати працівників, а й нівелювати кіберзагрози.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Віддалена робота – це розкіш для працівників але нелегка робота для роботодавця, адже він повинен подбати про безпеку «робочого місця» працівника задля безпеки активів компанії. Робити усе можливе для попередження витоку інформації та зменшення потенційним кіберзагрозам через віддалені робочі місця – найактуальніша проблема сучасності.

Більшість компаній зазначили, що такий вид роботи надійно закріпився у нашому житті, тож варто розглядати найбільш високий рівень безпеки в довгостроковій перспективі.

У статті запропоновано перелік рекомендацій щодо зниження кіберзагроз, що виникають під час віддаленої роботи на основі аналізу факторів виникнення кіберзагроз.

Працездатність рекомендацій можна перевірити на власній організації і переконатись у їх дієвості. Список рекомендацій не є вичерпними, оскільки факторів кіберзагроз з кожним днем все більшає, а кіберзлочинці вигадують нові способи викрадення інформації, а отже, перелік може доповнюватись і змінюватись. Рекомендації можна використовувати і в навчальних цілях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Куцаєв, В.В., Живило, Є.О., Срібний, С.П., Черниш, Ю.О. *Розширення термінології сучасного кіберпростору.* НЦЗІ ВІТІ ДУТ.

2 Ukrinform. (2021, 1 липня). *Більше половини компаній потребує комплексної стратегії з кібербезпеки – Microsoft.* Укрінформ - актуальні новини України та світу. https://www.ukrinform.ua/rubric-economy/3273717-bilse-polovini-kompanij-potrebue-kompleksnoi-strategii-z-kiberbezpeki-microsoft.html

3 *Нові аспекти кібербезпеки в умовах віддаленої роботи | Статьи | Компьютерное Обозрение*. Компьютерное Обозрение. https://ko.com.ua/novi_aspekti_kiberbezpeki_v_umovah_viddalenoyi_roboti_133984.

4 *Кібератаки на бізнес у 2020 році зросли на 58%.* Softline | Українська софтверная компанія. https://softline.ua/ua/news/kiberataky-na-biznes-u-2020-rotsi-zrosly-na-58protsent.html

5 Курій, Є. Дистанційна кібербезпека: як захистити інформацію під час віддаленого режиму роботи. https://mind.ua/openmind/20210952-distancijna-kiberbezpeka-yak-zahistiti-informaciyu-pid-chas-viddalenogo-rezhimu-roboti

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (17), 2022
ISSN 2663 - 4023

Iryna S. Pazynina
Researcher
Military base A1906, Kyiv, Ukraine
ORCID ID 0000-0002-0854-5393
litvinchuk.irina94@gmail.com

Ruslan O. Korchomnyi
Researcher
Military base A1906, Kyiv, Ukraine
ORCID ID 0000-0002-2457-6675
rra30@ukr.net

DEVELOPMENT OF RECOMMENDATIONS FOR REDUCING CYBER THREATS DURING REMOTE WORK FROM THE POINT OF VIEW OF CYBER SECURITY

Abstract. For several years in a row, Ukrainian organizations (first due to the Covid-19 pandemic and its consequences, and now military operations) and in general the world, have been forcibly transferring employees to a more optimal work format - this is remote work (work at home). According to statistics, this practice has shown its positive side in terms of higher labor productivity (less time spent on moving around the city, comfortable home conditions, etc.), however, from the point of view of cyber security, there has been an increase in cases of cyber threats (hereinafter - cyber threats) and the activation of cyber criminals.

Remote work mode means full or partial transition to the use of personal devices by employees.

Setting up remote work of employees requires a clear preparation of information systems within the organization, therefore information security (hereinafter - IS) and information technology (hereinafter - IT) services must ensure the security and continuity of the organization's business processes. Because remote work is associated with a high risk of cyber threats and the intervention of cybercriminals.

Cybernetic threats (cyberthreats) are existing and/or potentially possible phenomena and factors that pose a danger to the vital interests of a person and citizen, society and the state, the implementation of which depends on the proper functioning of information, telecommunication, and information-telecommunication systems [1].

The formation and effective implementation of cyber security, within the framework of which a set of recommendations and measures for predicting and countering cyber threats is developed, is a necessary condition for the safe and continuous functioning of the organization.

Keywords: cyber threat; cyber security; remote work; IT and IS services; cybercriminals

REFERENCES

1 Kutsaiev, V.V., Zhyvylo, Ye.O., Sribnyi, S.P., Chernysh, Yu.O. Rozshyrennia terminolohii suchasnoho kiberprostoru. NTsZI VITI DUT.
2 Ukrinform. (2021, 1 lypnia). Bilshe polovyny kompanii potrebuie kompleksnoi stratehii z kiberbezpeky – Microsoft. Ukrinform - aktualni novyny Ukrainy ta svitu. https://www.ukrinform.ua/rubric-economy/3273717-bilse-polovini-kompanij-potrebue-kompleksnoi-strategii-z-kiberbezpeki-microsoft.html
3 Novi aspekty kiberbezpeky v umovakh viddalenoi roboty | Staty | Kompiuternoe Obozrenye. Kompiuternoe Obozrenye. https://ko.com.ua/novi_aspekti_kiberbezpeki_v_umovah_viddalenoyi_roboti_133984.
4 Kiberataky na biznes u 2020 rotsi zrosly na 58%. Softline | Ukrainska softvernaia kompaniia. https://softline.ua/ua/news/kiberataky-na-biznes-u-2020-rotsi-zrosly-na-58protsent.html
5 Kurii, Ye. Dystantsiina kiberbezpeka: yak zakhystyty informatsiiu pid chas viddalenoho rezhymu roboty. https://mind.ua/openmind/20210952-distancijna-kiberbezpeka-yak-zahistiti-informaciyu-pid-chas-viddalenogo-rezhimu-roboti