ГОЛОВА ДОВГИНЦІВСЬКОЇ РАЙОННОЇ В МІСТІ РАДИ

Р О З П О Р Я Д Ж Е Н Н Я

31.07.2023 м. Кривий Ріг № 132-р

Про заходи щодо забезпечення кібербезпеки та кіберзахисту у виконкомі районної в місті ради

З метою недопущення несанкціонованого витоку важливої інформації, включаючи інформацію з обмеженим доступом, використання кіберпростору для порушення управлінської діяльності; задля посилення інформаційної безпеки в умовах збройної агресії Російської Федерації; ураховуючи доручення Прем'єр-міністра України від 07.02.2023 №2692/1/1-23 до листа Головнокомандувача Збройних сил України від 27.01.2023 №300/1/С/672; керуючись законами України «Про основні засади забезпечення кібербезпеки України», «Про правовий режим воєнного стану», «Про місцеве самоврядування в Україні», рішенням Криворізької міської ради від 31.03.2016 №381 «Про обсяг і межі повноважень районних у місті ради та їх виконавчих органів» зі змінами:

1. Керівникам структурних підрозділів виконкому районної в місті ради взяти до відома Інструкцію з використання застосунків для обміну повідомленнями, проведення аудіо- та відеоконференцій у виконавчому комітеті Довгинцівської районної в місті ради (додаток) далі - Інструкція.

2. Керівникам структурних підрозділів виконкому районної в місті ради:

2.1 довести до співробітників під особистий підпис Інструкцію з використання застосунків для обміну повідомленнями, проведення аудіо- та відеоконференцій у виконкомі районної в місті ради;

2.2 відповідно до чинного законодавства України забезпечити:

2.2.1 контроль за безумовним дотриманням вимог Інструкції;

2.2.2 обов'язкове виконання рекомендацій, розміщених на вебресурсі урядової команди реагування на комп'ютерні надзвичайні події України (https://cert.gov.ua), а саме:

2.2.2.1 загальних рекомендацій щодо зменшення наслідків від впливу шкідливого програмного забезпечення (https://cert.gov.ua/recommendation/2502);

2.2.2.2 рекомендацій щодо організації віддаленої роботи (https://cert.gov.ua/recommendation/11388);

2.2.2.3 рекомендацій CERT-UA з безпеки вебресурсів (https://cert.gov.ua/recommendation/19);

2.2.2.4 основних правил кібергігієни (https://cert.gov.ua/recommendation/31).

3. Контроль за виконанням розпорядження покласти на заступників голови районної в місті ради, керуючого справами виконкому районної в місті ради відповідно до розподілу обов’язків.

Голова районної в місті ради ***Ігор РАТІНОВ***

Додаток
до розпорядження голови
районної в місті ради
від 31.07.2023 № 132-р

ІНСТРУКЦІЯ
з використання застосунків для обміну повідомленнями, проведення аудіо- та відеоконференцій у виконкомі районної в місті ради

1. Галузь застосування

Ця інструкція поширюється на співробітників виконкому районної в місті ради при використанні застосунків для обміну повідомленнями, проведення аудіо- та відеоконференцій під час виконання робочих обов'язків.

Інструкція є обов'язковою для вивчення та виконання всіма співробітниками виконкому районної в місті ради.

2. Вимоги використання застосунків для обміну повідомленнями, проведення аудіо- та відеоконференцій

При використанні застосунків для обміну повідомленнями необхідно дотримуватись наступних правил:

забороняється передавати інформацію з обмеженим доступом;
використовувати двофакторну аутентифікацію;
використовувати скрізне шифрування.

При використанні застосунків для проведення аудіо- та відеоконференцій необхідно дотримуватись наступних правил:

підготувати середовище для роботи та переконатися, що в полі зору вебкамери не має жодних конфіденційних даних;
увімкнути функцію шифрування аудіо- та відеозв'язку;
не поширювати посилання на конференції у відкритому доступі та встановити пароль для входу, який необхідно змінювати кожної нової сесії;
контролювати підключення учасників;
під час спільного використання екрану поширювати лише необхідні дані;
налаштувати безпечну передачу файлів, для чутливих даних додатково налаштувати шифрування та парольний захист;
забороняється передавати інформацію з обмеженим доступом.

3. Налаштування безпеки використання застосунків для обміну повідомленнями, проведення аудіо- та відеоконференцій

Скрізне шифрування:

лише відправник і одержувач мають доступ до вмісту повідомлення;

індивідуальні та групові повідомлення видаляються з серверів одразу після доставки;
захищає персональні розмови від розповсюдження.

Навіщо необхідне скрізне шифрування?

При спілкуванні в Інтернеті ваші дані подорожують мережею, що дає можливість підслуховувати ваші чати та повідомлення електронної пошти всім бажаючим — чи це державні органи, зловмисники або просто цікаві люди. Наскрізне шифрування дозволяє покласти цьому кінець. Коли ви використовуєте засоби зв'язку із наскрізним шифруванням, ніхто, крім адресата, не може бачити та читати ваші повідомлення.

Двофакторна аутентифікація:

лише ви можете вносити зміни у свій обліковий запис, встановивши PIN-код;

ваш PIN-код дає змогу активації акаунту на іншому пристрою, тому ніхто не зможе вкрасти ваш обліковий запис, якщо не знає вашого PIN-коду;

якщо ваш PIN-код введено неправильно, певні частини вашого облікового запису буде заблоковано.

Навіщо необхідна двофакторна аутентифікація?

Цей метод використовується для захисту персональних даних, «ускладнення» роботи зловмисникам. У сучасному світі зламати простий і короткий пароль, яким користується більшість людей через зручність запам'ятовування, не важко. Тому якщо хакер пройде перший шар захисту, йому доведеться отримати доступ до телефонного номера або електронної пошти, що набагато складніше. Також двофакторна ідентифікація попереджає про спроби злому облікового запису. У цьому випадку вам на телефон або пошту може прийти одноразовий код, який ви не запитували, і потрібно якнайшвидше змінювати пароль.

Налаштування безпеки у мессенджері Viber

Як включити двофакторну аутентифікацію у Viber:
натисніть (Android) (iOS);
натисніть Налагодження;
натисніть Конфіденційність;
натисніть Двофакторна аутентифікація;
введіть 6-значний PIN-код;
натисніть Далі;
введіть PIN ще раз;
натисніть Далі;
адреса електронної пошти, яку ви раніше використовували для налаштування облікового запису Viber, з'явиться на сторінці підтвердження електронної пошти;

натисніть «Далі», щоб продовжити та завершити налаштування двофакторної аутентифікації;
або введіть адресу електронної пошти, якщо у вас не налаштовано електронну адресу або ви хочете використовувати іншу адресу;
ви отримаєте підтвердження налаштування двофакторної аутентифікації.

Як включити скрізне шифрування у Viber.
Чат 1-на-1:
натисніть Чати;
виберіть чат 1-на-1;
натисніть «Інформація» (Android) або назви чату (iOS) у верхній частині екрана;
натисніть Інформація чату;
знайдіть замок шифрування під зображенням контакту Груповий чат;
натисніть Чати;
виберіть групу;
натисніть «Інформація» (Android) або назви групи (iOS) у верхній частині екрана;
android: натисніть «Інформація про чат»;
знайдіть замок шифрування під зображенням групи.

Як перевірити яку інформацію про вас бачать інші користувачі:
натисніть (Android) (iOS);
натисніть Налагодження;
натисніть Конфіденційність;
оберіть інформацію, яку інформацію ви бажаєте сховати.

Налаштування безпеки у мессенджері WhatsApp

Як включити двофакторну аутентифікацію у WhatsApp:
виберіть свій Акаунт;
виберіть «Меню двофакторної аутентифікації»;
далі натисніть «Увімкнути» та створіть шестизначний пароль. Вам потрібно буде вводити його періодично та кожного разу, коли ви реєструєте WhatsApp на новому пристрої;
введіть адресу електронної пошти, якщо ви забудете або втратите код.

Як включити сповіщення безпеки у WhatsApp:
у налаштуваннях натисніть Акаунт;
виберіть Безпека;
натисніть перемикача «Показати сповіщення системи безпеки» та поставте важіль зеленого кольору.

Налаштування безпеки у мессенджері Telegram

Як включити двофакторну аутентифікацію у Telegram:

натисніть кнопку меню у верхньому лівому куті екрана;
натисніть Налаштування;
натисніть Конфіденційність і безпека;
натисніть Двофакторна аутентифікація;
введіть пароль

Як включити скрізне шифрування у Telegram:

відкрийте Telegram;
натисніть значок олівця (новий чат) у нижньому правому куті екрана;
натисніть « Новий секретний чат»;
виберіть контакт, щоб почати секретний чат.

Як перевірити яку інформацію про вас бачать інші користувачі:

натисніть кнопку меню у верхньому лівому куті екрана;
натисніть Налаштування;
натисніть Конфіденційність і безпека;
у розділі «Приватність» можна переглянути та змінити доступ до ваших даних.

Налаштування безпеки у мессенджері Facebook Messenger

Як включити скрізне шифрування у Facebook Messenger:

перейдіть до профілю користувача. Це можна зробити, вибравши чат, який ви маєте з ними, і натиснувши зображення профілю;
у розділі «Інші дії» виберіть «Перейти до секретної розмови», а потім почніть переписку.

Як включити двофакторну аутентифікацію у Facebook Messenger:

відкрийте настройки безпеки та авторизації у Facebook;
перейдіть до розділу Використати двофакторну автентифікацію та натисніть Редагувати;
виберіть потрібний спосіб перевірки та дотримуйтесь інструкцій на екрані.

При налаштуванні двофакторної автентифікації ви зможете вибрати один із способів перевірки:

ключ безпеки на сумісному пристрої;
коди для входу, що генеруються стороннім додатком для автентифікації;
коди у SMS, що надходять на мобільний телефон.

Основні аспекти безпечної роботи з системами проведення аудіо- та відеоконференцій:

Підготуйте середовище для роботи

Витоки даних часто трапляються ненавмисно. Наприклад, на дошці для записів позаду Вас могла залишитися певна конфіденційна інформація з попередньої онлайн-зустрічі. Тому перед початком розмови переконайтесь, що в полі зору веб-камери немає жодних конфіденційних даних.

Встановіть контроль доступу

Більшість платформ для проведення зустрічей в форматі відео дозволяють створювати групи користувачів або обмежувати доступ через Інтернет-домен, таким чином приєднатися до дзвінка зможе лише обмежене коло осіб.

Для додаткової безпеки відеоконференцій встановіть пароль. Як правило, під час створення конференції він генерується автоматично, і усі, кого було запрошено до розмови, повинні будуть його ввести. Однак, не варто вставляти пароль у посилання на зустріч. Ініціатор конференції також може повністю контролювати, хто підключається до розмови, залишаючи користувачів у режимі очікування.

Налаштуйте безпечну передачу файлів

У багатьох додатках відеозв’язок шифрується за замовчуванням. Деякі сервіси шифрують за замовчуванням лише чат, в такому разі шифрування відеозв’язку потрібно встановити самостійно. Іноді додатки також дозволяють встановлювати обмеження щодо типів файлів, які учасники можуть надсилати. Наприклад, можна заборонити надсилання виконуваних файлів формату .exe.

Керуйте залученістю учасників

Більшість платформ також дозволяють контролювати, хто і коли саме приєднався до дзвінка. Це можна відстежити за тим, хто з зареєстрованих учасників підключився, або за списком учасників, який можна завантажити після завершення дзвінка. У списку учасників також часто доступна інформація щодо часу підключення та відключення користувачів — таким чином можна перевірити, чи був користувач присутнім протягом усієї тривалості дзвінка.

Встановіть обмеження доступу до екрану

Обмежте можливість спільного доступу до екрана для хосту або людини, яка обирає хост. Так Ви уникнете ризику витоку даних. Під час спільного використання екрана поширюйте лише необхідні програми, а не весь робочий стіл. Оскільки, навіть піктограма або ім’я файлу на робочому столі може містити конфіденційну інформацію.

Керуючий справами виконкому ***Олександр ГИЖКО***