Додаток №1
до наказу № 49 від 08.06.2023року

Інструкції
з використання онлайн сервісів

1. Ця інструкція встановлює загальні вимоги, щодо роботи з онлан сервісами, зокрема із застосунками «Viber», «Telegram», «WhatsApp», «Facebook Messanger», «Google Messanger», «Apple iMessanger», «Microsoft Teams», «Microsoft Skype», «Signal», «Threma», «Wire», «Session», «Cisco Webex» та «Zoom» для обміну текстовими повідомленнями, проведення аудіо- та відеоконференцій в операційних системах Unix (IOS, Android) та Windows для здійснення освітнього процесу у Вищому професійному училищі №11 м. Червонограда.

2. Обробка державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом повинна здійснюватися відповідно до вимог Закону України «Про захист інформації в інформаційно-комунікаційних системах».

Відповідно до ст. 2 зазначеного закону об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Відповідно до вимог ст. 8 Закону України «Про захист інформації в інформаційно-комунікаційних системах» (далі - Закон) державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в ІКС із застосуванням комплексної системи захисту інформації (далі - КСЗІ) з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи, яка проводиться з урахуванням галузевих вимог та норм інформаційної безпеки у порядку встановленому законодавством.

Для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації або сертифікат відповідності, виданий органом з оцінки відповідності.

При цьому державні інформаційні ресурси та інформація з обмеженим доступом, крім державної таємниці, службової інформації та державних і єдиних реєстрів, створення та забезпечення функціонування яких визначено законами, можуть оброблятися без застосування КСЗІ у разі підтвердження відповідності системи управління інформаційною безпекою за результатами процедури з оцінки відповідності національним стандартам України, а також у разі виконання інших вимог, визначених у частинах третій та четвертій статті 8 Закону.

Перевірка реалізованих механізмів захисту інформації у засобах проводиться в рамках державної експертизи у сфері технічного та/або криптографічного захисту інформації.

Порядок проведення державної експертизи в сфері технічного захисту інформації визначається «Положенням про державну експертизу в сфері технічного захисту інформації», затвердженим наказом Адміністрації Держспецзв'язку від 16.05.2007 № 93, зареєстрованим у Міністерстві юстиції України 16.07.2007 за № 820/14087 (зі змінами).

Порядок проведення державної експертизи в сфері криптографічного захисту інформації визначається «Положенням про державну експертизу в сфері криптографічного захисту інформації», затвердженим наказом Адміністрації Держспецзв'язку від 23.06.2008 № 100, зареєстрованим у Міністерстві юстиції України 16.07.2008 за № 651/15342 (зі змінами).

На даний час державна експертиза у сфері криптографічного та/або технічного захисту інформації в застосунках «Viber», «Telegram», «WhatsApp», «Facebook Messanger», «Google Messanger», «Apple iMessanger», «Microsoft Teams», «Microsoft Skype», «Signal», «Threma», «Wire», «Session», «Cisco Webex» та «Zoom» не проводилась, експертні висновки щодо реалізованих механізмів захисту не видавалися/не реєструвалися.

3. При застосуванні в освітньому процесі у Вищому професійному училищі №11

4.3 Захист у месенджері 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.

4.4 Захист у месенджері 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 Viber:

- 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.

4.5 Захистити себе 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.

5. При застосуванні в освітньому процесі у Вищому професійному училищі №11 м. Червонограда вищезазначених застосунків дотримуватися основних правил кібергігієни, опублікованих на сайті CERT-UA (https://cert.gov.ua/recommendation/31), зокрема налаштуванням двофакторної аутентифікації на всіх облікових записах, а також:

5.1. Використовуйте ліцензійні/легалізовані операційні системи, інші програмні продукти, своєчасно й систематично їх оновлюйте.

5.2. Користуйтеся антивірусним програмним забезпеченням з технологією евристичного аналізу.

зловмисники можуть замаскувати доменне ім'я, щоб воно виглядало знайомим (facelook.com, goooogle.com тощо) . В іншому разі є велика ймовірність перейти на фішингову сторінку, ззовні ідентичну справжній, та самостійно «віддати» власні автентифікаційні дані.

5.15. У разі необхідності введення автентифікаційних даних упевніться в тому, що використовується захищене з'єднання HTTPS, перевіряйте SSL-сертифікат веб-сайту, щоб переконатися, що він не клонований або не підроблений.

5.16. Шкідливі URL-адреси можуть бути закодовані у вигляді QR-кодів та/або роздруковані на папері, у тому числі у формі скорочених URL, згенерованих спеціальними сервісами на кшталт tinyurl.com, bit.ly, ow.ly тощо. Не вводьте ці посилання до браузера та не скануйте QR-коди вашим смартфоном якщо ви не впевнені у їх вмісті та походженні.

5.17. Використовуйте VirusTotal для перевірки підозрілих посилань так само, як для сканування файлів.

5.18. Будьте обережні щодо випливаючих вікон та повідомлень у вашому браузері, програмах, операційній системі та мобільному пристрої. Завжди читайте вміст цих вікон та не "схвалюйте" і не "приймайте" нічого похапцем.

5.19. Під час використання віддаленного доступу необхідно обмежити доступ за допомогою "білого списку" (IP whitelisting) .

5.20. Установіть обмеження кількості введення помилкових логінів/паролей. Регулярно переглядайте журнали логування, планувальник завдань та автозавантаження на предмет несанкціонованих дій.

6. Під час проведення аудіо- та відеоконференцій слід дотримуватись наступних заходів безпеки:

- підготувати середовище для роботи та переконатись, 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 для 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.

7. При використанні особистих електронних пристроїв для підключення до відкритих каналів зв'язку, рекомендуємо здійснити наступні налаштування:

- заборонити автоматичне встановлення додатків з невідомих джерел;
- обмежити доступ додатків до функціоналу пристрою, в якому немає потреби;
- відключити функцію автоматичного підключення до незахищених точок доступу.

Заступник директора з НВР **Ольга ПОЖАР**

Інженер-електронік **Едуард КРИВОРОТ**