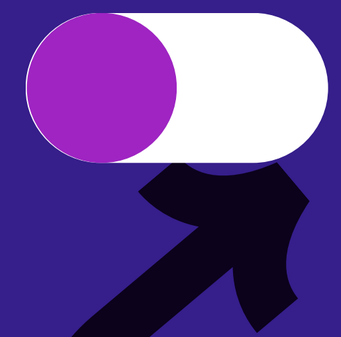
НМЦ ПТО
у Харківській області

ІНФОРМАЦІЙНА БЕЗПЕКА ОСВІТНЬОГО СЕРЕДОВИЩА

Захист інформації

Ірина ДУБРОВА,
методист НМЦ ПТО у
Харківській області

НЕбезпечний інтернет



1

ВІРУС - невелика програмна програма, яка поширюється з одного комп'ютера на інший і перешкоджає роботі комп'ютера

2

СПАМ – небажані повідомлення у будь-якій формі, які надсилаються у великій кількості

3

ХАКЕР – людина, котра добре розбирається в апаратному і програмному забезпеченні (залізо + програмування), спеціаліст в області комп’ютерних мереж і захисту інформації

4

ФІШИНГ – різновид онлайн-шахрайства, який полягає в тому, що шахраї шляхом обману намагаються дізнатися особисту інформацію для подальшого незаконного використання

НЕбезпечний інтернет

5

ТРОЛІНГ – вид взаємодії в онлайн-дискусіях на віртуальних комунікативних ресурсах

6

КІБЕРБУЛІНГ – це булінг із застосуванням цифрових технологій

- флеймінг – обмін короткими гнівними та запальними репліками між учасниками
- діссінг – передача або публікація компрометуючої інформації про жертву онлайн
- кетфішинг - створення вигаданого акаунту або сторінки в соціальних мережах, що, зазвичай, націлений на конкретну жертву
- кіберсталкінг – анонімне, приховане вистежування потерпілих задля організації злочинних дій

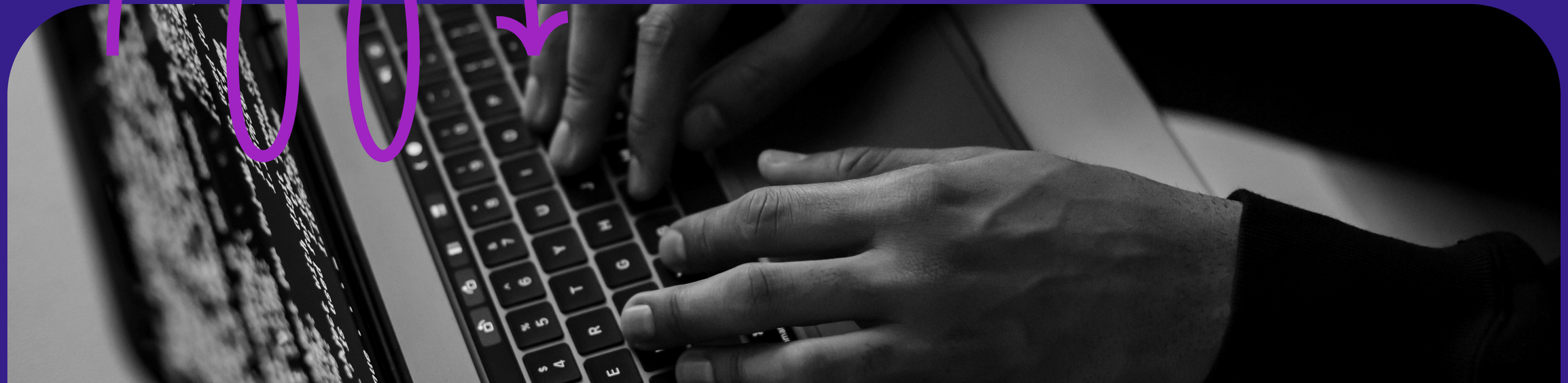
Як же педагогу при такому різноманітті небезпек захистити не тільки особисті дані, а й власне освітнє середовище?

1

Захист від вірусів

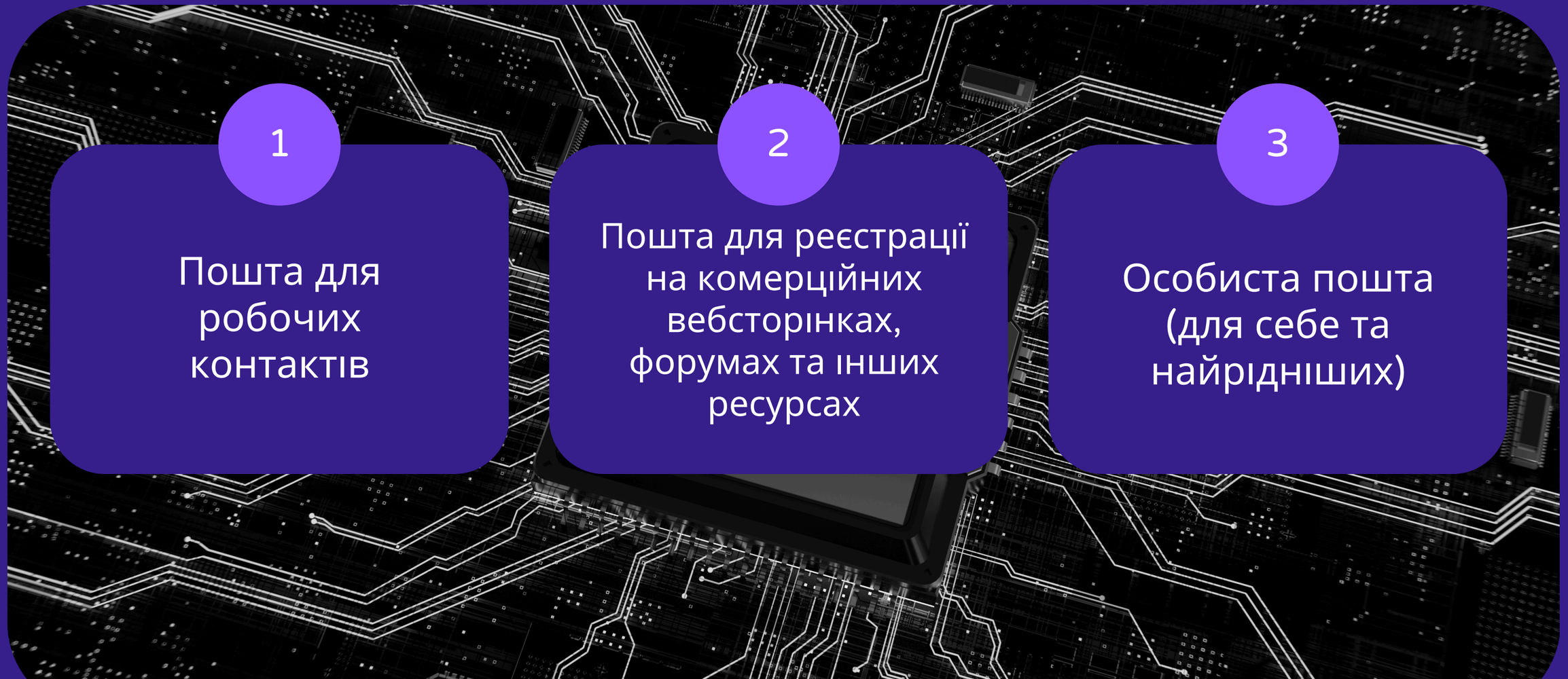
настроювання автоматичного оновлення у Windows

Ліцензійне програмне забезпечення, увімкнений брендмауер, автоматичне оновлення програм, перевірка програм перед завантаженням, використання особистого облікового запису



2

Захист від спаму



1

Пошта для робочих контактів

2

Пошта для реєстрації на комерційних вебсторінках, форумах та інших ресурсах

3

Особиста пошта (для себе та найрідніших)

3 Захист від хакерів та фішингу

- Перевірте, чи надійні ваші паролі
- Пароль – це ваш особистий секрет
- Використовуйте генератор паролів
- Встановіть двофакторну автентифікацію
- Не відкривайте повідомлення, що містять заклики до дії
- Довіряйте тільки перевіреним джерелам інформації

3 Захист від хакерів та фішингу

- Не відкривайте листів, які містять обіцянки чогось безкоштовного
- Зробіть на зовнішній носій резервну копію важливої для вас інформації

4 Попереджувальні ознаки того, що ви маєте справу з інтернет-тролем

- ігнорування реальних свідчень
- перенаправлення тем
- поблажливий тон
- надмірне перебільшення

4

Захист від тролей

- Не демонструйте свої емоції
- Встановіть чіткі правила модерації
- Поговоріть з ними про факти
- «Вбийте» їх добротою або гумором
- Блокуйте самі або звертайтесь до модераторів платформ
- Залишайтесь професіоналом своєї справи

5

Захист від кібербулінгу

- Блокуйте профілі кривдників
- Не мовчіть! Пам’ятайте, що знущання в Інтернеті не є провиною жертви
- Зберігайте копії публікацій, які використовувалися проти вас з метою кібербулінгу
- Звертайтесь до адміністраторів сервісів
- Звертайтесь до органів Національної поліції із заявою про вчинення адміністративного правопорушення

Поради з безпечного з’єднання в публічних Wi-Fi мережах:

1

Запам’ятайте та прийміть істину: публічні Wi-Fi мережі не захищені

2

Використовуйте при підключенні VPN

3

Слідкуйте за правильністю адреси сайту

Електронна пошта кіберполіції: callcenter@cyberpolice.gov.ua

Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA: cert@cert.gov.ua