Капля А. В., завідувач відділення загальноосвітньої підготовки
Дніпрорудненський індустріальний коледж

КІБЕРБЕЗПЕКА ЯК ВАЖЛИВИЙ АСПЕКТ СЬОГОДЕННЯ

Всі відчувають, як останнім часом змінюється світ. Промислові товари, послуги, продуктивність виробництва, капітал, знання та інформація користуються попитом незалежно від кордонів та обмін ними здійснюється у все більш короткі строки. Це зумовлено стрімким розвитком інформаційних технологій, процесами становлення і розвитку міжнародного кіберпростору, який триває з кінця XX століття та по сьогоднішній день.

В епоху інформаційних технологій неможливо почуватися захищеним у кіберпросторі. З розвитком технологій стрімко зростає кількість злочинів у цій сфері, а тому з впевненістю можна стверджувати, що саме «кіберзлочини» у XXI столітті будуть одними з найчисельніших.

Виникнення нових сфер суспільного життя породжує й нові загрози. Державна влада, в особі правоохоронних органів, повинна реагувати на суспільно небезпечні та протиправні дії. Тому необхідність в забезпеченні безпеки інтересів людини і громадянина, суспільства та держави, національних інтересів в кіберпросторі поступово набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки держави.

Кіберпростір – безмежний, а досвідчені хакери мають всі необхідні навички та засоби, щоб залишатися в ньому інкогніто. Сьогодні кібератаки шкодять не лише фізичним та юридичним особам, але й державам.

Кібербезпека – один із ключових аспектів життя в інформаційну добу. Наші смартфони, соцмережі й інші онлайн-відбитки особи містять про користувачів інформації більше, ніж вони самі знають про себе. При тому, вони можуть бути значно більш вразливими для атак зловмисників, ніж людина в реальному житті. Тому уся електронна інформація, сервіси і пристрою потребують захисту і дотримання певних правил безпеки [2].

Враховуючи прагнення України щодо євроінтеграції, потрібна уніфікація національного законодавства з нормативними документами Європейського союзу, тому при підготовці нормативних актів стосовно кібербезпеки доцільно орієнтуватися на аналогічні правові документи як загальноєвропейського рівня, так і рівня членів Євросоюзу, зокрема, ФРН. Оскільки європейські держави взяли до уваги питання кіберзахисту раніше за Україну, то варто також вивчати їхній досвід з практичної реалізації адміністративного, організаційного, технічного та іншого забезпечення кібербезпеки.

Об’єктом різних видів кіберзлочинів може стати будь-який користувач інтернету:

- Фішинг – нібито від адміністрації або служби безпеки платіжних систем клієнтам надсилають повідомлення з проханням вказати свої рахунки та паролі.
- Онлайн-шахрайство – несправжні інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв’язку.
- Мальваре – створення та розповсюдження шкідливого програмного забезпечення.

Видів такого злочину є дуже багато, всіх не перелічіть, але для хвилювань нема підстав, якщо знати як їх уникнути. Ось декілька порад щодо того, як вберегти себе від кіберзлочинів:

- створення надійних паролів та періодична їх зміна;
- поінформованість про злочинні прийоми, щоб розпізнати їх;
- захист пристроїв, встановлення антивірусних програм;
- використання захищених мереж;
- використання інструментів конфіденційності та безпеки Google [3].

Ефективність запобігання і протидії кіберзлочинності засобами державного управління безпосередньо залежить від узгодженості дій та заходів громадськості. Пам’ятайте всі вимоги кібербезпеки і дотримуйтесь їх!

Список використаних джерел

1. Офіційний портал Верховної Ради України: Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" [Електронний ресурс]: Верховна Рада України 15.03.2016. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/96/2016.

2. Баранов О. А. Про тлумачення та визначення поняття «кібербезпека» /О. А.Баранов // Правова інформатика. –2014. –№ 2. –С. 54-62.

3. Управління боротьби з кіберзлочинністю // МВС України. [Електронний ресурс]. – Режим доступу : http://mvs.gov.ua/mvs/control/main/uk/publish/article/544754.