## АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ

**Юрій ЛОМАКІН,**

*студент 1-го курсу Національного аерокосмічного університетуім. М. Є. Жуковського «ХАІ»*

***Науковий керівник:*** *Гуцу С.Ф., канд. юрид. наук, доцент, доцент кафедри права Національного аерокосмічного університету ім. М. Є. Жуковського «ХАІ»*

Сьогодні світ бурхливо розвивається у різних ІТ-сферах. Питання власної безпеки в Інтернеті все більше береться до уваги як серед громадян, так і на всесвітньому рівні. Події 2020 року, а саме коронакриза, прискорила цифровізацію багатьох послуг та загалом сприяла збільшенню числа активних онлайн користувачів. А це в свою чергу сприяло збільшенню Інтернет вразливостей та кібератак з боку темної сторони Інтернету та не зовсім законослухняних громадян. Майже 70% українських компаній за минулі 2 роки стикалися з проблемами у сфері кібербезпеки, а 33% стають жертвами кіберзлочинців понад три рази на місяць. Експерти зазначають, що боротьба з щоденнозростаючими глобальними кібератаками як у державному, так і приватному секторах, привела до зростання ринку кібербезпеки до 100 млрд дол. США на рік (згідно з Gartner Group 2019 Annual Global Cybersecurity Survey). Сукупне зростання обсягу закупівлі програмного забезпечення, обладнання і пов'язаних з ними професійних послуг у сфері кібербезпеки склав 12% у порівнянні з попереднім роком. І все ж, незважаючи на зростаючі інвестиції в кіберзахист, державний і приватний сектор не встигають за шахрайством, крадіжками і витоком даних, викликаних кібератаками, розмір збитку від яких до 31 грудня 2021 року досягне 4,2 трлн дол. США.

Керівниця служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України Наталія Ткачук назвала головну проблему національної системи кібербезпеки України - відсутність кадрів у кожному органі, який відповідає за цю сферу. Це питання слід вирішити шляхом побудови кіберрезерву фахівців - молодих хлопців і дівчат, які проходитимуть, у тому числі, строкову службу. Це буде такий своєрідний пул кадрів, який потім зможуть використовувати всі суб'єкти сектору безпеки й оборони, задіяні у завданнях кібербезпеки. Україна має для цього величезний потенціал, у жодній країні немає такої кількості молодих, талановитих айтішників, які при цьому є справжніми патріотами своєї країни й готові обороняти кіберпростір. Крім того, за результатами зустрічі Байдена та Зеленського до кінця цього року планується підписати угоду, яка передбачає обмін досвідом та інформацією щодо протидії «агресії РФ у кіберпросторі», а також розробку спільних протоколів дій.

Інші умови цієї угоди такі:

- побудова платформи обміну інформацією про кіберінциденти;

- спільні дії щодо захисту об'єктів критичної інформаційної інфраструктури та
- надання інформації для покращення системи реагування на кіберінциденти;
- обмін досвідом у межах системи управління ризиками (Risk Management).

У січні 2021 на території Харкова та Харківської області викрили групу хакерів, які здійснювали масові втручання в роботу серверів банківських установ європейських країн і США. Їм пред'явлено звинувачення у створенні, з метою кримінального використання, розповсюдження чи збуту шкідливих програмних або технічних засобів, а також заволодіння чужим майном шляхом обману (ч. 1 ст. 361-1, ч. 3 ст. 190 КК Україна). За даними слідства, група хакерів з України з 2014 року, використовуючи шкідливе програмне забезпечення - так званий вірус-шифрувальник («банківський троян»), призначений для крадіжки персональних даних - паролів, логінів і платіжних даних, здійснював масові втручання в роботу серверів приватних і державних банківських установ Великобританії, Німеччини, Австрії, Швейцарії, Нідерландів. Такими протиправними діями було завдано збитків банкам на суму близько 2,5 млрд доларів США.

На підставі вищезазначеного ми приходимо до висновків, що для посилення власної та загальної безпеки в мережі Інтернет необхідно дотримуватися деяких правил:

- обов'язково користуйтеся антивірусами.
- не завантажуйте сторонні програми та файли.
- не переходьте за підозрілими посиланнями.
- оновіть операційну систему, браузер та антивірус до останніх версій.
- налаштуйте резервну копію всіх необхідних вам у роботі файлів.
- не зв'язуйтеся з шахраями.

Звідки б не зайшла атака і поява вірусів, працюйте завжди на їхнє випередження - бережіть свої гаджети і дотримуйтеся рекомендацій експертів з їх захисту. А в разі зараження - треба звертатися до кіберполіції.

**Список використаних джерел:**

1. https://www.armyua.com.ua/інформаційний-резонанс-доби-12-10-2021/
2. https://eba.com.ua/kiberbezpeka-v-2020-rotsi-top-10-prognoziv-ta-rekomendatsij/
3. https://www.bdo.ua/uk-ua/news-2/2019/cybersecurity-2020
4. https://www.ukrinform.ua/rubric-antifake/3331654-v-rnbo-nazvali-golovni-problemi-nacionalnoi-sistemi-kiberbezpeki.html
5. https://www.ukrinform.ua/rubric-presshall/3327586-obgovorenna-pitan-kiberoboroni-derzavi-ta-perspektivi-stvorenna-kibervijsk.html