3. Малицька, І. Д. ІКТ грамотність – вимога сучасних систем освіти зарубіжних країн (досвід США) / І.Д.Малицька // Інформаційні технології в освіті. 2009. № 4. - С. 243-249.
4. Поліщук, Т. В. Цифрова освіта засобами бібліотек. Бібліотека. Наука. Комунікація. Розвиток бібліотечно-інформаційного потенціалу в умовах цифровізації : матеріали Міжнар. наук. конф. (6-8 жовт. 2020 р.) / НАН України, Нац. б-ка України ім. В. І. Вернадського, Асоц. б-к України, Рада дир. наук. б-к та інформ. центрів акад. наук – членів МААН; відп. за вип. М. В. Іванова. Київ, 2020. -С. 224-227.
5. Дія. Цифрова освіта // Міністерство цифрової трансформації України //Режим доступу: https://osvita.diia.gov.ua. (дата звернення: 25.03.2021).

Кириленко В. В.,
студентка ІІ курсу спеціальності 029 «Інформаційна, бібліотечна та архівна справа»,
Науковий керівник: Шуляк С. О., кандидат педагогічних наук, доцент, декан факультету менеджменту і бізнесу ВП «Миколаївська філія Київського національного університету культури і мистецтв», м. Миколаїв

КІБЕРТЕРОРИЗМ ТА КІБЕРЗЛОЧИННІСТЬ ЯК ТИПИ ЗАГРОЗ В РЕАЛІЯХ СУЧАСНОГО ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Комп’ютерні системи надають нові, найбільш досконалі можливості для невідомих раніше правопорушень, а також для скоєння традиційних злочинів, але нетрадиційними засобами [1]. Аналіз кібербезпекових стратегій різних країн дозволяє зробити висновок, що на сучасному етапі основними загрозами кібербезпеці у переважній більшості держав визначаються кібертероризм, кібервійна, кибершпигунство та кіберзлочинність [2].

Стрімкий прогрес у розвитку інформаційних технологій та поступове перетворення кіберпростору на поле й інструмент протистояння призвели до виникнення нових істотних проблем у сфері міжнародної безпеки, однією з яких стала актуалізація загрози кібертероризму як нового виклику безпековому середовищу держави.

На сьогодні, у світі не існує єдиного визначення кібертероризму, суперечливими є і підходи до розуміння його сутності. Деякі науковці відносять кібертероризм до різновиду кіберзлочинів, такий підхід закріплений і у законодавстві окремих країн. Наприклад, у Туреччині кібератаки здійснені терористами кваліфікуються як комп’ютерні злочини. Інші вчені вважають, що

кібертероризм є самостійним явищем та потребує окремого законодавчого механізму протидії [2].

Характеризуючи особу комп'ютерного злочинця, необхідно відмітити основне, а саме: в електронну злочинність втягнуто широке коло осіб – від висококваліфікованих фахівців до дилетантів. Правопорушники мають різний соціальний статус та різний рівень освіти (навчання та виховання).

З метою глибшого вивчення цієї проблеми треба чітко знати, хто ж вони – сучасні комп'ютерні злочинці: *хакери і кракери*. Вітчизняні та зарубіжні дослідження дозволяють намалювати реальний портрет типового комп'ютерного злодія, тобто змоделювати відповідний профіль даного соціального типу [1].

Хакер (англ. Hacker, від to hack – рубати) – особа, що намагається отримати несанкціонований доступ до комп'ютерних систем, як правило з метою отримання секретної інформації. Також на сленгі вживається у значенні – досвідчений комп'ютерний програміст або користувач [3].

Кракер (англ. crack – тріщина, удар) – той, хто порушує безпеку системи. Кракери взломують системи з ціллю отримання несанкціонованої інформації, пишуть програми-взломщики, наприклад, генератори серійних номерів. Їх діяльність переслідується законом. Іноді замість цього терміну вживають слово «хакер», та це не є правильним [4].

Класифікація хакерів. Існують різні можливі класифікації, найпоширенішою типологією, за якою можна розділити і визначити хакерів, є те, що відноситься до «капелюхів». Ця форма класифікації походить від класичного західного кіно, де персонажі носили капелюшок одного кольору або іншого кольору в залежності від того, чи були вони героями чи лиходіями. Згідно з цією класифікацією, ковбої з білими капелюхами були хороші, а ті, хто носив чорну капелюх, були поганими хлопцями. Ця форма класифікації була адаптована до комп'ютерного світу, де різні типи хакерів визначаються залежно від кольору капелюха, який надає їм [5].

1. Білий капелюх. Хакери білої шапки вважаються кращими. Цей тип хакерів зазвичай працюють з комп'ютерними компаніями, і його головною метою є пошук недоліків у системах безпеки з метою розв'язання цих прогалин [5].

2. Чорна шапочка. Цей тип хакера є протилежною шапці Білого. Її діяльність в основному ґрунтується на порушенні безпеки серверів для їхнього пошкодження або вилучення приватної інформації. У цьому сенсі хакери з чорною капелюхом здатні атакувати веб-сторінки або цілі сервери, а також вводити віруси в певне програмне забезпечення [6].

3. Сірий капелюх. Називається сірим, оскільки цей тип хакерів використовує свою науку про хакерство для добра і зла [6].

4. Золотий капелюх хакер. Це хакери, які проникають у безпеку компаній або програмного забезпечення для того, щоб повідомити про свою вразливість або як особистий виклик; тобто досягти того, чого досі ніхто не зробив. Вони також можуть використовувати хакерство для того, щоб відправити повідомлення, яке зазвичай асоціюється з соціальною або етичною причиною, яку вони вважають обґрунтованою та морально виправданою [5].

5. Хактивіс. Хактивіс мотивований особистими думками з питань політики, релігії, навколишнього середовища тощо [6].

*5. Кібертерористи. О*скільки ім'я кібертерористів використовує комп'ютер для тероризму, цей тип хакерів зазвичай використовує атаку Dos (Відмова в сервісі) для пошкодження урядових веб-сайтів [6].

Напрямки комп'ютерних атак. На сьогоднішній день комп'ютерні атаки, що здійснюються терористами або хакерськими групами, як правило, направлені на: виведення з ладу інформаційно-телекомунікаційних систем та систем зв'язку за допомогою вірусів або спаму; тимчасове блокування публічних веб-сайтів шляхом масованих DDOS-атак; атаки на офіційні веб-сайти або сторінки у соціальних медіа органів державної влади та комерційних організацій з метою розміщення повідомлень терористичного спрямування; несанкціонований доступ в систему з метою викрадення даних або її використання в організації кібератак на інші системи (н-д, створення бот-мереж); незаконне оприлюднення персональних даних у мережі Інтернет стосовно політиків, правоохоронців чи військовослужбовців у поєднанні із прямими погрозами [2].

Враховуючи виклики вітчизняного безпекового середовища та терористичну діяльність «ДНР» та «ЛНР» на сході України, яка повною мірою знаходить своє відображення і в кіберпросторі, виникає потреба у розбудові комплексного механізму протидії цьому явищу, який перш за все, має виконувати превентивну функцію [2]. Для цього, в першу чергу, необхідно підвищувати потенціал суб'єктів боротьби з кібертероризмом (у т.ч. розширити застосування новітніх інформаційних технологій в інтересах антитерористичної діяльності), підвищити рівень кіберзахисту критичної інфраструктури держави, а також забезпечити поінформованість населення про загрозу кібертероризму [2].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Кіберсвіт у новому тисячолітті. Хто вони: кіберзлочинці, кібершахраї, кібертерористи? [Електронний ресурс]. – Режим доступу: https://lexinform.com.ua/dumka-eksperta/kibersvit-u-novomu-tysyacholitti-hto-vony-kiberzlochyntsi-kibershahrayi-kiberterorysty/ – Назва з екрану.
2. Ткачук Н. А. Актуальні кіберзагрози сучасного безпекового середовища [Електронний ресурс] / Н.А. Ткачук // Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки». – 2018. – № 7. – Режим доступу: https://doi.org/10.25313/2520-2308-2018-7-4183 – Назва з екрану.
3. Хакер [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Хакер – Назва з екрану.
4. Кракер [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Кракер# – Назва з екрану.
5. Какие три типа хакеров? [Електронний ресурс]. – Режим доступу: https://uk.pasapic.com/9065-types-of-hackers-according-to-their-behavior – Назва з екрану.

6. Типи комп'ютерних хакерів [Електронний ресурс]. – Режим доступу: https://glennbouchard.com/uk/361-tipe-tipe-hacker-komputer.html – Назва з екрану.

Шаповал А. І.,
студентка ІІ курсу спеціальності 029 «Інформаційна, бібліотечна та архівна справа»,
Науковий керівник: Шуляк С. О., кандидат педагогічних наук, доцент, декан факультету менеджменту і бізнесу ВП «Миколаївська філія Київського національного університету культури і мистецтв»,
м. Миколаїв

КОМПЮ’ТЕРНІ ВІРУСИ ЯК ВИД ЗАГРОЗ В КІБЕРПРОСТОРІ

Сучасний світ характеризується інтенсивним розвитком інформаційних технологій. Але побічною стороною розвитку цих технологій є розвиток різного виду шкідливого програмного забезпечення, одним з найбільш розповсюджених якого є комп’ютерні віруси.

Комп'ютерний вірус (англ. computer virus) – комп'ютерна програма, яка має здатність до прихованого самопоширення. Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера.

Назва програми «комп'ютерний вірус» походить від однойменного терміну з біології за її здатність до саморозмноження. [2].

Не існує єдиної системи класифікації та іменування вірусів (хоча спроба створити стандарт була зроблена на зустрічі CARO в 1991 році). Серед них: віруси – супутники (використовують імена інших файлі), файлові віруси, завантажувальні віруси (здатні вражати як код boot-секторів, так і код файлів), віруси DIR (спотворюють системну інформацію про файлові структури), макровіруси (віруси, що заражують файли даних, наприклад, документи Word або робочі книги Excel [3].

Кожного року комп'ютерні віруси причиняють шкоди розміром в декілька мільярдів доларів, викликаючи системні критичні помилки, зупиняючи великі сайти та вебдодатки, знищуючи або модифікуючи файли, підвищуючи час відклику

Основні типи вірусів: