УДК 343.9.024:004.056

ГУЦАЛЮК М.В., *кандидат юридичних наук, старший науковий співробітник, доцент*, головний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України.
ORCID: https://orcid.org/0000-0003-4496-5173.

НОВІТНІ ТЕНДЕНЦІЇ КІБЕРЗЛОЧИННОСТІ

Анотація. *У статті досліджуються сучасні тенденції кіберзлочинності, у тому числі її організовані форми, надаються пропозиції щодо посилення протидії цьому явищу.*
Ключові слова: *кіберзлочинність, кібератака, COVID-19, шахрайство.*

Summary*. The article deals with current trends in cyber crime, including its organized forms, and proposes to strengthen the counteraction to this phenomenon.*
Keywords*: cyber crime, cyber attack, COVID-19, fraud.*

Аннотация*: В статье исследуются современные тенденции киберпреступности, в том числе ее организованные формы, представлены предложения по усилению противодействия этому явлению.*
Ключевые слова*: киберпреступность, кибератака, COVID-19, мошенничество*.

Постановка проблеми. Відповідно до Конституції України забезпечення інформаційної безпеки відноситься до найважливіших функцій держави, справою всього Українського народу. У зв'язку з динамічним розвитком інформаційних технологій та розширенням сфери їх застосування постійно зростає вплив кіберзагроз на сталий розвиток суспільства. Водночас на характер кіберзагроз та методи і способи вчинення кіберзлочинів впливають не тільки технологічні новації, але й різноманітні соціальні процеси. В статті досліджуються новітні тенденції кіберзлочинності, у тому числі пов'язані з впливом пандемії COVID-19.

Результати аналізу наукових публікацій. Вплив кіберзлочинності на цифрове суспільство досліджувалось багатьма закордонними Maras Marie-Helen, Eoghan Casey, Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar та вітчизняними вченими Н. Ахтирська, П. Біленчук, В. Бутузов, В. Гавловський, О. Кравцова, А. Марущак, К. Тітуніна, В. Шеломенцев, В. Хахановський, О. Юрченко та інші.

В той же час сьогодні ще не достатньо досліджені особливості діяльності кіберзлочинців та кіберугруповань під час суттєвого збільшення кількості працівників, що працюють дистанційно та збільшення часу використання мережі Інтернет, що збільшило кількість кібератак та Інтернет-шахрайства.

Виклад основного матеріалу. Найбільш значуща подія 2020 року, яка вплинула на увесь світ, була безперечно пандемія COVID-19. Понад 100 мільйонів випадків інфікування коронавірусом було виявлено у майже всіх країнах та територіях світу. Унаслідок захворювання понад 2,5 млн осіб померли. Стрімке поширення світом вірусу позначилось на діяльності державних установ, промислових підприємств та громадян абсолютної більшості країн світу.

Значний вплив коронавірусної пандемії на інформаційну сферу України підкреслено у Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 року № 392/2020. У документі зокрема зазначено про

виявлення критичних проблем в інформаційній сфері, системах охорони здоров'я та соціального захисту.

Внаслідок введення комплексних заходів соціального дистанціювання суттєво зросла кількість онлайн-комунікацій між державними органами, підприємствами та приватними особами. Зріс попит на програмне забезпечення для домашнього офісу, таке як Zoom, Microsoft Teams і їх аналоги. Значно зросла й кількість часу, який люди проводять в мережі Інтернет.

Інтернет-провайдери фіксованого та мобільного широкосмугового зв'язку, контенту та "хмарних обчислень", а також пункти для обміну трафіком (IXP) відзначили збільшення Інтернет-трафіку на 60 % у порівнянні з доковідним періодом.

Поява нових обставин, пов'язана з поширенням вірусу COVID-19 створила нові можливості для вчинення злочинів. Як окремі злочинці, так і організовані злочинні угруповання, надзвичайно швидко адаптувалися до змін у суспільстві для підвищення рівня кримінального прибутку та почали використовувати дану проблему у своїх цілях.

Через зростання кількості корпоративних клієнтів американської компанії Zoom Video Communications, що надає послуги віддаленого конференц-зв'язку, у порівнянні з аналогічним періодом 2019 року на 458 %, цей сервіс привернув увагу злочинців. У Даркнеті зявилися понад 500 000 облікових записів Zoom, які продаються на форумах менше, ніж за копійку кожен, а в деяких випадках даруються безкоштовно. Ці облікові дані збираються за допомогою кібератак. Потім успішні логіни та паролі складаються у списки, які продаються іншим хакерам [1].

Таку поведінку злочинців слід називати опортуністичною, адже під терміном опортунізм (франц. *opportunism* – пристосовництво, від лат. *opportunus* – зручний, вигідний, слушний) слід розуміти поведінку, метою якої є отримання вигоди нечесним шляхом [2].

Серед ключових передумов виникнення загрози кібербезпеці на фоні розгортання пандемії COVID-19 Національний інститут стратегічних досліджень виділяє наступні [3]:

1. Збільшення кількості людей, які працюють віддалено (використовуючи IT, але не маючи належних знань та досвіду).

2. Збільшення кількості та обсягів електронних платежів.

3. Загальна атмосфера кризи та паніки.

Згідно з даними міжнародного розробника програмного забезпечення в сфері кібербезпеки ESET, за 2020 рік в Україні вдвічі збільшилась кількість веб-загроз та кібератак, пов'язаних з пандемією COVID-19, в тому числі через електронну пошту (шкідливе програмне забезпечення, програми-вимагачі сімейства WannaCryptor, завантажувачі та криптомайнери, експлойти EternalBlue і т.п.).

Втрати світової економіки через кіберзлочини і витрати на забезпечення захисту від них у 2020 році ***перевищили 1 трлн. доларів***. Тоді як ще два роки тому ця сума становила близько 600 млрд. доларів. Про це йдеться у звіті виробника антивірусного програмного забезпечення McAfee [4].

Кіберзлочинці почали більш ефективно використовувати традиційні методи кіберзлочинності, такі як соціальна інженерія, фішинг (спеціальна методика маніпуляції, яка допомагає змусити людину віддати зловмисникам необхідні дані) та шахрайство.

Зазначимо, що поняття кіберзлочину було введено в чинне законодавство Законом України "Про основні засади забезпечення кібербезпеки України" як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке

визнано злочином міжнародними договорами України. У цьому аспекті перш за все слід мати на увазі Конвенцію про кіберзлочинність 2001р. (ратифікована із застереженнями і заявами Законом України від 07.09.05 р. № 2824-IV).

Водночас на сьогодні у чинному законодавстві України не існує чіткого переліку таких видів злочинів, які слід віднести до кіберзлочинів, що призводить до певних труднощів, адже небезпечні діяння у кіберпросторі виходять за рамки XVI розділу КК України "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку". Тому деякі науковці і практики паралельно з кіберзлочинами використовують термін "злочини, учинені із використанням високих інформаційних технологій" та інші назви [5].

За повідомленням Департаменту кіберполіції НП України в Україні кількість злочинів, учинених із використанням високих інформаційних технологій у 2020 зросла на 22,9 % у порівнянні з попереднім роком(2019 - 4263, 2020 - 5240). Найбільшу питому вагу серед них становлять ***кримінальні правопорушення***, передбачені чч. 3 і 4 ст. 190 КК України – 25,9 %, які ***зросли на 70,2 %*** (2018 - 796, 2020 - 1355).

При цьому слід зазначити високу латентність такого виду злочинів. Так, 80 % від всіх звернень громадян до кіберполіції становлять повідомлення про шахрайські дії в Інтернеті [6].

За словами фахівців, найбільш поширеними видами шахрайства у віртуальному просторі є продаж неіснуючих товарів, а також фішингові онлайн-магазини.

Найчастіше злодії ошукують громадян, продаючи неіснуючі товари на майданчиках оголошень або в соцмережах. Як правило, в таких випадках головна умова покупки – повна передоплата за товар, після чого "продавець" перестає контактувати з покупцем.

Кіберзлочинці дедалі частіше використовують в своїх цілях страх людей перед вірусом COVID-19: виставляють на продаж в Інтернеті підроблені лікарські препарати, неіснуючі дезінфікуючі засоби, засоби індивідуального захисту, медичні апарати і засоби гігієни. Інші види шахрайства включають пропозиції щодо інвестиційного консультування, в тому числі по криптовалюті, а також неправдиві медичні консультації і діагностику.

Особливо значний сплеск фішингових атак з використанням проблематики COVID-19 відбувся відразу після початку пандемії [7].

За один чотиримісячний період (з січня по квітень 2020 року) одним з партнерів приватного сектору INTERPOL було виявлено близько 907 000 спам-повідомлень, 737 випадків, пов'язаних зі шкідливим програмним забезпеченням, та 48 000 шкідливих URL-адрес – усіх, пов'язаних із пандемією COVID-19 [8].

Вплив COVID-19 на злочинність змінювався з часом, зокрема підвищення обізнаності громадян зменшило вплив, який мали деякі види злочинів, водночас за інформацією Європолу кількість шкідливих програм, які використовують COVID-19 як приманку і сьогодні продовжує зростати.

Крім правоохоронців певну роботу щодо протидії спекулятивній діяльності намагаються проводити власники майданчиків електронної торгівлі.

Зокрема, на платформі OLX модераторами видаляється контент з відповідним змістом, що містить назви товарів, заборонених до продажу на цій платформі та зупиняється можливість публікації інформації про товари, що вимагають особливих умов зберігання і збуту, у тому числі тих, що використовуються для боротьби з коронавірусом, щоб не наражати на небезпеку користувачів.

На порталі Prom.ua також обмежуються можливості продавців, які використовують підвищений інтерес до теми коронавірусу для отримання надприбутку шляхом видалення з каталогу товарів, у ключових словах, тегах і назвах яких є слова "коронавірус", COVID-19 та їх синоніми. Особливо це стосується профілактичних препаратів, БАДів. Наприклад, продавати "антисептик" можна без проблем, а от "антисептик для профілактики коронавірусу".

Як повідомляє BBC, соціальна мережа Facebook ввела заборону на розміщення реклами гігієнічних масок і дезінфікуючих засобів для рук з метою перешкодити ажіотажному попиту на них і зростанню цін.

Крім того, соцмережа посилила контроль за появою в мережі дезінформації про засоби, які нібито сприяють лікуванню від вірусу, а також про товари, на які нібито виник дефіцит.

"Ми уважно спостерігаємо за ситуацією навколо Covid-19 і в разі потреби будемо вносити зміни в нашу політику, якщо виявимо, що люди експлуатують цю надзвичайну ситуацію", – заявив директор з контролю за продуктами Facebook Роб Літерн [9].

Оскільки велика кількість громадян та бізнес шукали інформацію та джерела допомоги під час пандемії, кіберзлочинці активно використовують соціальну інженерію.

Фахівці Національного координаційного центру кібербезпеки (далі – НКЦК) зазначають, що на початку пандемії у світі щодня реєструвалося понад 18 мільйонів фішингових повідомлень, пов'язаних з темою COVID-19.

Із середини 2020 року їх кількість поступово зменшувалась, а фішингові атаки стали більш направленими, їхня тематика змінювалася: від доступності масок і тестів до розробки вакцин.

Наприкінці січня 2021 року НКЦК виявив фішингову кібератаку, спрямовану на українських користувачів Інтернету, основною темою якої був початок вакцинації від COVID-19 в Україні.

Під час атаки на популярній хостинговій платформі було створено фейкову веб-сторінку, що імітувала сайт Міністерства охорони здоров'я України. Для розміщення сторінки атакуючі зареєстрували кілька доменів, які нагадували офіційний домен МОЗ України – moz.gov.ua.

На цій фейковій сторінці було розміщено інформацію щодо початку з 25 січня обов'язкової вакцинації від COVID-19 із пропозицією завантажити файл (документ Word) із подробицями.

У цей документ було вбудовано шкідливий код (макрос), який при відкритті файлу приховано від користувача завантажує та виконує інший шкідливий скрипт, що забезпечує віддалене управління зараженим комп'ютером. Таким чином, атакуючі отримували повний доступ до комп'ютера жертви [10].

Кримінальне правопорушення у червні 2020 року викрили працівники управління протидії кіберзлочинам Харківщини спільно зі слідчим управлінням обласної поліції та регіональним управлінням СБУ.

Встановлено, що до шахрайських дій причетні сім мешканців Кривого Рогу віком від 20 до 30 років.

Зловмисники діяли за декількома шахрайськими схемами. Так, члени групи телефонували клієнтам одного з мобільних операторів, видаючи себе за представників внутрішньої служби безпеки. Під приводом підтвердження верифікації користувача мобільного номеру отримували інформацію щодо останніх трьох номерів телефонів, з якими абонент спілкувався. Далі цю інформацію використовували для відновлення і перевипуску відповідної sim-карти та оформлювали онлайн-кредити.

За іншою злочинною схемою правопорушники від імені співробітника кредитної організації телефонували громадянам та повідомляли, що на його ім'я нібито здійснюється оформлення кредиту. У такий спосіб зловмисники переконували потерпілого назвати надісланий пароль доступу до особистого кабінету у фінансовій установі. Після цього вони подавали від його імені заявку на видачу кредиту.

Отримані гроші злочинці розподіляли між собою. Від протиправних дій постраждали близько 40 осіб, загальна сума збитків сягає 500 тисяч гривень.

Фігурантам було оголошено про підозру за ч. 1, ч. 2 ст. 255 (створення злочинної організації, керівництво такою організацією, а також участь у ній), ч. 4 ст. 28, ч. 1, ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, вчинене членами злочинної організації), ч. 4 ст. 28, ч. 3 ст. 190 (Шахрайство, вчинене членами злочинної організації) Кримінального кодексу України [11].

Можливості для кіберзлочинності збільшуються завдяки поширенню дезінформації. Наявність дезінформації стала вирішальною рисою в загальному ландшафті загроз під час кризи COVID-19. Хибна і недостовірна інформація щодо вірусу продовжує поширюватися, головним чином, через соціальні мережі, а також через сервіси із зашифрованою передачею повідомлень.

Фейкові повідомлення сприяють злочинцям, які продають предмети, що, начебто допомагають запобігти або вилікувати COVID-19. Такі засоби продаються як через звичайний Інтернет так і через Даркнет. Кількість нових доменів та веб-сайтів, пов'язаних із COVID-19, значно зросла на початку пандемії.

Поряд з традиційними видами кіберзлочинності, продовжують удосконалюватися і використовуватися загрози підвищеної складності (APT – Advanced Persistent Threats) для отримання вигоди із ситуації з пандемією COVID19. Основною метою APT атак є критичні об'єкти інфраструктури, включаючи лікарні та лабораторії по розробці вакцин. При цьому застосовуються шкідливі програми, програми-вимагачі, а також DDoS-атаки. Мотивом для подібних атак є не тільки отримання прибутку, але і можливість доступу до персональних даних та іншої конфіденційної інформації, що представляє цінність.

Наприклад, за повідомленням Національної служби розвідки Південної Кореї Північна Корея намагалася отримати технологію, що стосується вакцини проти коронавірусу та його лікування, за допомогою кібератаки проти Pfizer. КНДР збиралася продати отримані дані про вакцину, а не запустити власне виробництво.

Також у ЗМІ потрапила інформація з конфіденційної доповіді експертної комісії ООН про те, що хакери з Північної Кореї протягом 2020 року викрали в однієї з неназваних країн віртуальні активи на суму 316,4 млн. доларів на свою ядерну програму [12].

Успіх більшості кіберзлочинів, пов'язаних з COVID-19, заснований на фішингових атаках по електронній пошті, в якості початкового вектора зараження. Як тільки люди переходять по посиланню або завантажують документ, обліковий запис стає зкомпрометованим. Компрометація облікового запису може бути помітна жертві, але частіше всього вона залишається прихованою і дозволяє встановити довгостроковий доступ до облікового запису, організації із схожим програмним забезпеченням. Крім збору конфіденційної інформації, APT атаки можуть зашкодити роботі веб-сайтів, вносити зміни в документи, видаляти дані, а також поширювати неправдиву інформацію.

Управління ООН з наркотиків та злочинності рекомендує урядам країн і представникам приватного сектору активно проводити кампанії з підвищення рівня

інформованості населення, з урахуванням культурної специфіки. Також рекомендується регулярне оновлення системи безпеки і резервне копіювання даних [13].

Значних збитків продовжують завдавати кібератаки на банківський сектор.

Експерти з кібербезпеки прогнозують, що в 2021 році кібератаки будуть відбуватися кожні 11 секунд. Це майже вдвічі більше, ніж було в 2019 році (кожні 19 секунд), і в чотири рази більше, ніж п'ять років тому (кожні 40 секунд в 2016 році) . Значно збільшуються збитки від кібератак.

У США трьох північнокорейців звинувачено у викраденні та вимаганні понад 1,3 мільярда доларів у банків та підприємств усього світу.

Містер Парк, Джон Чанг Хьок та Кім Ір звинувачуються у змові з метою банківського шахрайства.

Міністерство юстиції заявляє, що обвинувачені працюють в Генеральному бюро розвідки, агентстві військової розвідки Північної Кореї.

Вважається, що всі троє перебувають у Північній Кореї, яка не видає своїх громадян для звинувачення США [14].

Упродовж 2020 року підрозділами Національної поліції України у сфері протидії злочинам у банківській сфері виявлено 2110 правопорушень (1079 у 2019 році) Також правоохоронними органами України у 2020 році суттєво посилилась робота щодо виявлення організованих кіберугруповань, у тому числі міжнародних.

Зокрема було викрито транснаціональну групу хакерів, які розповсюджували найнебезпечніший у світі комп'ютерний вірус EMOTET.

Хакери за допомоги вірусного програмного забезпечення здійснювали масові втручання в роботу серверів приватних та державних установ країн Європи та Сполучених Штатів Америки.

За даними слідства, група хакерів з України з 2014 року, використовуючи шкідливе програмне забезпечення, так званий вірус-шифрувальник ("банківський троян"), призначений для викрадення персональних даних – паролів, логінів та платіжних даних, здійснювала масові втручання в роботу серверів приватних та державних банківських установ Великої Британії, Німеччини, Австрії, Швейцарії, Нідерландів, Литви та США.

Інфраструктура "EMOTET" включала сервери, розташовані по всьому світу, і фактично була БОТ-мережею. Вірус поширювався шляхом спам-розсилок, через документи Word, Excel тощо. Електронні листи виглядали як попередження про безпеку облікового запису, запрошення на вечірку і навіть як застереження від поширення COVID-19.

Проникнувши у програмне забезпечення, вірус використовував "інфіковану" техніку для подальшої розсилки, а також встановлював на пристрій додаткові віруси. У результаті шкідливе програмне забезпечення викрадало персональні дані користувачів, зокрема паролі, логіни, історію браузера, платіжні та банківські дані тощо. У подальшому зловмисники перераховували гроші на свої підконтрольні рахунки.

Слідчі викрили двох громадян України, які забезпечували належну роботу інфраструктури розповсюдження вірусу та підтримували його безперебійну діяльність.

На даний час підтверджено, що вірус завдав збитків банкам і фінансовим установам США та Європи на 2,5 мільярда доларів.

Кіберполіцейські спільно з правоохоронцями іноземних держав одночасно провели обшуки на території України, Нідерландів, Німеччини, Франції, Литви, Канади, США та Великобританії.

Зазначається, що наразі повністю заблоковано діяльність БОТ-мережі "EMOTET", яка розташовувалася на більш ніж 90 серверах у різних країнах світу [15].

За повідомленням прес-служби СБУ кіберфахівці Служби безпеки України заблокували діяльність транснаціонального злочинного хакерського угруповання. Багаторівнева масштабна спецоперація проводилася в рамках міжнародного співробітництва з компетентними органами США і Франції. Зазначається, що з вересня 2020 року цими хакерами було уражено понад 150 компаній країн Європи і США. Збитки від діяльності угруповання становлять понад 80 млн доларів США.

У ході розслідування співробітники спецслужби встановили, що на території України діяла група осіб, яка використовувала шкідливе програмне забезпечення Egregor. З його допомогою хакери:

- шифрували комп'ютерні мережі іноземних компаній;
- викрадали персональні дані своїх клієнтів і працівників;
- викрадали інформацію про фінансові показники і технологічні розробки;
- блокували роботу вебресурсів.

Потім зловмисники вимагали великі суми грошей, найчастіше в криптовалюті, за дешифрування уражених комп'ютерних мереж і нерозголошення викрадених персональних даних [16].

Всього за минулий рік СБУ було розкрито 20 хакерських угруповань.

Значних збитків банківським установам можуть завдавати і окремі правопорушники. Так вже у 2021 році правоохоронці України викрили зловмисника – жителя Тернопільщини, який розробляв небезпечні онлайн-сервіси для атаки на банки та пошти.

У результаті використання таких зловмисних програм постраждали фінустанови 11 країн світу – США, Італії, Іспанії, Мексики, Чилі, Великої Британії, Нідерландів, Швейцарії, Австралії, Франції та Німеччини. Їхні збитки сягають понад $10 млн.

Встановлено, що правопорушник розробив спеціальну адмінпанель, що контролювала облікові записи користувачів, які вводили платіжні дані. В подальшому ці дані отримували зловмисники.

Окрім цього, зловмисник створював шахрайські сервіси для зламу пошти, яку використовують понад 1,5 млрд. користувачів.

Для продажу своїх розробок хакер створив інтернет-магазин у DarkNet, де було понад 200 покупців шкідливого програмного забезпечення [17].

Слід зазначити, що майже 98 % всіх кібератак ґрунтуються на тій чи іншій формі соціальної інженерії для доставки корисного навантаження, такого як шкідливі програми та програми-вимагачі. Один з найбільш успішних форматів атак, які кіберзлочинці регулярно використовують для проведення атак соціальної інженерії, – це фішингові електронні листи. Таким чином, зловмисники розповсюджують шкідливе ПО по електронній пошті приблизно в 92 % випадків [18].

Наприклад, у січні 2021 року було зафіксовано понад 400 тисяч фішингових атак. Зокрема, було виявлено масове розсилання електронних листів по державних установах нібито від Адміністрації Держспецзв'язку.

Файл, який містився в цих електронних листах, надавав доступ зловмисникам для дистанційного управління зараженим комп'ютером. Тобто особа, яка отримала доступ, мала можливість знищувати, копіювати, змінювати дані, що містяться на таких комп'ютерах.

Зазначається, що в більшості випадків вдалося уникнути негативних наслідків, але в деяких держустановах зловмисникам все-таки вдалося отримати доступ до комп'ютерів [19].

Для атак на об'єкти критичної інфраструктури організовані злочинні кіберугруповання використовують ***компрометацію постачальників*** засобів захисту інформації.

Так федеральні цивільні відомства США отримали розпорядження Американського агентства з питань кібербезпеки та інфраструктури проаналізувати свої мережі та негайно відключити продукти фірми SolarWinds Orion після кібератаки на неї.

Компанія SolarWinds, що базується в Остіні (США), допомагає своїм клієнтам керувати комп'ютерними мережами та контролювати їх на предмет можливого порушення даних. В своїх продуктах компанія використовує складні системи виявлення, включаючи доступ, події та управління журналами, щоб допомогти IT-командам легше контролювати та забезпечувати кібербезпеку.

SolarWinds продає технологічну продукцію великому переліку організацій критичної інфраструктури, включаючи всі п'ять родів американської армії. За межами США, SolarWinds уклав контракти з Національною службою охорони здоров'я Великобританії, Європейським Парламентом та НАТО, згідно з деталями на своєму веб-сайті. Компанія заявила, що має понад 300 000 клієнтів по всьому світу, включаючи велику кількість організацій з Fortune 500 [20].

Механізми вчинення кібератак постійно вдосконалюються. Починаючи з лютого 2021 року Національний координаційний центр кібербезпеки при Раді національної безпеки та оборони фіксує масовані DDoS атаки на український сегмент Інтернет, переважно на веб-сайти сектору безпеки і оборони.

Зокрема атаки здійснювалися на сайти Служби безпеки України, Ради національної безпеки і оборони України, ресурси інших державних установ та стратегічних підприємств.

Встановлено, що джерелом цих атак були IP-адреси, які належать певним російським мережам обміну трафіком. Фахівці виявили, що зловмисники використовували новий механізм кібератак, який не спостерігався раніше під час подібних інцидентів.

Під час атаки вразливі веб-сервери державних органів інфікуються вірусом, який приховано робить їх елементом бот-мережі, що використовується для DDOS-атак на інші ресурси. При цьому системи безпеки Інтернет-провайдерів визначають скомпрометовані веб-сервери як джерело атак, та починають блокувати їх роботу шляхом автоматичного внесення до "чорних списків". Таким чином, навіть після закінчення фази DDoS атаковані веб-сайти залишаються недоступними для користувачів [21].

Особливо небезпечні тенденції спостерігаються останнім часом у сфері сексуального насильства та експлуатації дітей (Child Sexual Abuse Material – далі CSAM), що посилювалися значним збільшенням кількості людей, які працювали вдома, а також з тим, що діти проводять більше часу в Інтернеті, внаслідок чого збільшується попит на CSAM, що становить значну суспільну загрозу.

Співробітниками Департаменту кіберполіції України у 2020 році затримано 13 педофілів, що вдвічі більше за попередній період – 5.

Крім того діти шкільного віку, як нові, так і вже активні користувачі Інтернету, все частіше стають мішенню різноманітних нових видів онлайн-злочинів. Зокрема, злочинці проникають в онлайн класси, явище, що отримало назву "Zoom-бомбінг", і використовують грумінг і сексуальний шантаж по відношенню до дітей.

Також під час пандемії коронавірусу значно посилилася діяльність в соціальних мережах так званих "груп смерті" таких, як "Синій кит", "Море китів", "Біжи або вмри", "Розбуди мене в 4.20" та інші, які є вкрай небезпечні для дітей та підлітків.

Висновки.

Кіберзлочинність залишається однією з найбільш динамічних форм злочинності, яка постала перед правоохоронними органами усіх розвинутих країн. Хоча сьогодні програми-вимагачі, компрометація ділової електронної пошти та соціальна інженерія є звичними загрозами кіберзлочинності, їх виконання постійно еволюціонує та ускладнює цю злочинну діяльність для виявлення та розслідування. Технічний рівень інструментарію реалізації таких кіберзагроз постійно зростає. Особливе занепокоєння викликає використання для вчинення кібератак технологій штучного інтелекту, що призведе до зростання збитків від кіберзлочинності.

Сталий розвиток інформаційного суспільства залежить від багатьох чинників, до основних з яких слід віднести кіберзахист інформаційних систем та протидію кіберзлочинності.

Зважаючи на подальше зростання кількості кіберінцидентів Європейською Комісією 16 грудня 2020 року була представлена Нова Стратегія кібербезпеки. В документі, зокрема, зазначається, що питання до кібербезпеки є головним стримуючим фактором для використання Інтернет-послуг. Близько двох п’ятих користувачів із ЄС стикалися з проблемами безпеки, і три п’ятих відчувають, що не в змозі захиститися від кіберзлочинності. Третина отримувала шахрайські електронні листи або телефонні дзвінки з проханням ввести особисті дані за останні три роки, але ***83% ніколи не повідомляли про кіберзлочини***. Кожен восьмий бізнес постраждав від кібератак. Понад половина персональних комп’ютерів для бізнесу та споживачів, які інфікувалися шкідливим програмним забезпеченням, інфікуються повторно протягом року. Щорічно через витік даних втрачаються сотні мільйонів записів; середня вартість витоку для одного підприємства зросла до понад 3,5 млн EUR у 2018 році. Вплив кібератаки часто неможливо ізолювати, і він може спричинити ланцюгові реакції в економіці та суспільстві, охоплюючи мільйони людей [22].

Прийняття у 2016 році Стратегії кібербезпеки України стало важливим кроком у запровадженні планування у сфері забезпечення кібербезпеки та протидії кіберзлочинності [23]. Важливим етапом розвитку національної системи кібербезпеки стало прийняття Закону України “Про основні засади забезпечення кібербезпеки України”, який визначив завдання для основних суб’єктів національної системи кібербезпеки [5].

Водночас стан реалізації цієї стратегії був не на належному рівні. Багато запланованих завдань залишилися невиконаними [24]. Тому на заміну Стратегії 2016 року, яка діяла до 2020 року, постала необхідність підготувати новий стратегічний документ.

Відповідно до Рішення Ради національної безпеки і оборони України “Про Стратегію національної безпеки України” від 14.09.20 р., введеним в дію Указом Президента України від 14.09.20 р. № 392/2020, основне завдання розвитку системи кібербезпеки – гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації.

Враховуючи світові тренди в глобальному кіберсередовищі як фактори впливу на розбудову національної системи кібербезпеки, робочою группою при Національному координаційному центрі кібербезпеки Ради національної безпеки і оборони України було розроблено проєкт Стратегії кібербезпеки України на 2021 – 2025 роки, який схвалено 3 березня 2021 року, у якому визначено пріоритети, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Основою для розроблення цього документу стали досвід кращих світових практик; ряд соціологічних опитувань та емпіричних досліджень, які були проведені наприкінці 2020 та на початку 2021 року.

Зокрема відповідно до зазначеного дослідження загальний рівень безпечного функціонування національного кіберпростору респонденти оцінюють на рівні 42 %. Рівень спроможності суб'єктів кібербезпеки протидіяти кіберзагрозам в державному секторі оцінюється як низький (на рівні 36 %), а для приватного сектора ця оцінка становить близько 62 %. При цьому головним недоліком в державному і в приватному секторах вважається їх недостатня забезпеченість технічними засобами.

Проведений аналіз доводить, що ландшафт загроз за останні роки суттєво не змінився і загрозами високого рівня залишаються: шкідливе програмне забезпечення, фішинг та інші прояви соціальної інженерії, DoS/DDoS-атаки та APTатаки. На найближчі 3 роки очікується збільшення ризиків за всіма типами загроз на рівні 41 %.

Отже, на сучасному етапі розвитку інформаційного суспільства слід суттєво посилити спроможності у протидії кіберзлочинності, задля чого необхідно:

провести аудит імплементації в українське законодавство положень Конвенції про кіберзлочинність та завершити цей процес шляхом внесення необхідних змін до законів України;

врегулювати на законодавчому рівні питання щодо електронних доказів, використовуючи кращі практики та підхід країн-членів ЄС з цих питань;

вдосконалити законодавство України, передбачивши внесення необхідних змін з урахуванням сучасних викликів та тенденцій у сфері кібербезпеки;

запровадити механізми ідентифікації суб'єктів електронної комерції у кіберпросторі, забезпечивши внесення відповідних змін до законодавства України;

врегулювати на законодавчому рівні правовий статус криптовалют, визначити правові механізми щодо операцій із криптовалютами та створення ринків;

проводити інші заходи задля створення відкритого, вільного, стабільного і безпечного кіберпростору, де враховуються права і свободи людини, підтримуються соціальний, політичний і економічний розвиток.

Використана література

1. Понад 500 000 облікових записів Zoom продано на форумах хакерів, темної мережі. URL: https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web

2. Словник іншомовних слів ; за ред. члена-кореспондента АН УРСР О.С. Мельничука. Київ: Головна редакція "Українська радянська енциклопедія". 1977. 776 с.

3. Ускладнення COVID-19: пандемія дезінформації і загроза кібербезпеці. URL: https://nv.ua/ukr/biz/experts/pandemiya-covid-19-chas-dlya-kiberatak-i-feykiv-yak-zahistiti-sebe-i-biznes-ostanni-novini-50123696.html

4. The Hidden Costs of Cybercrime. URL: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

5. Науково-практичний коментар Закону України "Про основні засади забезпечення кібербезпеки України"; станом на 01.01.19 р. / М.В. Гуцалюк та ін. ; за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.

6. З початку 2020 року до кіберполіції надійшло понад 25 тисяч звернень щодо Інтернет-шахрайства. URL: https://cyberpolice.gov.ua/news/z-pochatku--roku-do-kiberpolicziyi-nadijshlo-ponad--tysyach-zvernen-shhodo-internet-shaxrajstva-6472

7. Гуцалюк М.В. Шляхи посилення спроможностей правоохоронних та інших державних органів у сфері боротьби з кіберзлочинністю. *Інформація і право*. № 3(34)/2020. С.75-87. URL: http://il.ippi.org.ua/article/view/220997

8. INTERPOL report shows alarming rate of cyberattacks during COVID-19. URL: https://www.interpol.int/News-and-Events/News/2020/COVID-19-crime-INTERPOL-issues-new-guideli nes-for-law-enforcement

9. Як на хвилі коронавірусу спекулянти намагаються збагатитися на eBay, Amazon, OLX, Prom.ua, Rozetka, Tabletki.ua та Liki24.com. URL: https://www.epravda.com.ua/publications/2020/03/19/658264

10. Фішингові атаки від фейкового МОЗ на тему вакцинації зафіксували в Україні. URL: https://www.pravda.com.ua/news/2021/02/12/7283229

11. На Харківщині судитимуть членів злочинної організації за шахрайські схеми оформлення онлайн-кредитів на громадян. URL: https://www.cyberpolice.gov.ua/news/na-xarkivshhyni-sudytymut-chleniv-zlochynnoyi-organizacziyi-za-shaxrajski-sxemy-oformlennya-onlajn-kredy tiv-na-gromadyan-5881

12. North Korean hackers stole more than $300 million to pay for nuclear weapons, says confidential UN report. URL: https://edition.cnn.com/2021/02/08/asia/north-korea-united-nations-report-intl-hnk/index.html

13. CYBERCRIME AND COVID19: Risks and Responses. URL: https://www.unodc.org/documents/Advocacy-Section/UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf

14. US charges three North Koreans over $1.3bn theft. URL: https://www.bbc.com/news/technology-56103921

15. Кіберполіція викрила транснаціональне угруповання хакерів у розповсюдженні найнебезпечнішого в світі комп'ютерного вірусу "EMOTET". URL: https://www.pravda.com.ua/news/2021/01/27/7281395

16. СБУ ліквідувала транснаціональне хакерське угруповання. URL: https://ua.korrespondent.net/ukraine/4328488-sbu-likviduvala-transnatsionalne-khakerske-uhrupovannia

17. Кіберполіція викрила найбільший у світі сервіс для атак на банки. URL: https:// fakty.com.ua/ua/proisshestvija/20210204-kiberpolitsiya-vykryla-najbilshyj-u-sviti-servis-dlya-atak-na-banky

18. Исследование: ущерб от киберпреступности в 2020-м по всему миру составил более 1 триллиона долларов. URL: https://internetua.com/issledovanie-usxerb-ot-kiberprestupnosti-v-2020-m-po-vsemu-miru-sostavil-bolee-1-trilliona-dollarov

19. В Україні з початку року вже майже 14 млн. кіберінцидентів. URL: https://ua.korrespondent.net/ukraine/4321796-v-ukraini-z-pochatku-roku-vzhe-maizhe-14-mln-kiberintsydentiv

20. Suspected Russian Hackers Gained Edge Through Tech Firm Attacks. URL: https://www.bloomberg.com/news/articles/2021-01-29/solarwinds-attackers-hit-strategic-targets-cyber-and-tech-firms

21. У РНБО попередили про новий механізм атак на українську інфраструктуру. URL: https://lb.ua/news/2021/02/22/478317_rnbo_poperedili_pro_noviy_mehanizm.html

22. The EU's Cybersecurity Strategy for the Digital Decade. URL: https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade

23. DR Mykhaylo Gutsalyuk Ukraine's Cybersecurity strategy and ways to implement it. *European Cybersecurity journal*. Volume 2 (2016). The Kosciuszko Institute. Poland. P. 65-69.

24. Гуцалюк М.В. Оцінка реалізації стратегії кібербезпеки України з урахуванням досвіду європейських і світових практик. *Інформація і право*. № 2(29)/2019. С. 90-99.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~