DOI: 10.15421/152033 УДК: 004.49+316.772.5

Валентина Воронкова
Запорізький національний університет Інженерний інститут

Напрями захисту суспільства та особистості у протидії кібезлочинності

Актуальність теми дослідження в тому, що з розвитком комп'ютерних потужностей у цифрову епоху зростає і потенціал людства, розширюються можливості машин, з'являються нові і впливі платформи, до яких залучаються злочинці з кримінального кіберпідпілля, що намагаються використати у своїх цілях технології завтрашнього дня, тому ураган технологічної небезпеки, що насувається, більше не можна ігнорувати. Мета статті – концептуалізація захисту суспільства та особистості у протидії кіберзлочинності, розробка шляхів і заходів спрямованих проти злочинів майбутнього у суспільстві і правове регулювання глобальної кібербезпеки.

Ключові слова: *кіберзлочинність, кібербезпека, кібероборона, хакерські кібероперції, цифрове підпілля, регулювання глобальної кібербезпеки*

Directions for the protection of society and the individual in the fight against cybercrime

Valentyna Voronkova, Engineering Institute of Zaporizhzhia National University

The relevance of the research topic is that with the development of computer power in the digital age, the potential of mankind grows, the capabilities of machines expand, new and influential platforms appear, which involve criminals from the criminal cyber underground trying to use tomorrow's technologies. , so the impending hurricane of impending technological danger can no longer be ignored. The purpose of the article is to conceptualize the protection of society and the individual in the fight against cybercrime, to develop ways and measures to ensure society against the crimes of the future and the legal regulation of global cybersecurity.

Keywords: *cybercrime, cybersecurity, cyber defense, hacker cyber operations, digital underground, regulation of global cybersecurity*

Актуальність теми дослідження в тому, що ми живемо у взаємопов'язаному світі, у якому всі ми є уразливими, так як кіберзлочинність заполонила інформаційний простір. Злочинці розробили цілий арсенал методів для отримання прибутків, надавши перевагу цифровому інтелекту перед людським, і опинилися осередками між реальністю і цифровими даними, що контролюються шахраями, у результаті чого виникла загальна загроза достовірності інформації та її втрати, яка накопичується під час «революції великих даних». Взаємопов'язаність та повсюдність уразливих за своєю суттю комп'ютерних систем свідчить про те, що ураган технологічної небезпеки, що насувається, більше не можна ігнорувати. Звичайно, проблема полягає не в тому, що технології – це суцільне зло, а в тому, що слід розуміти її уразливі місця. Через це весь спектр критично важливих інформаційних інфраструктур, що підтримують життєдіяльність нашого суспільства, перебуває під загрозою, не говорячи вже про ризики від штучного інтелекту та синтетичної біології. Поза всяким сумнівом, наука і технології позитивні для всього людства, однак, щоб впевнено процвітати у поточному столітті, нам доведеться витримати випробування технологічними ризиками, які неминуче створюють прогрес, що породжує потребу у захисті кіберпростору, що є актуальною як ніколи. Розвиток транснаціональної організованої кіберзлочинності. Транснаціональна організована злочинність – це сьогодні величезний бізнес, який заробляє 2 трильйони доларів на рік: гроші надходять від торгівлі наркотиками, крадіжок інтелектуальної власності, торгівлі людьми, дитячої порнографії, викрадення особистих даних, кіберзлочинності, руху людей та контрабандних товарів, отримання доступу до приватних облікових записів поштового сервісу Gmail, доступу до системи паролів, яка до-

зволяла користувачам входити у низку служб Google і успішно зламувати базу даних по всьому світу, які вважалися найвпливовішими компаніями епохи Інтернету. «Ця система була найважливішим об'єктом інтелектуальної власності, яку розробники вважали "коштовним каменем у короні" вихідних кодів компанії» (Гарріс, 2019, с. 199). Компанія неодноразово опинялася під прицілом спритних хакерських компаній, у результаті чого хакери ще у 2010 році викрали текст програми для системи управління паролями, яка дозволяла користувачам одночасно заходити у різні додатки Google. Крадіжка викликала паніку серед вищого керівництва Google – компанії, яка пишається власною системою безпеки користувачів та їхніх персональних даних і яка вибудувала собі репутацію, гарантуючи цю безпеку. Агентство проводить політику купівлі інформації про вразливості і платить за це найвищу ціну, а також проводить наступальні кібероперації, що можуть нанести ураження кіберопераціям. До створення кіберармії підштовхують масштабні шпигунські операції, спрямовані проти оборонних підприємств. Загалом, як вважають експерти, організована злочинність, яка формує сучасні корпоративні структури, створює від 15 до 20 % світового ВВП (Гудмен, 2019). Локальні кримінальні мережі та угрупування, що швидко збираються і підлаштовуються, щоб використати будь-які незаконні можливості і канали для своєї незаконної діяльності, добре структуровані та саморегулюються, створюють клірингові центри (посередників, фінансових організацій, що пропонують різноманітні послуги із взаєморозрахунків), гарантують незаконні продукти або викрадену інформацію. Злочинні корпорації мають онлайн-підручники з усіх найважливіших питань та навичок: від проблем з подоланням фаєрволів до клонування кредитних карток. Злочинці-початківці мають доступ до створених корпораціями онлайн-курсів, де вони навчаються запускати компанії з «фішингу», поширювати спам, а також користуватися заготівками для створення шкідливого програмного забезпечення, засвоюючи ремесло цифрової злочинності та кібершахрайства. У кіберпідпільному світі створені своєрідні «вікіпедії», що містять докладні посилання, розбиті за категоріями – як зламувати всі наявні пристрої, програмне забезпечення та операційні системи. Кіберзлочинці є набагато потужнішими і далекогляднішими, більш успішнішими і технологічно підготовленішими кримінальними командами, які забезпечують себе високими прибутками за відносно малих ризиків. Судові розслідування кіберзлочинів є надзвичайно рідкісними, тому що вироки за ними складають менше тисячної частки відсотка серед усіх кримінальних покарань, які продовжують здійснювати агресивні кібероперації, спрямовані на викрадення інформації, причому найактивніше хакерські контратаки здійснюються у банківській сфері. Розквіт організованої кіберзлочинності. Кримінальні підприємства створюють власні структури, завжди користуються власною юрисдикцією офшорних зон або країн із слабким державним управлінням, нестабільними політичними режимами, які за певну плату ладні закривати очі на нелегальну діяльність кримінальних структур. У межах цих злочинних синдикатів існують відділи праці та управління поставками, керівники відділів, зовнішні консультанти та команди виконавців. Хакери вдосконалюють та демонструють власну майстерність у використанні технологій, продовжуючи постійний пошук нових можливостей, кількість кіберзлочинів зростає, у той час як компанії не мають технічного ресурсу, щоб захистити себе. Існує ринок для кібернайманців, які розробляють і продають шпигунське ПЗ і хакерські інструменти, що не поступаються державним розробкам США кількарічної давності. Шпигунська програма учасників кіберпідпілля, здатна контролювати комп'ютер, копіювати файли та записувати кожне слово, набране користувачем, замаскована під оновлення популярного застосунку iTunes. Технологічні інновації, що виходять з підпільного світу, процвітають, а колективний злочинний інтелект упевнено бере гору над антивірусними компаніями, продавцями технологій безпеки та правоохоронними органами. Збитки від програмного забезпечення. Сьогодні, коли ми стикаємося з фактом поганого стану світового програмного забезпечення, програмісти говорять, немає ідеального програмного забезпечення, оскільки воно буде зламане, яким би воно не було, а користувачі прагнуть мати потужне багатофункціональне програмне забезпечення,

визначаючи безпеку пріоритетом і ключовим компонентом надійних обчислень. Ця проблема зростає у міру того, що все більше і більше пристроїв починають спілкуватись один з одним і всі помилки у ПЗ та дефекти безпеки мають кумулятивний характер в контексті глобальної інформаційної мережі і саме через це 75 % комп'ютерних систем можна зламати за лічені хвилини. Враховуючи, що ПЗ керує глобальною економікою та усіма критичними інфраструктурами, від електрики до телефонних мереж, ми не маємо права гаяти час. Ми маємо допомогти компаніям зрозуміти, що, з огляду на довгострокову перспективу, в їхніх інтересах створювати більш безпечне і стабільне ПЗ, необхідне для нашого технологічного майбутнього і що відмова робити це матиме для них важкі наслідки, тому необхідне правове регулювання нашої глобальної кібербезпеки. Висновок. Через усвідомлення і визнання цих загроз, що несуть технології для всього людства, слід започаткувати зміни, необхідні для зміцнення фундаменту нашого технологічного майбутнього. Необхідно посилення державного контролю у сфері кіберзлочинності, рівень активності якої зростає у мережах, та компаніям необхідно підвищувати стандарти безпеки й гарантувати кібербезпеку. Якими б складними не були технології чи інтернет-сервіси, учасники цифрового підпілля вже напоготові, щоб на власний розсуд використати новомодні засоби та орієнтуватися перш за все на гроші за рахунок більш масштабних, але точно вивірених крадіжок, здатних кинути виклики владі та йти на порушення правил та законів, створюючи зловмисне програмне забезпечення, прагнучи стимулювати інновації та створювати нові напрямки злочинного бізнесу, розробляючи нові види кіберафер, тому держава повинна запобігти хакерським атакам, щоб створити перепони для них. Держава повинна розробити різноманітні технічні, організаційні, освітні рекомендації щодо державної політики, спрямованої на зменшення ризиків, пов'язаних з технологіями, як застосовувати ті чи інші інструменти для отримання максимально можливої користі при мінімізації негативних наслідків, і тільки так ми зможемо витримати випробування прогресом. Для сучасного суспільства й економіки довіра до кіберпростору вкрай важлива, оскільки загроз сьогодні збільшилося, хакери щодня викрадають дані, а держава не в змозі їх захистити, тоді як компанії не мають технічного ресурсу, щоб самостійно захиститися. Сьогодні необхідне посилення державного контролю у сфері захисту суспільства та особистості у протидії кіберзлочинності, щоб спонукати підвищити стандарти безпеки й гарантувати посилення кібероборони та запобігання атакам на критично важливі об'єкти державної інфраструктури. Держава повинна сформувати ефективну концепцію національної безпеки, оприлюднювати інформацію про хакерів і посилювати контроль, щоб захиститися від хакерських злочинних атак. Якщо війни майбутнього будуть продовжуватися, то варто мати і кіберармію.

БІБЛІОГРАФІЧНІ ПОСИЛАННЯ

Гудмен, Марк. (2019). *Злочини майбутнього.* (І. Мазарчук, Я. Машико, Перекл.). Харків: Фабула.

Шейн, Гарріс. (2019). *Війн@ : битви в кіберпросторі.* Київ: Ніка-Центр; Львів: Видавництво Анетти Антоненко.