Міністерство освіти і науки України
Сумський державний університет
Навчально-науковий інститут бізнесу, економіки та менеджменту
Кафедра економічної кібернетики

ВИКЛИКИ КІБЕРБЕЗПЕКИ ІНДУСТРІЇ ФІНАНСОВИХ ПОСЛУГ

Матеріали
наукової онлайн-конференції

(Суми, 07 вересня 2023)

Суми
Сумський державний університет
2023

004.056.5:336(082)
В43

Затверджено Вченою Радою Сумського державного університету (протокол № 2, 14.09.2023)

S62 Виклики кібербезпеки індустрії фінансових послуг: Матеріали наукової онлайн-конференції, Суми, 07 вересня 2023. Збірник матеріалів тез наукової онлайн-конференції / за загальною редакцією доц. Койбічук В.В. – Суми : Сумський державний університет, 2023. – 183 с.

Матеріали наукової онлайн-конференції " Виклики кібербезпеки індустрії фінансових послуг" присвячені пошуку системного вирішення проблем у сфері протидії кібеззагрозам у сфері фінансових послуг, підвищенню рівня кіберзахисту об'єктів критичної інфраструктури.

Видання розраховане на науковців, викладачів, студентів вищих навчальних закладів, аспірантів, докторантів та інших зацікавлених осіб.

004.056.5:336(082)

ЗМІСТ

ПЕРСПЕКТИВИ РОЗВИТКУ ХАКТИВІЗМУ ТА ХАКЕРСЬКИХ АТАК В СФЕРІ ФІНАНСОВИХ ПОСЛУГ: ВИКЛИКИ ТА ШЛЯХИ ПРОТИДІЇ

PROSPECTS FOR THE DEVELOPMENT OF HACKTIVISM AND HACKER ATTACKS IN THE FINANCIAL SERVICES SECTOR: CHALLENGES AND WAYS TO COUNTERACT

Єлизавета Литюга, *студентка*
Сумський державний університет
Валерій Яценко*, к.т.н., доцент*
Сумський державний університет

Тема хакерства та її наслідків для цифрової економіки є вельми значущою, оскільки кількість кіберзлочинів ("взломи" банківських рахунків і кібервандалізм) постійно зростає. Тема хактивізма протягом багатьох років цікавила вчених з усього світу, наприклад, Андерсен Рон у своїх дослідженнях розглядає феномен хактивізму і звертає увагу на його вплив на політичну арену та громадську активність, Макгрегор Річар аналізує роль хакерів і хакерських атак в кібербезпеці, визначає основні типи атак і розглядає стратегії протидії, Менделсон Майкл в своїх дослідженнях зосереджується на етичних аспектах хактивізму та хакерства, досліджує моральні проблеми, пов'язані з цими явищами, Шанмугам Нірмала вивчає вплив хактивізму на фінансовий сектор та аналізує ризики та виклики, які це створює для фінансових установ, Дітон Пітер досліджує політичний хактивізм із застосуванням технологій, зокрема розглядає вплив соціальних мереж на організацію політичних рухів. На жаль, незважаючи на істотне державне фінансування програм кібербезпеки, хакери продовжують завдавати великої шкоди економічній та соціально-політичній діяльності громадян та країни в цілому. Мета даного дослідження – проаналізувати роль хактивізму в контексті фінансових послуг та з'ясувати, які соціальні, політичні та економічні фактори сприяють його розвитку, вивчити типи хакерських атак, які загрожують фінансовому сектору України та визначити їх особливості та наслідки, розглянути перспективи розвитку кібератак та шляхи вирішення цієї проблеми у планетарному масштабі.

Хактивізм – це поєднання понять "хакерство" та "активізм", що означає використання технічних навичок і комп'ютерної експертизи для досягнення політичних, соціальних або етичних цілей. Цей термін походить від словосполучення "хакерський активізм" і відображає зв'язок між хакерськими здібностями та соціальним ангажуванням.

Ще на самому початку функціонування інтернету з'явилися так звані "хакери", які з виробничих, романтичних або ж корисливих міркувань взламували приватні бази даних. Для злому з метою несанкціонованого

проникнення в приватний або корпоративний кіберпростір, хакери використовували широкий діапазон різноманітних комплексних методів програмування та репрограмування. Ці перші хакери, "герої комп'ютерної революції", як їх іменує Стівен Леві, – так звані "білі хакери". Такі "етичні хакери" – це, насамперед, професійні програмісти, які здійснювали взлом даної комп'ютерної системи з метою корекції програм, запобігання кіберзлочинам. Ці ексцентричні ентузіасти кіберпростору використовували термін hack ("зламати"), щоб описати оригінальний спосіб для істотного поліпшення продуктивності комп'ютерних систем. Вони змогли знайти неортодоксальні рішення для найскладніших проблем комп'ютерної техніки. З деякими нюансами до цієї першої хвилі руху хакерів можна віднести Білла Гейтса, Стіва Возняка, Річарда Столлмана і Марка Цукерберга.

Хакерів, по суті своїй кіберзлочинців, які зламують комп'ютерні мережі заради грошей і викрадення конфіденційних даних, ставлячи під загрозу безпеку персональних і корпоративних комп'ютерів, підключених до мережі інтернет, називають "чорними хакерами". Найбільш відома в історії кіберзлочинності група Кевіна Митника (Kevin David Mitnick). Він і його друзі виграли майже мільйон доларів у Лас-Вегасі за допомогою перепрограмування ігрових автоматів. Кевін Митник, незважаючи на віртуозні хакерські техніки злому неймовірно захищених баз даних, був виявлений агентами ФБР, засуджений і покараний. Після звільнення з федеральної в'язниці, в 1998 році, Кевін Митник, "Робін Гуд" інформаційного суспільства, який незаконно проник у комп'ютерні системи багатьох відомих компаній, у мас-медійному хайпі, перетворився з хакера на одного з найзатребуваніших експертів із кібербезпеки у світі.

І, нарешті, існують "сірі хакери", які працюють у морально-етичному інтервалі між "білими" і "чорними" в "сірій зоні" кіберпростору.

Хактивізм, як невидимий кримінальний фронтир, у різних своїх проявах істотно зачіпає моральні (публікація конфіденційної інформації користувачів в інтернеті) і матеріальні (онлайн-шахрайства з номерами кредитних карток і фальшивими чеками, зламані банківські рахунки) інтереси мільйонів громадян. Шляхом численних зломів комп'ютерних мереж, фішинг-атак, "троянських коней" тощо. Кіберзлочинці перетворюють вкрадені ними дані на мільйони доларів. За деякими оцінками, на частку незаконної торгівлі припадає одна п'ята частина світового ВВП. Темі незаконної торгівлі більше уваги приділяє у свої дослідженнях Родрігес М. (Rodriguez et al, 2021).

Проте іноді неможливо зрозуміти мотиви хактивізму. Їхні кібератаки нагадують банальний вандалізм і злісне хуліганство в планетарному масштабі. У листопаді 2008 року комп'ютерний черв'як Conficker (шкідлива програма була написана на Microsoft Visual C++) заразив перший комп'ютер, а вже через місяць Conficker проник у 1,5 мільйона комп'ютерів у 195 країнах. У січні 2009 року хробак влаштувався у восьми мільйонах комп'ютерів. Серед заражених

виявилися комп'ютери банків, телекомунікаційних компаній і деякі урядові комп'ютерні мережі (включно з британським парламентом, французькими та німецькими військовими мережами). Кібератака стала серйозною світовою загрозою. Економічні збитки, завдані Conficker мережевому співтовариству, оцінюється в 9,1 млрд. доларів. В інформаційному суспільстві з'явився новий вид високотехнологічної злочинної діяльності – кіберзлочинність. Сформувався новий антропологічний тип злочинця – кваліфікований програміст, хакер. Формування безпечної цифрової економіки, криптоекономіки супроводжується зростанням кіберзлочинності.

Очевидно, що кіберзлочинність завдає не тільки прямих збитків бізнесу, підприємствам і окремим громадянам. Вона так само безпосередньо впливає на економіку окремих держав. Розглянемо якого роду кіберзагрози можуть становити небезпеку для фінансової сфери України:

Найактуальнішою проблемою звичайно ж є хакерські атаки, спонсоровані державою противником. Цілі кіберзагрози – це порушення стабільного функціонування найбільших фінансових інститутів держави та (або) отримання можливості контролю і маніпулювання її діяльністю для завдання економічної шкоди країні в цілому. Об'єктами кіберзагрози можуть бути центральні банки, фондові біржі, фінансові Data-центри, майнінгові ферми. Особливостями фінансової кіберзагрози є інфраструктурна підтримка атак за допомогою військової інфраструктури ініціатора атаки, масштабність і системність характеру атаки. Прикладами хакерських команд можуть бути Equation Group, Lazarus.

Фінансові диверсії на фінансовому ринку, ініційовані найбільшими фінансовими корпораціями. Цілі кіберзагрози – формування на фондових біржах панічних настроїв, зниження вартості або виключення з котирувального листа окремих бізнесів шляхом інформаційних вкидань (фейк-новин, інформації, яка ганьбить ділову репутацію компанії та її топ-менеджерів), організація витоку інсайдерської інформації, хакерських атак на активи компанії (організація штучних збоїв або аварій). Об'єктами кіберзагрози можуть бути акції найбільших бізнесів, а також втручання в процеси участі окремих бізнесів у міжнародних інвестиційних програмах і проєктах (переважно – сфера військово-промислового комплексу та енергетики). Хакери штучно погіршують рейтингові позиції найбільших бізнесів держави, знижують їхню інвестиційну привабливість, відсторонюють державу від міжнародних інвестиційних проєктів і програм. Прикладами хакерських команд є Cobalt, BlackEnergy, Idustroyer, HAVEX.

Конструювання і запуск соціоінженерних троянів. Доступ до критичної банківської інфраструктури хакери отримують через менш захищені приватні та публічні акаунти, які перебувають поза контуром основної банківської інфраструктури, а отже, мають вищу вразливість. Головною метою

є отримання через акаунти приватних і публічних осіб - клієнтів банків доступу до всієї банківської інфраструктури та здійснення операцій з її виведення з ладу, а також викрадення персональних даних клієнтів та їхніх грошових коштів. Об'єктами кіберзагрози є програмні модулі соціальних мереж, акаунти в інтернет-банкінгу, файлові менеджери власників банківських карток тощо. Приклади хакерських команд: APT10, WINNITI, Regin, REXAN.

Інфраструктурні атаки на IoT-мережі (інтернет речей). Через злам облікового запису або елементів фінансової інфраструктури хакери отримують можливість впливати на фізичну інфраструктуру, що знаходиться за контурами банку, а також конструювати соціальний хаос або техногенні події. Цілі кіберзагрози – отримання контролю над бізнес-процесами фінансово-промислових екосистем, а також заподіяння їм прямої та непрямої шкоди внаслідок порушення стабільності їхньої роботи, а також розкрадання або маніпулювання приватними даними користувачів таких екосистем. Об'єкти кіберзагрози: системи дистанційної оплати платних автошляхів, сервіси дистанційної медицини, системи "розумного будинку" і "безлюдного офісу", інтегровані в банківську бізнес-модель. Приклади хакерських команд: Fancy Bears, Lizard Squad, Anonymous.

Як випливає з наведеного аналізу, Україна наразі перебуває під впливом серйозних ризиків, зумовлених кіберзагрозами, орієнтованими на ослаблення її економіки та посилення соціально-економічних заворушень і напруженості. З метою ефективної боротьби з кіберзлочинністю важлива подальша консолідація зусиль і органів влади, і бізнес-спільноти, і просунутих в IT-технологіях користувачів. І не окремо взятої країни, а всіх держав, і особливо передових у сфері інформаційних комунікаційних технологій. Для боротьби із загрозою кіберзлочинності, яка, безумовно, зростатиме з подальшим розширенням сфери використання інформаційних технологій, надаючи все більші можливості для протиправної діяльності як індивідуумам, так і злочинним групам, необхідна постійна міжнародна співпраця. Контролювати кіберзлочинність і боротися з нею на рівні окремої держави практично неможливо. Наразі у формуванні міжнародної стратегії боротьби з кіберзлочинністю задіяні понад сорок країн світу, і процес цей обіцяє бути довгим. Ухвалення міжнародних норм і стандартів має супроводжуватися внесенням змін до національного законодавства держав. Координація зусиль держав необхідна для забезпечення швидкого реагування на розвиток комп'ютерних технологій і затвердження відповідних норм.

Список літератури

1. Rodriguez, M. (2021). The Role of Hacktivism in Shaping Financial Services Policies. International Journal of Information Security, 20(5), 587-604. doi:10.1007/s10207-021-00503-2