Татомир Ірина. Кібербезпека університетів як спосіб протидії фішинговому шахрайству. *Економічний дискурс*. 2020. Випуск 1. С. 59-67.
DOI: https://doi.org/10.36742/2410-0919-2020-1-7

УДК 336.717.1:330
JEL Classification A12, A22, I24, I28, M53

Татомир Ірина
к.е.н., доцент кафедри економіки та менеджменту
Дрогобицький державний педагогічний університет імені Івана Франка
м. Дрогобич, Україна
E-mail: Tatomur@gmail.com
ORCID: 0000-0002-3274-7083

КІБЕРБЕЗПЕКА УНІВЕРСИТЕТІВ ЯК СПОСІБ ПРОТИДІЇ ФІШИНГОВОМУ ШАХРАЙСТВУ

Анотація

Вступ. *В умовах швидкого впровадження комп'ютерних та мережевих технологій заклади освіти приділяють недостатню увагу застосуванню заходів безпеки з метою забезпечення конфіденційності, цілісності та доступності даних внаслідок чого стають жертвою кібер-атак.*

Методи. *У процесі написання статті були використані: методи узагальнення, аналогії та логічного аналізу для визначення і структурування мотивів здійснення фішингових-атак, способів їх виявлення й попередження; статистичного аналізу даних – для побудови хронологічної вибірки найбільших світових кібер-інцидентів та визначення економічних втрат, яких зазнали заклади освіти; графічний метод – для наочного представлення результатів; абстрагування і узагальнення – для вироблення рекомендацій, які б сприяли зменшенню числа кібер-афер.*

Результати. *У статті показано, яку роль відіграє кібербезпека для протидії фішинговим-аферам в освітній сфері. Визначено та стуктуровано мотиви здійснення фішингових-атак, а також способи їх виявлення і попередження. Дано оцінку «списаному фішингу», «фішингу підводнику» та «китобійному фішингу» як найбільш небезпечним видам шахрайства, які орієнтуються як на малих, так і на великих гравців в інформаційному ланцюжку будь-якої освітньої інституції. Проведено аналітичний огляд ринку освітніх послуг та зроблено хронологічну вибірку найбільших кібер-інцидентів, які мали місце у період 2010-2019 рр. Описано суми економічних втрат, яких зазнали коледжі, науково-дослідні установи та провідні університети світу. Доведено, що найбільше піддалися атаці зловмисників заклади освіти США та Великобританії, дещо їм поступаються Канада та країни Азійсько-тихоокеанського регіону. Встановлено, що освіта стала топ-індустрією за кількістю виявлених троянських програм на пристроях, що належать навчальним закладам та другою у списку серед числа тих, які найчастіше постраждали від викупу. Запропоновано ряд заходів, що сприяли б зменшенню числа кібер-інцидентів.*

Перспективи. *Отримані результати мають бути враховані при формуванні стратегії розвитку закладів освіти, а також при підвищенні рівня обізнаності представників академічної спільноти у кібербезпеці.*

Ключові слова: *фішинг, кібербезпека, кібер-сталкери, інсайдерська загроза, руткіт, бекдор.*

Вступ.

У світі ескалації загроз, кібератак та шпіонажу працівники університету та студентство все частіше піддаються впливу більш досконалих форм соціальної інженерії, які використовують кіберзлочинці, щоб знати поведінку та вподобання потенційної жертви в Інтернеті. Саме тому, університети несуть більшу відповідальність за несанкціоновані спроби доступу до цифрових академічних даних, постійно переглядаючи основну структуру своїх комп'ютерних мереж та їх

відкритий стиль доступу.

Аналіз останніх досліджень і публікацій.

Аналіз останніх досліджень і публікацій показав, що сучасні заклади освіти генерують найбільшу кількість даних, ніж будь-коли в історії, що потребує убезпечення їх конфіденційності. Відсутність ресурсів та уваги до кібербезпеки в школах й університетах має стати причиною серйозного занепокоєння серед стейкхолдерів та освітньої галузі в цілому.

Так, у праці Betsy Foresman йдеться про те, що студенти є однією з найбільш бажаних категорій споживачів, дані про яких є найціннішими для отримання і подальшого продажу [1]. Проведене компанією Cisco у 2018 р. дослідження з кіберзагрози у вищій освіті, засвідчило, що 58% респондентів зазнали принаймі одного порушення безпеки. Окрім юридичних наслідків та шкоди репутації установи, 51% заявили, що напади коштують їх коледжу чи університету понад 500 тис. дол. США, а Інтернет-речі та персональні пристрої є найскладнішими сферами захисту [2].

Мета.

Мета дослідження полягає у визначенні мотивів та аналізі сучасних тенденцій фішингових-афер в освітній сфері й виробленні рекомендацій щодо захисту закладів освіти від шахрайських дій.

Методологія дослідження.

У процесі написання статті були використані: методи узагальнення, аналогії та логічного аналізу для визначення і структурування мотивів здійснення фішингових-атак, способів їх виявлення й попередження; статистичного аналізу даних – для побудови хронологічної вибірки найбільших світових кібер-інцидентів та визначення економічних втрат, яких зазнали заклади освіти; графічний метод – для наочного представлення результатів; абстрагування і узагальнення – для вироблення рекомендацій, які б сприяли зменшенню числа кібер-афер.

Результати. *Фішинг* **–** це замаскована спроба обману веб-користувачів для отримання доступу до чутливих систем даних, доставки та розповсюдження шкідливих програм у освітніх мережах з метою нанесення зловмисної шкоди та отримання економічного зиску.

Фішинг-атаки на академічну спільноту з кожним роком примножуються в експоненціальному масштабі і стають більш складнішими. Експерти з кібербезпеки в освіті відмічають [3; 4; 5], що найбільші ризики можуть бути пов'язані з безпекою мережі та використанням різного роду програмного забезпечення, залежність викладачів від якого є одним із найважливіших ризиків порушення даних.

Тепер, мережі є незамінними для доступу до матеріалів та ресурсів аудиторій, адже охоплюють велику кількість ноутбуків та планшетів, оскільки більше студентів і викладачів використовують хмарні сервіси для підключення до роботи між будинком й аудиторією. Нажаль, такі новітні освітні технологічні рішення, як: голосові асистенти, додатки для відстеження відвідуваності та перевірки робіт студентів, системи прокторингу, які покликані допомагати особам, що навчаються, все частіше, через низький рівень кібер-стійкості й відсутність «культури інформованої згоди», забирають від них можливості, піддаючись кібер-нападам.

Типовими їх прикладами є різні методи соціальної інженерії: зловмисне програмне забезпечення (віруси, трояни, шпигунські програми та ботові файли), бекдори, кейлоггери, руткіт, спам, підроблені домени, клоновані веб-сайти університетів, введення в оману щодо безпеки сайту шляхом відображення піктограм блокування як знак того, що вміст сайту є буцімто безпечним. Будь-яка фішинг-атака може досягти успіху, лише якщо цільова жертва натискає посилання. Після відкриття облікових даних фішери отримують ті самі права доступу, що й користувач, завантажуючи потрібні їм документи.

Експерти з кібербезпеки [6; 7] виокремлюють декілька способів виявлення фішинг-афер перш ніж вони завдадуть шкоди комп'ютерній системі користувача:

- *електронні листи, які містять недоречну граматику, пунктуацію чи нелогічний потік вмісту*, швидше за все, є шахрайськими;
- *листи, що містять гіперпосилання на підозрілі веб-сайти з невпізнанними URL-адресами*. Найбільш небезпечними слід вважати URL-адреси, які закінчуються альтернативними доменними іменами замість .com або .org. Скорочувані назви адресата фішери використовують, щоб обходити фільтри електронної пошти та обманювати користувачів;
- *повідомлення, які вимагають уточнення особистої інформації* логіну, паролю чи просять клікнути на посилання, щоб змінити пароль або ввести дані картки, слід вважати фішинговими, адже університети жодного разу не затребують такого роду інформацію;
- *зміст, який викликає занепокоєння*. Мова йде про повідомлення про злам облікових записів, переповнення їх вмісту, заблокування акаунту, повідомлення про необхідність термінової сплати-рахунку-фактури за відповідні послуги, фальсифіковані листи від адміністрації закладу освіти, які змушують їх отримувача швидше реагувати, виконуючи вказівки зловмисників щодо кліків на відповідні посилання для повторної активації облікового запису з метою встановлення зловмисного програмного забезпечення;
- *виявлення у вкладеннях небезпечних фішинг-посилань*. Усі фішинг-листи містять посилання, але це не завжди в електронній пошті. Щоб уникнути виявлення фільтрами захисту електронної пошти, хакери включатимуть фішинг-посилання у вкладення, наприклад, PDF або Word doc, а не тіло електронної пошти. А оскільки технологія фільтрації сканує вкладення на наявність шкідливих програм, а не посилань, електронна пошта буде виглядати чисто. Сам електронний лист, схоже, буде від законного відправника з проханням відкрити вкладення та натиснути на посилання, щоб переглянути чи оновити інформацію;
- *розміщення шкідливих програм у коді найбільш часто відвідуваними користувачами веб-сайтів*. Якщо студенти чи працівники університету заходять на такий сайт з університетського комп'ютера вся мережа може піддатися атаці (скажімо зараженню вірусом);
- розсилання хакерами *повідомлень про очікуваний термін*. Наприклад, про термін подачі заявок на грант, що втрачає чинність, відстежуючи активність представників академічної спільноти в Інтернеті. Зазвичай такі електронні листи просять негайно виконати дію або втратити значні переваги.

Більшою популярністю починає користуватися «списаний фішинг», коли електронні повідомлення відправляються від надійного відправника, з метою переконати адресата розкрити конфіденційну інформацію, переходити на шкідливе посилання або переказувати кошти. Другим за рівнем небезпеки є «фішинг-підводник», який орієнтується на конкретного користувача і передбачає повне дослідження його соціального профілю.

Інтернет полювання на особливу групу жертв здійснює «Фішинг-китобійник». Він орієнтується виключно на великих гравців в інформаційному ланцюжку будь-якої освітньої інституції відомих як «кити» в термінах фішингу (наприклад, адміністрація ЗВО). Однак навіть найбільш обережні кампуси, що використовують сучасні програми безпеки бази, вразливі до атак з боку складних мереж ботнетів, які працюють на базі штучного інтелекту та управляються досвідченими хакерами.

Основними **мотивами** здійснення фішинг-афер слід вважати:

1. *Шпіонаж через проникнення в систему відеоспостереження.*

2. *Фінансова вигода*. Зловмисники вдаються до пошуку нових маршрутів отримання швидкої готівки. Найпоширенішим видом вчинених шахрайств є крадіжка фінансової ідентичності, яка відбувається за умови використання злодієм даних особи для відкриття нових кредитних ліній чи доступу до існуючих фінансових рахунків. Завдяки університетам та коледжам, які отримують чимало внесків від благодійників та займаються великою кількістю фінансових стягнень зі студентів, що перераховують кошти через Інтернет-портал, вони є головною мішенню для кіберзлочинців, які перенаправляють платежі на кримінальні рахунки. Типовим прикладом є хакерські-атаки на

американські університети у період 2017-2019 рр., коли зловмисники заволоділи сплаченими коштами за навчання шляхом підміни рахунку адресата.

3. *Викрадення таких персональних даних та академічних записів,* як: імена, паспортні дані, номери телефонів та соціального страхування, медичні дані, результати навчання. Цей вид інформації може бути цінним для кіберзлочинців, які потенційно могли б передати дану інформацію третій особі. Такий інцидент мав місце у Берклі, коли під час зловмисної хакерської атаки було ввійдено в академічні бази даних та викрадено більш як 160 тис. медичних записів [8].

4. *Монетизація викрадених даних шляхом продажу чи викупу конфіденційної інформації.* В «темних закутках» Інтернет-простору існують, так звані, веб-сайти Dark Web, на яких продають облікові дані закладів вищої освіти. За 8 років сканування «темної павутини» дослідники ID Agent виявили 13 930 176 адрес електронної пошти та паролів, що належать викладачам, співробітникам, студентам та випускникам у ЗВО США, які стають доступними для кіберзлочинців на темних веб-сайтах. Майже 80% із 14 млн даних було відкрито дослідниками ID Agent у 2017 р. [9]. Крім даних електронної пошти зловмисники викрадають і номери банківських рахунків. Аналітики ринку кіберзлочинів підрахували, що вартість інформації за однією кредитною карткою оцінюється у 10 дол. США [10], а оскільки злочинці викрадають дані престижних університетів, кількість студентів, яких перевищує сотні тисяч осіб, то і відповідно економічний зиск є високим.

5. Привабливою мішенню для шпіонажу є *університетські дослідження та інші інтелектуальні активи*. Швидше за всіх у перехрестя кібератак потрапляють дослідницькі університети світу, викрадені дані з яких хакери продають іншим урядам, включаючи Іран, Росію та Китай. Британський Daily Telegraph [11] показав, що іранські хакери у 2018 р. продавали дослідження щодо ядерної енергентики, шифрування комп'ютерних файлів та захисту кібербезпеки через WhatsApp й Telegram, які були викрадені у провідних британських університетів, включаючи Оксфорд та Кембридж. На декількох веб-сайтах Farsi було надано безкоштовний доступ до наукових робіт, включаючи пропозицію крадіжок університетських досліджень на замовлення. Найбільш ціненими для хакерів є дослідження Нобелівських лауреатів, сервери яких стають потенційними мішенями.

6. *Нанесення кібер-сталкерами шкоди репутації* шляхом дискредитації університету через Інтернет-мережі. Типовими її прикладами може бути створення сайтів-близнюків орієнтованих на «університет-жертву».

7. *Інсайдерська загроза*, яка має на меті маніпулювати системою оцінок або сприяти організованій кібератаці.

8. Злочинці також можуть використовувати підроблені посвідчення особи, щоб скористатися знижками, пропонованими студентам та викладачам на програмне забезпечення та різні інші продукти.

9. *Отримання викупу* шляхом шифрування та блокування ключових локальних системних файлів.

Перші глобальні кібератаки на заклади освіти були здійснені у 2014 р., коли Іранський корпус ісламської революційної гвардії (IRGC) зламав комп'ютерні системи приблизно 320 університетів у 22 країнах. 144 жертви – американські університети, зловмисники викрали дослідження, які коштували університетам приблизно 3,4 млрд дол. США [12]. В 2015 у секторі освіти було зафіксовано порушення 1,35 мільйона особистих даних та зареєстровано понад 500 випадків порушення безпеки [13]. Друга хвиля атак припала на 2018 р., коли понад 300 університетів у всьому світі стали жертвами організованої кібератаки, яка поставила під загрозу 31 терабайт даних інтелектуальної власності на загальну суму понад 3 млрд дол. США.

Освіта стала топ-індустрією за кількістю виявлених троянських програм та другою у списку серед числа тих, які найчастіше постраждали від викупу. Експертами було підраховано, що троянські віруси становлять 25% усіх шкідливих програм виявлених у всьому світі на пристроях, що належать навчальним закладам. Ця тенденція продовжилася в першій половині 2019 року, коли

іранські хакери націлилися на 380 університетів з понад 30 країн і, ймовірно, залишатиметься загрозою для навчальних закладів у наступні роки [14; 15]. На рис. 1 показано розміри втрат, яких зазнали заклади освіти світу від нападів зловмисників.

ЕАВ, провідний консорціум з вищої освіти, провів у 2019 р. дослідження, в якому дійшов висновку, що середнє порушення даних для університету в США коштує закладу приблизно 245 дол. за запис. Це не включає будь-які регуляторні стягнення, які також можуть бути понесені [16]. Нині, на жаль, не всі університети достатню увагу приділяють системі захисту персональних даних, виділяючи зі свого бюджету кошти на кібербезпеку.

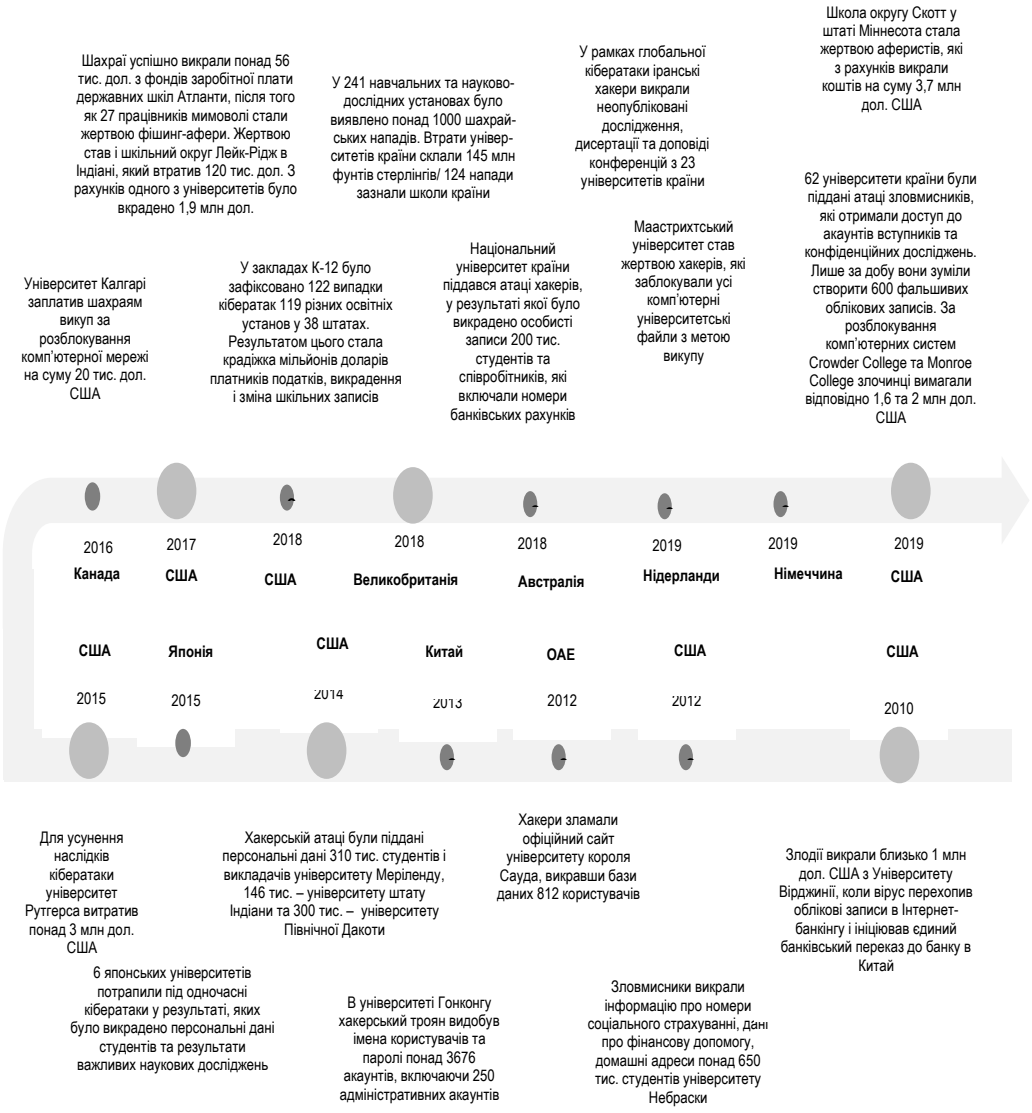

Рис. 1. Хронологічна вибірка найбільших кібератак на заклади освіти*

**Джерело: складено автором на основі: [17; 18; 19; 20; 21].*

Примітка. *Заштрихованими кругами позначено розмір фінансових та академічних втрат університетів та НДІ від кібер-афер. Чим більшою є величина фігури, тим втрати є, відповідно, вищими і навпаки.*

Ситуація, що склалася вимагає внесення швидких змін в цифрову політику, систему доступу та навчання університетів, які повинні покращити лінію захисту в галузі кібербезпеки. Доцільним стане вжиття ряду заходів:

1. Прийняття на державному рівні відповідних законодавчих ініціатив з питань кібербезпеки освітніх систем. Типовим прикладом можуть слугувати законопроекти уряду США: закон «Грамм-Ліч-Блілі» (Gramm-Leach-Bliley Act), який змушує захищати інформацію про фінансову допомогу студентам. Закон про права на сімейні права та конфіденційність (FERPA) захищає конфіденційність записів про освіту студентів, тоді як Закон про переносність та підзвітність медичного страхування (HIPAA) – медичні записи студентів. Ряд антифішингових законів були розроблені і урядом Великобританії. Закон про шахрайство був прийнятий в 2006 році, він передбачає позбавлення волі строком до 10 років за фішинг.

2. Ініціювання урядами створення центрів досліджень та освіти з кібербезпеки, віртуальних лабораторій, які надають тренінги з кібербезпеки, використовуючи привабливі хмарні навчальні середовища, та пропонують слухачам досвід з перших рук за прийнятною ціновою політикою з метою посилення рівня захисту своїх цифрових активів.

3. Об'єднання університетів з метою підтримання та просування кращих практик з питань кібербезпеки. Таку ініціативу на початку 2018 р. підтримали 40 університетів Канади, ініціювавши проект порівняльного забезпечення кібербезпеки університетів по всій країні.

4. Періодичне ознайомлення представників академічної спільноти зі змінами, які відбуваються у кібер-світі, що спонукатиме їх вивчати умови дотримання здорової «гігієни кібербезпеки». Обов'язковою нормою для студентів, професорсько-викладацького складу та адміністрації навчальних закладів має стати проходження спеціальних курсів з кібербезпеки. Типовим прикладом може слугувати досвід університету Карнегі Меллона [22], який представив програму із складною імітацією фішингу, що дозволяє IT-адміністраторам оцінити сприйнятливість користувачів до афер соціальних інженерій на основі електронної пошти. Коли користувачі потрапляють під імітаційну атаку, система не просто вказує на помилку в режимі реального часу, а й розповідає користувачам, як уникнути подібних атак у майбутньому. Ігрове навчання включене в основну навчальну програму, яку зобов'язують пройти усіх студентів-першокурсників.

5. Окремі університети починають вдаватися до послуг IT-фірм з кібербезпеки для контролю їх мережевого трафіку, своєчасного виявлення і блокування фішинг-нападів та запобігання витоку конфіденційних даних. Доцільним стане придбання університетами ліцензій для учасників освітнього процесу, які передбачають підписання щорічних угод про технічне обслуговування як це є у випадку з ліцензією Swivel Secure University, Swivel Secure, яка забезпечує мережеву безпеку як для адміністративного корпусу, так і викладачів та студентів незалежно від того, які через цифрові пристрої вони під'єднуються до мережі [23].

6. Переміщення інформаційної системи студентів та академічних даних у хмару з як мінімум двофакторною аутентифікацією в обліковому записі. Правильний хмарний хостинг збільшить ізоляцію даних та захистить їх від викупних програм та інших кіберзагроз. Він також повинен запропонувати додаткове резервне сховище резервного веб-сайту для швидкого відновлення, якщо трапляється якась катастрофічна подія [24].

7. Для зменшення ризику необхідно впроваджувати технічний контроль, наприклад, розширений фільтр спаму, який шукає підозрілі посилання та неперевірені вкладення, блокуючи переважну більшість фішингових електронних листів та зупиняючи їх доставку кінцевим користувачам, а також антифішинг панелі інструментів, нові антивірусні рішення з оновленнями безпеки, блокатори випливаючих вікон, оновлені веб-браузери, що підтримують всі сучасні функції безпеки, багатофакторна автентифікацію для доступу до облікових записів.

Висновки і перспективи.

Отже, як бачимо з вище викладеного матеріалу, заклади освіти все частіше стають ціллю нападників, які порушують право представників академічної спільноти на конфіденційність та безпеку персональних даних. З кожним роком карта кібер-інцидентів розростається, охоплюючи нові регіони та міста, а кількість уразливих навчальних закладів до звичних прийомів злому збільшується.

Пропоновані заходи протидії фішинговим кібер-злочинам мали б сприяти убезпеченню та зменшенню впливу їх негативних наслідків. Подальші ініціативи повинні включати зміцнення навчальних програм для освітян з кібербезпеки, а також пропаганду науково-дослідних можливостей (та розробок) й обізнаність у кібербезпеці.

Список використаних джерел

1. Foresman, B.. University tech presents growing privacy concern for students, educators. EDSCOOP. 2019. Dec. 30. URL : https://edscoop.com/university-tech-presents-growing-privacy-concern-educators/ (дата звернення: 05.02.2020).

2. *Cisco 2018. Annual Cybersecurity Report*. Cisco Security Research. *2018*. 68 p.

3. 2018 Education Cybersecurity Report Security. Scorecard. 2018. 13 p.

4. Cyber security and universities: managing the risk. Universities UK. 2013. 22 p.

5. Jang-Jaccard J., Nepal S. A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences. 2014. August. Vol. 80. Issue 5. P. 973–993 URL : https://doi.org/10.1016/j.jcss.2014.02.005. (дата звернення: 05.02.2020).

6. Best Practices Phishing Protection for Small & Medium Size Business. DuoCircle LLC. 2020. 123 p.

7. Alghamdi H. Can Phishing Education Enable Users To Recognize Phishing Attacks? Masters dissertation, Technological University Dublin. 2017. 74 p. https://doi.org/10.21427/D7DK8T. (дата звернення: 05.02.2020).

8. Why Cybersecurity needs to be a Priority for the Education. Sector Swivel Secure. 2020. URL : https://swivelsecure.com/solutions/education/why-cybersecurity-needs-to-be-a-priority-for-the-education-sector/. (дата звернення: 05.02.2020).

9. Cyber criminals, college credentials, and the dark web a security challenge facing U.S. university communities. Report. Digital Citizens Alliance. 2017. 23 p.

10. Coleman L., Purcell B. Data Breaches in Higher Education. Journal of Business Cases and Applications. 2015. Volume 15. P. 1–7.

11. Iranian hackers selling stolen academic research from top British universities online. Daily Telegraph. 2018. URL : https://www.telegraph.co.uk/technology/2018/09/14/iranian-hackers-sell-stolen-academic-research-top-british-universities/. (дата звернення: 05.02.2020).

12. German Universities Hit With Cyber-Attack by Iran Iran Focus. NEWS&ANALISIS. 2018. April 24. URL : https://www.iranfocus.com/en/index.php?option= com_content&view=article&id=32666:german-universities-hit-with-cyber-attack-by-iran&catid=9 &Itemid=114. (дата звернення: 05.02.2020).

13. Cyber Crime in Higher Education Center for Responsible Enterprise and Trade (CREATe.org). 2016. March 17. URL : https://create.org/news/cyber-crime-higher-education/. (дата звернення: 05.02.2020).

14. Williams Sh. Education prime target for cyber attacks, report finds. SecurityBrief. 2019. Oct 22. URL : https://securitybrief.eu/story/education-prime-target-for-cyber-attacks-report-finds. (дата звернення: 05.02.2020).

15. Cyber attacks on campus. AXA XL. 2019. August 20. URL : https://axaxl.com/fast-fast-forward/articles/cyber-attacks-on-campus. (дата звернення: 05.02.2020).

16. Cyber. Aware Lourdes University. 2019. URL : https://www.lourdes.edu/campus-life/information-technology/cyberaware/. (дата звернення: 05.02.2020).

17. How safe is your data? New report on cyber security in higher education. EDUCAUSE Publications. 2019. April 4. URL : https://www.hepi.ac.uk/2019/04/04/universities-high-value-data-can-be-obtained-by-hackers-in-under-two-hours/. (дата звернення: 05.02.2020).

18. Zurkus K. Education Sector Ranks Last in Total Cybersecurity Safety. Security Boulevard. 2018. December 19. URL : https://securityboulevard.com/2018/12/education-sector-ranks-last-in-total-cybersecurity-safety/. (дата звернення: 05.02.2020).

19. University of Calgary paid $20K in ransomware attack. CBC News. 2016. Jun 07. URL :

https://www.cbc.ca/news/canada/calgary/university-calgary-ransomware-cyberattack-1.3620979. (дата звернення: 05.02.2020).

20. DeGeurin M. Hackers targeted the admissions and enrollment departments at 62 universities and created thousands of fake student accounts. Insider. 2019. Jul 18. URL : https://www.insider.com/hackers-target-62-us-universities-through-flaw-in-enrollment-software-2019-7. (дата звернення: 05.02.2020).

21. Academic institutions are under cyber attack. *University Business.* 2015. September 9. URL : https://universitybusiness.com/academic-institutions-are-under-cyber-attack/. (дата звернення: 05.02.2020).

22. Sandle T. Q&A: Huge increase in cyber attacks against colleges reported. Digital journal. 2019. Oct 8. URL : http://www.digitaljournal.com/tech-and-science/technology/q-a-huge-increase-in-cyber-attacks-against-colleges-reported/article/559367. (дата звернення: 05.02.2020).

23. Татомир І.Л. Вища освіта як імператив розвитку інформаційного суспільства : монографія. Дрогобич: РВВ ДДПУ імені Івана Франка, 2020. 400 с.

24. Protecting students from cyber attack. University Business. 2019. 1st February. URL : https://universitybusiness.co.uk/Blog/protecting-students-from-cyber-attack/. (дата звернення: 05.02.2020).

Статтю отримано: 10.02.2020 / Рецензування 15.03.2020 / Прийнято до друку: 20.03.2020

Irina Tatomur
Ph.D. (in Economics), Associate Professor
Department of Theoretical and Applied Economy
Drohobych State Pedagogical University after Ivan Franko
Drohobych, Ukraine
E-mail: Tatomur@gmail.com
ORCID: 0000-0002-3274-7083

UNIVERSITY CYBER SECURITY AS A METHOD FOR ANTI-FISHING FRAUD

Abstract

Introduction. *With the rapid adoption of computer and networking technologies, educational institutions pay insufficient attention to the implementation of security measures to ensure the confidentiality, integrity and accessibility of data, and thus fall prey to cyber-attacks.*

Methods. *The following methods were used in the process of writing the article: methods of generalization, analogy and logical analysis to determine and structure the motives for phishing attacks, ways to detect and prevent them; statistical analysis of data – to build a chronological sample of the world's largest cyber incidents and determine the economic losses suffered by educational institutions; graphical method – for visual presentation of results; abstraction and generalization – to make recommendations that would help reduce the number of cyber scams.*

Results. *The article shows what role cyber security plays in counteracting phishing scams in the educational field. The motives for the implementation of phishing attacks, as well as methods for detecting and preventing them, have been identified and regulated. The following notions as "phishing", "submarine" and "whaling" are evaluated as the most dangerous types of fraud, targeting both small and large players in the information chain of any educational institution. An analytical review of the educational services market was conducted and a chronological sampling of the largest cyber incidents that occurred in the period 2010-2019 was made. The economic losses incurred by colleges, research institutions and leading universities in the world were described. It has been proven that the US and UK educational institutions have been the most attacked by attackers, somewhat inferior to Canada and countries in the Asia-Pacific region. It is found that education has become the top industry in terms of the number of Trojans detected on devices belonging to educational institutions and the second most listed among the most affected by the ransomware. A number of measures have been proposed to help reduce the number of cyber incidents.*

Discussion. *The obtained results should be taken into account when formulating a strategy for the development of educational institutions, as well as raising the level of awareness of the representatives of the academic community in cybersecurity.*

Keywords: *phishing, cyber security, cyber stalkers, insider threat, rootkit, backdoor.*

References

1. Foresman, B. (2019). University tech presents growing privacy concern for students, educators. *EDSCOOP*. *edscoop.com*. Retrivied from https://edscoop.com/university-tech-presents-growing-privacy-concern-

educators/

2. *Cisco 2018 Annual Cybersecurity Report. (2018)*. Cisco Security Research.
3. 2018 Education Cybersecurity Report Security. (2018). Scorecard.
4. Cyber security and universities: managing the risk. (2013). Universities UK.
5. *Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences,* 80, 5*, 973–993. doi.org. Retrivied from https://doi.org/10.1016/j.jcss.2014.02.005*
6. Best Practices Phishing Protection for Small & Medium Size Business (2020). DuoCircle LLC.
7. Alghamdi, H. (2017). Can Phishing Education Enable Users To Recognize Phishing Attacks? Masters dissertation, Technological University Dublin. *doi.org.* Retrivied from https://doi.org/10.21427/D7DK8T.
8. Why Cybersecurity needs to be a Priority for the Education Sector. (2020). Swivel Secure. *swivelsecure.com*. Retrivied from https://swivelsecure.com/solutions/education/why-cybersecurity-needs-to-be-a-priority-for-the-education-sector/
9. Cyber criminals, college credentials, and the dark web a security challenge facing U.S. university communities. Report. (2017). Digital Citizens Alliance.
1. Coleman, L., & Purcell, B. (2015). Data Breaches in Higher Education. Journal of Business Cases and Applications, *15,* 1–7. [in Eng.]
10. Iranian hackers selling stolen academic research from top British universities online. (2018). Daily Telegraph*. www.telegraph.co.uk.* Retrivied from https://www.telegraph.co.uk/technology/2018/09/14/iranian-hackers-sell-stolen-academic-research-top-british-universities/
11. German Universities Hit With Cyber-Attack by Iran. (2018). Iran Focus NEWS&ANALISIS. *www.iranfocus.com*. Retrivied from https://www.iranfocus.com/en/index.php?option=com_content&view=article&id=32666:german-universities-hit-with-cyber-attack-by-iran&catid=9 &Itemid=114.
12. Cyber Crime in Higher Education. (2016). Center for Responsible Enterprise And Trade (CREATe.org). *create.org*. Retrivied from https://create.org/news/cyber-crime-higher-education/
13. Williams, Sh. Education prime target for cyber attacks, report finds. (2019). SecurityBrief. *securitybrief.eu*. Retrivied from https://securitybrief.eu/story/education-prime-target-for-cyber-attacks-report-finds.
14. Cyber attacks on campus. (2019). AXA XL. *axaxl.com*. Retrivied from https://axaxl.com/fast-fast-forward/articles/cyber-attacks-on-campus.
15. CyberAware. (2019). Lourdes University. *www.lourdes.edu*. Retrivied from https://www.lourdes.edu/campus-life/information-technology/cyberaware/
16. How safe is your data? New report on cyber security in higher education. (2019). EDUCAUSE Publications. *www.hepi.ac.uk.* Retrivied from https://www.hepi.ac.uk/2019/04/04/universities-high-value-data-can-be-obtained-by-hackers-in-under-two-hours/
17. Zurkus, K. (2018). Education Sector Ranks Last in Total Cybersecurity Safety. Security Boulevard. *securityboulevard.com*. Retrivied from https://securityboulevard.com/2018/12/education-sector-ranks-last-in-total-cybersecurity-safety/
18. University of Calgary paid $20K in ransomware attack. (2016). CBC News. *www.cbc.ca*. Retrivied from https://www.cbc.ca/news/canada/calgary/university-calgary-ransomware-cyberattack-1.3620979.
19. DeGeurin, M. (2019). Hackers targeted the admissions and enrollment departments at 62 universities and created thousands of fake student accounts. Insider. *www.insider.com*. Retrivied from https://www.insider.com/hackers-target-62-us-universities-through-flaw-in-enrollment-software-2019-7.
20. Academic institutions are under cyber attack. (2015). *University Business. universitybusiness.com.* Retrivied from https://universitybusiness.com/academic-institutions-are-under-cyber-attack/
21. Sandle, T. (2019). Q&A: Huge increase in cyber attacks against colleges reported. Digital journal. *www.digitaljournal.com*. Retrivied from http://www.digitaljournal.com/tech-and-science/technology/q-a-huge-increase-in-cyber-attacks-against-colleges-reported/article/559367
22. Tatomur, I.L. (2020). *Vyshcha osvita yak imperatyv rozvytku informatsiynoho suspilstva* [Higher education as an imperative for the development of the information society]. Drohobych, Ukraine : RVV of the Ivan Franko State Duma.
23. Protecting students from cyber attack (2019). University Business. *universitybusiness.co.uk.* Retrivied from : https://universitybusiness.co.uk/Blog/protecting-students-from-cyber-attack/

Received: 02.10.2020 / Review 03.15.2020 / Accepted 03.20.2020