– Нікому не повідомляти свої особисті дані, навіть якщо спілкування йдеться з довіреною особою;

– Не завантажувати підозрілі чи неперевірені файли.

У випадку, якщо вас намагалися ввести в оману, потрібно поскаржитися Адміністрації платформи та спробувати максимально довго затримувати співбесідою шахрая, щоб користувач-скамер витратив більше часу на розмову з вами та втратив пильність. Завдяки затримці часу, Адміністрація швидше знайде та заблокує підозрілий акаунт.

Якщо дотримуватись усіх правил, то є великий шанс, що скам-процес для користувача платформи пройде без незаконних витрат та не відтвориться знову.

Список використовуваних джерел:

1. itua.info [Електронний ресурс] – Режим доступу до ресурсу: https://itua.info/software/27672.html.

Ключові слова: Скам, акаунт, користувач, Steam.
Ключевые слова: Скам, аккаунт, пользователь, Steam.
Keywords: Scam, account, user, Steam.

Науковий керівник: *д. ф-м. н., д.ю.н., професор Василенко М. Д.*

Стратієвська Аліна Олександрівна
Національний університет «Одеська юридична академія»
студентка 2-го курсу, факультету кібербезпеки
та інформаційних технологій

БІЛИЙ ХАКІНГ ЯК НОВИЙ ІНСТИТУТ ДЛЯ ПІДТРИМКИ КІБЕРБЕЗПЕКИ

Актуальність розглядаємої теми полягає у висвітленні інформації по білий хакінг як засіб підтримки високого рівня кібербезпеки з метою формування сучасного інформаційного громадського суспільства. Збільшення рівня кіберзлочинності, реалізації засобів та методів кібертероризму у багатьох сучас-

них конфліктах, потребує формування структури дотримання безпеки України у кіберпросторі.

Варто вказати, що хакер це та людина, яка намагається одержати заборонений доступ до комп'ютерних мереж та програм, зазвичай з метою отримання конфіденційної інформації. Хакерів також називають досвідченими комп'ютерними програмістами або користувачами, які зламують програми.

Щодо білого хакінгу, то це один із міжнародних сучасних трендів кібербезпеки. Все це проявляється через власну раціональність та ефективність. Наприклад, такі глобальні системи як Google, Facebook, Amazon – розпочали свої власні програми зі взаємної роботи з чесними хакерами. Щодо України, то дану практику мають тільки конкретні приватні фірми.

Сьогодні в умовах швидкого вдосконалення ІТ-технологій на міжнародній арені, проблеми кібербезпеки та кіберзахисту відносяться не лише до органів державної влади, однак і до всіх громадян нашої країни, котрі мають смартфони або користуються сучасним комп'ютером чи планшетом. Сьогодні ринок інтернет послуг та сервісів у галузі кібербезпеки має бути загально відкритим для приватного сектору в межах державно-приватного партнерства.

Яскравим прикладом сучасної боротьби з кіберзлочинністю, є те, що органи досудового розслідування визначили, що «Єдина судова інформаційно-телекомунікаційна система» не відповідає сучасним вимогам Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», постанови КМУ від 12.04.2002 № 522 «Про затвердження порядку підключення до глобальних мереж передачі даних», НД ТЗІ 2.5–010–03 «Вимоги до захисту інформації WEB сторінки від несанкціонованого доступу», прийнятих наказом ДСТСЗІ СБ України від 02.04.2003 № 33, та має дуже багато чутливих місць для несанкціонованого доступу [1; 2]. Оскільки правові визначені вимоги безпеки роботи інформаційно-телекомунікаційних систем та ЄСІТС не були прийняті відповідно до сучасних вимог, це призвело до блокування, знищення

та виведення з ладу у період з 24.12.2018 по 25.01.2019 судової системи України.

Проте, на сьогоднішній день з функціонування сучасних технологій та комп'ютерних систем кількість різновидів хакерів збільшилась. У ситуації коли хакер стає на неправову дорогу – він стає кракером (або як ще називають зломщиком, людиною, котра вривається в чужу комп'ютерну систему, через електронні мережі, визначає паролі та офіційні ключі комп'ютерних систем або іншим чином навмисно ламає комп'ютерну безпеку [3]. Проте, функціонування всіх хакерів та кракерів є схожим за методами і завданнями їх діяльності, однак існує серйозна розбіжність у меті їх функціонування. Сучасні хакери застосовують уразливість комп'ютерних структур для реалізації нападів на дані системи. Головна мета і завдання хакера – використати комп'ютер для підбору слабких точок в структурі безпеки та проінформувати розробників даної структури про це, а також визначити конкретні передумови та вимоги відносно рівня безпеки інформаційних структур [4].

Тому, у багатьох державах здійснюється легалізація праці хакерів. Їх усе частіше називають «білими» хакерами, які працюють на великі організації та державні органи влади. Наприклад, Британська секретна служба здійснює підбір на роботу молодих хакерів-самоучок, оформивши, як повідомляє інтернет-видання «Die Welt», інтернет-змагання, переможець якого має шанс одержати посаду в секретній службі. Функціонування даних осіб, котрі отримали роботу, полягає у цілеспрямованому встановленню дій, які хоч і мають ознаки протиправного діяння, однак учасники, котрі їх вчиняють, не підлягатимуть кримінальному переслідуванню та покаранню. Тому, залишається абсолютна більшість потенційних спеціалістів, котрі не залучаються до схожої законної роботи та прагнуть заробити гроші на цій неправовій діяльності.

Отже, на сьогодні визначену особу молодого хакера описує наявність активної та цілеспрямованої життєвої позиції, оригінальність думок та власної поведінки, акуратність, уважність,

зосередженість уваги на баченні результату, передбаченні та керівництвом управлінні процесами, їх дії дуже обережні та супроводжуються відмінним маскуванням.

Список використаних джерел:

1. Закон України Про захист інформації в інформаційно-телекомунікаційних системах від 094.07.2020 року. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.
2. Постанова КМУ від 12.04.2002 року № 522 Про затвердження Порядку підключення до глобальних мереж передачі даних. URL: https://zakon.rada.gov.ua/laws/show/522–2002-п#Text.
3. Анализ представлений о мотивации хакеров: [Електронний ресурс]. – Режим доступу: http://www.mytests.ru /articles/353.
4. Біленчук П. Д. Криміналістична характеристика способів скоєння комп'ютерних злочинів / П. Д. Біленчук // Наукові розробки академії по вдосконаленню практичної діяльності та підготовки кадрів органів внутрішніх справ. – К., 2017. – 271 с.

Ключові слова: хакінг, хакер, кракери, мережа, дані, кібербезпека.

Ключевие слова: хакинг, хакер, кракеры, сеть, данные, кибербезопасность.

Keywords: hacking, hacker, crackers, network, data, cybersecurity.

Науковий керівник: *доцент Задерейко О. В.*

Титиевский Виталий Олегович
Национальный университет «Одесская юридическая академия»
студент 1-го курса факультета кибербезопасности и информационных технологий

ПЕРСПЕКТИВЫ РАЗВИТИЯ DATA SCIENCE В УКРАИНЕ

Информационные технологии развиваются с невероятной скоростью, лишь за последние 20 лет всё изменилось до неузнаваемости. Ничто не стоит на месте, прямо сейчас мы на пороге «IT-революции». С каждым годом появляется всё больше и больше новейших технологий, наук, которые