Одеський державний університет внутрішніх справ
Кафедра кібербезпеки та інформаційного забезпечення
Факультет підготовки фахівців для підрозділів кримінальної поліції

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

International scientific-practical conference
"Cybersecurity in Ukraine: Legal and Organization Issues"

Матеріали
Міжнародної науково-практичної конференції
19 листопада 2021 року

Одеса 2021

Рекомендовано до друку рішенням кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ
(протокол № від грудня 2021 року)

Всі матеріали надані в авторській редакції та виражають
персональну позицію учасника конференції

Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук.
К38 практ. конф., м. Одеса, 26 листопада 2020 р. Одеса : ОДУВС, 2021. _____ с.
ISBN 678-717-7020

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на міжнародну науково-практичну конференцію «Кібербезпека в Україні: правові та організаційні питання», яка відбулася на базі кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ 19 листопада 2021 року.

У матеріалах конференції приділено увагу актуальним теоретичним та практичним проблемам забезпечення інформаційної безпеки в Україні. Висвітлюється широкий спектр питань, пов'язаних з удосконаленням правового регулювання та адміністративно-правового забезпечення кібербезпеки в Україні. Розглянуто використання інформаційних систем, технологій та інформаційно-аналітична діяльність правоохоронних підрозділів у боротьбі з злочинністю та надано обґрунтовані рекомендації щодо вдосконалення підготовки персоналу для боротьби з кіберзлочинністю в Україні.

Матеріали всеукраїнської науково-практичної конференції адресовано вченим, працівникам правоохоронних органів, аспірантам (ад'юнктам), слухачам магістратури, студентам та курсантам вищих навчальних закладів.

ПЕРСПЕКТИВИ РОЗВИТКУ КІБЕРЗАГРОЗ ТА БОРОТЬБИ З НИМИ

Пядишев В.Г.
професор кафедри кібербезпеки та інформаційного забезпечення ОДУВС
д. ю. н., доцент

Прийдешні успіхи інформаційних технологій обіцяють фантастичні можливості у подальшій інформатизації суспільства, що забезпечує стрімке піднесення продуктивних сил, від чого не зможе відмовитися жодне суспільство. Проте зворотний бік цієї блискучої медалі – кіберзлочинність – загрожує суспільству небувалими досі економічними втратами та нестабільністю, протистояння яким вимагає цілковитої концентрації економічних, інтелектуальних та інших можливостей суспільства. Яким же видається науковцям подальший розвиток сфери кібербезпеки?

1. Які загрози кібербезпеці залишаться проблемою?

Загрози, пов'язані з віддаленою роботою та розосередженням працівників. Найбільш очевидна проблема кібербезпеки в 2021 пов'язана з віддаленою роботою. Оскільки багато вимог COVID-19 діють досі, віддалена робота (і пов'язані з нею кібер-ризики) залишаються такими, що превалюють. Зловмисники шукають уразливі або неправильно налаштовані системи, що підключаються до Інтернету – завдання стало набагато простішим після того, як компанії почали заохочувати віддалену роботу через побоювання пандемії. Проблема полягає у тому, що ми більше не можемо припускати, що корпоративні ресурси захищені системою безпеки периметру; нам потрібно прийняти модель нульової довіри та припустити, що корпоративні ресурси та незахищені пристрої використовують один і той же простір і повинні бути захищені відповідним чином. Але і кіберзлочинці також почали використовувати у своїх інтересах розподілених віддалених працівників [1, с. 7].

Кібератаки підвищеної цільової спрямованості. Коли в силу вимог, зумовлених COVID-19, майже всі люди були прив'язані до домівок, деякі особи витратили час, що вивільнився, на дослідження нових цілей для кібер-атак. Через зростаючу економіку кіберзлочинності як послуг (cyber-crime-as-a-service – CaaS) кібер-зловмисники тепер можуть орендувати або купувати інструменти для атаки. Це вивільнило злочинцям час для дослідження та стратегічної орієнтації на компанії, які з більшою ймовірністю заплатять викуп або іншим чином забезпечать кращу окупність злочинних інвестицій. [2, с. 5].

Зловживання легальним програмним забезпеченням та інструментами з відкритим вихідним кодом. Інструменти подвійного призначення постійно підтримуються і розробляються законними співтовариствами, які займаються тестуванням на проникнення, і, таким чином, доводять свою ефективність щодо безлічі складних атак, на розробку та тестування яких в іншому випадку знадобилися б роки. Декілька недавніх витоків основних шкідливих програм, на розробку яких знадобилися роки та мільйони доларів, довели, що стандартні інструменти часто більш рентабельні та їх легше приховати у шумі мережевої активності [3, с. 3].

Поточні кампанії з дезінформації. Широке поширення сайтів та додатків соціальних мереж надало користувачам можливість доступу до різноманітного контенту, але вони також спростили зловмисникам можливість використовувати цю потребу в інформації. Ці суб'єкти маніпулюють контентом, зображеннями та відео для досягнення своїх політичних цілей. Дипфейки, боти в соціальних мережах та інші методи часто використовуються для поширення хибної інформації чи іншого впливу на думку [4, с. 7].

2. Які основні тенденції кібербезпеки?

У міру того, як 2021 рік добігає кінця, з'являється все більше тенденцій і потенційних загроз, за якими компанії повинні стежити, незалежно від розміру чи галузі.

Кіберзлочинність як послуга (CaaS). Економіка кіберзлочинності як послуги надає накопичені знання та інструменти тисяч хакерів та кіберзлочинців окремому зловмиснику. Це дозволяє недосвідченим хакерам швидко проводити складні атаки. Торгові майданчики CaaS продовжують працювати, незважаючи на кілька серйозних спроб з боку правоохоронних органів, оскільки зловмисники адаптують свою тактику та методи, щоб залишатися непоміченими.

Автоматизація шкідливого ПЗ. Атаки шкідливого ПЗ стають все більш автоматизованими, що є продовженням недавньої тенденції, що змусила галузь кібербезпеки надолужувати втрачене. Фахівці з безпеки тепер мають справу не з хакерами-одинаками, які перевіряють свої навички за допомогою складних атак. Тепер хакери можуть використовувати машини для автоматизації дій з кіберзлочинності, що дозволяє виконувати тисячі атак на день. Атаки програм-здирників стають настільки поширеними, що вони більше не потрапляють у новини [5, с.4].

Поліморфне шкідливе ПЗ. Все більша кількість варіантів шкідливих програм тепер містять поліморфні характеристики, що означає, що вони постійно змінюють свої властивості, що ідентифікуються, щоб краще ховатися від служб безпеки і загальних методів виявлення. Елемент коду, який містять багато пропозицій CaaS, може змінюватися, щоб залишатися нерозпізнаним [6, с. 7].

Складність судового переслідування кіберзлочинів. Незважаючи на те, що дедалі більше країн надає пріоритет кібербезпеці, відсутність відповідних даних про злочинні дії, що здійснюються в Інтернеті, може створити труднощі правоохоронним органам у переслідуванні кіберзлочинців. Нестача професіоналів у галузі кібербезпеки також посилює цю проблему, ускладнюючи проактивне виявлення кіберзагроз [7, с. 897.].

3. Майбутнє кібербезпеки та виявлення загроз

Можна виділити кілька тем щодо майбутнього кібербезпеки [8, с. 6]. По-перше, велика увага приділятиметься запобіганню та забезпеченню готовності. Необхідне планування реагування на інциденти безпеки або витоку даних. Посібники щодо забезпечення готовності до інцидентів та реагування на них, ймовірно, стануть більш звичайним явищем. Навчання співробітників всіх рівнях знизить роль людської помилки.

У міру того, як проблеми нормативного регулювання стають дедалі нагальнішими, першочерговим завданням стане забезпечення того, щоб програми кібербезпеки були достатньо надійними, щоб пройти перевірку під час аудитів або оцінок відповідності.

У міру того, як атаки продовжують розвиватися, необхідно створити міцну основу для правильних звичок та передових методів кібербезпеки.

Витративши час на створення цієї базової лінії, можна налаштувати бізнес на стійкий успіх у міру виникнення змін та появи нових загроз – хоч би якими вони були.

Висновки

Боротьба з кіберзлочинністю надалі буде ще більш гострою та ресурсомісткою, оскільки, з одного боку, інформаційні технології, зокрема штучний інтелект, з кожним днем пропонують все більш привабливі можливості для інформатизації суспільства, від яких неможливо відмовитися, з іншого – паралельно з цим зростають можливості кіберзлочинців зі зловживання новими потужними можливостями у корисливих цілях, а також з метою дестабілізації суспільства, по-третє – боротьба з цими проявами злочинності вимагає застосування дедалі більш дорогих і складних в опануванні технічних засобів.

Література:

1. Milne A. What is the future of cyber security? *Field Effect* 01.02.2021. URL: https://fieldeffect.com/blog/what-is-the-future-of-cyber-security/ [accessed 12 November 2021].

2. Balita-Centeno L. What Is Cybercrime as a Service? *Make Use Of*. Apr 25, 2021. URL: https://www.makeuseof.com/what-is-cybercrime-as-a-service/ [accessed 12 November 2021].
1. 3. Bernhard M. Open-source software: freedom form ethics. Engineering and Technology. April 20, 2021. URL: https://eandt.theiet.org/content/articles/2021/04/open-source-software-freedom-from-ethics/ [accessed 12 November 2021].
3. Combatting targeted disinformation campaigns. Public-provete analytic exchange program. A whole-of-society issue. October 2019. URL: https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf [accessed 12 November 2021].
4. Rickard J. Automated malware analysis and reverse engineering with SOAR. Swimlane Mar 14, 2019. URL: https://swimlane.com/blog/using-soar-for-automated-malware-analysis
5. Polymorphic Malware — Real Life Transformers. *Lastline* Jan 30, 2018: site. URL: https://www.lastline.com/blog/polymorphic-malware-real-life-transformers/ [accessed 12 November 2021].
6. Šepec M. Slovenian Criminal Code and Modern Criminal Law Approach to Computer-related Fraud. *International Journal of Cyber Criminology Vol 6 Issue 2 July - December 2012* C. 897. URL: https://www.cybercrimejournal.com/Mihasepec2012julyijcc.pdf [accessed 12 November 2021].
7. Germain J.M. The Future of Cybersecurity in 2021 and Beyond. *Tech News World*. February 16, 2021. URL: https://www.technewsworld.com/story/the-future-of-cybersecurity-in-2021-and-beyond-87018.html [accessed 12 November 2021].

Миронець О. М.
ІНФОРМАЦІЙНА БЕЗПЕКА ОСІБ З ІНТЕҐРОВАНИМИ ІМПЛАНТАТАМИ (ІМПЛАНТАМИ) 36
Kozhanenko Y.M., Myronets O.M.
CONCERNING CYBER SECURITY IN CIVIL AVIATION 38
Шиян Ю.В., Миронець О.М.
ОСНОВНІ ПРИНЦИПИ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ 39
Demchyshyn Y.V., Myronets O.M.
CONCERNING CYBER SECURITY IN UKRAINE 41

СЕКЦІЯ 3. ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ В БОРОТЬБІ ЗІ ЗЛОЧИННІСТЮ

Lamberg Kari
ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN THE SERVICE OF LAW ENFORCEMENT 42
Пядишев В.Г.
ПЕРСПЕКТИВИ РОЗВИТКУ КІБЕРЗАГРОЗ ТА БОРОТЬБИ З НИМИ 44
Міхальський Я.В., Пишна А.Г.
ДЕЯКІ ПИТАННЯ НАДАННЯ ІНФОРМАЦІЇ ПРО ЗАРЕЄСТРОВАНІ ТРАНСПОРТНІ ЗАСОБИ, ЇХ ВЛАСНИКІВ ТА НАЛЕЖНИХ КОРИСТУВАЧІВ ПІД ЧАС АДМІНІСТРАТИВНО-ЮРИСДИКЦІЙНОЇ ДІЯЛЬНОСТІ У СФЕРІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДОРОЖНЬОГО РУХУ 46
Жогов В.С.,
ЦИФРОВІ ТЕХНОЛОГІЇ, ЩО ВИКОРИСТОВУЮТЬСЯ В СФЕРІ ПОПЕРЕДЖЕННЯ ПРАВОПОРУШЕНЬ (НА ПРИКЛАДІ АПАРАТНО-ПРОГРАМНОГО КОМПЛЕКСУ «БЕЗПЕЧНЕ МІСТО») 48
Найдун Ю. О., Прокопов С.О.
ПРОТИДІЯ КІБЕРБУЛІНГУ ТА КІБЕРГРУМІНГУ В УКРАЇНІ 50
Балтовский О.А., Сіфоров О.І., Макарова І.Й.
ЗАГАЛЬНИЙ ПІДХІД ДО ОПИСУ СКЛАДНИХ СИСТЕМ УПРАВЛІННЯ 51
Сіфоров О.І, Гонтаренко Н.В.
«ВИХОВАТЕЛЬ БЕЗПЕКИ» – ДІЄВИЙ МЕХАНІЗМ ПРОТИДІЇ КІБЕРБУЛІНГУ 54
Кудінов В.А.
ЗАГАЛЬНИЙ ПОРЯДОК ПОБУДОВИ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІЙ СИСТЕМІ «ІНФОРМАЦІЙНИЙ ПОРТАЛ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ» 56
Слободянюк А.В., Форос Г.В.,
ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ В БОРОТЬБІ ІЗ КІБЕРЗЛОЧИННІСТЮ 58
Балтовский О.А., Мільчев А.І.,
ОЦІНКА ДАНИХ ТА ІНФОРМАЦІЇ АНАЛІТИЧНИМИ ПІДРОЗДІЛАМИ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ ДЛЯ ЗДІЙСНЕННЯ ПРОГНОЗУВАННЯ РИЗИКІВ НА СУХОПУТНІЙ ДІЛЯНЦІ ДЕРЖАВНОГО КОРДОНУ 60
Плешко Е.А., Коновець В.І.
ПРОБЛЕМА КІБЕРІНЦИДЕНТІВ У МОРСЬКИЙ СФЕРІ 63
Поліщук О. А., Мирошниченко В. О.
СУЧАСНІ НАПРЯМКИ РОЗВИТКУ ВЕБ-ТЕХНОЛОГІЙ 64
Ігнатушко Ю. І.
ВИКОРИСТАННЯ ІНФОРМАЦІЙНОЇ ПІДСИСТЕМИ "CUSTODY RECORDS" У БОРОТЬБІ ЗІ ЗЛОЧИННІСТЮ 65