Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Наукове товариство молодих вчених, аспірантів і студентів

ВСЕУКРАЇНСЬКА
НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

м. Одеса

29 листопада 2019 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
НАУКОВЕ ТОВАРИСТВО МОЛОДИХ ВЧЕНИХ,
АСПІРАНТІВ ТА СТУДЕНТІВ

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ
Всеукраїнської науково-практичної конференції

29 листопада 2019 року

Одеса
2019

УДК 004.056(063)
К38

Друкується за наказом ректора
Національного університету «Одеська юридична академія»
В. Є. Загороднього
(наказ №2410-62 від 2 жовтня 2019 року)

Відповідальний редактор – в.о. декана факультету кібербезпеки та інформацініних технологій , доцент О. В. Дикий .

Укладачі:
Кузьма Яна Іванівна – диспетчер деканату факультету кібербезпеки та інформацій них технологій .
Стоянова Тетяна Федорівна – диспетчер деканату факультету кібербезпеки та інформацій них технологій .
Пастернак Юрій Юрій ович – студент 3 курсу факультету кібербезпеки та інформацій них технологій .

Кібербезпека в сучасному світі: матеріали всеукраїнської науково-практичної конференції (м. Одеса, 29 листопада 2019 р.) / за ред. О.В. Дикого ; уклад.: Я.І. Кузьма, Т.Ф. Стоянова, Ю.Ю. Пастернак. – Одеса: Видавничий дім «Гельветика», 2019.–332 с.

ISBN 978-966-916-949-5

У збірнику містяться матеріали доповідей , присвячених актуальним проблемам кібербезпеки в сучасному світі.
Подані матеріали конференції відповідають сучасним тенденціям розвитку кібербезпеки в Україні та можуть бути корисним и як у навчальному процесі, так і при проведенні наукових досліджень студентами та молодими вченими, а також для практичних працівників у зазначеній сфері

УДК 004.056(063)

ISBN 978-966-916-949-5

Трофименко О. Г.

Національний університет «Одеська юридична академія», доцент кафедри інформаційних технологій , кандидат технічних наук, доцент

НАУКОВО-ТЕХНІЧНІ НАПРЯМИ КОНСТРУЮВАННЯ ЕФЕКТИВНОЇ СИСТЕМИ КІБЕРЗАХИСТУ

За умов стрімкого зростання кіберризиків і кіберзагроз Україна має шукати нові шляхи у нарощуванні кібернетичного потенціалу і захисту критично важливих інформаційних інфраструктур. Важливу роль у рамках комплексної протидії кіберзагрозам відіграють саме науково-технічні питання, позаяк саме їхнє успішне вирішення сприятиме реалізації автоматичного моніторингу інформаційного простору і формуванню механізму випереджального реагування на динамічні змінення, що відбуваються у кіберпросторі.

Нині критично важливі інфраструктурні компанії відстають у підготовці своїх операційних можливостей для протистояння кібератакам. Це робить їх легкою здобиччю для політично мотивованих нападників. Такі рішення, як цифрові підписи та шифрування, доступні для надійних пристроїв ідентифікації, можуть допомогти вирішити цю проблему.

Організаціям доцільно фінансувати та впроваджувати проривні технології автоматизованого захисту, які підтримуватимуть автоматизовані можливості управління та розширену поведінкову аналітику. Прикладами цього можуть бути технології штучного інтелекту для аналізу біометричних ідентифікаційних даних, складні алгоритми машинного навчання, здатні створювати профіль типової поведінки користувача, визначати незвичні закономірності діяльності та виявляти потенційні загрози в режимі реального часу, перш ніж зловмисники матимуть можливість реалізувати їх. Завдяки автоматичній ідентифікації підозрілих даних, увесь процес дотримання безпеки стане більш ефективним, а сама кібербезпека позбавиться потреби в кропіткому ручному огляді журналу даних. Досвід показує [2], що інвестиції у кібербезпеку окупаються і навіть дають своєрідні дивіденди, позаяк дозволяють уникнути неминучої шкоди і наслідків, завдяки чому організації виходять у бізнес-лідери, а завчасні витрати є нижчими, ніж активне інвестування після атак або злочинних дій .

З масовим розповсюдженням технології інтернету речей , переходом у хмарні сховища даних, формуванням обліку FinTech, зокрема цифрових та криптовалют, криптобірж, електронних виборів та «розумних контрактів», для зниження небезпечних вразливостей треба ретельно захищати метадані від можливого викрадення унаслідок зловмисних атак.

Згідно з останніми дослідженнями [1], відсоток комп'ютерів, заражених шкідливими програмами, в Україні один з найвищих у світі і складає 28,7%, тобто кожний третій комп'ютер інфіковани шкідливими програмами. За таких умов вкрай важливим є обов'язкове використання комплексу програмних і апаратних засобів, які б дозволили забезпечити прийнятний рівень захищеності інфраструктури, а саме: ефективне надійне антивірусне програмне забезпечення, системи запобігання вторгнень, міжмережеві екрани,

модулі контролю пристроїв і доступу до інтернету, системи шифрування даних, керування роботою мобільних пристроїв, засоби для захисту поштових серверів і систем колективної роботи тощо. Регулярне тестування на проникнення і перевірка конфігурацій (своїми силами або за допомогою зовнішніх організацій) дозволять виявити помилки в конфігураціях до того, як хакери віднай дуть доступ до управління сервером або комп'ютером користувача.

Нові покоління програмно-апаратного забезпечення повинні бути оснащені сильнішими та зручнішими вбудованими засобами захисту. Слід підвищувати рівень безпеки комп'ютерних мереж, які використовуються для роботи з секретними даними.

Потрібні координація і переорієнтація наукових досліджень і розробок у сфері комп'ютерної безпеки, в області вдосконалення інформацій них технологій , використання математичних методів багатовимірного аналізу даних, розробленні технологій комплексного захисту апаратних і програмних платформ, технологій виявлення ознак кібернетичного нападу з використанням активних і пасивних методів та датчиків спостереження, створення систем контролю, які визначатимуть факт скоординованого широкомасштабного нападу і формуватимуть ранні попередження про можливий напад і локалізацію джерела нападу [3].

Приділяти увагу треба розвитку безпечної і повсюдної електронної ідентифікації (eID), що полегшить транскордонне використання онлай н-послуг та створить умови для інтеграції України у світовий електронний інформацій ний простір. Оскільки най гострішим питанням надання електронних послуг провай дерами різних сфер на сьогодні є питання захисту персональних даних споживачів таких послуг, слід посилити контроль за дотриманням вимог законодавства [4] щодо унеможливлення доступу зловмисників до конфіденцій них даних споживачів [5] та забезпечення анонімності при еЮ за рахунок впровадження новітніх технічно-програмних рішень реалізації електронних транзакцій .

Для захисту цифрових даних і послуг провай дери цифрових послуг повинні впроваджувати технології з дотримання вимог кібербезпеки та стандартів інформацій ної безпеки. Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) як компетентний орган контролю у сфері боротьби з кіберзлочинністю має здій снювати нагляд за державними і приватними постачальниками цифрових послуг щодо дотримання вимог кібербезпеки. З метою регулярного моніторингу заходів безпеки оператори основних послуг мусять регулярно надавати докази ефективного впровадження політики інформацій ної безпеки (наприклад, результати аудиту та звітну документацію).

З огляду на сучасні суспільно-політичні та інформацій ні виклики визначення науково-технічних напрямів конструювання ефективної системи кіберзахисту у рамках комплексної протидії кіберзагрозам сприятиме розробленню ефективного механізму протидії загрозам у кібернетичній сфері, а також запровадженню контрзаходів, спрямованих на мінімізацію вразливості систем зв'язку.

Список використаних джерел:

1. Moody R. Which countries have the worst (and best) cybersecurity? URL: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/ (дата звернення: 10.10.2019).
2. Впровадження європей ської кібербезпеки: загальний огляд. ISACA. URL: https://www.isaca.org/Knowledge-Center/Research/Documents/European-Cybersecurity-Implementation-Overview_res_Ukr_1215.pdf (дата звернення: 10.10.2019).
3. Трофименко О.Г. Моніторинг стану кібербезпеки в Україні. Правове життя сучасної України: матер, міжнар. наук.-практ. конф. (17 травня 2019 р.). Т. 1, Одеса: Видавничий дім «Гельветика», 2019, с. 642-646.
4. Трофименко О.Г. Законодавча база забезпечення кібербезпеки держави. Кібербезпека в Україні: правові та організацій ні питання: м атер. II всеукр. наук.-практ. конф. (17 листопада 2017 р.). Одеса: ОД УВС. С. Б5-56.
5. Задерей ко 0., Логінова Н., Троянський 0., Трофименко 0. Проблемні а спекти забезпечення конфіденцій ності цифрового медіаконтенту. За хист інформації і безпека інформацій них систем: матер. VI міжнар. I EEE наук.-техн. конф. (1-2 червня 2017 р.). Львів, 2017. С. 148-149.

Наукове видання

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ Всеукраїнської науково-практичної конференції

29 листопада 2019 року, м. Одеса

Верстка – О. С. Данильченко

Підписано до друку 7.10.2019. Формат 60x84/16. Папір офсетний . Гарнітура Cambria. Цифровий друк. Умовно-друк. арк. 19,30. Тираж 150. Замовлення № 1119-229. Ціна договірна. Віддруковано з готового оригінал-макета.

Видавництво і друкарня – Видавничий дім «Гельветика» 65101, Україна, м. Одеса, вул. Інглезі, 6/1 Тел.: +38 (095) 934 48 28, +38 (097) 723 06 08 E-mail: mailbox@helvetica.com.ua Свідоцтво суб'єкта видавничої справи ДК № 6424 від 04.10.2018 р.