ОДЕСЬКИЙ ДЕРЖАВНИЙ
УНІВЕРСИТЕТ ВНУТРІШНІХ
СПРАВ

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

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

Матеріали
Міжнародної науково-практичної конференції
23 листопада 2022 року

ОДУВС
м. Одеса
2022

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

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

Матеріали
Міжнародної науково-практичної конференції
23 листопада 2022 року

Одеса
ОДУВС
2022

Рекомендовано до друку рішенням кафедри кібербезпеки
та інформаційного забезпечення
Одеського державного університету внутрішніх справ

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

Кібербезпека в Україні: правові та організаційні питання:
К38 матеріали міжн. наук. практ. конф., м. Одеса, 23 листопада 2022 р. Одеса : ОДУВС, 2022. 152 с.
ISBN 678-717-70204

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 23 листопада 2022 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 міжнародної науково-практичної конференції адресовано вченим, працівникам правоохоронних органів, аспірантам (ад'юнктам), здобувачам вищої освіти першого та другого півня освіти.

НАПРЯМИ ПІДГОТОВКИ ФАХІВЦІВ ІЗ ПРОТИДІЇ КІБЕРЗАГРОЗАМ У КРЕДИТНО-ФІНАНСОВІЙ СФЕРІ

Олександр СІФОРОВ
доцент кафедри кібербезпеки
та інформаційного забезпечення ОДУВС, к.т.н, доцент
Сергій СЕРГІЄНКО
слухач магістратури факультету №1
ННІПКБ ОДУВС
спеціальність 124 «Системний аналіз»

Період часу, що переживається людством, характеризується постійним зростанням впливу інформаційних технологій на людину та її діяльність. Спостерігається інтенсивний вплив інформаційної сфери на психіку та поведінку окремих осіб та цілих соціальних груп. Інфосфера сьогодні активно впливає на стан політичної, фінансово-економічної, оборонної та інших базових складових безпеки будь-якої держави. Загальноприйнятим фактом вважається те, що національна безпека сьогодні істотно залежить від комплексного забезпечення інформаційної та економічної безпеки, і в міру розвитку глобальної інформаційної інфраструктури ця залежність лише зростає [1].

Протягом останніх двох десятиліть провідні країни світу активно відпрацьовують тактику та стратегію ведення інформаційних воєн [1,2,3]. Різні аспекти та прийоми інформаційної експансії, що спостерігаються повсюдно, підживлюють новими ідеями та можливостями кіберзлочинність та, насампе-

ред, у її проявах у кредитно-фінансовій сфері (КФС), де кількість спроб проведення кібератак зростає практично щомісяця. Причому під загрозою викрадення коштів або дезорганізації роботи з метою їхнього здирництва опиняються не тільки банки та їх клієнти, а й інші критично важливі об'єкти інформаційної інфраструктури, що беруть участь у грошовому обігу. Сучасні кіберзлочинці діють все більш потай і завдають все більш серйозної шкоди, використовуючи при цьому викрадені персональні дані, методи соціальної інженерії та фішингу, проводячи вірусні атаки та атаки на веб-сайти з метою викрадення даних для їх подальшого перепродажу. Кіберзлочинцям вдалося витягти з, здавалося б, абсолютно захищених баз даних американського Чейз Манхеттен Банку відомості про рахунки понад 8 мільйонів бізнес-структур та 74 мільйони фізичних осіб [3].

За даними одного з провідних виробників засобів забезпечення кібербезпеки, у 2020 році у світі кіберзлочинністю викрадено понад 158 млрд доларів США.

На думку фахівців у галузі кібербезпеки, які опублікували свої прогнози в галузі забезпечення безпеки та зберігання даних, у 2022 році на передній план вийдуть «хмари», віртуалізація, а також безпека мобільних пристроїв та соціальних мереж.

Мільярди людей користуються мобільними телефонами з можливістю виходу до Інтернету. Раніше кіберзлочинці не виявляли великого інтересу до мобільних пристроїв, але в міру підвищення інтелектуального рівня цих пристроїв та формування платформ-лідерів у даному сегменті ринку злочинці неминуче направлятимуть свої атаки на мобільні пристрої. Отже, зростатиме обсяг конфіденційних даних, загублених через ці пристрої. Подібні проблеми створює і поширення віртуалізації.

Швидке та роз'єднане впровадження віртуальних інфраструктур, а також відсутність стандартів на їх побудову та функціонування продовжуватимуть створювати проломи у безпеці при резервному копіюванні та забезпеченні високої готовності віртуальних середовищ. І хоча віртуалізація знижує витрати на серверну інфраструктуру, вітчизняні та закордонні кредитно-фінансові організації (КФО) приходять до розуміння того, що вона одночасно створює нові загрози безпеці даних. Ще більше ускладнює ситуацію з кібербезпекою використання соціальних мережевих сервісів підвищення рівня комунікацій і персональної ефективності співробітників КФО.

Необхідність пошуку та застосування адекватних заходів протидії кібершахрайству, захисту банківських продуктів та інформаційної інфраструктури кредитно-фінансової сфери зумовлюють пильну увагу суспільства до якості підготовки фахівців із протидії кіберзагрозам КФО.

Які ж компетенції в галузі кібербезпеки мають володіти випускники ВНЗ? Як видається, ці компетенції мають охоплювати такі основні напрями.

*Фундаментальні знання в галузі інформаційних технологій та кібербезпеки:*архітектура та організація функціонування ЕОМ; сучасні обчислювальні системи та мережі зв'язку, мережеві технології; адміністрування сучасних

операційних систем; адміністрування баз даних; робота з великими даними; системи штучного інтелекту; засоби моніторингу інформаційних мереж; уразливості сучасних програмних та апаратно-програмних засобів; загальні методи та засоби забезпечення інформаційної безпеки; захищені мережеві технології глобального, корпоративного та локального призначення; математичні аспекти захисту інформації, криптографії, стеганографії, крипто- та стег аналізу;

– способи та засоби розробки захищених додатків;

– системотехніка та схемотехнічне проектування апаратних засобів інформаційної безпеки;

– побудова та функціонування електронних платіжних систем.

Розуміння технологій реалізації загроз інформаційній безпеці:

– програмування у сучасних операційних середовищах;

– аналіз алгоритмів;

– реверс-інжиніринг програмних текстів;

– атаки на електронні платіжні системи;

– пошук слідів та методи розслідування кіберзлочинів у кредитно-фінансовій сфері.

Розуміння принципів управління бізнесом та забезпечення його інформаційної безпеки:

– цивільно-правові відносини;

– основи управління підприємством та організацією;

– опис бізнес-процесів;

– основні бізнес-процеси банку;

– нормативно-правова база інформаційної безпеки;

– автоматизовані системи обробки, зберігання та передачі інформації з урахуванням рівнів та критеріїв безпеки.

Лідерські якості та презентаційні навички:

– основи соціології;

– основи психології;

– технології розробки бізнес-планів; методи командної роботи;

– тайм менеджмент;

– особиста ефективність;

– планування діяльності;

– дизайн-мислення;

– інструменти для створення презентацій.

Розуміння принципів управління ризиками:

– міжнародні стандарти управління ризиками та інформаційної безпеки;

– Базельські стандарти;

– теорія ймовірностей та математична статистика;

– теорія ігор;

– оцінка економічної ефективності.

З метою всебічного забезпечення навчального процесу, спрямованого на підготовку фахівців, які мають наведені вище компетенції, передбачається розгортання діяльності за трьома ключовими напрямками:

– організація взаємодії з кредитно-фінансовими організаціями – роботодавцями для випускників ВНЗ;

– вдосконалення освітнього процесу та рівня підготовки професорсько-викладацького складу;

– підвищення рівня підготовки студентів

Однією з важливих умов підвищення якості підготовки фахівців у галузі інформаційної безпеки є формування високих моральних якостей у студентів. І тут «людський фактор» — це інтегральна характеристика особистості, що визначає надійність захисту інформації при її отриманні, зберіганні та переробці в автоматизованих банківських системах. Незважаючи на різноманітність та постійне вдосконалення спеціальної техніки для захисту інформації, люди залишаються найслабшою ланкою в людино-машинних системах, одним із найімовірніших джерел витоку інформації, у зв'язку з чим найбільшою шкодою загрожують атаки на інформаційні та апаратно-програмні ресурси кредитно-фінансових організацій. із використанням інсайдерів.

Література:

1. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate / I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, D. Upton. Journal of Cybersecurity. 2018. Volume 4, Issue 1. URL: https://doi.org/10.1093/cybsec/tyy006 (дата звернення: 23.09.2020).

2. Bouveret A. Cyber risk for the financial sector: A framework for quantitative assessment. IMF Working Paper. 2018. WP/18/143. P. 28. URL: https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-theFinancial-Sector-A-Framework-for-Quantitative-Assessment-45924 (дата звернення: 23.09.2020).

3. Dupont B. The cyber-resilience of financial institutions: significance and applicability. Journal of Cybersecurity. 2019. Volume 5, Issue 1. URL: https://doi.org/10.1093/cybsec/tyz013 (дата звернення: 23.09.2020).

СЕКЦІЯ 4.
ПІДГОТОВКА ПЕРСОНАЛУ ДЛЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В УКРАЇНІ ОКРЕМІ АСПЕКТІ ІНФОРМАЦІЙНОІ ПРОТИДІЇ