УДК 355.085.5
DOI: 10.31733/15-03-2024/2/669-670

Ілля ЖЕЛНОВАЧ
курсант факультету №4
Денис ГРИЩЕНКО
старший викладач кафедри
протидії кіберзлочинності
Харківського національного
університету внутрішніх справ

АКТУАЛЬНІ ПРОБЛЕМИ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ

Професійна підготовка поліцейських відіграє вирішальну роль у розвитку поліцейських. Оскільки підготовка поліцейських поєднує в собі різні освітні компоненти та регулюється організаційними настановами, підготовка поліцейських є складною, багатогранною темою.

Проведені дослідження спеціалізованих підрозділів по боротьбі з кіберзлочинністю в Україні, дають змогу висвітлення питань і проблем, з якими стикаються співробітники поліції на передовій лінії кіберполіції.

Інформація про загальні загрози та виклики кіберзлочинності зазвичай надходить з численних джерел, як на національному, так і на міжнародному рівні. Однак, без належного аналізу та розміщення в загальному контексті безпеки, такі дані мають обмежене використання або призначення. Тому аналіз та обмін інформацією про загрози та виклики кіберпростору між політиками та професійними спільнотами має призвести до кращої координації та спільних підходів між усіма залученими партнерами – як із державного, так і з приватного секторів. Зрештою, це має сприяти досягненню того, що має бути кінцевою спільною метою: забезпечення безпечного кіберпростору для всіх.

Кіберзагрози можна визначити як «можливість зловмисної спроби пошкодити або вивести з ладу комп'ютерну мережу або систему» [1], зростаюча загроза кіберзлочинності створює значні виклики для поліцейських організацій. Хоча співробітники повідомляють про загальний позитивний рівень задоволеності роботою у сфері протидії кіберзлочинності, було виявлено три основні теми: збільшення обсягу роботи, оскільки кіберзлочинність стає все більшою соціальною проблемою; нажаль ресурсне забезпечення підрозділів не відповідає попиту на робоче навантаження; рівень навичок і підготовки в підрозділах потребує покращенню для того, щоб впоратися з унікальним характером і зростаючою складністю протидії кіберзлочинності.

До основних загроз належать такі кіберзлочини, як шахрайство, несанкціонований доступ до комп'ютерних систем та мереж, DDoS-атаки та мереж, різноманітне шкідливе програмне забезпечення, програми-вимагачі та атаки зі знищення даних. Часто зловмисники націлені на конфіденційну інформацію та персональні дані державних службовців. Тому кібершпигунство трапляється досить часто. Коли відбувався витік або крадіжка даних, у тому числі з урядових баз даних, зловмисники іноді пропонували їх для продажу.

Українські органи влади стали свідками просунутих постійних загроз, а також координації та планування атак. Зафіксовані випадки співпраці між зловмисниками та інсайдерами. Нерідко фішингові та соціальні інженерні атаки відбувалися раніше з метою отримання облікових даних або іншої інформації, що може бути використана для здійснення атаки на комп'ютерну систему чи мережу.

Атаки на комп'ютерні системи та мережі неодноразово включали в себе атаки на об'єкти критичної інфраструктури. Правоохоронні органи та розвідка також бачать, що злочинність як послуга що з'явилася. Для того, щоб завдати шкоди або паралізувати роботу комп'ютерних систем та мереж, у тому числі тих, що належать державі або об'єктам критичної інфраструктури, здійснюються фізичні атаки на мережеву інфраструктуру, в тому числі мідні та оптоволоконні кабелі [2].

Хоча більшість кіберзлочинів вчиняються злочинцями, все ж є підстави вважати, що часто за атаками можуть стояти хактивісти, кібербійці та терористи. Масштабні атаки, які складні та потребують багато ресурсів і зусиль для підготовки, могли мати державне

фінансування. У різних соціальних мережах та іноземних ЗМІ зафіксовані інформаційні операції та компанії з поширення фейкових новин. Компанії з розповсюдження фейкових новин, основною метою яких є викликати тривогу та розгубленість серед населення, а також створити серед населення негативний імідж влади та країни.

Слід зазначити, що за останні роки значно зросла обізнаність громадськості щодо кібернетичних ризиків, однією з головних причин цього є масована кампанія шкідливого програмного забезпечення проти українських державних і приватних мереж і комп'ютерів, а також кібершпигунство та кібератаки на громадськість, що мали місце останнім часом.

Внаслідок цих інцидентів, від яких постраждали як державні, так і приватні суб'єкти, у т.ч. зазнали економічних збитків, все більше уваги приділяється інформаційній безпеці, кібербезпеці та запобіганню кіберзлочинності.

Зміни у жорстких та м'яких технологіях роботи поліції, схоже, трансформують місцеві, державні поліцейські управління за низкою фундаментальних напрямів. Оцінки обмеженого впливу поліцейських технологій на роботу поліції, були зроблені різними дослідниками, які проаналізували наявні дослідження про вплив останніх технологічних інновацій на роботу поліції, які можливо впровадити в діяльність поліції в цілому.

У роботі поліції, а саме протидії кіберзлочинності слід приділити увагу професійній підготовці, з метою готовності до такої кількості роботи та інформації, і наявності достатньої кількості ресурсного забезпечення для виконання покладених завдань.

1. The challenges facing specialist police cyber-crime units: an empirical analysis. Вебсайт. URL : https://www.researchgate.net/publication/327793536_The_challenges_facing_specialist_police_cyber-crime_units_an_empirical_analysis (дата звернення: 19.02.2024).

2. Council of europe's convention on cyber-crime and other European initiatives. Вебсайт. URL : https://www.cairn.info/revue-internationale-de-droit- pénal -2006-3-page-473.htm (дата звернення: 18.02.2024).

3. Police Training in Practice: Organization and Delivery According to European Law Enforcement Agencies // вебсайт. URL : https://www.frontiersin.org/articles/10.3389/fpsyg.2021.798067/full (дата звернення: 20.02.2024).

Грищенко Д.О. Желновач І.О., «Актуальні проблеми підготовки фахівців для сектору безпеки і оборони» Міжнародна та національна безпека: теоретичні і прикладні аспекти : матеріали VIII Міжнар. наук.- практ. конф. (м. Дніпро, 15 бер. 2024 р.) ; у 2-х ч. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2024. Ч. ІІ.. 669-670 с