МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КАФЕДРА ЕКОНОМІЧНОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Матеріали Всеукраїнського науково-практичного семінару (м. Дніпро, 26 листопада 2020 р.)

Дніпро – 2020

ББК 67.9(4УКР)305

П 685
УДК 347.23 (477)

Рекомендовано до друку Науково-методичною радою Дніпропетровського державного університету внутрішніх справ.
(протокол № 4 від __.12 2020)

П 685 **ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ**: матеріали Всеукраїнського науково-практичного семінару (26 листопада 2020 р., м. Дніпро). – Дніпро: Дніпропетровський державний університет внутрішніх справ, 2020. – 147 с. *(в авторській редакції)*

СКЛАД ОРГАНІЗАЦІЙНОГО КОМІТЕТУ
Всеукраїнського науково-практичного семінару "Використання сучасних інформаційних технологій в діяльності Національної поліції України"

Голова оргкомітету – **Наливайко Лариса Романівна**, проректор університету, д.ю.н., професор, Заслужений юрист України

Заступник голови оргкомітету – **Рижков Едуард Володимирович,** завідувач кафедри економічної та інформаційної безпеки, к.ю.н., доцент

Члени оргкомітету:

Шнурко Яна Вікторівна - завідувач відділення зв'язків з громадськістю;
Самотуга Андрій Валерійович - к.ю.н., доцент, заступник завідувача редакційно-видавничого відділення;
Гребенюк Андрій Миколайович – відповідальний секретар семінару, доцент кафедри економічної та інформаційної безпеки; к.т.н., доцент;
Мирошниченко Володимир Олексійович – професор кафедри економічної та інформаційної безпеки, к.т.н., доцент;
Тютченко Світлана Миколаївна – старший викладач кафедри економічної та інформаційної безпеки
Рибальченко Людмила Володимирівна – доцент кафедри економічної та інформаційної безпеки, к.т.н., доцент;
Прокопов Сергій Олександрович – старший викладач кафедри економічної та інформаційної безпеки.

ББК 67.9(4УКР)305

© Автори, 2020
© ДДУВС, 2020

який зараз існує між різними нормативними актами та законодавством, допомагає переконати регулюючі органи, що організація постійно дотримується вимог законодавства.

Зміна нормативно-правової бази в сфері кібербезпеки – це виклик часу і тільки якнайскоріша модернізація організаційно-правового забезпечення дасть можливість забезпечити виконання поставленої задачі – сталого функціонування кіберпростору держави. Всупереч поширеній думці, безпека – це не стан, а процес.

Висновки.

1. Вважаємо, що існуюча нормативно-правова база у сфері кібербезпеки повинна бути істотно доповненою. На організаційно-правовому рівні необхідно чітко ідентифікувати проблему забезпечення кібербезпеки та своєчасно надавати нові, сучасні правові інструменти для протидії цим загрозам.
2. Пропонуємо внести зміни до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" і на законодавчому рівні закріпити вимоги стандартів сімейства СМІБ для окремих категорій інформації, захист якої забезпечується законодавством України.

Використані джерела:

1. Юрій Котляров. Архітектура права сфери кібербезпеки в Україні. Електронний ресурс. URL: https://www.pressreader.com/ukraine/yurydychna-gazeta/20180515/ (дата звернення: 10.11.2020).
2. Живко З. Б., Рудий Т. В., Сеник В. В., Родченко С. С. Проблеми нормативно-правової бази забезпечення кібербезпеки в Україні: стан і перспективи / Соціально-правові студії: науково-аналітичний журнал / гол. ред. О. Балинська. Львів: ЛьвДУВС, 2020. Вип. 3 (9). С. 18-25.
3.Костенко О.В. Проблеми правового регулювання та розвиток кібернетичної безпеки України на сучасному етапі / Інформація і право. Науково-дослідний інститут інформатики і права Національної академії правових наук України. Київ. № 3(30)/2019. С. 96-104.

Каблуков А. О.
доцент кафедри медичної і фармацевтичної інформатики та новітніх технологій Запорізького державного медичного університету, к.т.н., доцент
Страхова О.П.
ассистент кафедри медичної і фармацевтичної інформатики та новітніх технологій Запорізького державного медичного університету, к.фмн.н, асистент

ПІДГОТОВКИ СПЕЦІАЛІСТІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ВУЗАХ МВС УКРАЇНИ

В результаті стрімкого розвитку комп'ютерних технологій і їх застосування в

різних сферах нашого життя людство увійшло в нову еру інформатизації, коли комп'ютер є необхідним інструментом в самих різних сферах життєдіяльності людини.

Впровадження в управлінський процес і інші сфери життя суспільства електронно-обчислювальної техніки, без якої зберігання, обробка і використання величезної кількості найрізноманітнішої інформації було б неможливим, принесло неоціненну користь у розвиток науки, техніки та інших галузей знань. Однак вигоди, які можна отримати завдяки використанню цієї техніки, стали використовуватися і в злочинних цілях. Так, з'явився новий вид злочинної діяльності - комп'ютерні злочини, суспільно-небезпечні наслідки, від здійснення яких не йшли в порівняння зі шкодою від інших злочинів.

За оцінками експертів правоохоронних органів країн Центральної та Східної Європи з питань боротьби з комп'ютерною злочинністю, прибутки злочинців від злочинів у сфері використання електронно-обчислювальних машин посідають третє місце після доходів наркоторговців і від продажу зброї, а завдані збитки вже зараз оцінюється мільярдами доларів. На 73-й сесії Генеральної асамблеї ООН генеральний секретар Антоніу Гутерреш оцінив щорічні збитки від кіберзлочинності в світі в розмірі 1500 млрд доларів.[1, с.1]

Україна, як і всі країни світу, щодня стикається з викликами в сфері кібербезпеки. Тільки за останні кілька років державні установи неодноразово атаковані з кіберпростору. За інформацією голови Департаменту кіберполіції Сергія Васильовича Демедюк, щорічно кількість кіберзлочинів в Україні збільшується в середньому на 2,5 тисячі. Згідно зі звітом, який міститься на сайті цього правоохоронного органу, в 2019 працівники Департаменту кіберполіції були залучені до розслідування більше 11 000 кримінальних проваджень, скоєних в сфері високих інформаційних технологій.[1, с.3].

Таким чином, вивчення проблем запобігання та розслідування злочинів у сфері комп'ютерної інформації виступає однією з найгостріших проблем сучасної криміналістичної науки.

Сьогодні, поліція по всьому світу має підрозділи по боротьбі з комп'ютерними злочинами, створюються спеціальні центри з навчання фахівців у цій галузі. Так Європейський Союз створив орган під назвою «Форум по кіберзлочинності». Безліч країн підписала Конвенцію Ради Європи щодо кіберзлочинності, яка намагається стандартизувати європейські закони, що стосуються злочинності в Інтернеті [2, С.3].

В Україні політика з кібербезпеки покладається на ряд державних органів, а саме на Державну службу спеціального зв'язку та захисту інформації України, Національної поліції України, Службу безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. У кожному із зазначених органів діють відповідні підрозділи.

Наявність таких підрозділів в якійсь мірі дозволяє запобігати і розкривати кіберзлочини, однак сьогодні злочинні групи і спільноти для досягнення корисливих цілей все частіше застосовують системний підхід при плануванні своїх дій, розробляють оптимальні варіанти проведення і забезпечення кримінальних

«операцій», створюють системи конспірації прихованим зв'язку, вживають додаткових заходів з надання ефективної протидії співробітникам правоохоронних органів, використовуючи сучасні технології і спеціальну техніку, в тому числі і різні комп'ютерні пристрої і нові інформаційно-обробні технології.

Таким чином, очевидно, що сьогодні однією з найважливіших проблем є забезпечення підрозділів поліції МВС України грамотними комп'ютерними фахівцями. Співробітник поліції, який працює в областях пов'язаних із захистом секретної службової інформації, розслідуванням комп'ютерних злочинів і т.п. звичайно повинен володіти всіма необхідними навичками. Однак зараз, дуже часто, в цих областях працюють люди, які прийшли після закінчення цивільних ВНЗ, тому одним із пріоритетних напрямків розвитку освіти в МВС є навчання саме фахівців в комп'ютерній сфері.

В даний час тільки кілька відомчих вищих закладів МВС займаються підготовкою фахівців з кібербезпеки, а саме: Харківській національний університет внутрішніх справ, Дніпровський державний університет внутрішніх справ, Одеський державний університет внутрішніх справ. Аналіз результатів роботи МВС показує, що кількість фахівців з кібербезпеки, в МВС України, недостатньо для ефективної боротьби з даним видом злочинів. Для вирішення цієї проблеми необхідно в вузах МВС збільшити кількість студентв що навчаються за вищевказаною спеціальністю, а також створити курси підвищення кваліфікації з кібербезпеки для співробітників МВС, які курують цей напрям. Для курсів можна використовувати дистанційну форму навчання, що дозволить підвищувати кваліфікацію офіцерів за місцем служби. Найбільш доцільним для дистанційного навчання є використання сучасних хмарних технологій (Cloud computing), які забезпечують доступ до навчальних матеріалів протягом всього часу.

Висновок.

Для забезпечення ефективної боротьби з кіберзлочинами необхідно:

1. Вузам МВС підвищити кількість випускників за спеціальностями, пов'язаними з кіберзлочинами.

2. Створити курси підвищення кваліфікації для співробітників МВС, що працюють в підрозділах, що займаються кібербезпекою.

Використані джерела:

1. Кибербезопасность: начало эпохи новых видов преступлений// Информационный юридический портал Status-Quo.

(http://www.s-quo.com/ content/comment/ 288/7347/), 2019.

2. Д.Л. Шиндер. Компьютерная преступность - перед лицом проблемы // Центр исследования компьютерной преступности, 2010. (http://www.crime-research.ru/library/cybercrimes3.html).

3. А.Грабовий. Закон про кібербезпеку та стратегія кібербезпеки України// Електронне видання «Юрист & ЗАКОН», №26 -2017. (http://uz.ligazakon.ua/ua/magazine_article/EA010553).