ВІЙСЬКОВА АКАДЕМІЯ (м. ОДЕСА)
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
НСТИТУТ ВІЙСЬКОВО-МОРСЬКИХ СИЛ НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
«ОДЕСЬКА МОРСЬКА АКАДЕМІЯ»
НАЦІОНАЛЬНА АКАДЕМІЯ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ
УКРАЇНИ ім. БОГДАНА ХМЕЛЬНИЦЬКОГО (м. ХМЕЛЬНИЦЬКИЙ)
НАЦІОНАЛЬНА АКАДЕМІЯ
НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ (м. ХАРКІВ)

СПІЛЬНІ ДІЇ ВІЙСЬКОВИХ ФОРМУВАНЬ І ПРАВООХОРОННИХ ОРГАНІВ ДЕРЖАВИ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

Збірник тез доповідей
Міжнародної науково-практичної конференції

10-11 вересня 2020 року

ВІЙСЬКОВА АКАДЕМІЯ (м. ОДЕСА)
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
ІНСТИТУТ ВІЙСЬКОВО-МОРСЬКИХ СИЛ НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ «ОДЕСЬКА МОРСЬКА АКАДЕМІЯ»
НАЦІОНАЛЬНА АКАДЕМІЯ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ ім. БОГДАНА ХМЕЛЬНИЦЬКОГО (м. ХМЕЛЬНИЦЬКИЙ)
НАЦІОНАЛЬНА АКАДЕМІЯ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ (М. ХАРКІВ)

СПІЛЬНІ ДІЇ ВІЙСЬКОВИХ ФОРМУВАНЬ І ПРАВООХОРОННИХ ОРГАНІВ ДЕРЖАВИ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

Збірник тез доповідей
Міжнародної науково-практичної конференції

10–11 вересня 2020 року

м. Одеса

На сьогоднішній день в Держприкордонслужбі функціонує Інтегрована інформаційно-телекомунікаційна система «Гарт», яка дозволяє автоматизувати основні форми оперативно-службової діяльності. Однією з основних форм є прикордонний контроль, в межах якої необхідно приймати рішення, щодо пропуску/непропуску осіб та транспортних засобів які перетинають державний кордон України. Для автоматизації цієї задачі було розроблено інформаційно-телекомунікаційну систему «Гарт-1», яка дозволяє вирішувати завдання: обліку і контролю за базами даних паспортних (ідентифікаційних) даних осіб та реєстраційних даних транспортних засобів, що перетинають державний кордон України в пунктах пропуску.

Сучасні ризики та загрози, зокрема Covid-19, обумовлюють потребу у вдосконаленні процедур здійснення пропуску громадян та транспортних засобів через державний кордон України. Одним з важливих аспектів цих процедур є ефективне застосування при цьому сучасних інформаційно-телекомунікаційних технологій, зокрема відповідна модернізація ІТС «Гарт-1». Вбачається, що ця модернізація буде включати: розвиток баз даних в частині обліку і контролю осіб, які можуть становити загрозу поширення вірусної інфекції Covid-19;інтеграція ІТС «Гарт-1» з інформаційно-телекомунікаційними системами інших правоохоронних органів; розробка програмно-апаратного комплексу дистанційного скринінгу виявлення потенційних носіїв короновірусної інфекції та автоматичної фіксації на автоматизованому робочому місці «Інспектор»; удосконалення спеціального програмного забезпечення bkc-kordon, щодо обліку і контролю осіб, які можуть становити загрозу поширення вірусної інфекції Covid-19.

Виходячи з цього, розвиток телекомунікаційних мереж та інформаційних систем у Державній прикордонній службі України сьогодні є об’єктивною потребою і здійснюється з урахуванням світової тенденції побудови та інтеграції мереж, засобів та послуг зв’язку. Ця тенденція вимагає запровадження обладнання і технологій, що відповідають сучасним міжнародним стандартам та рекомендаціям.

Рибалов Б.О.
Одеська Національна академія харчових технологій, Україна

МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПРИ ПЕРЕДАЧІ ІНФОРМАЦІЇ ПО ВОЛОКОННО-ОПТИЧНИХ КАНАЛАХ ЗВ’ЯЗКУ

В даний час одним з перспективних напрямків розвитку телекомунікацій як в нашій країні, так і за кордоном є інтенсивне впровадження волоконно-оптичних технологій. Це пояснюється тим, що волоконно-оптичні канали значно перевершують електричні канали зв'язку за такими показниками, як пропускна здатність, перешкодозахищеність тощо. Крім того, до переваг слід віднести малі габаритні розміри і масу оптоволоконних кабелів.

Конфіденційність інформації, що передається по волоконно-оптичних каналах зв'язку (ВОКЗ) може бути забезпечена застосуванням спеціальних методів і засобів захисту від несанкціонованого доступу. Можна виділити три основних напрямки щодо впровадження методів захисту ВОКЗ від несанкціонованого доступу:

– розробка технічних засобів захисту від несанкціонованого доступу до інформаційних сигналів, що передаються по ВОКЗ;

– розробка технічних засобів контролю несанкціонованого доступу до інформаційного оптичного випромінювання, переданому по ВОКЗ;

– розробка технічних засобів захисту інформації, що передається по ВОКЗ, які реалізують принципи квантової криптографії.

У першому напрямку розроблено метод, заснований на використанні кодового зашумлення переданих оптичних сигналів. При реалізації цього методу застосовуються спеціально підібрані відповідно до необхідної швидкості передачі коди, що розмножують помилки. Навіть при невеликому зниженні оптичної потужності, викликаному підключенням пристрою знімання інформації до ВОКЗ, в сигналі на виході ВОКЗ різко зростає коефіцієнт помилок, що досить просто зареєструвати засобами контролю ВОКЗ.

У другому напрямку становить інтерес розробка різних датчиків контролю підключення до оптоволоконного кабелю. Найбільш перспективними по чутливості і швидкості спрацьовування є системи на основі волоконно-оптичних датчиків. Їх робота заснована на зміні в результаті зовнішнього впливу параметрів оптичних сигналів, зокрема, фази, ступеня поляризації і швидкості поширення оптичних сигналів. Це дозволяє будувати високочутливі інтерферометричні розподілені оптичні датчики контролю спроб несанкціонованого підключення до оптоволокна.

У третьому напрямку використовуються пристрої контролю параметрів відбитих оптичних сигналів на вході ВОКЗ. Для контролю величини потужності сигналу зворотного розсіювання в оптоволокні в даний час використовується метод імпульсного зондування, який застосовується в усіх зразках рефлектометрів. Суть його полягає в тому, що в досліджуваному ВОКЗ вводиться потужний короткий імпульс і потім на цьому ж кінці

реєструється випромінювання, розсіяне в зворотному напрямку на різних неоднорідностях, за інтенсивністю якого можна судити про втрати в ВОКЗ, розподілених по його довжині на відстань до 110-120 км.

Всі перераховані вище методи захисту і їх комбінації можуть забезпечувати безпеку інформації лише в рамках відомих моделей загроз нападу. При цьому ефективність систем захисту визначається як відкриттям нових, так і вдосконаленням технологій застосування вже відомих фізичних явищ.

З плином часу зловмисник може освоїти нові методи перехоплення інформації, тому виникатиме необхідність розробки доповнювальних методів захисту від несанкціонованого доступу по ВОКЗ, в тому числі – до місць прокладки волоконно-оптичних кабелів.

Роллер В.М.
Військовий інститут Київського національного університету імені Тараса Шевченка, Україна

КІБЕРВІНА – ВІЙНА МАЙБУТНЬОГО?

За останні два десятки років інформаційні технології здійснили значний ривок у своєму розвитку. Технології, про які людство навіть не мріяло у середині двадцятого сторіччя, нині доступні пересічному громадянинові навіть у країнах третього світу. Новітні технології значно полегшили спілкування та обмін інформацією, розкривши кордони спілкування між жителями різних континентів нашої планети. Але, необхідно не забувати, що більшість технологій, якими ми користуємося у побуті були першочергово розроблені у військових цілях. Взяти до прикладу хоча б мережу «Інтернет», яка першочергово створювалася як мережа обміну інформацією для американських військових. Вільна енциклопедія Вікіпедія зазначає: «1969 року Міністерство оборони США започаткувало розробку проєкту, котрий мав на меті створення надійної системи передачі інформації на випадок війни. Агентство DARPA запропонувало розробити для цього комп'ютерну мережу. Розробка була доручена Каліфорнійському університету Лос-Анджелеса, Стенфордському дослідному центрові, Університету штату Юта і Університету штату Каліфорнія в Санта-Барбарі. Ця мережа була названа ARPANET. У рамках проєкту мережа об'єднала названі заклади. Всі роботи фінансувались за рахунок Міністерства оборони. ARPANET почала активно рости й розвиватись, її дедалі ширше почали використовувати вчені із різних галузей науки.». Але розробка виявилася такою універсальною та корисною, що за наступні роки здобула шаленої популярності у всьому світі. На сьогоднішній день важко уявити роботу будь-якої установи чи організації без доступу до мережі Інтернет.

Необхідно зазначити, що мережа Інтернет, крім користі принесла ще й нові виклики та способи вчинення порушень. Ми можемо говорити як про злочини, що існували і до появи Інтернету,і просто набули нової форми вчинення з використання «всесвітнього павутиння», так і про нові види порушень, які можливо вчинити лише у мережі, як от викрадення особистості, тобто викрадення інформації про особу та використання її у злочинних цілях, або здійснення хакерських атак та інше.

Але для військової сфери корисний винахід обернувся ще одним полем бою. Весь світ активно говорить про війні нового покоління - кібервійни. Значною особливістю цих протистоянь є те, що хоч вони і відбуваються у мережі, тобто, фактично, між машинами підключеними до мережі, наслідки цих протистоянь можуть бути відчутними у реальному світі. Це було доведено у 2010 році використання вірусу STUXNET. Також при цьому, необхідно враховувати факт того, що багато процесів які відбуваються у державах, відбуваються за посередництвом мережі Інтернет, від покупки товарів у магазинах та подачі податкової звітності, до управління великими підприємствами. Тобто, всі ці об’єкти знаходяться у потенційній небезпеці, з усіма послідуючими наслідками, які важко переоцінити.

Одже, наразі перед військовими постає багато нових питань, щодо того, яку позицію формувати стосовно кібератак, та як оцінювати їх загрозу. Міжнародними експертами підготовлено Таллінське керівництво з застосування норм міжнародного гуманітарного права до кібервійн. Але цей посібник має теоретичний, рекомендаційних характер, а подекуди думки самих експертів не сходяться у тих чи інших питаннях.

Українське законодавство щодо регулювання питань кібербезпеки почало активно формуватися лише 2017 року, коли у нормативно-правових документах з’явився сам термін «кіберпростір». Єдиним натяком щодо можливості кібервіни є надання визначення кібероборони у Законі України «Про основні засади забезпечення кібербезпеки в Україні» та зазначення, що питання здійснення кібероборони покладаються на Міністерство оборони України.

Але вважаємо, що цьому питанню має бути приділено набагато більше уваги, як у теоретичному вивченні, так і нормативно - правовому регулювання. Всі розвинені країни світу вже мають достатньо потужні підрозділи з кібероборони, що дає привід замислитися щодо необхідності розбудови цієї ланки і в українському війську. Крім того, має бути підготовлена нормативно - правова база щодо функціонування цих підрозділів, та розроблені відповідні алгоритми надання відсічі різним видам кібератак.

СПІЛЬНІ ДІЇ ВІЙСЬКОВИХ ФОРМУВАНЬ І ПРАВООХОРОННИХ ОРГАНІВ ДЕРЖАВИ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

Збірник тез доповідей
Міжнародної науково-практичної конференції

10-11 вересня 2020 року

Редакційна група за якість матеріалів відповідальності не несе.
Матеріали доповідей авторів надано у вигляді, відповідно
до заявок на участь у конференції.
Дякуємо авторам за дотримання рекомендованого шаблону та обсягу виступів.

Відповідальний за випуск – Франчук Ю.В.
Комп'ютерний набір Франчук Ю.В.
Комп'ютерна верстка Кучерук К.М.

Здано до набору 31.08.2020 р. Підписано до друку 28.09.2020 р.
Формат паперу 297х420/2. Авт. арк. – 23,1. Обл. вид. арк. – 23,2. Друк. арк. – 254.
Ум. друк. арк. – 58,42. Папір офсетний. Гарнітура Times New Roman.
Замовлення № 289-2020 РВВ ВА. Наклад – 100 прим.