Таким чином, аналіз популярних програмно-апаратних девайсів та гаджетів в діяльності поліцейських показав, що їх впровадження здійснюється відповідно до національних законодавств, направлено на забезпечення правопорядку з дотриманням конституційних прав громадян та підвищення ефективності діяльності поліцейських. Аналіз дозволив виділити найбільш актуальні для впровадження в України програмно-апаратних засобів: натільні відеокамери, розумні відеокамері, квадрокоптери, розумні окуляри з функцією розпізнавання особистості, електронні портативні сканери відбитків пальців та ідентифікації осіб.

УДК 007[732.214]
ЯРОСЛАВ АНДРІЙОВИЧ ЧЕРКАШЕНКО
рядовий поліції курсант 2 курсу факультету № 4 Харківського національного університету внутрішніх справ

КІБЕРВІЙНА ТА ІНФОРМАЦІЙНИЙ ВПЛИВ НА СУСПІЛЬСТВО

В умовах глобальної і тотальної інформатизації, коли суспільство стало залежним від інформаційних систем, політичні і військові еліти стали застосовувати віртуальний вплив на людей, приховано, а інколи й відкрито. Настав час війни не на полі бою, а в мережі Інтернет ,та витрати на такий засіб бою потребується менш. При цьому ефективно проводити дезінформацію компаній, виявляти та контролювати громадську думку, направляти соціальні групи на певні дії дозволяють соціальні мережі.

Недооцінювання та нехтування тою чи іншою державою питань власної кібербезпеки й інформаційного домінування може спричинити не лише суттєві матеріальні збитки через втрату або спотворення стратегічної важливої інформації, а й можливі техногенні катастрофи, збитки цивільної, фінансової та військової інфраструктури аж до втрати суверенітету держави.

Мережева війна – це спосіб ведення конфліктів, коли її учасники застосовують мережеві форми організації, доктрини, стратегії та технології, пристосовані до сучасної інформаційної доби.

З іншого ж боку на сьогоднішній день більшість держав вже приділяють захисту від кібервійни належну увагу: виділяють необхідні кошти для організації систем захисту і підтримання спеціальні підрозділи, основним завданням яких є вдосконалення кібербезпеки країни та захисту від нападів.

[2] У кібервійні часто неможливо визначити не тільки учасників, час її початку і завершення, а й важко довести у багатьох випадках сам факт застосування руйнівної кіберзброї, не кажучи вже про шпигунське програмне забезпечення. За своїми наслідками застосування кіберзброї під час наступальних операцій в електромагнітному спектрі можна порівняти із втратами від застосування зброї масового ураження. Зокрема, використання кіберзброї може бути замасковано під техногенні катастрофи чи системні збої в системі комп’ютерних мереж і сервісів тощо. Так, прикладом, 23 грудня

2015 року за допомогою троянської програми «Black Energy» російські зловмисники атакували комп'ютерні системи управління в диспетчерській «Прикарпаттяобленерго» та вимкнули понад 30 підстанцій, залишивши 230 тисяч мешканців без світла на 1-6 годин. Ця атака стала першою у світі підтвердженою кібератакою спрямованою на виведення з ладу енергосистеми.

[1] Також з одного боку, існує багато спроб звести інформаційну війну до проблем комп'ютерних технологій, тобто до реалізації можливостей технологічних засобів передавання, опрацювання та використання інформації, а з іншого – до психологічної війни, тобто до використання засобів впливу на людину.

Нині в нашій країні інформаційні відносини та питання гарантування інформаційної та кібернетичної безпеки врегульовуються законами України «Про основи національної безпеки України».

Але проблема в тому, що якщо окремі держави не будуть обмінюватися інформацією, то інформаційна безпека не буде кращим виглядом підніматися в рівні захищеності та здобуття навичок запобігання кібератак, якщо буде виявлення в момент різкого виявлення загрози інформаційного напрямку.

Незважаючи на глобальний характер кібератак, на сьогодні відсутнє єдине міжнародно-правове визначення поняття кіберзлочинності, інформаційної війни та кібервіни. Немає міжнародно-правового механізму регулювання відносин у кіберпросторі.

Перспективи зміни системи міжнародної безпеки досить туманні, проте вже зрозуміло, що більшість інститутів і загальноприйнятих механізмів зараз малоефективні. Надалі в умовах розбудови глобального інформаційного суспільства можливим є тільки спільне підтримання балансу у сфері міжнародної безпеки на базі міждержавних союзів. Для безпеки кіберпростору нашої держави потрібно узгоджувати та поєднувати національну та міжнародну стратегію кіберзахисту у рамках спільної безпеки й оборонної політики ЄС, а також інтенсифікувати співпрацю України та НАТО, встановлення балансу між інформаційною безпекою і повагою приватного життя, створення конфіденційних механізмів обміну інформацією, встановлення основних вимог до кібербезпеки, відповідальності за кіберзлочинність, зміцнення програм освіти і професійної підготовки, підвищення обізнаності громадськості з питань кібербезпеки в нашій державі.

Список використаних джерел:

1. Попов.М.О., Лук'янець А.Г. До забезпечення воєнної безпеки в умовах загрози інформаційної війни. Наука й оборона.1999,№2. С.37–43.

2. Размєтаєва Ю.С. Кібервійна: загальнотеоретичні аспекти. Вісник АМСУ. Серія «Право». 2015, №1(14). С.17–22.