1. Тоффлер Э. Война и антивойна. Москва: АСТ Транзиткнига, 2005. с 240.
2. За матеріалами сайту компанії “I-intelligence”. URL: http://www.i-intelligence.eu
3. Open Source Intelligence. FMI 2-22.9. December 2006. Federation of American Scientists. URL: http://www.fas.org/irp/doddir/army/fmi2-22-9.pdf.
4. Доронин А. И. Бизнес-разведка. Москва: “Ось-89”, 2003. 384 с.

УДК 681.3

ТЕТЯНА ПЕТРІВНА КОЛІСНИК
кандидат педагогічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету №4 Харківського національного університету внутрішніх справ
ДІАНА ОЛЕКСІЇВНА БЛЄДНА
курсант 2 курсу факультету №4 Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ БОРОТЬБИ ЗІ ЗЛОЧИННІСТЮ В УМОВАХ СЬОГОДЕННЯ

Одним з важливих підходів для реалізації цілей «Стратегії розвитку органів системи Міністерства внутрішніх справ України на період до 2020 року», затвердженої розпорядженням Кабінету Міністрів України від 15 листопада 2017 року № 1023-р, є інформатизація діяльності, а саме, підвищення ефективності роботи і взаємодії через максимальне використання інформаційно-комунікаційних технологій у реалізації завдань органами системи МВС [1].

У науково-технічній літературі інформаційна технологія - цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розподіл даних, доступ до джерел інформації незалежно від місця їх розташування. Упорядкована послідовність взаємозв’язаних дій, що виконуються з моменту виникнення інформації до одержання результату, називається технологічним процесом. Інформаційна технологія, таким чином, невід’ємна від того специфічного середовища, в якому вона реалізується, тобто від технічного і програмного середовища.

Інформаційно-комунікаційні технології (ІКТ, від англ. Information and communications technology, ICT) - це сукупність методів, засобів та прийомів пошуку, зберігання, опрацювання, подання та передавання графічних, текстових, цифрових, аудіо та відеоданих на базі персональних комп`ютерів, комп`ютерних мереж та засобів зв`язку. Термін ІКТ в сучасному освітленні також використовується для позначення об’єднання (конвергенції)

аудіовізуальних та телефонних мереж з комп'ютерними мережами. Іншими словами, ІКТ складається з ІТ, а також телекомунікацій, медіа-трансляцій, усіх видів аудіо і відео обробки, передачі, мережевих функцій управління та моніторингу. Ефективне управління інформаційними ресурсами, їх надійний захист від кібератак, уміння використовувати аналітичні інструменти це основа для підтримки управлінських рішень керівництва Міністерства внутрішніх справ.

Загальною ознакою злочинів у сфері ІТ є їх підвищена суспільна небезпека, а також інноваційність, обумовлена невідомими раніше схемами скоєння злочинів, новизною самих технологій. Сучасність яскраво демонструє стрімкий розвиток високих технологій. Цей період ознаменував собою стрімкий розвиток кібернетичних технологій, різке збільшення обсягів впливу глобальної мережі інтернет, всеосяжність інформаційних потоків і глобалізацію інформаційних процесів. Це, у свою чергу, прямо сприяє на розвиток злочинності в даній сфері. Отже, одночасно з прогресом, спостерігається і зростання злочинності у сфері інформаційної безпеки.

Проблема забезпечення інформаційної безпеки України знайшла відображення в законах «Про основи національної безпеки України», «Про концепцію національної програми інформатизації», «Про національну програму інформатизації», а також у Концепції національної безпеки України. Утворений кібернетичний простір являє собою не просто сукупність окремих технічних об'єктів, здатних сприймати сліди активності людини, та утворює щільно пов'язане середовище, в якому криміналістичні зображення можуть перетворюватися, копіюватися і передаватися від одного пристрою до іншого. В результаті ці сліди шляхом великої кількості локальних взаємодій починають передаватися на великі відстані та зберігатися в цифровому вигляді в необмеженій кількості місць і практично необмежений час. Такі особливості привели до того, що криміналістика була змушена дослідити особливості цих об'єктів, вивчати специфіку механізмів кіберпростору.

На законодавчому рівні визначено, що кіберзагроза – наявність та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів [2].

Серед найбільш розповсюджених кіберзлочинів слід відзначити наступні:

- наявність пристрою, зараженого вірусом чи іншою загрозою безпеці (53%);
- проблеми з дебетовими або кредитними картками (38%);
- усунення пароля облікового запису (34%);
- несанкціонований доступ або хакерство електронної пошти чи облікового запису соціальних медіа (34%);
- придбання онлайн, яке виявилося шахрайським (33%);

– натискання на шахрайську електронну пошту або надання конфіденційної інформації у відповідь на шахрайство з електронною поштою (32%).

Зазначимо, що сьогодні експерти звертають увагу на нові кіберзагрози, які пов'язані з масовим розвитком технологій І 4.0, концепція яких передбачає швидкий розвиток та нарощування сегменту технологій четвертої хвилі в економічній і позаекономічній сферах. Причому станом на 2018-2019 р. р. цей процес лише розпочався. І на поточному етапі розвитку І 4.0 точкою входу для найбільшої кількості кібератак є персональні, підключені до Мережі портативні пристрої (смартфони, планшети тощо), парк яких набув тотального охоплення і продовжує швидко зростати, збільшуючи можливості кібератаки для зловмисників [3].

У 2018 році увагу працівників кіберполіції було зосереджено на розслідуванні злочинів, вчинених у сфері високих інформаційних технологій. Так протягом року працівники Департаменту кіберполіції були залучені до розслідування більше 11 тисяч кримінальних проваджень.

Зокрема, протягом року найбільша кількість злочинів була зосереджена у місті Києві, а також на території Одеської, Миколаївської та Львівської областей. Упродовж року поліцейські виявили 6 тисяч злочинів, вчинених у сфері використання високих інформаційних технологій.

У 2018 році працівники поліції викрили більше 800 осіб, які були причетні до вчинення злочинів у сфері високих інформаційних технологій. Водночас, у сфері кібербезпеки найбільше виявлено користувачів шкідливого програмного забезпечення, які вчиняли злочини, використовуючи придбані віруси у DarkNet.

Сьогодні українська кіберполіція розробляє і успішно впроваджує у практичну діяльність поліції сучасні методики виявлення, фіксації і дослідження цифрових доказів. Зокрема, упродовж 2018 року спеціалістами з кіберполіції оглянуто та проаналізовано 5,5 петабайтів інформації, яка у подальшому була визначена як цифрові докази.

За результатами міжнародної співпраці у 2018 році було викрито 8 транснаціональних хакерських угруповань та взято участь у понад 30 міжнародних операціях.

Крім того, у 2018 році було підписано договори про взаємодію у сфері боротьби з кіберзлочинністю з організаціями як державного, так і приватного секторів. Серед них – представники міжнародних кампаній у сфері інформаційної безпеки та ІТ-компанії, а також поліцією Австралії, Сінгапуру, Катару та ще ряду країн. Крім того, налагоджено ефективну взаємодію з найвідомішими світовими соціальними мережами [4]. Зростання інформатизації країни та зростання тиску кібервпливів актуалізує роль

держави та відповідного державного регулювання у забезпеченні кібернетичної безпеки. Це обумовлено тим, що саме держава визначає політику національної безпеки, сталого розвитку, цифровізації економіки і т. ін.

Список використаних джерел:

1. Розпорядження КМУ від 15 листопада 2017 р. № 1023-р «Про схвалення Стратегії розвитку органів системи Міністерства внутрішніх справ на період до 2020 року». URL: https://zakon.rada.gov.ua/laws/show/1023-2017-%D1%80
2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-YIII. Відомості Верховної Ради (ВВР). 2017. № 45. ст.403.
3. Гнатюк С.Л. Кібербезпека в умовах розгортання четвертої промислової революції (industry 4.0): виклики та можливості для України. Аналітичні матеріали. URL: https://www.niss.gov.ua/doslidzhennya/analitichni-materiali/informaciyni-strategii/kiberbezpeka-v-umovakh-rozgortannya
4. Підсумки 2018 року в цифрах. Кіберполіція України: офіц. сайт. URL: https://cyberpolice.gov.ua/results/2018/
5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 за № 2594-IV. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80/conv

УДК 681.3.06

ОЛЕНА ГЕОРГІЇВНА СОКОЛОВСЬКА
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету №4 Харківського національного університету внутрішніх справ
АМІНА ІГОРІВНА ГОЛОВНЯ
курсант 1 курсу факультету №4 Харківського національного університету внутрішніх справ

ЗАСТОСУВАННЯ НАГРУДНИХ КАМЕР ПРАЦІВНИКАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Нагрудний відеореєстратор – це спеціальний пристрій, що використовується для запису, обробки та збереження інформації у форматі відео.

Body-камери, які повинні носити патрульні мають декілька недоліків. По перше, вони знімають не постійно. По друге, дуже легко виявити ведеться зйомка чи ні. По третє, записану картинку поліцейський самостійно видалити не може.

Українські правоохоронці тільки нещодавно спростували слухи, що з’явилися з початком запуску патрульної поліції про те, що body-камери працюють безперервно, в реальності все зовсім інакше.