ISO/IEC 14598 «Software engineering - Product evaluation» та адаптованих до них ДСТУ ISO/IEC 14598 «Інформаційні технології. Оцінювання програмного продукту» та має на меті допомогти оцінювачу програмного продукту ефективно провести експертизу щодо встановлення факту відповідності програмного забезпечення вимогам безпеки та захищеності.

Одержано 19.10.2018

УДК 681.3.06

Христина Андріївна ЄМЕЛЬЯНОВА,
курсант 1 курсу групи Ф4-103 факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Розвиток інформаційного суспільства призвів до появи інформаційних технологій, які стали невід'ємною частиною нашого життя. Вони дають не тільки можливість для розвитку здібностей, покращення знань та розширення кола інтересів, але й містять у собі реальні загрози. На сьогоднішній день в країні є низка нормативно-правових документів та законів, що описують проблеми забезпечення кібербезпеки держави. Проте ця база у сфері кіберзлочинності лише частково охоплює елементи, які потрібні для протидії кіберзагрозам [2].

Необхідність створення ефективної системи кібернетичної безпеки України відбулася після подій 2014 року. Інформаційна війна, яка відбувається між Росією і Україною, включає не тільки воєнні дії та інформаційно-психологічні операції, а також проведення кібернетичних атак. Виклик та загрози національній безпеці України в кібернетичному просторі призвели до створення Стратегії кібербезпеки України, що була введена в дію указом Президента України від 15 березня 2016 [1].

У законі України «Про основи національної безпеки України» та в «Доктрині інформаційної безпеки України» згадуються поняття про «комп'ютерна злочинність» та «комп'ютерний тероризм», проте визначення цих термінів в законі немає. В законі «Про боротьбу з тероризмом» поняття «комп'ютерний тероризм» не висвітлюється зовсім, а те що до нього відноситься називається «технологічним тероризмом». Для покращення нормативно-правової бази у сфері кіберзлочинності Верховною Радою України було розглянуто законопроекти: «Про основні засади забезпечення кібербезпеки України» (реєстр. №2126а від 19.05.2015) та «Про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з

кібезлочинністю» (реєстр. № 2133а від 19.06.2015). В законопроекті № 2126а визначили терміни «кіберзлочинність» та «кібертероризм».

З розпорядження Кабінету Міністрів України «Про затвердження плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України» та законопроектом «Про основні засади забезпечення кібербезпеки України» одним з військових формувань, яке займається питаннями кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України (далі – Держспецзв'язок).

В Державному центрі кіберзахисту та протидії кіберзагрозам Держспецзв'язку є структурований підрозділ Computer response team of Ukraine (далі – Cert-UA) – команда реагування на комп'ютерні надзвичайні події України. Основна мета Cert-UA – забезпечити захист інформаційних ресурсів та інформаційних та телекомунікаційних систем від несанкціонованого доступу, неправомірного використання, а також порушень їх конфіденційності, цілісності та доступності. Також сфера діяльності включає заходи, що спрямовані на ліквідацію інцидентів інформаційної безпеки, які виникають в кіберпросторі українського сегменту мережі Інтернет. В 2016-2017 рр. планується створення штатного підрозділу, який буде займатися деякими заходами, які покладені з розпорядження Кабінету Міністрів України «Про затвердження плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України» на Держспецзв'язок.

Отже, кіберпростір на сьогоднішній день відіграє велику роль у забезпеченні інформаційної безпеки людини, суспільства, держави. За останній час Україна зробила прогресивні кроки у створенні ефективної національної системи кібербезпеки. Чітке окреслення термінів дало змогу вдосконалити нормативно-правове регулювання діяльності правоохоронних органів, органів виконавчої влади та військових формувань. Але цього виявляється не достатньо для повного подолання кіберзлочинності в нашій країні. В країні потрібно підвищити обізнаність населення щодо кіберзагроз, збільшити кількість кваліфікованих спеціалістів у цій сфері. Правове реагування на проблеми посилення комп'ютерної злочинності є надзвичайно важливим. І тому, представляється досить важливим розширити правову і законодавчу базу у сфері боротьби з комп'ютерними злочинами, а саме прискорити прийняття вказаних законопроектів з обов'язковим врахуванням пропозицій державних органів, що в подальшому будуть застосовувати таку нормативно базу та постійно удосконалювати національне законодавство з метою успішної співпраці з іншими країнами та міжнародними організаціями.

Список бібліографічних посилань

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : указ Президента України від 15 березня 2016 року № 96/2016 // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 31.10.2018).

2. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. Вип. 1. С. 312-320. URL: http://nbuv.gov.ua/UJRN/boz_2012_1_37 (дата звернення: 31.10.2018).

Одержано 31.10.2018

УДК 004.056.53:004.89

Олег Вікторович ЗОЛОТУХІН,
кандидат технічних наук, доцент
доцент кафедри штучного інтелекту
Харківського національного університету радіоелектроніки;
ORCID: https://orcid.org/0000-0002-0152-7600;
Олексій Феліксович ЛАНОВИЙ,
кандидат технічних наук, доцент
доцент кафедри програмної інженерії
Харківського національного університету радіоелектроніки;
ORCID: https://orcid.org/0000-0002-4504-4301

ІДЕНТИФІКАЦІЯ БЕЗКОНТАКТНИХ ПЛАТЕЖІВ В СИСТЕМАХ КІБЕРБЕЗПЕКИ

В даний час інтернет-комерція стала невід'ємною частиною бізнесу в сфері інформаційних технологій. При цьому важливу роль в системах інтернет-комерції грають системи електронних платежів.

Як технології для безконтактних платежів розглядається технологія NFC (Near Field Communication), яка реалізується у вигляді чіпа (адаптера), вбудованого в мобільний телефон.

Технологія NFC об'єднує інтерфейс смарт-картки зчитувача в єдиний пристрій. Це дозволяє охопити в стандарті більш широкий спектр завдань і стандартизувати набагато більший набір пристроїв. На даний момент NFC технологія активно використовується перш за все у величезній кількості цифрових мобільних пристроїв, таких як мобільні телефони, в які NFC чіпи вбудовуються за замовчуванням, а також використовується в громадському транспорті і разноманітних платіжних системах (наприклад, системи АЗС).

Безконтактні технології платежів засновані на стандарті радіозв'язку ближнього радіусу дії NFC, активно впроваджуються зараз в різноманітні мобільні пристрої – смартфони, планшети, ноутбуки.

Технології безконтактних платежів дозволяють проходження операцій на малі суми тільки прикладанням карти до магнітного зчитувача – без введення ПІН-коду. При цьому карта не передається в руки касирові. Крім того, передбачена можливість «вбудовування» пристроїв (чіпів) в будь-які форми (мобільний телефон, годинник,