

Бібліографічні посилання

1. Линник О. І. Стратегія економічної безпеки підприємства як фактор зменшення впливу зовнішніх та внутрішніх загроз. *Вісник НТУ «ХПІ»*. Серія : Технічний прогрес і ефективність виробництва. Харків : НТУ «ХПІ». 2013. № 67 (1040). С. 159–169.
2. Рибальченко Л. В., Рижков Е. В., Тютченко С. М., Гавриш О. С., Варяниченко А. О. *Безпека підприємництва : монографія*. ДДУВС, 2020. 180 с.

Туряк Ч. Д., курсант 4-го курсу факультету підготовки фахівців для підрозділів стратегічного розслідування Дніпропетровського державного університету внутрішніх справ
Науковий керівник – Гребенюк А. М., доцент кафедри економічної та інформаційної безпеки, кандидат технічних наук, доцент
(Дніпропетровський державний університет внутрішніх справ)

СУЧАСНИЙ СТАН ЗАХИСТУ ІНФОРМАЦІЇ НА МОБІЛЬНИХ ПРИСТРОЯХ В КОНТЕКСТІ РОЗВИТКУ ЗАГРОЗ ТА ВИКОРИСТАННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Захист інформації на мобільних пристроях – це прийняття правових, організаційних і технічних заходів для забезпечення захисту інформації від несанкціонованого доступу, знищення, перекручення, блокування інформації, копіювання, надання, поширення та інших незаконних дій щодо такої інформації. Конфіденційність інформаційних ресурсів з обмеженим доступом, реалізація основоположного права на вільний доступ до інформації є запорукою основних прав і свобод людини.

Варто почати з того, що сучасна проблематика інформаційної безпеки на мобільних пристроях містить разом з забезпеченням безпеки інформації та інформаційних систем ще два компоненти: захист від впливу шкідливої інформації, забезпечення ухвалення обґрунтованих рішень за максимального використання доступної інформації [1].

Забезпечення інформаційної безпеки на мобільних пристроях повинно вирішувати такі основні завдання:

- виявлення, оцінка та запобігання загрозам інформаційним системам і ресурсів;
- захист прав юридичних і фізичних осіб на інтелектуальну власність;
- збір, накопичення і використання інформації;

– захист державної, службової, комерційної, особистої та інших таємниць.

Загрози інформаційним системам і ресурсів для користувачів сучасних мобільних пристроїв умовно можна поділити на чотири основні групи:

1) програмне забезпечення – впровадження «вірусів», апаратних і програмних закладок; знищення і зміна даних в інформаційних системах;

2) технічні, в тому числі електронне перехоплення інформації в лініях зв'язку, електронне придушення сигналу в лініях зв'язку і системах управління;

3) фізичне знищення технологічного обладнання і носіїв інформації; крадіжка медіа та апаратних або програмних ключів та/або паролів;

4) інформація – порушення правил обміну інформацією; незаконне збирання і використання інформації; несанкціонований доступ до інформаційних ресурсів; незаконне копіювання даних в інформаційних системах; дезінформація, приховування або фальсифікація інформації; викрадення інформації з баз даних [2].

Цим загрозам можна протистояти, створивши і запровадивши ефективні системи захисту інформації від шкідливого ПЗ на мобільних пристроях.

Події останніх років вказують на те, що досить часто обговорюється і є дискусійною проблема інформаційного протиборства в Інтернеті – так званої кібервійни. Її основна мета – дестабілізувати інформаційні системи і доступ до Інтернету в державних установах, фінансових і ділових центрах, а також створити безлад і хаос в державах, які покладаються на Інтернет у своєму повсякденному житті.

Міждержавні відносини і політичні протистояння можуть тривати в Інтернеті у формі кібервійни: вандалізм, пропаганда, шпигунство і прямі атаки на комп'ютерні системи і сервери, шкідливе ПЗ на мобільних пристроях.

З поширенням інформаційних технологій на мобільних пристроях громадяни, підприємства і державні установи буквально стали залежати від Інтернету у повсякденному житті. Їх використання для атаки на інформаційні системи іншої держави може завдати значних економічних збитків і призвести до розбіжностей в повсякденному житті держави.

У міру того як нові технології переходять на мобільні пристрої, масштаби кібервійни постійно збільшуються і підвищують її загрози. Деякі держави приділяють особливу увагу захисту від кібервійни і надають необхідні ресурси для організації систем захисту і підтримки спеціальних сил, завданням яких є підвищення і поліпшення інформаційної безпеки. Контроль над мобільними пристроями з доступом до мережі «Інтернет» в наш час визначає стан національної безпеки держави [3].

Міжнародне право відіграє дуже важливу роль в боротьбі з кіберзлочинністю. Створення цілодобових контактних центрів, юридичне

визначення кіберзлочинності, екстрадиція злочинців, міжнародна взаємодія компетентних органів, проведення навчань і обмін інформацією – все це сприяє впровадженню ефективних методів реагування на міжнародні злочини і боротьби зі злочинами, скоєними в кіберпросторі.

Розвиток інформаційних технологій для користувачів сучасних мобільних пристроїв має тенденцію до все більшого прискорення, тому правова база повинна не тільки йти в ногу з часом, а й змінюватися для вирішення всіх нагальних проблем людей, суспільства та міжнародної спільноти в галузі інформаційної безпеки.

Бібліографічні посилання

1. Дмитренко М. Проблеми інформаційної безпеки України. URL: <http://socialscience.com.ua/article/807> (дата звернення: 25.03.2021).
2. Логінов О. Сучасні проблеми забезпечення інформаційної безпеки в контексті формування системи державного управління. *Науковий вісник Юридичної академії МВС України*. Київ, 2003. Вип. 3. 224 с.
3. Кормич Б. Інформаційна безпека: організаційно-правові основи : навч. посіб. Київ : Кондор, 2004. 384 с.

Утвенко В. В., курсант 2-го курсу факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ
Науковий керівник – Гребенюк А. М., доцент кафедри економічної та інформаційної безпеки, кандидат технічних наук, доцент
(Дніпропетровський державний університет внутрішніх справ)

ПРОБЛЕМАТИКА УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННИХ ОРГАНІВ

Детально розглянувши сучасний стан розвитку суспільства, потрібно звернути увагу на значне підвищення ролі інформаційних технологій у людській життєдіяльності, а також у суспільстві і державі. Стрімкий розвиток інформаційних процесів, започаткування нових винаходів, досягнень та технологій у виробничі та управлінські процеси – ці події зумовили не лише можливість поступального розвитку нашої держави, але і стали факторами зростання кількості злочинів, які, зі свого боку, вдосконалили засоби і способи вчинення кримінальних правопорушень. Ця