1. Сили та засоби правоохоронних органів, об'єднані надійними мережами, мають змогу покращеного обміну інформацією та досягнення інформаційної переваги супротивником, в ході охорони громадської безпеки і порядку.

2. Обмін інформацією підвищує якість (достовірність, своєчасність, адекватність, об’єктивність та інш.) інформації та загальної ситуаційної поінформованості.

3. Загальна ситуаційна обізнаність дозволяє забезпечувати взаємодіє між силами правоохоронних органів і самосинхронізацію між відповідними засобами, підвищує стійкість і швидкість управління, а це, своєю чергою, різко підвищує ефективність виконання спланованих завдань.

Використання IoBT пов’язано із виникненням ризиків, основним з яких є несанкціонований доступ до важливих систем та безпосередньо даних. Недостатня захищеність може привести до перехоплення інформації, пошкодження та знищення техніки.

Надійність систем є ще одним суттєвим ризиком у застосуванні IoBT. Проблеми з надійністю або непередбачувані відмови можуть призвести до серйозних проблем в ході спланованих заходів та під час проведення операцій. В свою чергу, можна додати, що висока залежність від технологій IoBT може привести до ситуації, коли відсутність або несправність відповідних технічних засобів може привести до зриву виконання відповідних заходів.

Ще одним з перспективних ризиків у застосуванні IoBT є автономність застосування зброї, відповідальність за прийняття рішень системами штучного інтелекту та можливість шкоди для цивільного населення.

Таким чином, управління вказаними ризиками вимагає не лише технічних заходів забезпечення безпеки, але й ретельного регулювання, визначення стандартів та навчання персоналу щодо безпеки та етики використання IoBT.

**Донець Я. О.**
курсант факультету № 4 Харківського національного університету внутрішніх справ
**Світличний В. А.**
доцент кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ, кандидат технічних наук, доцент

## КІБЕРБЕЗПЕКА – ЗБРОЯ У БОРОТЬБІ З ШАХРАЯМИ

**Вступ.** В наші дні, злодій – це не обов'язково холоднокровна озброєна людина. Інформаційна революція призвела до того, що кожен може виявитися злодієм, навіть звичайний студент із ноутбуком та доступом до інтернету. Процес інформатизації сьогоденного суспільства призвів до того, що інформація перетворюється у так званий стратегічний ресурс, який володіє цінністю, тобто має якості товару. Суспільство вже не може існувати та звичайно функціонувати без інформаційного обміну в інформаційно-телекомунікаційних системах. На даному етапі, внаслідок швидкого розвитку та застосування сучасних технологій, питання захисту людства від їхнього використання в злочинних цілях усе більше загострюється.

**Виклад основного матеріалу**. З початку війни в Україні, ми стали свідками чисельних кібератак, які охопили державні установи, громадян та приватні організації. Підприємства, які є частиною критичної інфраструктури, зокрема, телекомунікаційні, енергійні, медіа та фінансові компанії, також повинні знаходитися у режимі підвищеної готовності, тому що саме ці галузі часто стають пріоритетними цілями у період війни.

Сьогодні, війна в інформаційному просторі може завдати не меншої шкоди, чим війна на полі бою.

Кіберзлочиність не має державних кордонів, таким чином злочинець може загрожувати інформаційним системам, які знаходяться в будь-якій державі світу. Ці злочини сильно відрізняються від інших, давно визначених злочинів, що обумовлює складність цієї процедури розслідування відповідно до чинних законодавствами держав

Взагалі, комп'ютерна злочинність має наступні характеристики [1]:

- Предметами комп'ютерних злочинів є права на об'єкти нерухомості. Інформаційні атаки працюють відносно інформації пенсійних та інвестиційних фондів, через них відбувається котирування інструментів фондового ринку, обертаються індекси на валютних, торгових та фондових ринках. Фактами таких атак на об'єкти є інформаційна інфраструктура, котрі вона забезпечує функціонуванням сфер, критичних для державного управління та економіки;
- Боротьба з кіберзлочинами для постанов багатьох країн не є пріоритетністю, через що не можна зрозуміти достатній рівень небезпеки від комп'ютерних злочинців у багатьох державах;
- Брак у деяких державах своєрідної взаємодії між правоохоронними відомствами та приватним бізнесом з питань дозволу частини інформації (елементів доказу у електронному вигляді) та її збереження в комп'ютерних системах.

На перший погляд, кожна людина може подумати, що кібератаки не завдають великої шкоди та не забирають людських життів, але це не так. Можна навести декілька прикладів [2].

Збір інформації – злом приватних сторінок або серверів, бази даних для збору цінної інформації. У такому випадку дезінформація та викрадення матеріалів. Можна навести наприклад з відомостей щодо пересування військ у районі ведення бойових дій, призводить до неминучих людських втрат. Це називають – кібершпигунством.

Пропаганда – розсилка повідомлень (спаму ), що містять інформацію пропагандистського напрямку, неправдиві новини для просування своєї ідеології та дезорієнтації населення.

Вандалізм – це атаки, які не вбивають людство, але завдає удару по репутації держави у світі та серед населення, простими словами, завдає втрат по авторитету.

Не для кого не секрет, що використовуючи кіберпростір, хакери можуть зламати захищені дані та отримати необхідну інформацію, тому вам варто спрямувати свої сили на захист мереж і забезпечити їх безпеку. Треба дотримуватися таких рівнів захисту інформації:

Запобігання – доступ до інформації має тільки персонал, який отримав спеціальний допуск та вже має необхідні фахові навички.

Виявлення – треба запобігати проявам злочинів і зловживань, навіть коли системи захисту були обійдені.

Обмеження – зменшити обсяг втрат, у випадку, коли злочин все-таки здійснився, незважаючи на спроби щодо його виявлення.

Відновлення – слід забезпечити продуктивне очищення інформації та даних за наявності документованих і перевірених планів з відновлення.

Суспільство вимагає правил, утворення стандартів, норм, положень, інструкцій та безліч інших документів, задля того, щоб почувати себе захищеним у кіберпросторі.

Кожен день з’являються нові галузеві нормативні документи, які відносяться до кіберризиків, підвищується інтерес до певної галузі зі органів.

В Україні створюються норми з безпеки для об’єктів критичної інфраструктури. Все частіше можна почути заклики до більш активної участі у обміні інформацією, а також до надання обов’язкової звітності про кібератаки для нашої протидії виникненню наслідків таких атак. Треба розуміти встановлення обов’язкових вимог у цій сфері. До речі, якщо це і не відбудеться в найближчому часі, загальна думка сьогодні така, що державні органи, структури і навіть клієнти хочуть розширити свої знання про кібербезпеку.

На нашу думку, необхідно надалі розвивати співпрацю у сфері надання інформаційної безпеки використовуючи двосторонні і багатосторонні договори через об'єднання національних законодавств у сфері інформаційної безпеки, організацію спільних виробництв захисту інформації, звісно підготовку професіоналів у сфері інформаційної безпеки інформаційно-телекомунікаційних систем.

**Висновки.** Успішне вирішення проблем інформаційної безпеки може існувати лише при хорошій взаємодії державних структур усіх держав на основі прийнятих нормативно-правових документів у сфері інформаційної безпеки держав. Державі необхідне збільшення інвестування в кібербезпеку, щоб протидіяти атакам на великі державні й приватні компанії і запобігати спробам дестабілізувати суспільство. Основи законодавчих механізмів для продуктивного кіберзахисту в умовах воєнного стану закладені. Обов'язок для кожного – при виявленні кібератаки швидко запустити цей механізм задля того, щоб у майбутньому таких атак та збитків від них ставало як найменше.

**Література**


1. Балашов В. Гаджет как опасность. Как украинцам уберечься от кибератак во время войны? – Delo.ua. Останні новини України та світу онлайн -Головний діловий портал Delo.ua. URL: https://delo.ua/ru/technologies/gadzet-kak-opasnost-kak-ukraincam-uberecsya-ot-kiberatak-vo-vremya-voiny-395687/
2. Шахрайство під час війни: схеми, що діють зараз. finance.ua. URL: https://finance.ua/ua/saving/moszenniczestvo-vo-vremia-vojny



**Єсімов С. С.**

професор кафедри адміністративно-правових дисциплін Інституту права Львівського державного університету внутрішніх справ, кандидат юридичних наук, доцент


## ПОНЯТТЯ, ОЗНАКИ І КЛАСИФІКАЦІЯ ЦИФРОВОЇ ІНФОРМАЦІЇ

Незважаючи на повсюдне активне використання терміна «цифрова інформація», легальне визначення цього поняття відсутнє. Чинне законодавство переважно використовує такі визначення, як «електронне повідомлення – інформація, передана чи отримана користувачем інформаційно-комунікаційної мережі», електронний документ – документована інформація, подана в електронній формі, тобто у вигляді, придатному для сприйняття людиною з використанням електронних обчислювальних машин, для передачі інформаційно-комунікаційних мереж або обробки в інформаційних системах та аналогічні їм.

Незважаючи на використання категорії «цифрова інформація» більшістю галузей права, у тому числі цивільним правом, наукові дослідження щодо визначення даного