Куницький Данило Віталійович
Студент н. гр. 214_СПРБ ННІ права та психології НАВС

Науковий керівник:
Тарасенко Володимир Петрович
кандидат фізико-математичних наук, старший викладач кафедри інформаційних технологій ННІ права та психології НАВС

БОРОТЬБА З КОМП'ЮТЕРНИМИ ПРАВОПОРУШЕННЯМИ

Комп'ютерні правопорушення «cybercrime» – це злочинність, пов'язана як з використанням комп'ютерів, так і з використанням інформаційних технологій і глобальних мереж. Це є одним з найактуальніших викликів сучасного суспільства. Швидкий розвиток технологій створює нові можливості для кіберзлочинців, ускладнюючи завдання правоохоронних органів.

Розглянемо деякі з основних проблем, з якими стикаються в цій галузі: кіберзлочинці можуть легко приховати свою справжню особистість, використовуючи різноманітні інструменти анонімізації (VPN, TOR, проксі-сервери тощо); складність встановлення юрисдикції: Коли злочин скоєно з використанням комп'ютерів, розташованих в різних країнах, виникають питання щодо того, за якими законами слід судити злочинця; з'являються нові типи кіберзлочинів, для розслідування яких необхідні нові знання та інструменти; законодавство часто не встигає за темпами розвитку технологій, що ускладнює боротьбу з новими видами кіберзлочинів; не існує єдиного міжнародного закону про кіберзлочинність, що ускладнює міжнародне співробітництво в цій галузі; рівень захищеності інформаційних систем в різних країнах значно відрізняється, що створює умови для кіберзлочинців; існує гостра нестача фахівців з кібербезпеки, здатних ефективно протистояти кіберзагрозам; підготовка висококваліфікованих фахівців з кібербезпеки вимагає значних фінансових ресурсів; сучасні кіберзлочини часто залишають після себе величезні обсяги цифрових слідів, аналіз яких вимагає значних обчислювальних ресурсів і часу; збереження цілісності цифрових доказів під час їх збору, фіксації та аналізу є складним завданням; багато країн не виділяють достатньо коштів на боротьбу з кіберзлочинністю; забезпечення кібербезпеки вимагає значних фінансових витрат як з боку держави, так і з боку приватних компаній.

Шляхи розв'язання проблем боротьби з комп'ютерними правопорушеннями:

- *Міжнародне співробітництво*:

1. Уніфікація законодавства: розробка єдиних міжнародних стандартів та законів, що регулюють кіберпростір, дозволить ефективніше переслідувати кіберзлочинців, незалежно від їхнього місцезнаходження.

2. Спільні розслідування: створення міжнародних слідчих груп для розслідування складних кіберзлочинів, що виходять за рамки національних юрисдикцій.

3. Обмін інформацією: створення безпечних каналів для обміну розвідувальною інформацією між країнами щодо кіберзагроз.

- *Розвиток технологій*:

1. Штучний інтелект: застосування ШІ для виявлення та запобігання кіберзагрозам, аналізу великих обсягів даних та автоматизації рутинних процесів у кібербезпеці.

2. Блокчейн: використання технології блокчейн для забезпечення безпеки та прозорості транзакцій, а також для створення доказової бази в кіберрозслідуваннях.

3. Квантові комп'ютери: розробка квантових алгоритмів для створення незламних систем шифрування та розкриття складних криптографічних систем, які використовують кіберзлочинці.

- *Підвищення кваліфікації фахівців*:

1. Освіта: розширення програм підготовки фахівців з кібербезпеки на всіх рівнях освіти, від шкіл до університетів.

2. Постійна освіта: створення систем постійної освіти для фахівців у галузі кібербезпеки, щоб вони могли бути в курсі останніх тенденцій і загроз.

3. Стимулювання кар'єри: створення сприятливих умов для роботи в галузі кібербезпеки, включаючи гідну оплату праці та перспективи кар'єрного зростання.

- *Співпраця держави, бізнесу та громадянського суспільства*:

1. Інформування населення: проведення масштабних інформаційних кампаній для підвищення обізнаності громадян щодо кіберзагроз та засобів їх запобігання.

2. Створення центрів кібербезпеки: створення спільних центрів кібербезпеки, де державні органи, бізнес та громадські організації зможуть обмінюватися інформацією, розробляти спільні стратегії та координувати свої дії.

3. Створення програм bug bounty: стимулювання етичних хакерів до виявлення вразливостей в інформаційних системах шляхом виплати винагород за знайдені вразливості.

- *Удосконалення законодавства*:

1. Оновлення кримінального кодексу: внесення змін до кримінального кодексу для посилення відповідальності за кіберзлочини та адаптація його до нових видів кіберзагроз.

2. Захист прав користувачів: забезпечення захисту прав користувачів у цифровому середовищі, включаючи право на конфіденційність, захист персональних даних та свободу слова.

***Основні види кіберзлочинів**:*

1. *Хакерство*: несанкціонований доступ до комп'ютерних систем з метою отримання інформації, модифікації даних або порушення роботи системи.

2. *Фішинг*: отримання конфіденційної інформації (паролів, номерів кредитних карток) шляхом обману користувачів за допомогою підроблених веб-сайтів або електронних листів.

3. *Вайшинг*: використання вразливостей бездротових мереж для перехоплення даних.

4. *Вимога викупу (ransomware)*: блокування доступу до комп'ютерних систем або шифрування даних з вимогою виплати викупу за їх розблокування.

5. *Розповсюдження шкідливого програмного забезпечення*: створення та розповсюдження вірусів, троянів, черв'яків та іншого шкідливого програмного забезпечення.

6. *Кредитні шахрайства*: використання викрадених банківських даних для здійснення незаконних транзакцій.

7. *Дифамація та кібербулінг*: розповсюдження недостовірної інформації або образливих повідомлень про інших осіб в Інтернеті.

8. *Інтелектуальна власність*: порушення авторських прав, торгівля піратськими копіями програмного забезпечення, музики, фільмів тощо.

Як закордонні країни, так і Україна активно працюють над розробкою та впровадженням ефективних механізмів протидії кіберзагрозам. Давайте проведемо порівняльний аналіз їхніх підходів.

Спільні риси:

- *Визнання кіберзлочинності як серйозної загрози*: і за кордоном, і в Україні кіберзлочинність розглядається як одна з найсерйозніших загроз національній безпеці.
- *Розробка законодавчої бази*: в більшості країн світу, в тому числі й в Україні, існують закони, що регулюють відповідальність за кіберзлочини.
- *Створення спеціалізованих підрозділів*: в правоохоронних органах створені спеціальні підрозділи для розслідування кіберзлочинів.
- *Міжнародне співробітництво*: країни активно співпрацюють в рамках міжнародних організацій для обміну інформацією та координації дій у боротьбі з кіберзлочинністю.

Відмінності та особливості:

- *Рівень розвитку законодавства*: зарубіжні країни, особливо країни Європи та США, мають більш розвинену законодавчу базу в галузі кібербезпеки. Українське законодавство постійно оновлюється, але все ще потребує вдосконалення.

- *Технічне оснащення*: багато закордонних країн мають більш сучасне технічне оснащення для боротьби з кіберзлочинністю, що дозволяє їм ефективніше проводити розслідування.
- *Рівень кібергігієни населення*: в розвинених країнах рівень кібергігієни населення, як правило, вищий, що ускладнює роботу кіберзлочинців.
- *Фінансування*: зарубіжні країни, як правило, виділяють більші кошти на боротьбу з кіберзлочинністю.
- *Співпраця з приватним сектором*: за кордоном більш розвинена практика співпраці державних органів з приватним сектором у сфері кібербезпеки.

Список використаних джерел:

1. Legal IT group. Комп'ютерні злочини. Правове регулювання відповідальності за кіберзлочини в Україні.
2. Кримінальний кодекс Розділ XVI. Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.
3. Кіберзлочинність: актуальна судова практика – Think brave. Liga:Zakon. https://biz.ligazakon.net
4. Конвенція про кіберзлочинність.