Актуальні питання боротьби з кіберзлочинністю як складової загально-кримінальної злочинності

Огієвич В.
студент 3 курсу факультету №4
Чінь Тху Нга
студент 3 курсу факультету №4
Науковий керівник: Косаревська О.В.
к.пед.н., доцент
доцент кафедри кібербезпеки та
інформаційного забезпечення ОДУВС

В сучасних умовах інтенсивного розвитку інформаційного суспільства значно поширюється загальна кількість злочинів , пов'язаних з використанням комп'ютерної техніки та мережі інтернет, що дає підставу визначити актуальність появи самостійного прошарку в структурі загально-кримінальної злочинності транснаціонального характеру – кіберзлочинності, оскільки злочинні акти щодо інформаційних систем утворюють загрозу організаціям, установам, фізичним особам і взагалі інформаційній безпеці як України так і інших держав.

Огляд сучасної науковій думки стосовно проблем протидії кіберзлочинності, а саме робіт: Довбиш А.С., Іванченко О.Ю., Орлов О.В., Онищенко Ю.М., Семенов В.В., Гусева В.О., Пархоменко Л.В., Войціховський А.В. та інші дає підставу наголосити на основні напрямки цієї проблеми.

1. Невизначеність основних категорійних понять у сфері кіберзлочинності та неузгодженість сталої класифікації кіберзлочинів.

Термін «кіберзлочинність» в теорії наукового пізнання ще досі не знайшов свого остаточного визначення. Узагальненим поняттям є розуміння кіберзлочинності як сукупності злочинів в кіберпросторі, ознаками яких буде скоєння їх за допомогою комп'ютерних систем (мереж), а також інших засобів доступу до кіберпростору і проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних.

Тому сама класифікація кіберзлочинів відбувається відповідно до об'єкта та предмета посягання, способу його скоєння.

В залежності від виду загроз кібербезпеку можна розглядати як забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації, інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб, інформаційних прав і свобод людини і громадянина.

З огляду функцій кіберполіції, як новоутвореного 5 листопада 2015 р. структурного підрозділу Національної поліції України, класифікація кіберзлочинів має таку структуру:

1. У сфері використання платіжних систем:

- скімінг (шимінг) - незаконне копіювання вмісту треків магнітної смуги (чіпів) банківських карток;
- кеш-тренінг - викрадення готівки з банкомату шляхом встановлення на шатер банкомату спеціальної утримуючої накладки;
- кардінг – незаконні фінансові операції з використанням платіжної картки або її реквізитів, що не ініційовані або не підтверджені її держателем;
- не санкціоноване списання коштів з банківських рахунків за допомогою систем дистанційного банківського обслуговування.

2. У сфері електронної комерції та господарської діяльності:

- фішинг - виманювання у користувачів Інтернету їх логінів та паролів до електронних гаманців, сервісів онлайн аукціонів, переказування або обміну валюти, тощо;
- онлайн шахрайство – заволодіння коштами громадян через інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку;

3. У сфері інтелектуальної власності:

- піратство – незаконне розповсюдження інтелектуальної власності в Інтернеті;
- кардшарінг – надання незаконного доступу до перегляду супутникового та кабельного TV;

4. У сфері інформаційної безпеки:

- соціальна інженерія – технологія управління людьми в Інтернет просторі;
- мальваре – створення та розповсюдження вірусів і шкідливого програмного забезпечення;

- протиправний контент – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства;
- рефайлінг – незаконна підміна телефонного трафіку.

2. Транснаціональний характер мережі «інтернет» та відсутність механізмів контролю над інформаційними мережами необхідного для правозастосування.

Ця проблема виникає за рахунок децентралізованої структури інформаційної мережі і відсутності національних кордонів у кіберпросторі.

Розвиток законодавчої бази і реагування на всі проблеми боротьби з кіберзлочинністю поки що відстає від розвитку інформаційних технологій. Механізми контролю запобігання та розслідування посягань у кіберпросторі сьогодні дуже обмежені як соціально, так і технічно. Це обумовлює можливість стати жертвою використання інформаційних технологій в злочинних цілях, за рахунок автоматизації та швидкості використання комп'ютерів.

Також слід звернути увагу, що останнім часом з'явилася тенденція укріплення зв'язку між кіберзлочинністю та організованою злочинністю. Інтернет використовується як індивідами, так і невеликими злочинними групами. При цьому, він виконує функцію не тільки як допоміжний засіб скоєння злочину, а як місце і основний засіб вчинення традиційних злочинів – шахрайств, крадіжок, вимагань. Злочинці створюють сектори тіньового ринку, з поділом праці між злочинними групами і цілими майданчиками, для торгівлі програмним забезпеченням для вчинення злочинів, продажу інформації тощо.

3. Вдосконалення кодифікації кіберзлочинів у кримінальному законодавстві України.

Дослідження провідних науковців стосовно комп'ютерної злочинності та комп'ютерної безпеки, а саме: Біленчука П.Д., Геллера А.В., Калюжного Р.А., Карчевського М.В., Супруженка А.М., Чиркова Д.К., та інших доводить, що поняття «комп'ютерний злочин», «кіберзлочин» в загальному розумінні можуть бути ефективно використані при дослідженні кримінологічних, кримінально-процесуальних, криміналістичних аспектів.

Щодо національного кримінально-правового дискурсу, то найбільш доцільним слід вважати визначення кіберзлочинності як «злочинів у сфері використання інформаційних технологій».

Так, розділ XVI Особливої частини КК України містить перелік злочинів у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електронного зв'язку, що зазначається у ст. ст. 361, 361-1, 361-2, 362, 363, 363-1.

Крім цього, окремі дослідження (Орлов О.В., Онищенко Ю.М.) розглядають розширення переліку так званих «старих злочинів» кіберзлочинів, які підпадають під дію Конвенції про кіберзлочинність [с. 37]. До таких діянь відносяться:

- різні види підробок (ст. ст. 199, 200, 215, 216, 224, 290, 318, 358, 366 ККУ);
- шахрайство з різними предметами (ст. ст. 190, 192, 222, 262, 308, 312, 313, 357, 410 ККУ);
- ввезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 301 ККУ);
- порушення авторського права й суміжних справ (ст. 176 ККУ).

Все це зумовлює необхідність кодифікації законодавства України у сфері боротьби з кіберзлочинністю.

Швидкий розвиток і інформаційно-комунікативних технологій, зокрема мережі Інтернет, вплинув на збільшення способів злочинних посягань на власність.

Злочинці все частіше використовують нові способи зараження комп'ютерів шкідливими програмами, які дозволяють отримати злочинний прибуток.

Так, відповідно до Звіту [3, с. 208, 4] (див. ст. 40-41) корисливі злочини вчиняють так звані «хакери».

Так, за дослідженнями Яблукова М.П. та Біленчука П.Д., суб'єктами скоєння злочинів, пов'язаних з несанкціонованими доступами до електронно-обчислювальної техніки, систем комп'ютерних мереж вчиняються:

- програмістами;
- інженерами;
- операторами;
- співробітниками банків [41, 9%];
- іншими співробітниками банку [20, 2%];
- звільненими [8, 6%];
- сторонніми особами [25,5%][с. 23].

На підставі вищезазначеного можна зробити наступні висновки.

1. Комп'ютерні злочини це одна з найдинамічних груп суспільно-небезпечних посягань у структурі загально-кримінальної та транснаціональної злочинності.

2. Криміналістична особливість кіберзлочинів полягає в тому, що їх розкриття не можливе без застосування та використання комп'ютерних технологій. Особливо гостро постає проблема збирання доказів в електронній формі при виконанні оперативно-розшукових заходів у сфері протидії кіберзлочинності.

3. Сучасні кіберзлочинці є представниками новітньої цифрової доби та характеризуються підвищеним рівнем обізнаності у сфері інформаційно-телекомунікаційних систем, що ускладнює розкриття цих злочинів.

4. Основними недоліками у протидії кіберзлочинності є неузгодженість нормативно-правових актів стосовно процедури проведення та кадрового потенціалу експертів для проведення комп'ютерно-технічних експертиз в цій сфері.

5. Однією із нагальних проблем кадрового забезпечення підрозділів кримінальної поліції Національної поліції України є нестача ІТ-спеціалістів, за рахунок: недостатньої інформаційно-технологічної спеціалізованої підготовки оновленого складу підрозділів кіберполіції, низького матеріально-технічного оснащення оперативних підрозділів кіберполіції, неврегульованості процесуальної взаємодії між національними та міжнародними поліцейськими структурами в світлі вимог Конвенції про боротьбу з кіберзлочинністю.

Література:

1. Актуальні напрями державної політики України у сфері боротьби з кіберзлочинністю / О.В. Орлов, Ю.М. Онищенко // Теорія та практика державного управління.-2013.- Вип. 3. – С 3-9. – Режим доступу: http://gov.ua/j-pdf/Tpdu_2013_3_3.pdf

2. 2015 Internet Securit Threat Report [Електронний ресурс]. –Режим доступу: http://www.symantec.com/security_respons/publication/ whitepapers.jsp

3. В тенетах світової павутини: тенденції розвитку кібербезпеки у 2016 році // [Електронний ресурс]. Режим доступу: http://defence-ua.com/index.php/statti/

Загальна методика експертної оцінки рівнів захищеності інтегрованих інформаційних систем МВС України

Кудінов В.А.
кандидат фізико-математичних наук, доцент,
професор кафедри інформаційних технологій та кібернетичної
безпеки Національної академії внутрішніх справ

Серед основних напрямів державної інформаційної політики в Україні сьогодні, відповідно до ст. 3 Закону України «Про інформацію», є створення інформаційних систем і мереж інформації, розвиток електронного урядування; постійне оновлення, збагачення та зберігання національних інформаційних ресурсів; забезпечення інформаційної безпеки України. Тому останнім часом в Україні спостерігається інтенсивне впровадження сучасних інформаційних технологій практично у всі сфери життєдіяльності держави, у тому числі в діяльність органів та підрозділів Національної поліції, МВС України.

В МВС України вже протягом більше 45 років накопичено чималий досвід використання різноманітних інтегрованих інформаційних та інформаційно-телекомунікаційних систем оперативно-розшукового та інформаційно-довідкового призначення. Департаментом інформаційних технологій МВС України створена та постійно удосконалюється система інформаційного забезпечення, яка здійснює інформаційну підтримку діяльності органів та підрозділів Національної поліції щодо забезпечення запобігання кримінальним правопорушенням, їх виявлення, припинення, розкриття і розслідування, розшуку осіб, які вчинили кримінальні правопорушення, надає багатоцільову статистичну, аналітичну та довідкову інформацію, допомагає при розв'язані інших завдань боротьби зі злочинністю.

Одним з важливих напрямів ефективного функціонування інтегрованих інформаційних систем МВС України є забезпечення їх захищеності.

Побудова комплексної системи захисту інформації (далі – КСЗІ) в цих системах повинно дозволити запобігти або ускладнити можливість реалізації загроз порушення цілісності, доступності та конфіденційності інформації, а також належного функціонування ресурсів з її обробки, знизити