методи боротьби з кіберзлочинами – юридичні, програмні, технологічні, організаційні, економічні, політичні і т.д. Ці дії матимуть успіх лише в тому випадку, якщо будуть спиратися на систему постійного моніторингу кіберпростору на загальнопланетарному та національному рівнях.

Література

1. Голубев В.А. «Кибертероризм» - миф или реальность? [Електронний ресурс] / В.А. Голубев; Центр дослідження комп'ютерної злочинності. – Режим доступу: http://www.crime-research.org. – Computer Crime Research Center
2. Карчевський М.В. Кримінально-правова охорона інформа-ційної безпеки України : монографія / М. В. Карчевський ; МВС України, Луг. держ. ун-т внутр. справ ім. Е. О. Дідоренка. – Лу-ганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. – 528 с.
3. Номоконов Виталий. Актуальные проблемы борьбы с киберпреступностью [Електронний ресурс] / Виталий Номоконов ; Владивостокский центр исследования организованной преступности, Центр исследования компьютерной преступности. – Режим доступу: http://www.crime-research.org/library/Nomokon1.html
4. Безпека комп'ютерних систем. Злочинність у сфері комп'ютерної інформації та її попередження / М.С. Вертузаєв, В.О. Голубєв, О.І. Котляревський, О.М. Юрченко. – Запоріжжя: «Павел», 1998. – 315 с.

СУЧАСНИЙ СТАН ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Власова Ю.А.
слухач 2-го курсу магістратури факультету №2
Одеського державного університету внутрішніх справ

Форос Г.В.
кандидат юридичних наук, доцент
професор кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ

На сьогодні актуальність проблеми кібербезпеки не викликає жодних сумнівів. Щодня кожен з нас стикається із необхідністю користування інформаційними технологіями. Від соціальних мереж, розміщення інформації про свої персональні дані в Інтернеті до користування банкоматами, банківськими рахунками. У зв'язку із цим виникає питання, чи врегульовано дану проблему вітчизняним законодавством і як себе захистити від кіберзлочинців.

Аналіз вітчизняного законодавства дав зрозуміти, що, на жаль, в Україні на сьогодні, навіть не визначено таких ключових понять: кіберзлочин, кіберзлочинець, кіберпростір, кібербезпека, кіберзахист. Це призводить до того, що навіть спеціальні підрозділи силових відомств, у назві яких вживається поняття „кіберзлочинність", „кібербезпека", не забезпечені відповідними нормативними документами для

визначення предмету своєї роботи.

Певною мірою термінологічні проблеми кібербезпекової сфери пов'язані і з особливостями створення та прийняття нормативних документів різного рівня [1].

Незважаючи на зусилля спеціальних відомств, на думку деяких фахівців, Україна залишається уразливою, не в останню чергу через надмірно широке впровадження західних програмних продуктів (зокрема фірми Microsoft) та використання матеріально-технічної бази іноземного виробництва. Пошук можливих „закладок" у цій продукції практично унеможливлений, а залежність української держави від згаданих продуктів становить загрозливий рівень для національної безпеки. Актуальною залишається проблема створення національної операційної системи, стимулювання з боку держави створення національного антивірусу [2].

В останні роки інформаційні мережі розвиваються занадто швидко, щоб існуючі механізми контролю встигали реагувати на нові проблеми. Хмарна обробка даних, автоматизація атак, вразливість персональної інформації в соціальних мережах на всі ці проблеми правове регулювання поки не може знайти адекватної відповіді.

Зі збільшенням числа користувачів зростають, такі фактори ризику: збільшується залежність суспільства від інформаційних технологій; збільшується можливість використання мережі для вчинення злочинів, росте потенційна можливість стати жертвою використання інформаційних технологій в злочинних цілях. При цьому вчинення злочину не вимагає великих зусиль і витрат - достатньо мати комп`ютер, програмне забезпечення та підключення до інформаційної мережі. Не потрібно навіть глибоких технічних знань: існують спеціальні форуми, на яких можна придбати програмне забезпечення для вчинення злочинів, вкрадені номери кредитних карт і ідентифікаційні дані користувачів, а також скористатися послугами з допомоги в здійсненні електронних розкрадань і атак на комп`ютерні системи як в цілому, так і на окремих стадіях вчинення злочинів [3].

Розслідування злочинів в інформаційних мережах зазвичай вимагає швидкого аналізу та збереження комп`ютерних даних, які дуже вразливі за своєю природою і можуть бути швидко знищені. У цій ситуації традиційні механізми правової взаємодопомоги і принцип суверенітету, одним з проявів якого є те, що тільки правоохоронні органи держави можуть проводити слідчі дії на його території, вимагають безліч формальних погоджень, роблячи розслідування транснаціональних кіберзлочинів проблематичним.

Серед причин комп'ютерних злочинів відзначають такі:

- швидкий перехід від традиційної паперової технології зберігання та передавання;
- інформації до електронної за одночасного відставання технологій захисту інформації, зафіксованої на машинних носіях;
- широке використання локальних обчислювальних мереж, створення глобальних мереж і розширення доступу до інформаційних ресурсів;
- постійне ускладнення програмних засобів, що викликає зменшення їх надійності та збільшення кількості уразливих місць;
- недостатньо розвинене спеціальне законодавство щодо різних аспектів

комп'ютерної злочинності, у той час як цей вид злочинів швидко прогресує;

- технологічна залежність від закордонних виробників ПЗ, і, як наслідок, іноземних держав;
- широко розповсюджена практика несанкціонованого копіювання, неліцензійне програмне забезпечення;
- брак державних коштів на дороговартісні заходи із забезпечення кібербезпеки, проблеми з визначенням економічної доцільності таких заходів.

Виділяють комп'ютерні злочини, в яких: а) комп'ютер є об'єктом правопорушення та б) комп'ютер використовується як засіб, що сприяє вчиненню злочину.

Комп'ютер є об'єктом правопорушення, коли мета злочинця - викрасти інформацію або завдати шкоди системі, що цікавить його. З комп'ютером як з об'єктом пов'язані такі види злочинів: а) вилучення засобів комп'ютерної техніки. До цієї групи відносяться традиційні способи здійснення звичайних видів злочинів, у яких дії злочинця направлені на вилучення чужого майна; б) розкрадання інформації; в) розкрадання послуг (отримання несанкціонованого доступу до якоїсь системи з метою безоплатного користування послугами, що надаються нею); г) пошкодження системи. Дана група об'єднує злочини, здійснені з метою зруйнувати або змінити дані, що є важливими для власника одного або багатьох користувачів системи - об'єкта несанкціонованого доступу;

Використовувані в даний час заходи попередження комп'ютерних злочинів можна об'єднати в три групи: технічні; організаційні; правові.

Технічні заходи захисту від несанкціонованого доступу до комп'ютерних систем передбачають: використання засобів фізичного захисту, включаючи засоби захисту кабельної системи або електроживлення, засоби архівації та копіювання інформації на зовнішні носії; організацію обчислювальних мереж з можливістю перерозподілу ресурсів у разі порушення працездатності окремих ланок; розробку програмних засобів захисту, в тому числі антивірусних програм, систем; розмежування повноважень, програмних засобів контролю доступу; прийняття конструктивних заходів захисту від розкрадань і диверсій; установку резервних систем електроживлення; оснащення приміщень замками, установку сигналізації і багато іншого.

До організаційних заходів можна віднести: ретельний підбір персоналу; виключення випадків ведення особливо важливих робіт лише однією особою; шифрування даних для забезпечення конфіденційності інформації; заходи захисту, що включають контроль доступу в приміщення, розробку стратегії безпеки, планів дій у надзвичайних ситуаціях і т. ін.; організація надійної та ефективної системи архівації і дублювання найбільш цінних даних; захист інформації від несанкціонованого доступу, включаючи використання різних пристроїв для ідентифікації особи за біометричною інформацією - райдужній оболонці ока, відбитками пальців, голосу, розмірами кисті руки; покладання персональної відповідальності на конкретних осіб, покликаних забезпечити безпеку об'єкта, введення в штат фахівців у галузі безпеки інформації; забезпечення універсальності засобів захисту від усіх користувачів (включаючи вище

керівництво); розробка плану відновлення працездатності об’єкта після виходу його з ладу і т. п.

До правових заходів належать: посилення норм, що встановлюють відповідальність за комп'ютерні злочини; захист авторських прав програмістів; · вдосконалення кримінального та цивільного законодавства в цій сфері. Також належать питання громадського контролю за розробниками комп'ютерних систем і прийняття міжнародних договорів про обмеження у їх діяльності.

Таким чином, до числа основних заходів протидії комп’ютерній злочинності можна віднести: створення єдиної стратегії боротьби з кіберзлочинністю відповідно до якої функції силових відомств чітко розподілені і координуються державою; створення загального центру для моніторингу загроз кібертероризму і розробки заходів швидкого реагування; організацію якісного захисту матеріально-технічних об'єктів, що складають фізичну основу інформаційної інфраструктури, насамперед критичної; розвиток технологій виявлення впливів на інформацію та її захисту від несанкціонованого доступу, спотворення чи знищення; безперервну підготовку персоналу інформаційних систем до ефективного протистояння різним варіантам дій терористів; · розвиток міждержавного співробітництва у боротьбі з кіберзлочинністю.

Література

1. Інтернет-цензура: матеріали Вікіпедії. [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/

2. Історія виникнення Інтернету. [Електронний ресурс]. – Режим доступу: https://sites.google.com/site/kovaliovaalenaua/istoria-viniknenna-i-rozvitku-internet

3. Кібербезпека: світові тенденції та виклики для України. - К.: НІСД, 2011. // [Електронний ресурс]. - Режим доступу: http://www.niss.gov.ua/content/articles/files/kyber_bezpeka-aab17.pdf

АКТУАЛЬНІСТЬ ПРОБЛЕМИ КІБЕРЗЛОЧИННОСТІ В СУЧАСНІЙ УКРАЇНІ ТА ПЕРШІ КРОКИ В БОРОТЬБІ

Тесленко Д.В.
слухач 2 курсу магістратури факультету №2
Одеського державного університету внутрішніх справ

Форос Г.В.
кандидат юридичних наук, доцент
професор кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ

Кіберзлочинність - це найсучасніший вид злочинності, що існує в сьогоднішньому суспільстві. Проблематика полягає в тому, що сучасні технології розвиваються та вдосконалюються з кожним днем, а так само і розвивається, поширюється