

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 сьогоденному суспільстві. Проблематика полягає в тому, що сучасні технології розвиваються та вдосконалюються з кожним днем, а так само і розвивається, поширюється

кіберзлочинність. 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 і т. п. 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.

На щастя, 27 січня 2016 року Радою національної безпеки та оборони України було прийнято за основу Стратегію кібербезпеки України [1].

На засіданні прийнято за основу Стратегію кібербезпеки України з урахуванням викликів, які стоять перед нашою державою: агресивних дій Російської Федерації, посилення тенденцій використання кіберпростору розвідувальними і спеціальними військовими структурами, терористами, криміналітетом.

Стратегія передбачає розвиток національної системи забезпечення захисту кіберпростору, своєчасного виявлення та нейтралізації кіберзагроз, а також запобігання їм з урахуванням досвіду та практики країн НАТО і Євросоюзу. Крім того, в документі обговорені питання координації, взаємодії та розподілу повноважень між органами безпеки та оборони України у питаннях кібербезпеки, кіберзахисту та протидії кіберзлочинності.

Метою стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особистості, суспільства і держави. В документі підкреслюється, що поряд з перевагами сучасного цифрового світу і розвитком інформаційних технологій, вони можуть використовуватися для вчинення терористичних актів, у тому числі шляхом порушення штатних режимів роботи автоматизованих систем управління технологічними процесами на об'єктах інфраструктури. Більше поширення одержує політично мотивована діяльність у кіберпросторі у вигляді атак на урядові і приватні сайти в мережі Інтернет. "Економічна, науково-технічна, інформаційна сфера, сфера державного управління, оборонно-промисловий і транспортний комплекси, інфраструктура електронних комунікацій, сектор безпеки і оборони України стають все більш уразливими для розвідувально-підривної діяльності іноземних спецслужб в кіберпросторі. Цьому сприяє широке, іноді домінуюче, присутність в інформаційній інфраструктурі України організацій, груп, осіб, які прямо або побічно пов'язані з Російською Федерацією", - йдеться в концепції [1, ст. 14-23].

Стратегія передбачає комплекс заходів, пріоритетів та напрямів забезпечення кібербезпеки України, зокрема, створення і оперативну адаптацію державної політики, спрямованої на розвиток кіберпростору і досягнення сумісності з відповідними стандартами ЄС і НАТО, формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кібернетичного захисту.

Крім цього, Стратегія передбачає залучення експертного потенціалу наукових установ, професійних і громадських об'єднань до підготовки проектів концептуальних документів у цій сфері; підвищення цифрової грамотності громадян та культури безпеки поведінки в кіберпросторі; розвиток міжнародного співробітництва і підтримку міжнародних ініціатив у сфері кібербезпеки, в тому числі поглиблення співпраці України

з ЄС і НАТО. Згідно з документом, основу національної системи кібербезпеки складуть Міністерство оборони, Державна служба спеціального зв'язку та захисту інформації, СБУ, Національна поліція, НБУ, розвідувальні органи.

Крім того, РНБО доручила Кабінету міністрів разом з СБУ, Службою зовнішньої розвідки та за участю Національного інституту стратегічних досліджень затвердити у двомісячний строк план заходів на 2016 рік щодо реалізації Стратегії кібербезпеки України і надалі розробляти і затверджувати такі плани щорічно та інформувати про стан реалізації. Також вирішено створити Національний координаційний центр кібербезпеки як робочий орган РНБО.

Президент України Петро Порошенко 8 червня, підписав указ "Про Національний координаційний центр кібербезпеки". Діяльність Центру дозволить забезпечити координацію суб'єктів національної безпеки і оборони України під час реалізації Стратегії кібербезпеки України, підвищити ефективність системи державного управління у формування та реалізації державної політики у сфері кібербезпеки. Підставою для розроблення зазначеного Положення є Указ Президента України від 15 березня 2016 року №96, яким введено в дію рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" і затверджена Стратегія кібербезпеки України. Національний координаційний центр кібербезпеки є робочим органом РНБО. Серед основних завдань вказуються здійснення аналізу стану кібербезпеки; результатів проведення огляду національної системи кібербезпеки; стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з протидії кіберзагрозам; стану виконання вимог законодавства щодо захисту від кіберзагроз державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури; даних про кіберінцидентах щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах та інше [2, с. 1-13].

Центр здійснює прогнозування і виявлення потенційних і реальних загроз у сфері кібербезпеки України, а також оперативне інформаційно-аналітичне забезпечення РНБО з питань кібербезпеки.

Література

1. Указ Президента України № 96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України».
2. Указ Президента України № 242/2016 від 07 червня 2016 року «Про Національний координаційний центр кібербезпеки».
3. Розпорядження Кабінету міністрів України № 440-р від 24 червня 2016 року «Про затвердження плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України».