Міністерство внутрішніх справ України

Одеський державний університет внутрішніх справ

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

Матеріали

ІІ Всеукраїнської науково-практичної конференції

17 листопада 2017 року

Одеса
ОДУВС
2017

Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»

УДК 343.9:004.7(477)
ББК 67.51+67.408.135(4Ук)
К 38

Рекомендовано до друку рішенням кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ
(протокол № 5 від 22 листопада 2017 року)

Всі матеріали надані в авторській редакції та виражають персональну позицію учасника конференції

Кібербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ.
К38 конф., м. Одеса, 17 листопада 2017 р. - Одеса : ОДУВС, 2017. - 204 с.
ISBN 678-717-7020

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на всеукраїнську науково-практичну конференцію «Кібербезпека в Україні: правові та організаційні питання», яка відбулася на базі кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ 17 листопада 2017 року.

У матеріалах конференції приділено увагу актуальним теоретичним та практичним проблемам забезпечення інформаційної безпеки в Україні. Висвітлюється широкий спектр питань, пов'язаних з удосконаленням правового регулювання та адміністративно-правового забезпечення кібербезпеки в Україні. Розглянуто використання інформаційних систем та технологій в боротьбі з кіберзлочинністю та надано обґрунтовані рекомендації щодо вдосконалення підготовки персоналу для боротьби з кіберзлочинністю в Україні.

Матеріали всеукраїнської науково-практичної конференції адресовано вченим, працівникам правоохоронних органів, аспірантам (ад'юнктам), слухачам магістратури, студентам та курсантам вищих навчальних закладів.

УДК 343.9:004.7(477)
ББК 67.51+67.408.135(4Ук)

ISBN 678-717-7020

Сучасне кіберсередовище держави як театр бойвих дій

Задерейко О.В.
кандидат технічних наук,
доцент кафедри інформаційних технологій
Національний університет «Одеська юридична академія»
Логинова Н.І.
кандидат практичних наук.,
доцент кафедри інформаційних технологій
Національний університет «Одеська юридична академія»
Троянський О.В.
кандидат технічних наук, доцент
директор Інституту інформаційної безпеки, радіоелектроніки та телекомунікацій
Одеського національного політехнічного університету

Згідно з військовими доктринами більшості країн світу, виділяються традиційні поля бою: суша, море, повітря, космос і кіберпростір, які у корені відрізняються від інших полів бою. Традиційні поля бою чітко визначені, відокремлені один від одного і розділяються державними кордонами і тому є локалізовані [1].

Останніми роками в інформаційному просторі багатьох країн обговорюється питання розв'язування кібервоєн - війн, в більшості випадків яких неможливо визначити не лише учасників, час їх початку і завершення, а й важко довести сам факт застосування кіберзброї. За своїми наслідками кібервійни можна порівняти з наслідками від застосування зброї масового ураження усіх видів. Зокрема, використання кіберзброї може бути замасковане під техногенні катастрофи, системні збої в роботі комп'ютерних мереж, автоматизованих систем тощо [2].

У сфері національної кібербезпеки держави головним військово-стратегічним завданням є забезпечення її стратегічної переваги за допомогою використання технологій електромагнітного спектру (ТЕС) для безумовного досягнення національних цілей в усіх областях при повному пригніченні можливостей потенційного супротивника реалізовувати власні спрямування.

Відсутність геополітичних і природних меж для електромагнітного спектру дозволяє здійснювати активні операції з використанням ТЕС практично в будь-якому місці незалежно від існуючих державних кордонів. З урахуванням того, що швидкість передачі електромагнітного імпульсу впритул наближається до швидкості світла, ці операції можуть проводитися в режимі реального часу і здійснюватися у часі - від частки мілісекунди до днів і місяців.

Надзвичайно важливо знати головну відмінність кіберзброї від інших типів озброєнь. Будь-яка складна кіберзброя може виступати як платформа, яка спочатку впроваджується в мережі і комп'ютери, потім здійснює шпигунські функції, а в потрібний момент активізується і виступає бойовим засобом,

що руйнує роботу військових і цивільних об'єктів та інфраструктури. Кіберзброя, яка може бути використана в багатовимірних нелінійних війнах, може бути розділена на такі основні групи:

1) мережева кіберзброя, для доставки якої до кінцевих об'єктів використовуються різного роду мережі і, передусім, Інтернет в його класичному розумінні;

2) комунікаційна кіберзброя, яка є програмним кодом, спотворюючим, блокуючим і підміняючим обмін сигналами між видаленим оператором і бойовим автоматизованим або роботизованим пристроєм. Завдяки цьому виду озброєнь може бути здійснене як руйнування об'єкту, так і перехоплення керування;

3) передвстановлена кіберзброя, електронні пристрої, вмонтовані у високотехнологічні, автоматизовані і роботизовані озброєння. Вона побудована на базі мікропроцесорів та інших електронних компонентів, вироблених головним чином компаніями під юрисдикцією США, Великобританії і Тайваню. Відповідно в цій елементній базі знаходиться передвстановлений *софтвер,* який керує, і з високою вірогідністю містить різного роду "логічні бомби" та "закладки".

Враховуючи темпи інтеграції інформаційних систем держави в економічну, політичну і соціальну сфери, забезпечення стійкості їхнього функціонування є ключовим елементом незалежності самої держави. Саме тому більшість світових держав, усвідомлюючи важливість цього питання, вже достатньо давно вносять відповідні корективи до своїх державних політик, які відображені у вигляді національних стратегій кібербезпеки або інформаційної безпеки, де окремим розділом виділяють кібербезпеку.

Слід зазначити, що нині активно стала підніматися тема забезпечення не стільки кібербезпеки держави, а її кіберстійкості, під якою розуміється можливість її інформаційних систем здійснювати свої функції навіть в умовах безперервних внутрішніх і зовнішніх кібератак [3]. Реалізація стратегії забезпечення кіберстійкості держави традиційно включає такі етапи:

1) профілактика системи кібербезпеки - створення автоматичного процесу керування профілактикою системи кібербезпеки;

2) розробка плану - створення крос-функціональної команди вищого керівництва для планування регламенту заходів щодо кібербезпеки подій у контексті гіпотетичних атак;

3) планування людського ризику - вивчення моделей і режимів кібератак з метою розробки індивідуального підходу до захисту активів компанії;

4) отримання точних даних та їхня оцінка - зосередження на необроблених цифрах, а не точних оцінок і уникнення блокування їх аналізу.

5) зниження ризиків кібербезпеки - інвестування заходів щодо зниження ризиків для захисту активів компанії, яким загрожує найвищий ризик;

6) кіберстрахування - організація страхування кібербезпеки та отримання спеціалізованої допомоги у разі кібератаки;

Такий підхід до реалізації стратегії кібербезпеки є найбільш актуальним для критичних інфраструктур держави (енергетика, держкерування, воєнізовані об'єкти). Безумовно, реалізація таких проектів неминуче пов'язана з практичною реалізацією таких аспектів:

1) питання нормативно-правового характеру, пов'язані з термінологією і законодавчою базою, визначення кіберпростору як простору ведення війни, нормативно-правового забезпечення державної політики в області створення і функціонування підрозділів спеціального призначення;

2) питання організаційного характеру - створення, функціонування, взаємодія, керування і інше [4];

3) питання технічного характеру - системи перехоплення і зберігання метаданих, їх індексації, автоматизованої обробки і видачі уповноваженим державним структурам [5].

Лідери кіберпростору зрозуміли, що кіберактиви держави провокують на різні варіанти реалізації дистанційних атак, перехват керування та захисту, які раніше були неможливі для традиційних військових операцій. У взаємо-зв'язаному світі, де істотні досягнення в сфері комунікаційних технологій були звичною справою, можливості і зброя у кіберпросторі стали ще більш вражаючими.

Кібероперації сьогодні можуть бути здійснені в усіх областях ведення бойових дій: у повітрі, космосі, кіберпросторі, на суші і морі. Саме тому доктрини для повітря і космічного простору залишаються актуальними і застосовними до сфери кіберпростору.

Кібернавчання повинні здійснюватись відповідно до вимог запланованих документів, в окремих випадках - за вказівками відповідних посадовців [6]. Основними умовами підготовки і проведення кібернавчаннь є:

4) всебічне оцінювання характеру можливих наслідків інформаційно-технічних дій атакуючої сторони;

5) практичний досвід нейтралізації групових і масових кібератак.

У ході кібернавчань повинні відпрацьовуватися заходи щодо забезпечення необхідної стійкості функціонування критично важливих об'єктів національної інфраструктури в умовах інформаційно-технічної дії вірогідного супротивника, у тому числі:

1) приведення служб інформаційних технологій та інформаційної безпеки в стан, оптимальний для своєчасного припинення, виявлення і нейтралізації відомих і невідомих раніше кібератак;

2) визначення оптимальних способів скорочення термінів приведення в різні міри готовності критично важливих інформаційних об'єктів національної інфраструктури;

3) усунення раніше виявлених недоліків і зауважень.

Впровадження у реальному секторі відповідної інфраструктури держави розглянутого комплексу питань що сприятиме підвищенню рівня спеціальної підготовки керівного складу і підлеглих органів управління, сил і засобів кібербезпеки для забезпечення надійної стійкості функціонування критично важливих об'єктів національної інфраструктури держави в умовах вірогідних інформаційно-технічних дій супротивника.

Література:

1. Кибермогущество как базис обеспечения цифрового суверенитета в современном мире - ключевые подходы. - [Электронный ресурс]. - Режим доступа: http://riss.ru/bookstore/journal/2014-2/j25/.
2. Integrated infrastructure: cyber resiliency in society. - [Электронный ресурс]. - Режим доступа: https://www.ciosummits.com/Online_Assets_Lockheed
3. Martin_Integrated_Infrastructure_-_Report_Cambridge.pdf.
4. От кибербезопасности к устойчивости информационных систем. [Электронный ресурс]. - Режим доступа: http://www.securitylab.ru/blog/personal/Business_without_danger/308585.php.
5. Critical infrastructure resilience strategy. [Электронный ресурс]. - Режим доступа: http://fire-com-live-wp.s3.amazonaws.com/wp-content/uploads/EMV-CIRS_Web1.pdf.
6. СОРМ-3: формальное закрепление реализованного. [Электронный ресурс]. - Режим доступа: http://www.securitylab.ru/analytics/446852.php.
7. Петренко А. А., Петренко С. А. Киберучения: методические рекомендации enisa //Вопросы кибербезопасности. - 2015. - №. 3 (11).

Міжнародна науково-практична конференція
Кібербезпека в Україні: правові та організаційні питання
30 листопада 2018 року
м. Одеса, Україна

ЗАПРОШЕННЯ

Інформуємо Вас, що **30 листопада 2018 року** в м. Одеса відбудеться Міжнародна науково-практична конференція «Кібербезпека в Україні: правові та організаційні питання».

Для участі в конференції запрошуються вчені, співробітники науково-дослідних установ, аспіранти, курсанти, студенти.

Робочі мови конференції: українська, англійська, російська.

ПОДАННЯ ДОКУМЕНТІВ:

Для участі в конференції представити наступні документи:

1. Заявку у відповідності з формою;
2. Тези доповіді на одній із робочих мов, оформлені у відповідності із запропонованим зразком;

ПУБЛІКАЦІЯ ПРАЦЬ КОНФЕРЕНЦІЇ

Тези доповідей, отримані Організаційним комітетом та прийняті до друку, будуть видані до початку конференції у збірнику праць конференції та вислані безкоштовно на електронні адреса учасників конференції.

АДРЕСА ОРГКОМІТЕТУ:

Кафедра кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ

Адреса: вул. Успенська, 1, м. Одеса, 65000, Україна
Сайт: http://oduvs.sem-dev.co.ua/kafedra-kiberbezpeki-ta-informatsijnogo-zabezpechennya/
E-mail: 0997060070@ukr.net
facebook: https://www.facebook.com/kiberoduvs

Контактні особи:

Ісмайлов Карен Юрійович +38 (099) 70-600-70;
+38 (097) 70-600-90;
0997060070@ukr.net
Форос Ганна Володимирівна +38 (067) 485-30-84

Одеський державний університет внутрішніх справ
«Кібербезпека в Україні: правові та організаційні питання»
Наукове видання

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

Матеріали

ІІ Всеукраїнської науково-практичної конференції

17 листопада 2017 року

Підписано до друку 22.11.2017.Формат 60х90/8. Папір офсетний.
Гарн. «Times New Roman» Друк цифровий. Ум. друк .арк. 26,1.
Наклад 500 прим.
Видавництво ОДУВС
м. Одеса, вул. Успенська, 1
Свідоцтво суб'єкта видавничої справи ДК № 3507 від 25.06.2009 р.
тел. 0487024884; 0949547884 email - *ndrvvl@gmail.com*