СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА
ЛІГА СТУДЕНТІВ АСОЦІАЦІЇ ПРАВНИКІВ УКРАЇНИ

РЕФОРМУВАННЯ ПРАВОВОЇ СИСТЕМИ В КОНТЕКСТІ ЄВРОІНТЕГРАЦІЙНИХ ПРОЦЕСІВ

МАТЕРІАЛИ
IV Міжнародної науково-практичної конференції
(Суми, 21–22 травня 2020 року)

У двох частинах

Частина 2

Суми
Сумський державний університет
2020

РЕАЛІЗАЦІЯ КІБЕРБЕЗПЕКИ ТА ШЛЯХИ ЇЇ ВДОСКОНАЛЕННЯ В УКРАЇНІ

Прокопець Я. Ю.
Студентка ІІІ курсу ННІ права
Сумського державного університету
Науковий керівник: Думчиков М. О.
к. ю. н., асистент кафедри КПДС ННІ права
Сумського державного університету

Сучасні глобалізаційні процеси не стоять на місці.Цифрові технології проходять шлях удосконалення, зважаючи на постійні покращення в усіх інформаційних сферах суспільного життя. Зважаючи на все більший вплив електронних технологій усе більш актуальною стає проблема захисту від загроз кібернетичного характеру.

Більшість країн світу практикують надійні засоби кібербезпеки, що основані на загальнодержавній системі захисту з можливістю швидкого та ефективного виявлення кіберзагрози, а також надання спеціальним органам повноважень та технологій для попередження, припинення та запобігання кібернападам.

У ході нещодавніх подій дуже актуальною є проблема кібербезпеки і для України. Одним з прикладів важливості сектору кібербезпеки є те, що вірусами вражається велика кількість інформаційних ресурсів будь-якої зі сфер державного регулювання. ВірусомPetya, наприклад, було вражено значну кількість інформаційних ресурсів центральних органів державної влади. До цього призвеланедостатня кількість ресурсів із кіберзахисту в Україні, що породжує прогалини в організації діяльності даних суб'єктів.

На сьогоднішній день є перелік суб'єктів, які відповідають за забезпечення кібербезпеки в Україні. Розпочну з того, що під суб'єктами забезпечення кібернетичної безпеки у проекті Стратегії забезпечення кібернетичної безпеки України було визначено державні органи (передусім, інституції сектору безпеки і оборони України), органи місцевого самоврядування, підприємства, установи, організації незалежно від форми власності, які здійснюють проектування, впровадження та експлуатацію складових елементів критичних об'єктів національної інформаційної інфраструктури або забезпечують їхкіберзахист [1].

До основних суб'єктів у сфері забезпечення кібербезпеки є:

1) Міністерство оборони України, Генеральний штаб Збройних сил України, на які покладено функції з перешкоджання та відбиття воєнних нападів в кібернетичному просторі (т. з. – кібероборона). Здійснюють свої повноваження спільно з Державною службою спеціального зв'язку та захисту інформації України і Службою безпеки України, щодо проявів кіберагресії на території нашої держави.

2) Державна служба спеціального зв'язку та захисту інформації України,

котраформуєдержавну політику щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації. Вона керується при цьому спеціально встановленими критеріями кіберзахистукритичної інформаційної інфраструктури (тобто комплексу заходів, реалізованих у нормативно-правових, організаційних, технологічних інструментах, спрямованих на забезпечення безпеки та стійкості критичної інфраструктури).

3) Служба безпеки України, здійснює здійснює оперативні операції з виявлення та придушення кібератак, ведуть розвідувальні дії, сприяючи захисту державним електронним системам, та подальшому їх захисту.

4) Органи Національної поліції здійснюють виявлення та розкриття злочинів у сфері кібербезпеки.

5) Національний банк України (який, доречі, часто стає ціллю хакерів з метою заволодіння електронними коштами, інформаційними даними про клієнтів, а також ключами доступу до рахунків).

6) Розвідувальні органи України створені з метою оперативного розшуку з проявів кібернападів, здійснюючи так звану «кібернетичу розвіду» – добування наявних у кібернетичному просторі даних та інформації противника, моніторинг його автоматизованих систем управління, систем управління зброєю, інформаційних мереж та систем і технологічних процесів, що в них циркулюють [2].

Утім, досі не сформовано поняття національної системи кібербезпеки, що включало б тісну співпрацю між національними органами, та залученням до співпраці іноземних фахівців з даного питання. Можливо, актуальним було б створення потужних центрів з нанообладнанням, котре б відповідало сучасним загрозам.

Щоб з’ясувати наскільки ефективною є реалізація заходів захисту у сфері кібербезпеки, необхідно зазначити головні функції суб’єктів, котрі регулюють дане питання, відповідно до положень Закону України «Про основи національної безпеки України».

Отже, такими функціями, зокрема,є:

1) розробка і доповнення Стратегії кібербезпеки України на основі концепцій, шляхом заходів з протидії кібернападам та їх побічним ефектам;

2) поліпшення нормативного закріплення щодо організаційної структури органів з протидії та запобігання кібернетичним злочинам;

3) забезпечення кадрової діяльності підрозділів цих органів фінансовими, матеріальними, технічними та іншими благами, котрі є важливими під час здійснення регулювання у сфері кібербезпеки;

4) налаштування систем для їх подальшого функціонування за призначенням,

створення програмних програм за допомогою яких здійснюється контроль та попередження кібернападів;

5) нагляд за кібернетичними процесами у всіх сферах суспільного життя (зокрема, політичному) з метою недопущення зовнішнім чинникам впливати на діяльність органів державної влади, породженням недовіри до них та розхитуванням національної єдності країни;

6) зважаючи на те, що технології не стоять на місці, забезпечувати налаштування вже існуючих програм, та розробка нових, з метою вчасного реагування та відвернення загрози.

Як бачимо, процеси у сфері кібербезпеки постійно потребують моніторингу та внесення коректив, шляхом реформування інформаційної безпеки та створення дієвих механізмів, що потягне за собою зрушення у кожній зі сфер життя. Для створення ефективного інституту кібербезпеки у нашій державі необхідно:

По-перше, чітко розмежувати функції у сфері кібербезпеки, щляхом точного їх закріплення за кожним із суб'єктів у сфері кібербезпеки, забезпечуючи при цьому контроль за ефективністю їх діяльності та створенням спеціальних суб'єктів з наданням їм особливих функцій;

По-друге, створення належних умов для залучення фахівців, компетентних на найвищому рівні запобігати проявам кібератак, а також впровадження найбільш сучасних систем і методів у боротьбі з кіберзлочинністю.

Важливо звернути увагу на організаційне забезпечення кібербезпеки, оскільки воно створене з метою упорядкування структурних підрозділів важливих для забезпечення кібербезпеки та узгоджує процеси з прийняття управлінських рішень з приводу дій спеціальних органів із запобігання проявам кібератак.

Організаційне забезпечення системи кібербезпеки, у свою чергу, характеризується місцем і роллю спеціальних суб'єктів (відповідних державних органів та їх спеціалізованих підрозділів), їх функціями, повноваженнями, а також підставами, умовами і напрямами їхвзаємодії під час здійснення заходів із забезпечення безпеки у кіберпросторі [3, с. 301].

Більш того, для поліпшення вже існуючих механізмів здійснення захисту кібербезпеки, важливим елементом є моніторинг та контроль за новими існуючими вірусними атаками, з метою створення ефективних методів для боротьби з ними.

Підвищенню ефективності засобів з протидії кіберзлочинності на кібернетичних просторах є дотримання певного балансу між охороною державних інтересів (гарантуванням політичної, соціальної, економічної та ін. стабільності у державі) та

покращення міждержавного та внутрішньодержавного співробітництва з даного питання, яке б здійснювалось з дотриманням усіх основних принципів, основними серед яких є верховенство права, дотримання конституційних прав та свобод людини на доступ до інформації та ін.

Таким чином, питання кіберзлочинності зростає з року в рік, оскільки технології не стоять на місці, що потребує перегляду та постійного моніторингу нових загроз у кіберпросторі. Шляхом інформаційної обізнаності громадян можна буде зменшити прояв таких кібератак та знищити їх на початковому рівні, а налагоджена система організації органів, які забезпечують кібербезпеку, надасть змогу вдосконалити механізм з виявлення, запобігання та припинення кіберзлочинності.

ЛІТЕРАТУРА:

1. Стратегія забезпечення кібернетичної безпеки України (Проект). URL: www.niss. gov.ua/public/File/2013_nauk.../kiberstrateg.pdf.

2. Куцаєв В. В., Живило Є. О., Срібний С. П., Черниш Ю. О. Розширення термінології сучасного кіберпростору. URL: mino.esrae.ru/ pdf/2014/3Sm/1387.doc.

3. Шеломенцев В. П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. № 2. С. 299–309.

ТЕНДЕНЦІЇ ЗЛОЧИННОСТІ НЕПОВНОЛІТНІХ

Сич К. І.
Студентка IV курсу ННІ права
Сумського державного університету
Науковий керівник: Думчиков М. О.
к. ю. н., асистент кафедри КПДС ННІ права
Сумського державного університету

Навколишнє середовище неповнолітніх криміналізується, серед іншого, посиленням проникнення жорстокості як суспільно небезпечного явища. Зараз жорстокість проникає у сім'ю, життя, освіту, культуру, свідомість, закріпившись у традиціях та звичаях, трансформуючи систему особистих та соціальних потреб та інтересів. Жорстокість - один з найважливіших показників морального здоров'я та статусу неповнолітніх. Кількість злочинів із насильницькою мотивацією, коли насильство пов'язане з насильством, садизмом, порочною агресією, цинізмом, зловживанням людьми, щороку збільшується. Зростає і тяжкість насильницьких злочинів неповнолітніх, включаючи злочини проти