ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Кафедра захисту інформації

АНАЛІЗ НОРМАТИВНО-ПРАВОВОЇ БАЗИ КІБЕРБЕЗПЕКИ УКРАЇНИ

Виконали ст. гр. РТ-814: Гайтота Є.В., Чуницька В.В.

Науковий керівник: Нікуліщев Г.І.

Мета роботи:

- Фаховий аналіз положень нормативно-правових документів України, які регулюють відносини і діяльність в сфері кібербезпеки, розробка пропозицій щодо впровадження відповідних норм на практиці.

Проводиться:

- аналіз новітніх нормативних документів України в галузі кібербезпеки та визначається їх узгодженість з існуючим законодавством;
- оцінюються перспективи впровадження положень нормативно-правових актів, вносяться пропозиції щодо практичної реалізації відповідних норм.

- У зв`язку з розвитком інформаційних технологій на сьогоднішній день дуже гостро стоїть питання про забезпечення безпеки інформаційно-телекомунікаційних систем, а також захист інформаційних ресурсів України.

- З огляду на це ведеться робота з розробки законодавчої бази кібербезпеки на додачу до вже існуючих нормативних актів, які стосуються захисту інформації. Так, протягом останніх років Президент України Петро Порошенко своїми указами ввів в дію розроблені спеціалістами з кібербезпеки та затверджені на засіданнях РНБОУ Стратегію кібербезпеки України, Доктрину інформаційної безпеки України та Закон «Про основні засади забезпечення кібербезпеки України».

АНАЛІЗ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ

15 березня 2016 року Президент України Петро Порошенко підписав указ «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». Цим указом вводиться в дію розроблена спеціалістами з кібербезпеки та затверджена на засіданні РНБОУ Стратегія кібербезпеки України.

Метою Стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Складнощі реалізації	Переваги
Для реалізації Стратегії потрібно внесення низки змін до українського законодавства, що мають як створити підґрунтя для втілення в життя положень Стратегії, так і посилити відповідальність за порушення в сфері кібербезпеки.	Одним з перших кроків з втілення Стратегії, стало створення в червні 2016 року Національного координаційного центру кібербезпеки як робочого органу Ради національної безпеки і оборони України.
Нова Стратегія є необхідною, однак не достатньою для того, щоб належним чином захистити Україну від кіберзлочинності.	Стратегія передбачає створення «активного кіберзахисту», що означає здійснення воєнно-політичних, військово-технічних та інших заходів, спрямованих на розширення прав і можливостей воєнної організації держави, сектора безпеки і оборони в кіберпросторі, створення, розвиток сил, засобів та інструментів для можливої відповіді на агресію у віртуальному просторі, що може бути використаний як засіб стримування воєнних конфліктів і загроз в кіберпросторі.
Для оперативного реагування на порушення кібербезпеки спецслужбам потрібні інструменти онлайн доступу до комп'ютерних даних абонентів, але при цьому необхідно зберегти баланс між правом громадян на недоторканність приватного життя та інтересами національної безпеки, бо для доступу до персональних даних необхідне судове рішення. Однак у ситуації кіберзлочину – має бути миттєва реакція розвідувальних служб, і отримання рішення суду може затримати цю реакцію.	
На даний час державні органи з кіберпезпеки не можуть захистити всіх суб'єктів кіберпростору.	

АНАЛІЗ ДОКТРИНИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Президент України Петро Порошенко підписав указ від 25 лютого 2017 року «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України».

Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни.

Складнощі реалізації	Переваги
Надто розмиті підстави для блокування сайтів, через що залишається широкий простір для зловживань з боку державних органів влади.	Розробка пріоритетів та стимулів розвитку українського кіно, телевізійного контенту та книгодрукування.
Звинуватити в "загрозі національним інтересам" можна будь-який інформаційний ресурс.	Поза увагою не лишається й можливість доступу до публічної інформації.
Доктрина інформаційної безпеки дає підстави для побоювань щодо виникнення загроз свободі слова і демократії та диктатури в країні за умови зловживань з боку відповідальних органів.	

АНАЛІЗ ЗАКОНУ “ПРО ОСНОВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ”

5 жовтня 2017 року Верховна Рада України ухвалила в повторному другому читанні і в цілому законопроект №2126а «Про основні засади забезпечення кібербезпеки України». 7 листопада 2017 року документ повернуто з підписом від Президента.

Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Складнощі реалізації	Переваги
Деякі норми прописані так, що можуть бути трактовані неоднозначно. Зокрема, Закон дає право спецслужбам блокувати будь-які сайти, як загрожують безпеці України. Приводи для звинувачення досить абстрактні, що можуть тлумачитись по-різному.	В Законі приділяється увага державно-приватній взаємодії у сфері кібербезпеки та встановлюється відповідальність за порушення законодавства у цій сфері і контроль за законністю заходів із забезпечення кібербезпеки України. Законом передбачається відповідальність не тільки за кіберзлочини, а й за неякісний захист інформації відповідальними особами.
Звинуватити в "загрозі національним інтересам" можна будь-який інформаційний ресурс.	Закон визначає місце України в міжнародних системах забезпечення кібербезпеки, що дозволить поліпшити співпрацю з визнаними фахівцями, а також інтеграцію України в світову спільноту та підвищити рівень знань вітчизняних фахівців.
Закон дає приводи для виникнення загроз свободі слова і демократії та диктатури в країні за умови зловживань з боку відповідальних органів.	Введення в правове поле термінів, які починаються з "кібер": атака, безпека, загроза, захист, злочин, простір, тероризм, розвідка, шпигунство та інше.
	В Законі йдеться не тільки про освіту в вишах для фахівців, а й для суспільства, для підняття загальної освіченості населення в питаннях кіберзахисту, тому пересічні користувачі теж мають стати більш захищеними.

Для вирішення складнощів реалізації авторами запропоновано:

- виокремити в структурі судової системи такий спеціальний орган правосуддя, який буде розглядати справи лише у сфері кіберзлочинності;
- підвищити рівень кіберграмотності громадян та культури безпечного поводження у кіберпросторі. В проведенні даних заходів повинні брати участь не тільки влада, але й громадські організації, приватний бізнес та звичайні громадяни;
- має бути розміщенні статті про захист персональних даних у вигляді реклами в Інтернеті, банерах, а також засобах мас медіа.
- детальніше прописати, в чому конкретно вбачається загроза національній безпеці.
- прописати більш конкретні кроки, дії і заходи у підзаконних актах, прийнятих як відомствами, які входять в Національну систему кібербезпеки, так і всіма іншими, які так чи інакше провадять діяльність з залученням інформаційно-телекомунікаційних систем.