12. Фляжнікова Я.В. Правила адвокатської етики як ціннісний орієнтир студента-правника. Сучасні виклики та актуальні проблеми судової реформи в Україні: Матер. III Міжнародної наукової конференції (м. Чернівці, 24-25 жовтня 2019 р.). Чернівці: Технодрук, 2019. С. 250-252

УДК: 004.056.5:351.852.3

Ніколайчук О.В.
здобувач вищої освіти
Вінницького національного технічного університету
Науковий керівник
Шелепало Г.В. , *к.ф.м.н. доцент кафедри захисту інформації*
Вінницького національного технічного університету

КІБЕРБЕЗПЕКА В ДЕРЖАВНИХ ОРГАНАХ ТА ОРГАНАХ МІСЦЕВОГО САМОВРЯДУВАННЯ

З кожним новим технологічним проривом і кроком у сфері цифрової трансформації, кібербезпека стає все більш нагальною та значущою проблемою. У сучасному світі, де державні органи грають ключову роль у забезпеченні добробуту та безпеки суспільства, захист їх інформаційних систем стає критичним завданням. Загрози кібербезпеки в даних органах зростають як за своєю складністю, так і за масштабом.

Хакерські атаки, фішинг, витоки даних та інші кіберзагрози можуть спричинити серйозні наслідки, такі як порушення конфіденційності даних, втрати фінансових ресурсів та навіть вплинути на безпеку громадян та функціонування критично важливих інфраструктур.

Кібербезпека в державних органах є критично важливою, оскільки ці організації мають значний обсяг чутливої інформації та відповідають за забезпечення ефективної роботи державних систем і надання послуг громадянам. Зростання кількості та складності кіберзагроз вимагає посилення заходів кібербезпеки для запобігання кібератакам та забезпечення стійкості і надійності інформаційних систем.

Згідно з дослідженнями, які були описанні в роботі "Принципи застосування органами місцевого самоврядування законодавства України у сфері кібербезпеки" автора Демиденко В. О. існують конкретні загрози, що впливають на кібербезпеку цих організацій. Серед них можна виділити соціальний інжиніринг та фішинг, які широко використовуються для отримання неправомірного доступу до систем або конфіденційної інформації.

Ці атаки спираються на маніпулювання людським фактором і вимагають підвищеної уваги та освіти персоналу для їх виявлення та запобігання.

Протягом останніх п’яти років ми стали свідками низки масштабних кібератак проти України. Остання масова кібератака 2017 року, здійснена за допомогою модифікованої версії вірусу Wannacry – Petya.A, яскраво засвідчила неготовність державного апарату, органів місцевого самоврядування, правоохоронних органів, медіа, приватного сектору до протидії таким кіберзагрозам і мінімізації їх негативних наслідків. Від неї постраждали органи державної влади (Кабінет Міністрів України, МВС України, Міністерство інфраструктури України, Київська міська державна адміністрація, департамент кіберполіції тощо), органи місцевого самоврядування (сервісні системи Київської та Львівської міських рад), великі стратегічні підприємства, зокрема критичної інфраструктури (наприклад, аеропорт «Бориспіль», ЧАЕС, Укртелеком, Укрпошта, Ощадбанк, Укрзалізниця), медіакомпанії (телеканали «Інтер», «СТБ», «ICTV», «24 канал», різні інтернет-видання) тощо. Фінансові збитки становлять декілька мільярдів гривень [1] .

Згідно з цим, ключовим елементом кібербезпеки є свідомість працівників щодо загроз і безпекових процедур. Додатково, державні органи повинні розробляти та впроваджувати політики та стандарти кібербезпеки, щоб забезпечити належний рівень захисту своїх інформаційних систем.

Прийняття ефективних політик кібербезпеки є важливим кроком у забезпеченні безпеки інформаційних ресурсів держави та її громадян. Ці політики повинні визначати вимоги щодо захисту даних, встановлювати

механізми управління ризиками та впровадження безпекових заходів, а також встановлювати відповідальність за порушення безпеки та механізми реагування на інциденти.

В Україні прискорюється інформатизація усіх сфер суспільного життя на фоні постійного зростання кількості та рівня кіберзагроз.

Це потребує побудови адекватної цим кіберзагрозам національної системи кібербезпеки, одним з суб'єктів якої законодавчо визначені органи місцевого самоврядування (ОМСВ). ОМСВ мають свої, відмінні від інших суб'єктів забезпечення кібербезпеки, характеристики і ознаки (особливості), які суттєво впливають на місце і роль ОМСВ в національній системі кібербезпеки. Тому з'ясування цих особливостей є важливим для створення ефективної системи забезпечення кібербезпеки України та визначення шляхів її удосконалення. Проте, як показує аналіз останніх досліджень і публікацій з проблематики кібербезпеки, практично усі дослідники розглядають систему забезпечення кібербезпеки в цілому і тільки основних суб'єктів забезпечення кібербезпеки, до яких вони ОМСВ не відносять. В небагатьох працях ОМСВ розглянуті як суб'єкти забезпечення національної безпеки та інформаційної безпеки без акцентування на кібербезпеці; як суб'єкти захисту об'єктів критичної інфраструктури України; також розглянуті принципи застосування ОМСВ законодавства України у сфері кібербезпеки.

Можна зробити висновок, що питання комплексного розгляду ОМСВ як суб'єктів забезпечення кібербезпеки України залишається малодослідженим. Відсутність вказаних досліджень призводить до неврахування впливу певних особливостей ОМСВ на їхню управлінську діяльність у сфері кібербезпеки та законодавчого регулювання цієї діяльності. Саме тому метою дослідження було визначено виокремлення вказаних особливостей [2].

Для забезпечення ефективності заходів кібербезпеки, освіта працівників є невід'ємною складовою. Навчання персоналу та свідомості щодо принципів кібербезпеки є важливими елементами вдосконалення безпеки інформаційних

систем державних органів та органів місцевого самоврядування. Регулярне навчання працівників щодо нових загроз, методів атак та заходів безпеки може підвищити їх свідомість та здатність виявляти та уникати потенційні загрози.

Крім того, впровадження стандартів кібербезпеки є важливим етапом для забезпечення належного рівня захисту.

Згідно зі проектом Закону України від 14.04.2016 № 2126а "Про основні засади кібербезпеки" стаття 5 'Суб'єкти забезпечення кібербезпеки' , державні органи та органи місцевого самоврядування повинні дотримуватись вимог щодо захисту інформації, використовувати стандарти безпеки, розроблені національними та міжнародними організаціями. Ці стандарти встановлюють необхідні заходи для забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів.

У результаті це дасть можливість провести огляд кібербезпекової сфери держави, що дозволив би більш чітко визначити сучасний стан її нормативного забезпечення та основні проблеми, які мають бути вирішені вже найближчим часом

Розробити на підґрунті моделей розвитку світового кібернетичного простору власну модель та реалізувати її.

А також впорядкувати політику України у сфері інформаційної та кібербезпеки і виробити так звані загальні правила поведінки в кіберпросторі [3]. Закон України «Про національну безпеку України» від 21 червня 2018 року (стаття 31) під-креслює, що стратегія кібербезпеки є частиною системи національної безпеки і оборони [5].

Також дослідниками підкреслюється, що біль- шість українських компаній не готові вчасно та швидко реагувати на кіберінциденти, не мають в штаті підготовлених спеціалістів. Відсутнє цен- тралізоване управління силами реагування, гро- мадяни не мають достатнього рівня обізнаності в цих питаннях. Приватний бізнес не залучаєть- ся до вирішення важливих питань

кібербезпеки. Також дослідники бачать проблему в неефек- тивності системи кіберрозвідки та низький рівень аудиту кібербезпеки [6].

Всі ці підходи, включаючи свідомість працівників, політики та стандарти кібербезпеки, є важливими кроками у забезпеченні ефективного захисту державних органів та органів місцевого самоврядування від кіберзагроз. Застосування цих заходів допоможе забезпечити стійкість і надійність їх інформаційних систем, підвищити довіру громадян та забезпечити ефективну роботу органів у сфері публічного управління.

Кібербезпека в державних органах є надзвичайно важливим аспектом сучасного інформаційного суспільства. Загрози, які виникають у цих органах, вимагають постійного удосконалення стратегій та політик, застосування стандартів безпеки та налагодження свідомості щодо кібербезпеки серед працівників.

На основі проведених досліджень і аналізу існуючих джерел, було виявлено, що забезпечення кібербезпеки вимагає комплексного підходу та спільних зусиль. Основні напрямки покращення кібербезпеки включають усвідомлення загроз, впровадження ефективних політик та стандартів безпеки, а також навчання та підвищення освіченості персоналу. Враховуючи рекомендації досліджень і використання наявних джерел, можна зміцнити захист інформаційних ресурсів, запобігти кібератакам та забезпечити належний рівень кібербезпеки в державі.

Список використаних джерел

1. Демиденко В. О. Принципи застосування органами місцевого самоврядування законодавства України у сфері кібербезпеки. Юридичний часопис Національної академії внутрішніх справ 2018. № 1 (15)URL: http://elar.naiau.kiev.ua/bitstream/123456789/6660/1/14.pdf (дата звернення: 13.05.2023).

2. Стець В. В. Органи місцевого самоврядування як особливі суб'єкти забезпечення кібербезпеки України. Матеріали Міжнародної наук.-практ. конференції "Україна у сучасному міжнародному просторі" «УКРАЇНА У СУЧАСНОМУ МІЖНАРОДНОМУ ПРОСТОРІ». Україна : Одеса 2021 С. 56 – 58 URL: http://dspace.op.edu.ua/jspui/bitstream/123456789/12143/1/09_Full_Block_ (дата звернення: 18.05.2023).

3. Козюра В.Д., Хорошко В.О., Система кібернетичної безпеки в Україні. Науково-практичний журнал. Сучасна спеціальна техніка. 2017. №4 (51) С. 34 – 41 URL:

http://elar.naiau.kiev.ua/bitstream/123456789/13635/1 (дата звернення: 19.05.2023).

4. Проект Закону України від 14.04.2016 № 2126а "Про основні засади забезпечення кібербезпеки України" URL: https://ips.ligazakon.net/document/JH1N268B?an=3 (дата звернення: 21.05.2023).

5. Закон України № 2469 VIII (2021). Про національну безпеку. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 22.05.2023).

6. Янковський О. Україні потрібна нова кіберстратегія. Українська правда. 2019. URL: https://www.pravda.com.ua/rus/columns/2019/09/14/7226291/ (дата звернення 22.05.2023)

Вітковський А.В.

здобувач вищої освіти
Вінницького національного технічного університету
Науковий керівник
Шелепало Г.В. , *к.ф.м.н. доцент кафедри захисту інформації*
Вінницького національного технічного університету

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ШЛЯХОМ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

В сучасному цифровому світі, де персональні дані стають все більш цінними та піддатливими на атаки зловмисників, забезпечення безпеки та