Юридичні науки

Коваль Юлія Андріївна

студент

Національного юридичного університету імені Ярослава Мудрого

СУЧАСНИЙ СТАН ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Анотація. *У даній статті аналізується забезпечення кібербезпеки в державі та робота Ситуаційного центру при Службі безпеки України, основні його завдання та проблеми.*

***Ключові слова*:** *кібербезпека, Служба безпеки України, Ситуаційний центр, Трастовий фонд, НАТО, атаки.*

Постановка проблеми. Інформаційно-комп'ютерна революція відкриває широкі можливості для впливу на народи та владу, маніпулювання свідомістю та поведінкою людей навіть на віддалених просторах.

З процесом глобалізації телекомунікаційних мереж, що відбувається у світі, саме інформаційному виду агресії віддається пріоритет наразі.

Потрібна серйозна увага фахівців різного профілю задля цього питання, щоб уникнути найбільш негативних наслідків цієї війни для нашої держави.

Враховуючи цілу низку проблем, які завдає нам Російська Федерація, додається ще одна, розхитування внутрішньої дестабілізації в країні.

Аналіз публікацій, у яких започатковано розв'язання даної проблеми. Вивченням цієї тематики займалось багато науковців, зокрема: О. Янковський, Д. Нікулеско, О. Бакалінська, О. Бакалинський та інші.

Мета статті полягає у дослідженні сучасного стану кібербезпеки в Україні та шляхи вирішення основних проблем, що постають перед нашою країною на сьогодні.

Виклад основного матеріалу. Сьогодні ми живемо в епоху інформаційного суспільства, що охоплює усі сфери життєдіяльності як людини, так і держави в цілому.

Проте, з прогресом комп'ютерних технологій, приходять разом з ними і проблеми, що наразі, становлять чи не найбільшу загрозу для людства.

Кіберзброя — одна з найбільш небезпечних інновацій суспільства, що здатна уразити комунікаційні системи всіх форм власності.

Наша держава на собі відчула перші атаки з боку Російської Федерації у 2013 році. Тоді, російсько-українська війна стала першим конфліктом у кіберпросторі.

У 2015 році російські зловмисники вивели з управління комп'ютерні системи в енергетичних компаніях України. Прикладом може служити «Прикарпаттяобленерго», внаслідок чого там було вимкнено близько 30 підстанцій, а жителі даного регіону залишилися без світла протягом декількох годин. Дана атака відбувалась з використанням програми «BlackEnergy».

Під дію кібератаки потрапила також Державна казначейська служба у грудні 2016 року, що призвело до затримок бюджетних виплат.

Проте у червні 2017 року сталась найбільш відома хакерська атака з використанням вірусу "NotPetya". На той момент, вона порушила роботу численних українських державних і приватних підприємств, серед них варто виділити банки, енергетичні компанії, аеропорти, метрополітени, Чорнобильську АЕС, а також роботу Кабінету Міністрів України і декількох ЗМІ, що тривалий час дозволяло зловмисникам отримувати інформацію та відкривати надалі доступ до комп'ютерних мереж.

«Petya» - одна з шкідливих програм для комп'ютерного забезпечення, яка здатна вражати навіть останні оновлення операційної системи. Тоді, її признали наймасштабнішою хакерською атакою, що завдала найбільших збитків в історії.

Внаслідок цього, в Україні виникла потреба підсилити роботу фахівців із кібербезпеки.

Початком до запровадження повноцінного захисту інформаційно-телекомунікаційних систем стало прийняття Закону України "Про основні засади забезпечення кібербезпеки України".

Проте, задля повноцінної реалізації даного закону, необхідно було створити орган, або ж підрозділ, який вів би активну боротьбу з кіберзлочинцями.

Тому у 2018 році, за підтримки іноземних партнерів в СБУ було створено Ситуаційний центр забезпечення кібернетичної безпеки на базі Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ за стандартами НАТО.

Розробили його згідно з угодою про реалізацію Трастового фонду Україна-НАТО. На проект виділили понад $1 млн.

Новостворений центр здатен миттєво вирахувати будь-який віртуальний наступ. Ключовими його можливостями є виявлення та реагування на різноманітні онлайн-інциденти, що дозволяє попереджати кібератаки, встановлювати їх походження, аналізувати для вдосконалення протидії.

Основними завданнями даного центру є:

1) запобігання, виявлення, припинення та розкриття злочинів проти миру та безпеки людства, які вчиняються у кіберпросторі;

2) здійснювати контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством;

3) негласна перевірка готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів;

4) протидія кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави;

5) розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів критичної інформаційної інфраструктури;

6) забезпечення реагування на кіберінциденти у сфері державної безпеки.

Наразі, існує лише два регіональних центрів забезпечення кібербезпеки, створених на базі управлінь Служби безпеки України у відповідних областях.

Перший було створено наприкінці 2018 року у Дніпрі. Основними завданнями якого є реагування на кіберінциденти та кібератаки, цілями яких є державні електронні інформаційні ресурси та об'єкти критичної інфраструктури Дніпропетровської області. Наприкінці минулого року спеціалісти у сфері забезпечення кібербезпеки у даному регіоні заблокували одну з хакерських атак, зловмисники якої здійснювали масштабні розсилки електронних листів з комп'ютерними вірусами.

Другий регіональний центр було відкрито у травні 2019 року в Одесі, що стало наступним кроком у розбудові національної системи кібербезпеки, яке проходить у межах другого етапу Угоди «Про реалізацію Трастового фонду Україна-НАТО з питань кібербезпеки».

Також, відповідно до пленарного засідання Волинської обласної ради, що внесла зміни до програми протидії тероризму, передбачається і третій регіональний Ситуаційний центр при Управлінні Служби безпеки України у Волинській області.

Дану програму планують реалізувати у 2020 році.

Проте задля її втілення необхідно здійснити закупівлі комп'ютерної техніки, відповідних засобів відображення та фіксації інформації, на що потрібно виділити з обласного бюджета близько 300 тис. гривень.

Висновки. Підсумовуючи вище перелічене, необхідно зазначити, що для нашої країни потрібно не лише приймати закони, які визначають правові та організаційні основи забезпечення захисту кібербезпеки, а й створювати необхідні органи спеціального призначення у кожному регіоні України, що дозволить своєчасно реагувати на кібератаки, виявляти кіберзлочинців та недопускати недотримання основних прав та свобод людей у сфері інформаційно-телекомунікаційних ситем, адже відповідно до статті 31 Конституції кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції.

Також, потрібно створити більше робочих місць для професіоналів у сфері інформаційних технологій та поліпшити техніку, що дозволить якісніше реагувати на спроби хакерів завдати нашій країні збитків.

Література

1. Конституція України.
2. Стратегія національної безпеки України, затверджено Указом Президента України від 26 травня 2015 року № 287/2015. Опубліковано в офіційному виданні Урядовий кур'єр — № 95.
3. Офіційний веб-сайт Служби безпеки України. URL: https://ssu.gov.ua/ua/pages/330
4. URL: https://youtu.be/Hep3A9mFn0I
5. Закон України «Про основні засади забезпечення кібербезпеки України».