

- *Звертайтеся за допомогою*: якщо ви стали жертвою онлайн-шахрайства чи кібербулінгу, зверніться за допомогою до дорослого, якому ви довіряєте, або до правоохоронних органів.

4. Безпека дітей в Інтернеті:

- *Спілкуйтеся з дітьми про безпеку в Інтернеті*: поясніть їм, як уникнути онлайн-загроз та як поводитися відповідально в Інтернеті.

- *Використовуйте батьківський контроль*: батьківський контроль може допомогти вам обмежити доступ дітей до певних веб-сайтів і контенту.

- *Будьте зразком для наслідування*: покажіть дітям, як безпечно користуватися Інтернетом, будучи добрим прикладом для них.

- *Створіть атмосферу довіри*: заохочуйте дітей розповідати вам про те, що вони роблять в Інтернеті, щоб ви могли допомогти їм у разі виникнення проблем.

Пам'ятайте: Інтернет може бути чудовим ресурсом, але він також може нести в собі певні ризики. Дотримуючись цих порад, ви можете зробити свій досвід в Інтернеті більш безпечним і приємним.

Драченко Захар Дмитрович

*студент 102 БПМС навчальної групи
ННІ № 1 НАВС*

Науковий керівник:

Яровий Кирило Васильович

*кандидат юридичних наук, старший
викладач кафедри інформаційних
технологій та кібербезпеки ННІ № 1
НАВС, капітан поліції*

СУЧАСНІ ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ В УМОВАХ СЬОГОДЕННЯ

Протягом історії людства способи розв'язання проблем захисту інформації визначались рівнем розвитку технологій. У сучасному інформаційному суспільстві технологія відіграє роль активатора зазначеної проблеми – комп'ютерні злочини стали характерною ознакою сьогодення.

Незважаючи на те, що проблеми кіберзахисту в Україні були предметом наукових дискусій у роботах: П.П. Андрушка, Ю.М. Батуріна, О.І. Бойцова, О.Г. Волеводза, Б.В. Волженкіна, В.Д. Гавловського, М.В. Гуцалюка, А.М. Жодзішського, В.О. Копилова, Ю.І. Ляпунова, В.Ю. Максимова, О.І. Панфілової, А.М. Попова та інших. В даний час питання кіберзахисту в кіберпросторі є найбільш розповсюдженим і актуальним для суспільства, оскільки питання захисту інформації у мовах сьогодення залишається актуальним.

Проаналізувавши роботи вітчизняних науковців можна резюмувати, що в Україні кіберзлочинність пов'язується передусім із віртуальним простором. Комп'ютерні злочини являють собою передбачені законодавством суспільно небезпечні дії, що посягають на встановлений в суспільстві порядок інформаційних відносин і скоєння їх відбувається з використанням електронно-обчислювальних машин, тобто комп'ютерів, систем та комп'ютерних мереж [1].

Наприклад, на думку Д.П. Біленчука, кіберзлочинністю є злочинність у змодельованому за допомогою комп'ютера інформаційному просторі, в якому перебувають відомості про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символічному або будь-якому іншому виді, й рухи, що перебувають у процесі, по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального устрою, а також іншого носія, спеціально призначеного для їхнього зберігання, обробки й передачі [2, с. 32]. Таке поняття є найбільш адаптованим та наближеним до української кримінально-правової доктрини, оформленої Кримінальним кодексом України [3], але воно не повністю розкриває всю сутність поняття «злочинність».

На думку О.М. Литвака, злочинністю - це відносно масове явище кожного суспільства, що складається з сукупності окреслених кримінальним законом вчинків, вчинених на тій чи іншій території протягом певного часу [4, с. 9].

Таким чином об'єктом злочину зазначених правопорушень виступають інформаційні відносини у суспільстві, що охороняються законом, а предметом – електронно-обчислювальні машини (комп'ютери), системи та комп'ютерні мережі, а також комп'ютерна інформація, що обробляється за їх допомогою.

Комп'ютерними злочини, пов'язані з втручанням у роботу комп'ютера, і злочини, в яких комп'ютери використовуються як необхідні технічні засоби.

У науковій літературі головними причинами комп'ютерних злочинів і пов'язаних з ними викрадень інформації є такі:

- швидкий перехід від традиційної паперової технології зберігання та передавання інформації до електронної за одночасного відставання технологій захисту інформації, зафіксованої на машинних носіях;
- широке використання локальних обчислювальних мереж, створення глобальних мереж і розширення доступу до інформаційних ресурсів;
- постійне ускладнення програмних засобів, що викликає зменшення їх надійності та збільшення кількості уразливих місць [5, с. 21].

На сьогоднішній день неможливо точно визначити обсяги збитків від комп'ютерних злочинів, але фахівці узгоджують, що ці суми вимірюються мільярдами доларів. Також слід враховувати морально-психологічні наслідки для користувачів, персоналу і власників інформації.

Щодо порушення безпеки так званих «критичних» додатків у державному і військовому управлінні, атомній енергетиці, медицині, ракетно-космічній галузі та у фінансовій сфері, це може призвести до серйозних наслідків для навколишнього середовища, економіки і безпеки держави, а також здоров'я та навіть життя людей.

У висновку можна сказати, що сучасні технології захисту інформації в умовах сьогодення відіграють критичну роль у забезпеченні безпеки та конфіденційності даних. Слід відзначити, що із зростанням кількості інформації та розвитком цифрових технологій загрози для безпеки даних постійно зростають.

Тому постійне вдосконалення та впровадження новітніх методів захисту стає невід'ємною частиною стратегії будь-якої організації або компанії. Підсумовуючи, ефективна захист інформації вимагає комплексного підходу, що включає в себе як технічні засоби, так і культурні та організаційні заходи. Тільки таким чином можна забезпечити надійну захищеність в умовах сучасного цифрового світу в умовах сьогодення.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: <http://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 03.04.2024).
2. Біленчук Д. П. Кібрешахраї – хто вони? Міліція України. 1999. № 7–8. С. 32–34.
3. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. Відомості Верховної Ради України. 2001. № 25–26. Ст. 131.
4. Литвак О. М. Злочинність, її причини та профілактика. Київ : Україна, 1997. 168 с.
5. Інформаційна безпека комп'ютерних систем і мереж: Методичні вказівки // Укл. А.Ф. Карачка, М.П. Карпінський, А.В. Кулик, Т.В. Лендюк. – Тернопіль: ТАНГ, 2007. – 68 с.