Гончарова Анастасія Володимирівна
Студентка н.гр. 101_СПД ННІ права та психології НАВС

Науковий керівник:
Кудінов Вадим Анатолійович
кандидат фізико-математичних наук, доцент, завідувач кафедри інформаційних технологій ННІ права та психології НАВС

ВИКЛИКИ ДЛЯ УКРАЇНИ У СФЕРІ КІБЕРБЕЗПЕКИ ТА ОСНОВНІ ПІДХОДИ ЩОДО ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ

Кібербезпека – це захист комп'ютерних систем, мереж, програм і даних від цифрових атак, несанкціонованого доступу та крадіжок. Вона забезпечує конфіденційність, цілісність та доступність інформації, використовуючи комплекс технологій, процесів і рекомендацій. Ця сфера є критично важливою для захисту особистої, корпоративної та національної інформації в цифровому світі.

Викликами для України у сфері кібербезпеки є:

- активне використання кіберзасобів у міжнародній конкуренції;
- змагальний характер розвитку засобів кібербезпеки в умовах швидких прогресуючих змін інформаційно-комунікаційних технологій, зокрема хмарних та квантових обчислень, 5G-мереж, великих даних, Інтернету речей, штучного інтелекту тощо;
- мілітаризація кіберпростору та розвиток кіберзброї, що дає можливість приховано проводити кібератаки для підтримки бойових дій і розвідувально-підривної діяльності у кіберпросторі;
- вплив пандемії COVID-19 на економічну діяльність та соціальну поведінку, що спричинив стрімку трансформацію і організацію значного сегмента суспільних відносин у дистанційному режимі з широким використанням електронних сервісів та інформаційно-комунікаційних систем;
- упровадження нових технологій, цифрових послуг та механізмів електронної взаємодії громадян з державою, що здійснюється безсистемно в частині заходів з кібербезпеки та без належної оцінки ризиків.

Типи загроз для кібербезпеки

Шкідливе програмне забезпечення (віруси, хробаки, зловмисні програми з вимогою викупу, шпигунські програми). Воно шкодить комп'ютерам і мережам, змінюючи або видаляючи файли, видобуваючи делікатні дані, як-от паролі й номери рахунків, а також надсилаючи зловмисні електронні листи чи трафік.

Зловмисні програми з вимогою викупу, також відомі як кібервимагання – це тип шкідливого програмного забезпечення, який шифрує дані жертви та вимагає плати (часто в криптовалюті) за відновлення доступу.

Шкідливе програмне забезпечення можуть інсталювати зловмисники, які отримують доступ до мережі, але частіше окремі користувачі випадково розгортають його на своїх пристроях

Атаки з використанням фішингу та соціотехніки. Використовуючи соціотехніку, зловмисники втираються в довіру до користувачів і обманом змушують їх передавати відомості облікового запису або завантажувати шкідливе програмне забезпечення. Фішинг – це тип соціотехники, який використовує електронні листи, текстові або голосові повідомлення начебто з надійного джерела, щоб заохотити користувачів перейти за посиланням, що вимагає входу, і вкрасти їхні облікові дані.

Внутрішні загрози. Походять від працівників організації, які випадково або навмисно порушують безпеку. Ці загрози можуть виникати через незадоволених працівників або тих, хто має доступ до делікатної інформації.

Запобігання кіберзлочинності повинно ґрунтуватися на таких основних підходах:

1. *Міжнародний підхід* передбачає консолідацію зусиль правоохоронних органів різних держав, а також створення спеціальних органів і підрозділів по боротьбі з кіберзлочинністю.

2. *Правовий підхід* пов’язаний з удосконаленням правових механізмів національного та міжнародного законодавства, що передбачає відповідальність за кіберзлочини. Оскільки на сьогоднішній день жодна держава не може захистити себе від кіберпосягань приймаючи правові заходи тільки на національному рівні, вбачається необхідним організація і реалізація комплексної програми запобіганні кіберзлочинності, що включає: гармонізацію кримінального законодавства про кіберзлочини; дієвий механізм вирішення юрисдикційних питань в кіберпросторі.

3. *Технічний підхід* передбачає запобігання кіберзлочинам за рахунок реалізації заходів технічного характеру, що забезпечують безпеку в інформаційній сфері, а також формування матеріально-технічної бази підрозділів по боротьбі з кіберзлочинністю, виходячи з принципу «найсучасніша техніка».

4. *Організаційний підхід* має на меті розробку і запровадження в практику, удосконалених організаційно профілактичних заходів.

Висновки. Для запобігання кіберзлочинності необхідні комплексні заходи, які охоплюють міжнародний, правовий, технічний та організаційний підходи. Слід відійти від вирішення проблеми запобігання кіберзлочинності шляхом подолання існуючих тенденцій і перейти до активної розробки інформаційної безпеки на випередження. Необхідно об’єднання зусиль всіх учасників, зацікавлених у запобіганні кіберзагрозам: правоохоронних органів, підприємницького середовища, громадських організацій, науково-дослідних установ і громадян.

Список використаних джерел:

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 20.10.2025).
2. Микитчик А. В. Заходи запобігання кіберзлочинності в Україні». URL: https://univd.edu.ua/general/publishing/konf/18_04_2019/pdf/63.pdf (дата звернення: 20.10.2025).

Шинкаренко Ангеліна Юріївна
Студентка н.гр. 101_СПД ННІ права та психології НАВС

Науковий керівник:
Кудінов Вадим Анатолійович
кандидат фізико-математичних наук, доцент, завідувач кафедри інформаційних технологій ННІ права та психології НАВС

ОСНОВИ КІБЕРГІГІЄНИ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

У наш час цифрові технології стали невід'ємною частиною повсякденного життя. Інформаційні технології та системи охоплюють безліч сфер діяльності: освіта, медицина, бізнес, держуправління тощо. Люди щодня користуються комп'ютерами, смартфонами, соціальними мережами, електронною поштою, хмарними сервісами та іншими інформаційними системами. Однак з поширенням цих технологій зростають і загрози: кіберзлочинність, шахрайство, витік персональних даних, вплив шкідливого контенту. Будь-яка технологічна система залишається вразливою, якщо користувач не дотримується правил безпеки. У цьому контексті особливу роль відіграє *кібергігієна* – система правил, звичок і заходів, спрямованих на безпечне користування інформаційними технологіями. Її дотримання є ключовим фактором у збереженні особистої цифрової безпеки, а також безпеки ІТ-систем у цілому.

Кібергігієна – це сфера, яка зосереджується на забезпеченні фізичного та психічного здоров'я користувачів в умовах постійної взаємодії з інформаційними технологіями. Вона включає в себе розвиток стратегій для зменшення негативного впливу цифрових технологій на людське здоров'я, таких як синдром перевантаження інформацією, втома від роботи за комп'ютером та інші проблеми, пов'язані з інтенсивним використанням електронних пристроїв [1].