Замула Дар'я Володимирівна
студентка 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

ПРОБЛЕМИ ЗАХИСТУ ДАНИХ У МЕРЕЖІ-ІНТЕРНЕТ В УМОВАХ ВОЄННОГО СТАНУ

У світі, де віртуальна реальність все більше переплітається з реальним життям, проблеми захисту даних у мережі Інтернет набувають надзвичайної актуальності. Швидкість технологічного розвитку призводить до появи нових загроз та викликів для конфіденційності та приватності інформації в онлайн середовищі. У цьому контексті розгляд проблем захисту даних стає невід'ємною складовою наукового дослідження, оскільки від нього залежить забезпечення безпеки користувачів та надійність інформаційних систем. В даній статті ми дослідимо актуальні аспекти цієї проблематики та запропонуємо шляхи її вирішення в умовах сучасного цифрового світу.

Захист даних, захист інформації – це сукупність заходів і відповідних засобів, які забезпечують захист прав власності власників інформаційної продукції, у першу чергу – програм, баз і банків даних від несанкціонованого доступу, використання, руйнування або завдання шкоди в будь-якій іншій формі [1, с. 78].

У галузі знань із захисту інформації сформульовано такі основні твердження:

1) абсолютно надійний захист створити неможливо. Система захисту інформації може бути, в кращому разі, адекватною потенційним загрозам;

2) система захисту інформації повинна бути комплексною: слід використовувати не тільки технічні засоби захисту, а й адміністративні та правові;

3) система захисту інформації повинна бути гнучкою, здатною адаптуватися до умов, що змінюються.

Виходячи з можливих порушень у роботі системи та загроз несанкціонованого доступу до інформації існують множинні види захисту, які можна поділити на такі умовні групи: морально-етичні, правові, адміністративні (організаційні), технічні (фізичні), програмні. Зокрема, сучасні технології розвиваються в напрямку сполучення програмних та апаратних засобів захисту.

На думку Виганяйло С.М., під правовими засобами захисту слід розуміти, чинні закони, укази та інші нормативні акти, які регламентують правила користування інформацією і відповідальність за їх порушення, захищають авторські права програмістів та регулюють інші питання використання інформаційних технологій [2, с. 38].

Адміністративні (організаційні) заходи забезпечення безпеки інформації визначають правила та процедури, що регулюють роботу інформаційної системи, використання її ресурсів та діяльність персоналу. Вони також визначають способи взаємодії користувачів із системою з метою ускладнення або запобігання порушенням безпеки. Адміністративні заходи охоплюють:

1) розмежування доступу до інформації за допомогою паролів, профілів повноважень тощо; розроблення адміністративних норм та системи покарань за їх порушення тощо);

2) розроблення правил обробки та зберігання інформації, а також стратегії її захисту (організація обліку, зберігання, використання і знищення документа і носіїв з конфіденційною інформацією);

3) заходи, які здійснюються під час добору та підготовки персоналу (перевірка нових співробітників, ознайомлення їх із порядком роботи з конфіденційною інформацією і ступенем відповідальності за його недодержання; створення умов, за яких персоналу було б невигідно або неможливо припускатися зловживань, тощо);

4) заходи, які передбачаються під час проектування, будівництва та облаштування об’єктів охорони (врахування впливу стихії, протипожежна безпека, охорона приміщень, пропускний режим, прихований контроль працівників тощо);

5) заходи, що вживаються під час проектування, розроблення, ремонту й модифікації обладнання та програмного забезпечення (перевірка на відповідність стандартам всіх технічних і програмних засобів, строге затвердження, оцінка та ухвалення будь-яких змін) [3, с. 138].

Адміністративні засоби захисту інформації є важливим елементом, оскільки вони можуть доповнювати законодавчі норми та застосовуватися у випадках, коли потрібно забезпечити безпеку організації. Часто вони передбачають використання інших видів захисту, таких як технічний чи програмний, що забезпечує більш надійний рівень захисту. Проте велика кількість адміністративних правил може ускладнювати роботу працівників і навіть знижувати ефективність захисту, оскільки інструкції можуть залишатися невиконаними [4, с. 216].

Проблематика полягає в тому, що надмірна кількість адміністративних правил у сфері захисту інформації може призвести до недоліків у роботі персоналу та зниження ефективності заходів безпеки. Відповідно, це може стати загрозою для безпеки інформації, оскільки інструкції можуть бути ігнорованими або виконуватися неадекватно через їх велику кількість.

Надмірна адміністративна складність може призвести до витрат часу та ресурсів на виконання процедур, що не завжди може бути обґрунтованим з точки зору реальних загроз безпеці.

Таким чином, забезпечення захисту даних та інформації є важливим аспектом у сучасному світі. У зв'язку з цим, існує ряд різноманітних методів захисту даних, які можна класифікувати на кілька основних категорій: правові, адміністративні, технічні та програмні. Кожен з цих підходів спрямований на захист даних та інформації від несанкціонованого доступу, використання та руйнування.

Список використаних джерел:

1. Кудінов В. А., Яровий К. В. Інформаційне забезпечення правоохоронної діяльності: навч.-практ. посіб. Київ: Нац. акад. внутр. справ, 2024. 120 с.

2. Виганяйло С. М. Інформаційне забезпечення професійної діяльності: навч. посіб. Харків: ХНУВС, 2021. 108 с.

3. Іванов В. Г. Правова інформація та комп'ютерні технології в юридичній діяльності: навч. посіб. / В. Г. Іванов, С. М. Іванов, В. В. Карасюк та ін.; за заг. ред. В. Г. Іванова. – Х.: Право, 2010. – 240 с.

4. Вишня В. Б. Інформаційні технології: навч. підручник / В. Б. Вишня, К. Ю. Ісмайлов, І. В. Краснобрижий, С. О. Прокопов, Е. В. Рижков. Дніпро: ДДУВС, 2020. 418 с.

Іваненко Катерина Володимирівна
студентка 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

ОПТИМІЗАЦІЯ РОБОТИ СИСТЕМИ «ЦУНАМІ» В ПРАВООХОРОННИХ ОРГАНАХ

Системи централізованого управління нарядами поліції є важливим елементом забезпечення громадського порядку та безпеки в сучасних містах. Однак, у зв'язку з постійними змінами у соціальному, технологічному та кримінальному середовищі, необхідність постійного вдосконалення цих систем стає невідкладною. Особливо в контексті великих міст, де складність та обсяги завдань, що стоять перед правоохоронними органами, постійно зростають.