- Використовуйте унікальний пароль для кожного веб-сайту. Якщо краде відомості облікового запису з одного сайту, вони намагатимуться використовувати ці облікові дані на сотнях інших відомих веб-сайтів, таких як банківські послуги, соціальні мережі або покупки в Інтернеті, сподіваючись, що пароль повторно використовується в іншому місці. Це називається "Атака, яка має облікові дані", і вона дуже поширена.
- Якщо ви не хочете запам’ятовувати декілька паролів, скористайтеся диспетчером паролів. Найкращі диспетчери паролів будуть автоматично оновлювати збережені паролі, зберігати їх у зашифрованому вигляді та вимагати багатофакторну автентифікацію для отримання доступу.
- Поки ви їх захистите, ви можете записати паролі. Не пишіть їх на наліпках або картках біля тієї, яку захищає пароль, навіть якщо ви вважаєте, що вони добре приховані.
- Увімкніть багатофакторну автентифікацію за наявності. Для входу до облікового запису багатофакількома типами облікових даних, наприклад для введення пароля та одноразового коду, створеного програмою. Це додає ще один рівень безпеки на випадок, якщо хтось вгадає або викраде пароль.

Злочинці можуть спробувати зламати пароль, але іноді простіше скористатися слабкостями людини і виманити його в неї. Якщо ви отримали повідомлення електронної пошти від інтернет-магазину (наприклад, eBay або Amazon) або телефонний виклик від «банку», який намагатиметься переконати вас про «законне» отримання пароля або іншої важливої інформації, це може бути фішингове повідомлення.

Карпенко Анна Миколаївна
курсант 204 навчальної групи ННІ № 3 НАВС, рядовий поліції

Науковий керівник:
Яровий Кирило Васильович
кандидат юридичних наук, старший викладач кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС, капітан поліції

РОЛЬ СУЧАСНИХ ТЕХНОЛОГІЙ У ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ ІНФОРМАЦІЇ

В сучасному світі, де цифрові технології проникають у всі сфери життя, питання безпеки інформації стає все більш актуальним. З кожним днем зростає кількість кіберзлочинів, загрози кібератак та порушень приватності.

Таким чином, важливість сучасних технологій захисту інформації набуває все більшої ваги, оскільки вони стають вирішальними для збереження конфіденційності, цілісності та доступності даних у цифровому середовищі.

Незважаючи на те, що проблеми сучасних технологій кібербезпеки були предметом наукових дискусій у роботах Савченко В.С., Колосовський Є.Ю., Круць Е.М., Бандурко О.М., Березовська І.Р., Гнатюк О.С., Дзьобань О.П. та інших, насьогодні, зазначене питання не втрачає своєї актуальності.

У сучасних умовах глобалізації та зростаючої конкуренції, захист інформації стає надзвичайно важливим аспектом як для організацій, так і для державних підприємств та корпорацій України. Створення надійних систем захисту і збереження інформаційних ресурсів на рівні всієї організації і її окремих підрозділів стає все більш актуальним, а успішність таких заходів безпосередньо впливає на конкурентоспроможність організації в цілому.

У юридичній літературі, захист інформації - це сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації та осіб, які користуються інформацією [1].

Одним із основних методів забезпечення безпеки інформації у складних інформаційних системах є удосконалення системного підходу до цієї проблеми. Під системним підходом мається на увазі не лише створення відповідних захисних механізмів, але й впровадження систематичного процесу, що застосовується на всіх етапах життєвого циклу інформаційної системи та використовує усі доступні засоби захисту.

Задорожнюк Н.О. вважає, що забезпечення безпеки інформаційних технологій являє собою комплексну проблему, яка охоплює правове регулювання використання ІТ, удосконалення технологій їх розробки, розвиток системи сертифікації, забезпечення відповідних організаційно-технічних умов експлуатації під час війни [2, с. 106].

Зазначене свідчить, що захист інформації повинен бути розглянутий як невід’ємна частина всієї інформаційної системи, а не просто як окремий компонент.

Крім цього, багато проблем, пов’язаних із захистом цієї інформації, можуть бути вирішені шляхом відомих правових та організаційних заходів. Проте з урахуванням прогресу інформаційних технологій, спостерігається зростаюча потреба в застосуванні технічних засобів та заходів для її захисту.

Наприклад, організаційні заходи включають в себе створення концепції інформаційної безпеки, а також:

- складання посадових інструкцій для користувачів та обслуговуючого персоналу;
- створення правил адміністрування компонент інформаційної системи, обліку, зберігання, знищення носіїв інформації, ідентифікації користувачів;

- розробка планів дій у разі виявлення спроб несанкціонованого доступу до інформацій-них ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації;

- навчання правилам інформаційної безпеки користувачів [3, с. 7].

Комплексний (системний) підхід до побудови будь-якої системи містить в собі:

- аналіз об'єкта впроваджуваної системи;

- оцінка загроз безпеки цього об'єкта; аналізуються ресурси, які будуть використовуватися під час розробки системи;

- оцінка економічної доцільності проєкту;

- аналіз самої системи, її характеристик, принципів функціонування та можливостей для підвищення ефективності;

- взаємодія всіх внутрішніх і зовнішніх факторів [4, с. 15].

Сучасний ринок програмних продуктів містить різні програми для забезпечення інформаційної безпеки. Програмні засоби захисту забезпечують ідентифікацію та аутентифікацію користувачів, розмежування доступу до ресурсів згідно з повноваженнями користувачів, криптографічний захист інформації, захист від комп'ютерних вірусів тощо. Такі програми можна поділити на системні та прикладні програми. Для ефективного захисту слід використовувати комплексний підхід, який враховує як зовнішні, так і внутрішні загрози. Важливо поєднувати програмні, технічні та організаційні засоби і заходи. Побудова єдиної концепції інформаційної безпеки дозволить забезпечити всебічний захист і оптимальну політику безпеки. Всебічний аналіз даних та інформаційного забезпечення допоможе виробити оптимальну стратегію захисту.

Забезпечення доступу до надійної та актуальної інформації для правоохоронних органів, співпраця між ними на національному та міжнародному рівнях, а також використання передових технологій інформаційної безпеки є важливими складовими ефективної системи правоохоронного заходу. Розвиток інформаційних технологій та постійне удосконалення процесів обробки та аналізу даних мають визначальне значення для підвищення ефективності правоохоронної діяльності та забезпечення гармонійного розвитку суспільства [5, с. 106].

Підводячи підсумок, можна зазначити, що кожен підхід та засіб захисту інформації впливають на безпеку та захист інформації, а також на діяльність підприємства чи організації по-різному. Важливо розуміти, що потенційні загрози від недосконалих систем захисту інформації можуть завдати шкоду діяльності підприємства. Тому належне управління інформацією на підприємстві повинно враховувати останні досягнення в галузі програмного, технічного та інших аспектів забезпечення інформаційної безпеки.

Список використаних джерел:

1. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. №80/94-ВР URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.
2. Задорожнюк Н. О. Сучасні технології бізнес-аналітики. Економічна аналітика: сучасні реалії та прогностичні можливості : збірник матеріалів міжнар. наук.-прак. конф. (Київ, 19 квітня 2019 р.). Київ, 2019. С. 105–107.
3. Ляпін К. Е. Виклики та можливості сучасності: комплексна система захисту інформації. Збірник матеріалів VI міжнародної науково-практичної конференції «Інформаційна безпека та комп'ютерні технології»: тези доповідей, 20-21 квітня 2023 р. Кропивницький: ЦНТУ, 2023. 96 с.
4. Яремчук Ю. Є. Комплексні системи захисту інформації: навч. посіб. та ін. 63-тє вид. Вінниця: ВНТУ, 2018. 119 с.
5. Кудінов В. А., Яровий К. В. Інформаційне забезпечення правоохоронної діяльності: навч.-практ. посіб. Київ: Нац. акад. внутр. справ, 2024. 120 с.

Кедик Єлизавета Миколаївна
курсант 203 навчальної групи ННІ № 3 НАВС, рядовий поліції

Науковий керівник:
Яровий Кирило Васильович
кандидат юридичних наук, старший викладач кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС, капітан поліції

ПРОБЛЕМИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КОМП'ЮТЕРНИХ СИСТЕМАХ

В інформаційному суспільстві спостерігається експонентне зростання інтенсивності процесів інформаційного обміну та обробки даних, що викликає необхідність використання потужних комп'ютерних систем. До таких систем пред'являють такі вимоги, як висока швидкодія, великий обсяг пам'яті, здатність обробляти велику кількість транзакцій одночасно, підвищена надійність.

Надійність, яка є однією з головних вимог до комп'ютерних систем, адже від рівня надійності системи залежить, наскільки відповідальні інформаційні процеси їй можна довірити. Оскільки абсолютна надійність комп'ютерних систем та результатів інформаційних процесів, які у них виконуються, не може бути забезпечена, задачею досліджень є визначення критичних областей, де такі помилки та збої в роботі не допустимі.