**Олена Матусевич**

**(Біла Церква, Україна)**

**ІНФОРМАЦІЙНА БЕЗПЕКА У СУЧАСНОМУ СВІТІ**

Сьогодні ми живемо з вами у інформаційному суспільстві,в епоху інформаційної передозу. Інформаційне суспільство - це концепція, що описує сучасний етап розвитку цивілізації, в якому інформація та знання відіграють ключову роль у всіх сферах життя: економіці, політиці, культурі та соціальних відносинах. Інформаційний простір – це океан даних.

Інформація та знання стають головним продуктом виробництва та споживання. Технології проникають у всі сфери діяльності, сприяючи автоматизації та підвищенню ефективності. Кожного дня Інтернет забезпечує нам миттєвий доступ до інформації та спілкування з людьми по всьому світу.

У сучасному світі інформація є одним з найцінніших ресурсів. Ми використовуємо її для спілкування, роботи, навчання та розваг. Ми маємо швидкий та легкий доступ до величезних обсягів інформації, доступ до онлайн-курсів, лекцій та інших освітніх ресурсів. Створюються нові технології та наукові відкриття завдяки обміну інформацією та співпраці між вченими. Тому важливо забезпечити її безпеку, щоб захистити себе від різних загроз. Саме інформаційна безпека відіграє ключову роль у захисті особистих даних, бізнесу та національної безпеки.

Що таке інформаційна безпека?

Інформаційна безпека - це комплекс заходів, спрямованих на захист інформації від несанкціонованого доступу, використання, розголошення, зміни або знищення. Вона включає в себе технічні, організаційні та правові аспекти.

Інформаційна безпека важлива, тому що вона допомагає захистити:

* особисті дані: імена, адреси, номери телефонів, дані кредитних карток;
* фінансову інформацію: банківські рахунки, паролі, транзакції;
* конфіденційну інформацію: комерційну таємницю, інтелектуальну власність;
* репутацію: як особисту, так і організаційну.

Захист особистих даних - це Ваші персональні дані, такі як ім'я, адреса, номер телефону, дані кредитних карток та інші, можуть бути використані зловмисниками для крадіжки особистості, фінансового шахрайства або інших злочинів.

Інформаційна безпека допомагає запобігти витоку цих даних та забезпечити їх конфіденційність.

Інформаційна безпека відіграє важливу роль у захисті критичної інфраструктури, державних таємниць та інших важливих ресурсів від кібершпигунства, терористичних атак та інших загроз. Забезпечення кібербезпеки є важливим аспектом національної безпеки будь-якої країни.

Загрози інформаційній безпеці можуть бути різними:

* віруси та шкідливе програмне забезпечення: можуть пошкодити або знищити ваші дані, а також дозволити зловмисникам отримати доступ до вашої інформації;
* хакери: можуть зламати ваші комп'ютери або облікові записи, щоб отримати доступ до вашої інформації;
* фішинг: це вид шахрайства, коли зловмисники намагаються отримати вашу особисту інформацію, видаючи себе за відомі організації;
* соціальна інженерія: це вид маніпуляції, коли зловмисники змушують вас розкрити свою особисту інформацію або виконати дії, які можуть зашкодити вашій безпеці;
* внутрішні загрози: можуть виходити від працівників, які мають доступ до вашої інформації, але зловживають цим.

Сьогодні, коли наше життя нерозривно пов'язане з комп'ютерами та інтернетом, і кожного дня ми подорожуємо простором Інтернет у пошуках різної інформації та програмного забезпечення, користуємося для спілкування і комунікації електронною поштою, комп'ютерні віруси стали серйозною загрозою для нашої безпеки. Вони можуть завдати шкоди не тільки нашим пристроям, але й особистим даним, фінансам та навіть репутації.

Вірус - це тип ШПЗ, який здатний самовідтворюватися та поширюватися, заражаючи інші файли та системи. Віруси можуть пошкоджувати файли, красти дані, порушувати роботу комп'ютера або навіть блокувати його.

Шкідливе програмне забезпечення (ШПЗ) - це загальний термін, який охоплює різні види зловмисних програм, включаючи віруси, троянські програми, черв'яки, шпигунське ПЗ, програми-вимагачі та інші. ШПЗ може потрапити на ваш пристрій різними шляхами, наприклад, через заражені файли, веб-сайти, електронну пошту або USB-накопичувачі.

Яку шкоду можуть завдати комп'ютерні віруси?

* Пошкодження або знищення файлів: віруси можуть пошкодити або знищити ваші особисті файли, такі як фотографії, документи або відео.
* Крадіжка особистих даних: віруси-шпигуни можуть викрасти ваші паролі, номери кредитних карток та інші особисті дані, які можуть бути використані зловмисниками для шахрайства або крадіжки особистості.
* Порушення роботи комп'ютера: віруси можуть уповільнити роботу комп'ютера, спричинити збої в роботі програм або навіть призвести до повного виходу з ладу системи.
* Фінансові втрати: віруси-вимагачі можуть заблокувати доступ до ваших файлів та вимагати викуп за їх розблокування, що може призвести до значних фінансових втрат.
* Втрата репутації: якщо вірус заразить ваш комп'ютер та використає його для розсилання спаму або шкідливого програмного забезпечення, це може зашкодити вашій репутації.

Одним із ключових елементів захисту від різноманітних загроз є використання надійних антивірусних програм.Антивіруси розроблені для виявлення, блокування та видалення різноманітних шкідливих програм, таких як віруси, трояни, шпигунське ПЗ, програми-вимагачі та інші. Ці програми можуть завдати значної шкоди вашим файлам, системі та особистим даним.

Кіберзлочинці постійно шукають способи отримати доступ до вашої особистої інформації, такої як паролі, номери кредитних карток, банківські рахунки тощо. Антивірусні програми допомагають захистити ці дані від крадіжки та несанкціонованого використання.

Під час користування Інтернетом ми часто стикаємося з різноманітними загрозами, такими як фішингові сайти, шкідливі посилання та заражені файли. Антивірусні програми допомагають блокувати ці загрози та забезпечити безпечне перебування в Інтернеті.

Деякі віруси та шкідливе ПЗ можуть сповільнювати роботу комп'ютера та призводити до збоїв у системі. Антивірусні програми допомагають очистити систему від цих шкідливих програм та підвищити її продуктивність.

Як же вірно зробити свій вибір та обрати антивірусну програму?

На сьогоднішній день існує безліч антивірусних програм, як платних, так і безкоштовних. При виборі антивірусу слід звернути увагу на такі фактори:

* ефективність виявлення та видалення вірусів: оберіть антивірус, який має високі показники виявлення та видалення різноманітних видів шкідливого ПЗ;
* функціональність: зверніть увагу на наявність додаткових функцій, таких як захист від фішингу, блокування спаму, батьківський контроль;
* продуктивність: оберіть антивірус, який не сповільнює роботу комп'ютера та не споживає багато системних ресурсів;
* оновлення: переконайтесь, що антивірус регулярно оновлює свої бази даних вірусів, щоб забезпечити актуальний захист;
* ціна: оцініть свої фінансові можливості та оберіть антивірус, який відповідає вашому бюджету.

Якщо ж раптом ваш пристрій заражений, скористайтеся наступними порадами:

* відключіть пристрій від Інтернету, щоб запобігти подальшому поширенню ШПЗ;
* запустіть повне сканування системи антивірусним програмним забезпеченням: та видаліть виявлені загрози;
* якщо можливо, відновіть систему з резервної копії: створеної до зараження;
* зверніться до фахівця з інформаційної безпеки: якщо ви не можете самостійно впоратися з проблемою.

Звичайно не слід забувати про резервне копіювання даних, адже воно є запорукою збереження вашої інформації.

Резервне копіювання даних - це процес створення копії важливої інформації з метою її відновлення у разі втрати, пошкодження або випадкового видалення.

Навіщо потрібно робити резервне копіювання?

Уявіть собі ситуацію, коли ваш комп'ютер вийшов з ладу, а на ньому зберігалися важливі документи, фотографії, відеозаписи та інші цінні дані. Без резервної копії ви могли б втратити все це назавжди. Резервне копіювання допомагає уникнути таких неприємностей. Воно забезпечує збереження вашої інформації та дозволяє відновити її у будь-який момент.

На сьогоднішній час існують наступні способи резервного копіювання:

* зовнішні жорсткі диски: це один з найпростіших та найдоступніших способів створення резервних копій. Ви можете придбати зовнішній жорсткий диск та періодично копіювати на нього свої важливі файли;
* хмарні сховища: сервіси, такі як Google Drive, Dropbox, iCloud та інші, надають можливість зберігати ваші дані в хмарі. Це зручно, оскільки ви можете отримати доступ до своїх файлів з будь-якого пристрою, підключеного до Інтернету;
* мережеві сховища (NAS): NAS - це спеціалізований пристрій, який підключається до вашої домашньої мережі та дозволяє зберігати файли централізовано;
* програмне забезпечення для резервного копіювання: існує безліч програм, які автоматизують процес створення резервних копій та забезпечують додаткові функції, такі як шифрування та стиснення даних.

Частота створення резервних копій залежить від того, як часто ви змінюєте або створюєте нові файли. Якщо ви працюєте з важливими даними щодня, рекомендується робити резервні копії щодня або кілька разів на тиждень. Якщо ж ви користуєтесь комп'ютером не так часто, можна робити резервні копії раз на тиждень або на місяць.

Отже, інформаційна безпека в сучасному світі є критично важливою для кожного з нас. Ми живемо в цифрову епоху, де інформація є цінним активом, який потребує захисту. Загрози інформаційній безпеці постійно розвиваються та стають все більш складними, тому ми повинні бути пильними та обережними.

Кожен з нас несе відповідальність за забезпечення інформаційної безпеки своїх особистих даних та пристроїв.

На завершення, хочу наголосити на наступних моментах:

* бути освіченими та обізнаними: важливо постійно підвищувати свою обізнаність про загрози інформаційній безпеці та методи захисту від них;
* бути відповідальними: кожен з нас несе відповідальність за забезпечення інформаційної безпеки своїх особистих даних та пристроїв;
* бути пильними та обережними в Інтернеті, не відкривайте підозрілі електронні листи та не переходьте за сумнівними посиланнями;
* забезпечення інформаційної безпеки потребує комплексного підходу, який включає в себе технічні, організаційні та правові аспекти.

Дотримуючись цих простих правил та рекомендацій, ви зможете значно зменшити ризик стати жертвою інформаційних загроз та захистити свою інформацію від зловмисників.

Пам'ятайте, інформація - це цінний ресурс, безпека інформації - це ваша відповідальність. Будьте пильними та обережними.

**Література:**

1. Гребенюк А.М. Основи управління інформаційною безпекою: навч.посіб./А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.
2. Присяжнюк М.М.Інформаційна безпека та кібербезпека держави: навч.посіб./ Н.М. Титова, Н.М. Рідей, В.П. Настрадін, М.М. Присяжнюк, С.М. Мамченко, С.В. Артюх, Р.О. Яворська. Київ: Ліра-К, 2024. – 224с.
3. В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. НастрадiнОснови кiберпростору, кiбербезпеки та кiберзахисту:навч. посiб. /В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадiн. Київ: Ліра-К, 2020. — 554 с.