Текст 1. ***Що таке кібербезпека?***

**Кібербезпека** або **cyber security** — це заходи, які вживають для захисту даних або пристроїв, підключених до мережі, від несанкціонованого доступу та використання у злочинних цілях; практика захисту комп'ютерів, серверів, мобільних пристроїв, електронних систем, мереж і даних від зловмисних атак. Вона також відома як безпека інформаційних технологій або електронна інформаційна безпека. Цей термін застосовується в різних контекстах, від бізнесу до мобільних обчислень, і може бути розділений на кілька загальних категорій. Кібербезпека це те, що забезпечує конфіденційність, цілісність і доступність даних протягом їх всього життєвого циклу. Якщо фізична безпека спрямована на захист від злочинної діяльності або випадкового пошкодження людей та фізичного майна, то кібербезпека захищає комп’ютерні та серверні системи, програми користувачів та дані, які вони в них зберігають. Кібербезпека може захистити все: від особистої інформації до складних державних систем.

Також у межах даної теми було б доречно розібратися з базовими термінами для кращого та глибшого розуміння визначення КІБЕРБЕЗПЕКА:

**Кіберзахист** — це здатність запобігати кібератакам. Це вжиття активних заходів для прогнозування кібератак з боку зловмисника та протидії вторгненням. Усі стратегії та тактики кіберзахисту мають спільну мету — запобігати кіберзагрозам, припиняти та реагувати на них.

**Мережева безпека** - це практика захисту комп'ютерної мережі від зловмисників, чи то цілеспрямованих зловмисників, чи то опортуністичного шкідливого програмного забезпечення.

**Безпека додатків** - зосереджена на захисті програмного забезпечення та пристроїв від загроз. Скомпрометована програма може отримати доступ до даних, які вона покликана захищати. Успішне забезпечення безпеки починається на етапі розробки, задовго до розгортання програми або пристрою.

**Інформаційна безпека -** захищає цілісність і конфіденційність даних як під час зберігання, так і під час передачі.

**Операційна безпека -** включає в себе процеси і рішення для обробки і захисту активів даних. Дозволи, які користувачі мають при доступі до мережі, і процедури, які визначають, як і де дані можуть зберігатися або передаватися, - все це підпадає під цю парасольку. Відновлення після аварій і безперервність бізнесу визначають, як організація реагує на інцидент кібербезпеки або будь-яку іншу подію, що призводить до втрати операцій або даних. Політика аварійного відновлення визначає, як організація відновлює свої операції та інформацію, щоб повернутися до тієї ж операційної спроможності, що й до інциденту. Безперервність бізнесу - це план, до якого повертається організація, намагаючись працювати без певних ресурсів. Навчання кінцевих користувачів стосується найбільш непередбачуваного фактору кібербезпеки - людей. Будь-хто може випадково занести вірус до захищеної системи, не дотримуючись належних практик безпеки. Навчити користувачів видаляти підозрілі вкладення електронної пошти, не під'єднувати невідомі USB-накопичувачі та іншим важливим урокам є життєво важливим для безпеки будь-якої організації.

Якщо Ви бажаєте дослідити дану тему детальніше, тоді щиро радимо ознайомитися з джерелами:

1)https://dan-it.com.ua/uk/blog/chto-takoe-kiberbezopasnost-mery-obespechenija-kiberbezopasnosti/

2)https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

3)"Кібербезпека та ризики цифрової трансформації компаній" Автор Юрій Когут