

ОСНОВНІ ЗАСАДИ КІБЕРБЕЗПЕКИ УКРАЇНИ

На сьогоднішній день провідні держави світу та суспільство в цілому все більшою мірою покладаються і, відповідно, залежать від безперешкодного функціонування п'ятого простору – кіберпростору, під яким пропонується розглядати сукупність взаємопов'язаних інформаційних ресурсів, програмного забезпечення, баз та банків даних. Кожна з систем повинна бути захищена своїм функціоналом для того щоб суспільні, державні, конфіденційні дані не були втрачені або викрадені, для цього виникло поняття «кібербезпека».

Кібербезпека – це стан систем, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах.

Згідно іноземних рейтингів Україна займає провідні місця на арені цифровізації, що підвищує вплив загроз на внутрішню кібербезпеку держави та повинна розвивати цю систему задля збереження економіки, уникнення пропаганди, шантажу та шахрайства. Згідно Указу Президента України №447/2021: Загрозами та викликами для України у сфері кібербезпеки є: агресія Російської Федерації проти України у кіберпросторі.

Держава-агресор кожного дня та кожної години намагається створити загрозу кібербезпеці України для того щоб вплинути на громадян країни завдяки пропаганді, дискредитації української армії, зневаження країн НАТО та ЄС. Ця загроза є самою провідною на даний час у сфері забезпечення безпеки інформаційного простору України. Кібербезпека України залишається непокорною завдяки роботі спеціалістів які стоять на захисті нашої державності.

Це активне використання кіберзасобів у міжнародній конкуренції щоб отримувати конфіденційні файли держави; 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. Причиною став розвиток програмного забезпечення та вірусів які наразі можуть дуже сильно вразити державу та зупинити розвиток у тій чи іншій сфері. кіберзлочинність, яка завдає шкоди інформаційним ресурсам, суспільним процесам, особисто громадянам, знижує довіру суспільства до інформаційних технологій та призводить до значних матеріальних втрат. Кіберзлочини стають популярнішими з кожним роком через появу нових закритих сайтів та доменів на яких можуть торгувати забороненими препаратами, людьми, втраченими речима та даними людей.

Україна розбудовуватиме національну систему кібербезпеки, ґрунтуючись на: розумінні та постійному аналізі глобальних трендів кібербезпечового середовища, неухильному захисті національних інтересів України у сфері кібербезпеки. Це означає повну переробку системи на зразок західних аналогів та самосійного виготовлення допоміжного програмного забезпечення. Для цього країна починає вже зараз розвивати міжнародну інтеграцію та співробітництво у сфері цифровізації; втручання заходів з перегляду та уточнення повноважень і відповідальності суб'єктів забезпечення кібербезпеки держави; удосконалення законодавства у сфері кібербезпеки та оперативності дій щодо його актуалізації відповідно до безпекових умов, що змінюються; пріоритетності економічного і соціального розвитку суспільства; балансу забезпечення потреб держави і прав громадян, дотриманні законності, повазі до основоположних цінностей, прав людини і громадянина які закріплені Конституцією та іншими нормативно-правовими актами; впровадженні сучасних принципів, методів, систем, підходів та механізмів публічного управління у сфері кібербезпеки; виявленні нових загроз та способів уникнення небезпеки у сфері кіберзабезпечення.

Задля подальшого розвитку виходить на ринок Європи та інший країн які готові в подальшому розвивати пліч-о-пліч кібербезпеку та цифровізацію навколо всієї планети. Вже зараз Україна передає свої технології іншим країнам та вивчає нові сфери у розвитку безпеки цим самих даних.

Проблема ефективного забезпечення кібербезпеки потребує комплексного вирішення і вимагає скоординованих дій на національному, регіональному та міжнародному рівнях для запобігання, підготовки, реагування та відновлення інцидентів з боку органів влади, приватного сектора і громадянського суспільства.