КІБЕРБЕЗПЕКА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Скриннік Н.А., канд. філол. наук
Харківський автомобільго-дорожній фаховий коледж
Муравйова О.М.
Державний біотехнологічний університет

У цифрову епоху кібербезпека стала першочерговим завданням кожної людини, оскільки цифрові технології набули стрімкого розповсюдження. Отже, неважко припустити, що злочинна, в том числі шахрайська діяльність набула широкого масштабу. Відомо багато форм і методів загроз для приватних користувачів інтернету. Кібератаки стають все більш поширеним явищем. Тому виникає потреба в посиленій кібербезпеці, яка передбачає захист всієї інформації в кіберпросторі, включаючи особисту інформацію, інтелектуальну власність, внутрішню інформацію, державну інформацію тощо.

Останнім часом кібератаки стають частим явищем при використанні інтернет мереж, а саме: вірусні атаки; кіберзлочинність (спамерство, кардінг, фішинг, ботнети тощо); загрози від мережевого серфінгу (кібер-булінг, «дорослий» контент, незаконний вміст, насильство в режимі онлайн, розголошення приватної інформації, платні послуги тощо) [1, с. 319].

Найпоширеними видами кібератак є такі:

Віруси – програми, які атакують комп'ютер користувача, блокуюючи його роботу з метою знищення або отримання конфіденційної інформації.

Фішинг – спроба отримання логіну користувача та іншої особистої інформації, номера кредитної картки, пароля тощо.

Черв’яки – програми, що поширюються через мережі й здатні заражати та видаляти файли.

Троянські коні – програми, що мають вигляд звичайних файлів з метою надання зловмисникам віддаленого доступу до особистої інформації.

DDoS-атаки – це атаки, які спрямовані на блокування роботи системи шляхом перевантаження її трафіком, що унеможливлює доступ до ресурсу.

Крім вищезазначених існує велика кількість інших видів кібератак, що діють через телефони, хмарні сховища. Важливо розуміти, що існує необхідність у використанні певних заходів з метою захистити конфіденційну інформацію. Проведення перевірки щодо загроз безпеки інформації повинно носити системний характер [2, с. 237].

Крім того, всесвітній ринок цифрової електроніки та цифрових пристроїв надає доступ до приватних даних через соціальні мережі, що сприяє зросту нових кібератак.

За таких умов виникає необхідність у безпеці основних інструментів цифрової економіки – захист електронних підпису, платежів, токенів, sim-карт, online-сервісів, захис тінформації в електронних хмарах, базах даних, розвиток криптографії і технологій аутентифікації особи, захист системи електронного документообігу, каналів передачі інформації, захист серверів, безпека діяльності комерційних і державних електронних майданчиків, захист від

загроз впливу через інформаційні канали на літальні апарати, зброю, транспорт, новітні технології тощо [3, с. 102].

У відповідь на кібератаки запроваджують певні методи та технологічні засоби для захисту інформації, серед них:

поінформованість суспільства;

відвідування лекцій, семінарів, конференцій з підвищення знань з інформаційної безпеки;

впровадження регламентів з безпеки або інструкцій;

встановлення антивірусного програмного забезпечення та системи виявлення й запобігання кібератак;

уважність щодо джерел, які потребують надання конфіденційних даних;

критичне ставлення до невідомих посилань та сумнівних джерел;

часта зміна пароля;

створення системи паролів для ідентифікації користувача;

криптографічний захист інформації (шифрування);

резервне копіювання баз даних і операційних систем [1].

Таким чином, методи суспільної поінформованості в сукупності з використанням технічних засобів усіх структурних рівнів кіберзахисту здатні вирішити питання збереження конфіденційних даних.

Інформаційні джерела:

1. Биков, В. Ю., Буров, О. Ю., Дементієвська, Н. П. Кібербезпека в цифровому навчальному середовищі. Інформаційні технології і засоби навчання. 2019, 2(70), С. 313–331.

2. Фесьоха Н.О. Стан та тенденції розвитку кібербезпеки в епоху цифрової трансформації аналіз сучасних загроз та заходів захисту // Вісник ХНТУ. 2024 № 2 (89), С. 235- 241.

3. Цифровізація як нова реальність України. [Електронний ресурс] – Режим доступу: https://trixati.org.ua/shkola/novyny-shkoly/cyfrovizaciya-yak-nova-realnist-ukra%D1%97ny/

МОЖЛИВОСТІ ТА ПЕРСПЕКТИВИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ АГРАРНОГО СЕКТОРУ УКРАЇНИ

Сотников Ю.О., канд. екон. наук, доц.
Державний біотехнологічний університет

Сільське господарство у всі часи було і є одним наріжних каменів стабільного розвитку України. Сучасне стан сільського господарства нашої стикається з численними викликами через військові дії, зміну клімату, зростання населення та необхідність підвищення продуктивності харчування. У відповідь на ці проблеми цифрові інновації стають важливим інструментом, який може значно підвищити ефективність аграрного сектору. Цифровізація сільського господарства, яка включає такі технології, як Інтернет речей, машинне навчання, дрони та передові системи моніторингу, відкриває нові