УДК 338.22:004

М.В. Марченков, радник директора ННІ «Кіберпорт» (*ДБТУ, Харків*)

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КІБЕРБЕЗПЕКА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Цифрова трансформація набирає обертів у всьому світі, і Україна не є винятком. За останні роки Україна досягла великих успіхів, зокрема, у цифровізації державних послуг, таких як «Дія», що є унікальним мобільним додатком, який надає доступ до більш ніж 10 основних документів у цифровому форматі. За версією журналу Times застосунок «Дія» увійшов до списку кращих винаходів 2024 року. Окрім застосунку «Дія» Україна запустила ініціативи з електронного врядування, які включають податкові та правові сервіси для громадян і бізнесу. Впровадження цифрових сервісів для реєстрації бізнесу та отримання адміністративних послуг сприяє спрощенню ведення бізнесу та покращенню інвестиційного клімату.

Пріоритетні цілі цифрової трансформації визначаються спрямованістю на підвищення ефективності, автоматизацію процесів, інтеграцію інновацій:

– цифрова трансформація дозволяє підприємствам і організаціям збільшувати продуктивність за рахунок автоматизації рутинних процесів і зменшення людського фактору;

– інноваційні технології, такі як штучний інтелект, великі дані (Big Data) та інтернет речей (IoT), допомагають створювати нові можливості для розвитку бізнесу та покращення обслуговування клієнтів.

Більшість наших пристроїв та систем підключені до локальних мереж та/або мережі Інтернет, тому інтеграція сучасних технологій часто супроводжується новими кіберризиками, що вимагає посилення заходів кіберзахисту. Серед нових векторів атак, пов'язаних із хмарними технологіями та IoT, можна відзначити:

– хмарні технології – переваги хмарних сервісів (зручність, доступність та масштабованість) супроводжуються ризиками несанкціонованого доступу, витоків даних і атак на хмарну інфраструктуру;

– Інтернет речей (IoT) – зростання кількості IoT-пристроїв у сфері виробництва, транспорту, медичних послуг та домашнього використання відкриває нові шляхи для атак. Недостатня безпека пристроїв часто використовується хакерами для здійснення DDoS-атак та викрадення даних.

Основні види кіберзагроз:

1. Фішинг – один із найпоширеніших методів атак, який полягає у відправленні електронних листів або повідомлень, що виглядають як офіційні запити від надійних джерел. Метою є отримання доступу до конфіденційної інформації користувача, такої як паролі, персональні дані чи фінансові дані.

2. Ransomware (віруси-вимагачі) – зловмисники зашифровують дані користувача або організації та вимагають викуп за розшифрування. Такий тип

атак може паралізувати діяльність підприємств і спричинити значні фінансові збитки.

3. Соціальна інженерія – використання для переконання користувачів видати конфіденційну інформацію або виконати дії, які шкодять їхній безпеці.

4. DDoS-атаки – спрямовані на перевантаження мережевих ресурсів, що призводить до тимчасової недоступності веб-сайтів чи сервісів. Це впливає на репутацію організацій та може завдати значних фінансових збитків.

Через постійні загрози кібербезпека в Україні стала національним пріоритетом. Уряд розробив стратегію кібербезпеки та запровадив інституції, такі як Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) та Національний координаційний центр кібербезпеки. Їх основне завдання – забезпечення стійкості держави до кіберзагроз та формування відповідних стандартів безпеки для організацій.

Основні функції кібербезпеки в захисті цифрових активів:

– захист конфіденційності – захист персональних даних та інформації користувачів;

– забезпечення цілісності даних – підтримка достовірності та цілісності даних у системах;

– доступність – гарантія безперебійної роботи систем навіть у разі кібератак;

– моніторинг і виявлення загроз – постійний моніторинг мережі для виявлення потенційних загроз у реальному часі.

Окрім захисту інформаційних потоків кібербезпека допомагає забезпечити сталість бізнес-процесів, забезпечуючи:

– безперервність роботи – запобігання простою бізнес-процесів у результаті атак, що допомагає підтримувати стабільну роботу підприємств;

– мінімізацію фінансових збитків – використання проактивних заходів захисту зменшує ризики фінансових втрат через витоки даних або збої;

– довіру клієнтів і партнерів – організації, які дотримуються високих стандартів кібербезпеки, завойовують більшу довіру серед своїх клієнтів та партнерів, що позитивно впливає на їх репутацію.

Розширення доступу до даних і використання хмарних технологій створюють нові виклики в управлінні безпекою, що потребує впровадження передових рішень, таких як багатофакторна автентифікація та модель Zero Trust. Українським компаніям рекомендується впровадження моделі Zero Trust, яка передбачає «нульову довіру» до всіх користувачів та пристроїв без підтвердження. Цей підхід дозволяє ефективно захищати корпоративні мережі від атак зсередини та ззовні.

Принципи функціонування моделі Zero Trust:

– аутентифікація та авторизація – кожен доступ має бути перевіреним незалежно від того, чи користувач знаходиться всередині мережі чи поза її межами;

– мінімальний доступ – надання доступу лише до тих ресурсів, які потрібні для виконання завдань;

– постійний моніторинг – використання аналітики для виявлення підозрілої активності та швидкого реагування на потенційні загрози.

Для захисту державних систем та приватного сектору в кібербезпеці активно застосовується штучний інтелект. Наприклад, методи машинного навчання допомагають відстежувати аномалії у мережах та блокувати можливі атаки ще на стадії їх підготовки. Вектори застосування ШІ у кібербезпеці:

1. Виявлення аномалій – системи на базі ШІ можуть аналізувати великий обсяг трафіку та виявляти підозрілі патерни, які можуть вказувати на можливу атаку.

2. Автоматизація реагування – алгоритми ШІ здатні автоматично застосовувати заходи для запобігання загрозам, зменшуючи час реакції на інцидент.

3. Прогнозування загроз – використовуючи історичні дані, ШІ може передбачати майбутні атаки та вдосконалювати захисні механізми.

Одним з дієвих інструментів стратегії кібербезпеки України визначено підвищення обізнаності співробітників у кібербезпеці. Україна впроваджує спеціальні навчальні програми з кібербезпеки для державних службовців, що допомагає уникнути людських помилок, які можуть призвести до серйозних наслідків. Такі тренінги також пропонуються бізнесу та є важливим елементом для підвищення загального рівня кіберкультури. Основні типи навчальних програм із підвищення обізнаності співробітників у кібербезпеці:

– інтерактивні тренінги – залучення співробітників до моделювання ситуацій, що допомагає краще розуміти потенційні загрози;

– онлайн-курси – доступні для більш широкої аудиторії, що дозволяє проходити навчання у зручний час;

– практичні семінари та воркшопи - дають змогу відпрацювати навички розпізнавання загроз і реагування на них.

Отже, цифрова трансформація в Україні супроводжується активним розвитком кібербезпеки. Україна вже має значний досвід у боротьбі з кіберзагрозами, але щоб досягти стабільності, потрібно продовжувати інвестувати у нові технології, підвищувати рівень обізнаності співробітників та розширювати співпрацю між державою, бізнесом і освітніми установами.

Сучасні кіберзагрози вимагають постійного оновлення підходів та швидкої адаптації до нових реалій. Використання передових технологій, таких як штучний інтелект та багатофакторна автентифікація, є обов’язковою умовою для ефективного захисту в умовах цифровізації. Дієвими кроками із підвищення рівня кібербезпеки в умоівах цифрової трансформації є зміцнення правової бази та політик, що регулюють кібербезпеку, та розширення міжнародної співпраці для обміну досвідом і кращими практиками у сфері кіберзахисту.