ЕКОНОМІЧНІ ВИКЛИКИ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА ПІД ЧАС КІБЕРАТАК В УМОВАХ ЖОРСТКОЇ КОНКУРЕНТНОСТІ

ECONOMIC CHALLENGES OF THE COMPANY'S ACTIVITY DURING CYBERATTACKS IN THE CONDITIONS OF TOUGH COMPETITION

УДК 338.424.2:334]:004.056.5
DOI: https://doi.org/10.32782/dees.9-3

Каліна І.І.[1]
д.е.н., професор,
професор кафедри маркетингу,
Навчально-науковий Інститут
управління, економіки та бізнесу
ПрАТ «ВНЗ Міжрегіональна Академія
управління персоналом»
Шуляр Н.М.[2]
к.е.н., старший викладач
кафедри економіки та бізнес-технологій,
Національний авіаційний університет
Грищенко А.В.[3]
здобувач третього (освітньо-наукового)
рівня вищої освіти
«доктор філософії» (Phd),
Державний заклад вищої освіти
«Університет менеджменту освіти»

Kalina Iryna
Educational and Scientific Institute
of Economic and Business Management,
Interregional Academy
of Personnel Management
Shulyar Natalia
National Aviation University
Hryshchenko Anatolii
State Higher Educational Institution
"University of Educational Management"

Сучасне життя стало набагато комфортнішим завдяки різноманітним цифровим технологіям. Інтернет приніс позитивні зміни в життя суспільства, але разом із цим постає величезна проблема щодо захисту персональних даних. Цим питанням переймаються і підприємства, яким потрібно зберегти дані клієнтів чи конфіденційну інформацію самого підприємства від інформаційної загрози - кібератак. З кожним роком кількість кібератак та їх видів збільшуються, а конкуренція стає ще гострішою і в результаті підприємства удосконалюють свою систему управління та безпеки. Незважаючи на нові системи захисту та їх удосконалення підприємства потерпають від різного роду кібератак, які впливають на фінансові результати та репутацію. Їх пагубний вплив може призвести до призупинення підприємства, витік даних (як клієнтів так і підприємства) та поширення вірусів, які в подальшому зможуть знищити систему. В статті досліджено дефініцію поняття "кібератака", а також проаналізовано градаційний перелік наймасштабніших кібератак: атака зловмисним програмним забезпеченням, фішингові атаки, атака паролем, атака «людина посередині», атака SQL Injection, атака відмова в обслуговуванні (DOS) та відмова в обслуговуванні (DDOS), внутрішня загроза, криптоджекінг, експлойт нульового дня, атака водопою, тунелювання DNS, атаки завантажень Drive-by, міжсайтові скриптові атаки, підробка DNS або «отруєння», атака Інтернету речей, перехоплення сесії, маніпуляції з URL.
Ключові слова: *кібератака, кібербезпека, конкуренція, підприємства, економічні виклики, умови.*

Modern life has become much more comfortable thanks to various digital technologies. The Internet has brought positive changes to society's life, but with it comes a huge problem of personal data protection. Enterprises that need to protect customer data or confidential information of the enterprise itself from an information threat – a cyberattack – are also concerned with this issue. Every year, the number and types of cyberattacks increase and expand, and the competition becomes even more intense as companies improve their management and security systems. Despite new protection systems and their improvement, enterprises suffer from various types of cyberattacks that affect financial results and reputation. Their detrimental effects can lead to business downtime, data leakage (both customer and business) and the spread of viruses that can eventually destroy the system. Digitization is a powerful engine of economic growth in the world and almost all business markets are becoming increasingly digitized, and businesses that go digital not only increase efficiency, but also profitability. It also helps businesses better adapt to changes that occur under the influence of external factors. That is, the transition to digital technologies accelerates all business processes in each unit of the enterprise structure, which accelerates the interactive process with customers who have also transformed to a digital process. But the transition to digitization tools of operation, the enterprise is risky. The risk of digitalization is the leakage of data and cyberattacks that destroy platforms, sites and other information technology components or suspend the work of the enterprise for at least one day. For a business to stop work for a day is a huge expense, as well as eliminate the problems involved in a cyberattack and strengthen cyber security. The article examines the definition of the concept of "cyberattack", and also analyzes the gradation list of the largest cyberattacks: malware attack, phishing attacks, password attack, man-in-the-middle attack, SQL Injection attack, denial of service (DOS) attack and distributed denial of service (DDOS), insider threat, cryptojacking, zero-day exploit, watering hole attack, DNS tunneling, Drive-by download attacks, cross-site scripting attacks, DNS spoofing or "poisoning", IoT attack, session hijacking, URL manipulation.
Key words: *cyber attack, cyber security, competition, enterprises, economic challenges, conditions.*

Постановка проблеми у загальному вигляді. З кожним днем підприємства стикаються з новими реалістичними бізнес-процесами, які допомагають ефективно функціонувати та використовувати повний потенціал креативних та інноваційних ідей як працівників, так і потужність самого підприємства. Новими реалістичними бізнес-процесами є запровадження великих структурних змін не тільки на підприємстві, а й в економіці для того, щоб економічна ефективність підсилювала конкуренцію вже розвинених галузей та підприємств, а також впроваджувала цифровізаційні технології в нові чи ті, які починають розвиватися. Така трансформація сприятиме тому, що економіка країни стане активізаційнішою і дасть, врешті-решт, змогу зростати середньому рівню життя населення. Зміни такого масштабу є одним із найскладніших завдань в нових реаліях, але призведе до ефективного управління на підприємствах. В нових трансформаційних реаліях розвитку підприємств з'явився великий інтерес до підвищення інформатизаційного рівня кожного відділу та департаменту на підприємстві. Тому на сьогодні є актуальним вирішення питань безпеки підприємства (різних її

[1] ORCID: https://orcid.org /0000-0001-5662-6967
[2] ORCID: https://orcid.org /0000-0002-4109-5961
[3] ORCID: https://orcid.org /0009-0008-9896-0056

видів), яке призводить до активізації бізнес середовища не тільки окремого підприємства, а й суспільства. Досліджуючи питання безпеки підприємства в умовах цифровізації, варто приділити увагу власне інформаційній безпеці підприємства та ризикам, що постали перед ним.

Аналіз останніх досліджень і публікацій. Вчені, які приділили увагу кібератакам та їх вплив на розвиток підприємств це: Арістова І.В. [1], Арсенович Л.А. [2], Кіндзерський Ю.В. [3], Радівілова Т.А. [4], Ставицький О.В. [5], Улічев О.С. [6], Чупріна М.О. [7].

Аналіз опублікованих праць, матеріалів наукових конференцій, присвячених дослідженню цієї багатогранної проблеми, показав, що вона є ще недостатньо дослідженою як у теоретичному, так і в практичному аспектах, адже цифровізація розвивається та кожного дня з'являються нові методи, принципи та закони кібербезпеки. Об'єктивна потреба у подальшому поглибленні відповідних теоретичних досліджень і методичних розробок пов'язана з необхідністю уточнення поняття «кібербезпека підприємств» та розповсюджені види кібератак. Саме цими обставинами і зумовлюється актуальність теми наукової статті.

Мета дослідження. Обґрунтування економічних викликів діяльності мікросистем під час кібератак в умовах жорсткої конкурентності.

Виклад основного матеріалу дослідження. Слід зауважити, що майже в усіх класифікаціях які розглядались раніше, у тому чи іншому вигляді згадується інформаційна безпека, тобто можливість інформаційного забезпечення та захисту конфіденційної інформації соціально-економічної системи. Незважаючи на те, що у кожній країні є певна група галузей та секторів національної економіки, які створюють фундамент для економічної безпеки, прагнення реалізувати свій потенціал і в ІТ-сфері постає одним із головних глобальних трендів. Тобто, з урахуванням тотальної діджіталізації економічних процесів з одночасним переміщенням масивів інформації у кіберсистеми все більшого значення набувають питання кібербезпеки.

Саме тому слід наголосити на таких поняттях як кібербезпека, кіберзагроза та кібератака у розрізі економічної та юридичної складових.

Загалом, відповідно до Закону України «Про основні засади забезпечення кібербезпеки в Україні» були визначені згадані вище поняття. Так, кібератака – це спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [9].

При цьому, кібербезпека – це захищеність життєвоважливих інтересів людини, суспільства та держави, а також організацій під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [9].

У розрізі цього, кіберзагрозами визначено наявні та потенційно можливі явища і чинники, що створюють небезпеку життєвоважливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів [9].

Загалом, згідно зі стандартом ISO/IEC 27032:2012 кібербезпека виступає як збереження цілісності, конфіденційності та доступності інформації, що циркулює в кіберсистемі (тобто інформації, що надходить у кіберсистему, накопичується та зберігається для подальшого опрацювання), з метою забезпечення стійкості й безперервності реалізації кіберсистемою управлінських функцій щодо відповідних об'єктів управління [11].

В останні роки можна спостерігати трансформацію категорії «кібербезпека» з поступовим її пересуванням із мікро- на макрорівень. Тобто питання вже не тільки в захисті інформації на окремому пристрої чи в межах локальної мережі. Мова йде про необхідність створення єдиної системи кібербезпеки на рівні держави як повноцінної складової національної та, в тому числі, й економічної безпеки.

Одночасно відбувається й поступова зміна напряму загроз: з локального та галузевого на загальнонаціональний. Основними об'єктами кібератак виступає діяльність уряду, кібербезпека як складова економічної безпеки України правоохоронних органів, збройних сил, засобів масової інформації, системи життєзабезпечення міст, транспортні та комунікаційні мережі, ядерна та хімічна промисловість, національна енергетична та фінансова системи тощо.

Власне сам кіберпростір вже апріорі розглядається як середовище для потенційних злочинних дій у сфері несанкціонованого доступу до конфіденційної інформації, збоїв у роботі програмного забезпечення, порушення режиму

функціонування автоматизованих систем. Серед характеристик, що становлять сутнісну основу сучасних тенденцій трансформації кіберпростору, основну цінність для процесів у національній економіці становлять:

– зміна характеру діяльності осіб, які ухвалюють рішення щодо заходів з кібербезпеки системних об'єктів;

– цифровізація економічної, наукової, освітньої та соціально-культурної діяльності держави і соціуму, яка передбачає утворення й інформаційно-технологічну підтримку електронно-цифрових форм створення, опрацювання, зберігання, захисту та переміщення інформації;

– перехід від паперового документообігу до електронно-цифрового;

– підтримка безпечної, стійкої й надійної роботи електронного операційного/інформаційного середовища, яке підтримує національну безпеку країни, мінімізує наслідки злочинних кібервтручань та максимізує переваги цифрової економіки [10].

Отож, створюючи бізнес сьогодні слід враховувати не тільки ризики пов'язані з конкуренцією, новаціями, битвами з «акулами бізнесу», які надають послуги дотичні до створених вами, але й інформаційну безпеку підприємства. Слід розуміти, що відтепер безпека підприємства пов'язана не лише з організаційними моментами роботи компанії, а й із загрозами з боку зовнішнього середовища, що полягають у зупиненні чи знищенні продукту через кібератаки конкурентів чи шахраїв.

Реальні прояви кібератак є мало прогнозованими, а їх результатом, стають значні фінансово-економічні збитки або непередбачувані наслідки порушень функціонування інформаційно-телекомунікаційних систем, які впливають на стан фінансової та економічної безпеки бізнесу та процесу його споживання.

Варто наголосити, що наразі кібератаки почали сильніше і частіше зачіпати власне малий і середній бізнес, оскільки такі компанії помилково вважають себе «нецікавими» в плані інформаційних ресурсів, якими володіють [11].

Коли третя сторона здійснює несанкціонований доступ до системи/мережі, ми називаємо це кібератакою. Особа, яка здійснює кібератаку, називається хакером/зловмисником.

Кібератаки мають кілька негативних наслідків. Здійснення атаки може призвести до витоку даних, що призведе до втрати даних або їх маніпулювання. Організації зазнають фінансових втрат, довіра клієнтів підривається, а репутація завдає шкоди. Щоб приборкати кібератаки, підприємства впроваджують кібербезпеку. Кібербезпека – це метод захисту мереж, комп'ютерних систем та їх компонентів від несанкціонованого цифрового доступу. Хронологія найбільших кібератак на інформаційні системи України представлена на рис. 1.

На сьогодні існує багато різновидів кібератак, які проаналізуємо. Якщо спеціалістам підприємства відомі різні типи кібератак, то їм легше захистити мережі та системи від них.

Атака зловмисним програмним забезпеченням. Це один з найпоширеніших типів кібератак, який стосується шпигунських програм, троянів, рекламних програм, програм-вимагачів, віруси та клавіатурні шпигуни.

Програми-вимагачі блокують доступ до ключових компонентів мережі, тоді як програми-шпигуни – це програми, які викрадають конфіденційні дані. Рекламне ПЗ – це програмне забезпечення, яке відображає рекламний вміст, наприклад банери на екрані користувача.

Зловмисне програмне забезпечення проникає в мережу через уразливі місця. Коли користувач натискає небезпечне посилання, воно завантажує вкладення до електронної пошти або коли використовується інфікований накопичувач.

Фішингові атаки є одним із найпоширеніших типів кібератак. Це тип атаки соціальної інженерії, коли зловмисник видає себе за довіреного контакта та надсилає підприємству (жертві) підроблені фішингові листи чи фішингові посилання.

Не підозрюючи про це, жертва відкриває лист і натискає на шкідливе посилання або відкриває вкладення листа. Таким чином зловмисники отримують доступ до конфіденційної інформації та облікових даних. Вони також можуть інсталювати зловмисне програмне забезпечення за допомогою фішингової атаки.

Атака паролем – це форма атаки, при якій хакер зламує ваш пароль за допомогою різних програм і інструментів для злому паролів.

Атака «людина посередині» також відома як атака підслуховування. У цій атаці зловмисник входить між двостороннім зв'язком, тобто зловмисник захоплює сеанс між клієнтом і хостом (зміна IP-адреси). Роблячи це, хакери викрадають дані та маніпулюють ними.

Атака SQL Injection – ін'єкційна атака структурованої мови запитів (SQL) відбувається на вебсайті, керованому базою даних, коли хакер маніпулює стандартним запитом SQL. Він здійснюється шляхом введення шкідливого коду в вікно пошуку вразливого веб-сайту, таким чином змушуючи сервер відкривати важливу інформацію. Це призводить до того, що зловмисник може переглядати, редагувати та видаляти таблиці в базах даних. Завдяки цьому зловмисники також можуть отримати права адміністратора.

Атака відмова в обслуговуванні (DOS) та розподілена відмова в обслуговуванні(DDOS). Атака типу «відмова в обслуговуванні» є серйозною загрозою для компаній. Тут зловмисники атакують

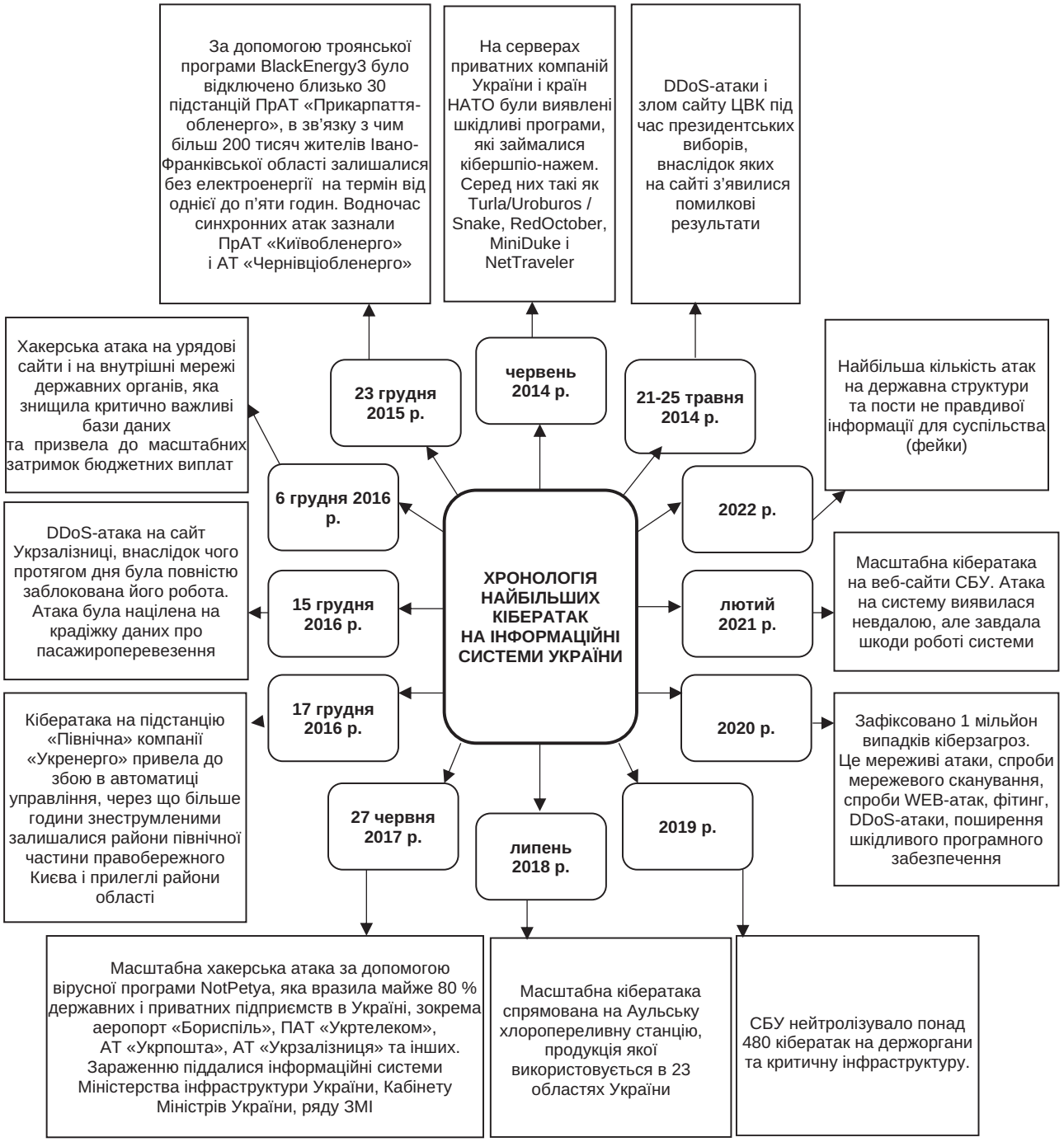

Рис. 1. Хронологія найбільших кібератак на інформаційні системи України

системи, сервери чи мережі та переповнюють їх трафіком, щоб вичерпати їхні ресурси та пропускну здатність. Коли це трапляється, обслуговування вхідних запитів стає непосильним для серверів, у результаті веб-сайт, на якому він розміщений, або закривається, або сповільнюється. Це залишає законні запити на обслуговування без уваги.

Внутрішня загроза. Як випливає з назви, внутрішня загроза стосується не третьої сторони, а інсайдера. У такому випадку це може бути особа з організації, яка знає все про організацію. Внутрішні загрози можуть завдати величезної шкоди. Інсайдерські загрози поширені в малому бізнесі, оскільки там співробітники мають доступ до кількох облікових записів із даними. Причин такої форми нападу багато, це може бути жадібність, злий умисел або навіть необережність. Інсайдерські загрози важко передбачити, тому це складно.

Криптоджекінг. Термін Cryptojacking тісно пов'язаний з криптовалютою. Криптоджекінг відбувається, коли зловмисники отримують доступ до чужого комп'ютера для майнінгу криптовалюти.

Доступ отримується шляхом зараження веб-сайту або маніпулюванням жертви, щоб вона натиснула зловмисне посилання. Для цього вони також використовують онлайн-оголошення з кодом JavaScript. Жертви не знають про це, оскільки код майнінгу Crypto працює у фоновому режимі. затримка виконання є єдиною ознакою, яку вони можуть побачити.

Експлойт нульового дня відбувається після оголошення про вразливість мережі і у більшості випадків немає рішення для уразливості. Таким чином, постачальник повідомляє про вразливість, щоб користувачі були в курсі, але однак ця новина доходить і до нападників. Залежно від уразливості постачальнику або розробнику може знадобитися будь-який час, щоб усунути проблему. Тим часом зловмисники атакують виявлену вразливість. Вони гарантують використання вразливості ще до того, як для неї буде реалізовано виправлення або рішення.

Руткіти – це тип шкідливого програмного забезпечення, яке надає хакерам контроль і доступ на рівні адміністратора до цільової системи. Руткіти ховаються глибоко всередині операційної системи вашого пристрою, тому їх важко виявити, але вони також є неймовірно небезпечними.

Руткіт може дозволити хакерам викрасти конфіденційну інформацію, встановити кейлоггери або навіть видалити антивірусне програмне забезпечення.

Тунелювання DNS – це тип кібератаки, який хакери використовують, щоб обійти традиційні системи безпеки, такі як брандмауери, щоб отримати доступ до систем і мереж. Хакери кодують шкідливі програми в DNS-запитах і відповідях (які більшість програм безпеки ігнорують). Коли програма знаходиться всередині, вона замикається на цільовому сервері, надаючи хакерам віддалений доступ.

Атаки DNS-тунелювання особливо небезпечні, оскільки вони часто залишаються непоміченими протягом днів, тижнів або місяців. За цей час кіберзлочинці можуть викрасти конфіденційні дані, змінити код, встановити нові точки доступу та навіть встановити шкідливе програмне забезпечення.

Атаки завантажень Drive-by. Більшість кібератак вимагають від вас певних дій, наприклад натискання посилання чи завантаження вкладеного файлу, але атака відбувається, коли ви просто переглядаєте заражений веб-сайт. Хакери використовують вразливі місця в плагінах, веббраузерах і програмах, щоб без вашого відома встановити зловмисне програмне забезпечення на ваш пристрій для подальших зловмисних дій.

Міжсайтові скриптові атаки. Атака міжсайтового сценарію (XSS) дозволяє хакерам отримати несанкціонований доступ до програми або вебсайту.

Кіберзлочинці користуються перевагами вразливих веб-сайтів і змушують їх встановлювати користувачам шкідливий JavaScript. Коли код виконується у вашому браузері, хакер може маскуватися під ваш обліковий запис і робити все, що ви можете. Сайти, вразливі до XSS, включають дошки оголошень, форуми та веб-сторінки. Ці сторінки залежать від введення користувачами, які не перевіряються на шкідливі коди.

Підробка DNS або «отруєння» дозволяє хакерам надсилати онлайн-трафік на «підроблений» веб-сайт. Ці сайти виглядають майже так само, як ваш пункт призначення (наприклад, сторінка входу в ваш банк або обліковий запис у соціальних мережах). Але будь-яка інформація, яку ви надсилаєте, потрапляє прямо до хакерів, надаючи їм доступ до ваших облікових записів.

Хакери також можуть використовувати DNSспуфінг для саботування компаній, перенаправляючи відвідувачів їхніх сайтів на сайт низької якості з непристойним вмістом.

Атака Інтернету речей (IoT). Пристрої Інтернету речей (IoT), такі як розумні колонки, телевізори та іграшки, також можуть бути цілями кібератак. Атака IoT відбувається, коли хакери викрадають дані з пристрою або об'єднують кілька пристроїв IoT у ботнет, які можна використовувати для DDoS-атак. Пристрої IoT зазвичай не мають антивірусного програмного забезпечення, що робить їх легкою мішенню для хакерів. Багато найбільших у світі DDoS-атак використовували «армію ботів», що складається з пристроїв Інтернету речей. Це може здатися малоймовірним, але навіть ваш «розумний будинок» може стати мимовільним солдатом у кібератаці.

Перехоплення сесії. Викрадення сеансу – це тип атаки "людина посередині", під час якої зловмисник "переймає" сеанс між клієнтом і сервером. Комп'ютер зловмисника змінює свою IP-адресу на адресу клієнта та продовжує доступ до сервера, не потребуючи жодної автентифікації. Після того, як вони захопили сеанс, хакери можуть зробити все, що може зробити обліковий запис клієнта. Він отримає доступ до всіх файлів вашої компанії поки ви працюєте з ними.

Маніпуляції з URL-адресою відбувається, коли хакери змінюють параметри в URL-адресі, щоб переспрямувати вас на фішинговий сайт або завантажити зловмисне програмне забезпечення.

Наприклад, багато людей використовують засоби скорочення URL-адрес, щоб допомогти запам'ятати довгі веб-адреси або конкретні сторінки. Якщо хакери «отруять» цю скорочену URL-адресу, вони можуть переслати вас на фішинговий сайт, призначений для викрадення вашої особистої інформації. В інших ситуаціях хакери маніпулюють URL-адресою, щоб змусити сервер показати сторінки, до яких вони не повинні мати доступу.

Отже, в умовах жорсткої конкуренції, підприємства використовують всі методи для отримання уваги клієнта та збільшення фінансових результатів. Одним із найважливіших чинників забезпечення ефективного функціонування підприємства є економічна безпека підприємства, яка враховує інформаційну безпеку. Підприємства сьогодні витрачають левову частку доходу на системи захисту інформації від нападу (кібератак).

Висновки. Розвиток підприємства є невід'ємною частиною бізнес-середовища. Незважаючи на небезпечні обставини та жорстку конкуренцію в сьогоденних умовах, підприємства націлені на організацію, формування та розвиток. І цей розвиток є рушійною силою нових економічних досягнень як для самого підприємства, так і для емоційного та функціонального задоволення споживачів, а також для економічного процвітання держави. Слід також зазначити, що оскільки діяльність підприємства та кіберпезпеки безпосередньо на сьогоднішній день пов'язані з фінансовою складовою, то це перші складові, які мають бути захищені від кібератак, адже це інструменти розвитку підприємства. Таким чином, удосконалення та оновлення системи управління та безпеки дозволяє проводити всебічний аналіз якості діяльності підприємства та своєчасно відслідковувати як позитивні, так і негативні зміни в різних сферах управління та впливати на них.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. I. Aristova,O. Brusakova, D. Koshikov, O. Kaplya. Developing information technology law and legislation: analysis of international experience and possibilities of its application in Ukraine. *Revista de Derecho*. Vol. 10 (II) (2021), pp. 117–128. ISSN: 1390-440X – eISSN: 1390-7794. DOI: https://doi.org/10.31207/ih.v10i2.287

2. Арсенович, Л.А. (2021). Організація професійної підготовки фахівців із кібербезпеки основними суб'єктами національної системи кібербезпеки: практичний аспект. *Ефективність державного управління*. 2021. № 62. DOI: https://doi.org/10.33990/2070-4011.62.2020.205817

3. Пашко П.В., Лазебник Л.Л., Кіндзерський Ю.В. Підприємство в епоху глобальних трансформацій: виклики та перспективи розвитку: монографія. *Університет державної фіскальної служби України*. Ірпінь, 2019. 476 с.

4. Kirichenko, L., Radivilova, T., & Carlsson, A. (2017) Detecting cyber threats through social network analysis: short survey. *SocioEconomic Challenges*, 1, 1, 20DOI: 34.

5. Ставицький О.В., Шинкаренко А.Ю. Кібербезпека як один з механізмів забезпечення стабільного розвитку економіки України. *Актуальні проблеми економіки і управління*: Зб. наук. праць. Київ : НТУУ «КПІ». Вип. 11. 2017. URL: http://ape.fmm.kpi.ua/article/ view/102862.

6. Ulichev O.S., Meleshko Ye.V., Sawicki D., Smailova S. Computer modeling of dissemination of informational influences in social networks with different strategies of information distributors. Proc. SPIE 11176, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments, Wilga, Poland (ISSN: 0277-786X). 2019. 111761T.

7. Чупріна М.О., Орозонова О.О. Світові тренди розвитку IT-індустрії та технології. Бізнес, інновації, менеджмент: проблеми та перспективи : матер. *1 Міжнар. наук.-практ. конф*. С. 144–145. URL: http://confmanagement.kpi.ua/proc/article/view/201193/201226

8. Aleinikova, O.V., Datsii, O.I., Kalina, I.I., Zavgorodnia, A.A., Yeremenko, Y., & Nitsenko, V.S. (2023). Digital technologies as a reason and tool for dynamic transformation of territory marketing. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, (1), pp. 154–159. doi:10.33271/nvngu/2023-1/154

9. Закон України «Про основні засади забезпечення кібербезпеки України». ВВРУ 2017, № 45, ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

10. Горбаченко С. Кібербезпека як складова економічної безпеки України. *Галицький економічний вісник*. 2020. № 5 (66). С. 180–186.

11. Кібербезпека підприємства: що враховувати. 2022. URL: https://jurliga.ligazakon.net/news/209245_kberbezpeka-pdprimstva-shcho-vrakhuvati

REFERENCES:

1. I. Aristova, O. Brusakova, D. Koshikov, O. Kaplya. (2021) Developing information technology law and legislation: analysis of international experience and possibilities of its application in Ukraine. Revista de Derecho. Vol. 10 (II), pp. 117–128. DOI: https://doi.org/10.31207/ih.v10i2.287 [Ukraine]

2. Arsenovich, L.A. (2021). Orhanizatsiia profesiinoi pidhotovky fakhivtsiv iz kiberbezpeky osnovnymy subiektamy natsionalnoi systemy kiberbezpeky: praktychnyi aspekt. [Organization of professional training of cyber security specialists by the main subjects of the national cyber security system: practical aspect]. *Efficiency of public administration,* no. 62. DOI: https://doi.org/10.33990/2070-4011.62.2020.205817 [Ukraine]

3. Pashko P.V., Lazebnyk L.L., Kindzerskyi Yu.V. (2019) Pidpryiemstvo v epokhu hlobalnykh transformatsii: vyklyky ta perspektyvy rozvytku. [Enterprise in the era of global transformations: challenges and development prospects: monograph]. State Fiscal Service University of Ukraine. Irpin, P. 476. [Ukraine]

4. Kirichenko, L., Radivilova, T., & Carlsson, A. (2017) Detecting cyber threats through social network analysis: short survey. SocioEconomic Challenges, 1, 1, pp. 20–34. [Ukraine]

5. Stavytskyi O.V., Shinkarenko A.Yu. (2017) Kiberbezpeka yak odyn z mekhanizmiv zabezpechennia stabilnoho rozvytku ekonomiky Ukrainy. [Cyber security as one of the mechanisms for ensuring the stable development of the economy of Ukraine]. Actual problems of economy and management: Collection. of science works. K.: NTUU "KPI". Issue 11. URL: http://ape.fmm.kpi.ua/article/view/102862. [Ukraine]

6. Ulichev O.S., Meleshko Ye.V., Sawicki D., Smailova S. (2019) Computer modeling of dissemination of informational influences in social networks with different strategies of information distributors. Proc. SPIE 11176, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments, Wilga, Poland. [Ukraine]

7. Chuprina M.O., Orozonova O.O. Svitovi trendy rozvytku IT-industrii ta tekhnolohii [World trends in the development of the IT industry and technology] Business, innovations, management: problems and prospects: mater. 1 International science and practice conf. P. 144–145. URL: http://confmanagement.kpi.ua/proc/article/view/201193/201226 [Ukraine]

8. Aleinikova, O. V., Datsii, O. I., Kalina, I. I., Zavgorodnia, A. A., Yeremenko, Y., & Nitsenko, V. S. (2023). Digital technologies as a reason and tool for dynamic transformation of territory marketing. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, (1), pp. 154–159. doi: 10.33271/nvngu/2023-1/154 [Ukraine]

9. Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» (2017) [The Law of Ukraine "On the Basic Principles of Cyber Security of Ukraine"]. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text [Ukraine]

10. Gorbachenko S. (2020) Kiberbezpeka yak skladova ekonomichnoi bezpeky Ukrainy. [Cyber security as a component of economic security of Ukraine]. *Galician Economic Bulletin*, no. 5 (66), pp. 180–186. [Ukraine]

11. Enterprise cyber security: what to consider. (2022). Kiberbezpeka pidpryiemstva: shcho vrakhovuvaty [Enterprise cyber security: what to consider]. URL: https://jurliga.ligazakon.net/news/209245_kberbezpeka-pdprimstva-shcho-vrakhuvati [Ukraine]