нищівних ударів по Україні, руйнуючи все на своєму шляху, не шкодуючи при цьому цивільне населення, важливо дотримуватись вищенаведених рекомендацій, які мінімізують ризики стати випадковою жертвою війни.

Список використаних джерел

1. Безпека життєдіяльності та цивільний захист [Електронний ресурс]: підручник для студ. спеціальностей з природничих, соціально-гуманітарних наук та інженерно-комунікаційних технологій / О. Г. Левченко, О. В. Землянська, Н. А. Праховнік, В. В. Зацарний; КПІ ім. Ігоря Сікорського. Електронні текстові данні (1 файл: 10,2 Мбайт). Київ: КПІ ім. Ігоря Сікорського, 2019. 267 с.
2. Дії населення в умовах воєнного стану. URL: http://stepanivka-school1.edukit.sumy.ua/Files/downloads/Diyi-naselennya-voyennyj-stan.pdf
3. Росія вторглась в Україну. URL: https://babel.ua/profit/73258-spodivayemos-rosiya-ne-sprobuye-zahopiti-ukrajinu-a-yakshcho-velike-vtorgnennya-taki-bude-os-poradi-specialistiv-z-riznih-krajin-yak-pidgotuvati-do-viyni-sebe-ta-svoye-zhitlo
4. У разі надзвичайних ситуацій або війни. URL: https://ukrainska-gromada.gov.ua/wp-content/uploads/2022/02/ns_vijna_01.pdf
5. Чеботарьова О. В., Мікуліна І. О. Конспект лекцій з дисципліни «Безпека життєдіяльності» (для студентів всіх форм навчання за напрямами підготовки 6.030504 «Економіка підприємства», 6.030509 «Облік і аудит»). Харк. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Х.: ХНУМГ, 2014. 124 с.

ІНФОРМАЦІЙНА БЕЗПЕКА В ЕХОПУ ЦИФРОВИХ ТРАНСФОРМАЦІЙ

Близнюк Микола Миколайович

Полтавський національний педагогічний університет імені В. Г. Короленка

Анотація. *Розглядаються питання інформаційної безпеки в сучасних умовах цифрових трансформацій. Зазначено, що основна мета інформаційної безпеки в контексті цифрової трансформації – це забезпечити захищеність як інформації, так і інформаційно-технологічної інфраструктури від випадкових чи навмисних впливів, які можуть завдати неприйнятної шкоди власникам інформаційних систем. Як висновок, проблема інформаційної безпеки в умовах цифровізації набуває особливої актуальності, а загрози, які породжує цифрова трансформація можуть бути успішно подолані лише взаємопов'язаною дією технічних, організаційних та економічних методів і засобів.*

Ключові слова: *інформація, інформаційна безпека, епоха, цифрова трансформація.*

У рамках цифрової трансформації суспільства жодна із сфер діяльності не обходиться без комп'ютерних технологій збору, обробки та зберігання інформації. Таким чином, інформація має унікальну цінність і є критично важливим ресурсом, який потребує надійних методів захисту. Превентивні заходи щодо усунення загроз та ризиків в умовах цифрової економіки, забезпечення безпеки сучасного інформаційно-технологічного (ІТ) середовища стали сьогодні основою конкурентоспроможності для людини, бізнесу та держави [1-6].

Не секрет, що інформаційна безпека – це одна з найважливіших складових сучасного життя. Кібератаки на інфраструктуру, транспорт, банки тощо відображаються в кінцевому підсумку на кожному з нас. У зв'язку з цим виникає низка запитань? Які дані ми маємо викладати в мережу? Якими даними ми можемо оперувати? Як захистити ці дані? Хто має право на доступ до них? Рішення цих і пов'язаних з ними інших питань веде до підвищення надійності інфраструктури державних організацій, бізнесу, захищеності приватних осіб та держави в цілому.

Під інформаційною безпекою розуміється такий стан інформаційних ресурсів і

пов’язаних з ними інформаційних засобів і систем суб’єкта господарювання, який гарантує якісне і безперебійне забезпечення його діяльності необхідною інформацією за умови високого рівня її захищеності від внутрішніх і зовнішніх загроз [5]. Відповідно, ряд науковців, зокрема В.М. Кузьомко виокремлює два проблемних поля забезпечення інформаційної безпеки: а) діагностика і протидія загрозам інформації та б) створення передумов ефективного її використання в контексті тих викликів і актуальних завдань, які стоять в даний час.

Основна мета інформаційної безпеки в контексті цифрової трансформації – це забезпечити захищеність як інформації, так і IT-інфраструктури від випадкових чи навмисних впливів (атак тощо), які можуть завдати неприйнятної шкоди власникам інформаційних активів.

Заходи безпечного характеру пов’язані, в першу чергу, з використанням сучасних технічних засобів і технологій, які, з одного боку, дозволяють ефективно накопичувати, зберігати, обробляти і передавати інформацію, а, з іншого, – забезпечувати її високий рівень захищеності (розподілені бази даних, блокчейн-технології, мережеві екрани, хмарні сервіси, захищені сервери, антивірусні програми тощо). Ключовими суб’єктами в цій сфері є фахівці з інформаційних систем і технологій, системні адміністратори, які вживають заходів щодо безперебійності функціонування інформаційних мереж організації і забезпечують їх захист. Даний аспект є технічним і вузькоспеціалізованим. Сьогодні активно впроваджуються системи ранньої діагностики вторгнення і діагностики в режимі реального часу (SIEM), штучний інтелект, удосконалюється архітектура IT-рішень в межах організації, створюються єдині центри забезпечення безпеки (SOC), системи розгортання розподіленої інфраструктури хибних цілей (DDP) тощо.

Цифрова трансформація – це насамперед інноваційний процес, що вимагає внесення докорінних змін у промислові технології, соціум та культуру, фінансові транзакції та принципи створення нових продуктів та послуг. Фактично, це не просто набір IT-продуктів і рішень, що підлягають розгортанню, в компаніях і на виробництві, а глобальний перегляд підходів і стратегій у бізнесі, що виконується за допомогою інформаційних технологій.

Цифрова трансформація – це не просто автоматизація та цифровізація окремих виробничих процесів «на місцях», це інтеграція звичайних офісних та промислових технологій, які ми використовуємо щодня, з абсолютно новими IT-напрямками, специфічними для цифрової трансформації (хмарні обчислення, штучний інтелект та машинне навчання і т.д.).

Проте процеси, які викликає цифрова трансформація, мають і негативну сторону. Революційні зміни, які привносить цифрова трансформація, породили певні проблеми для служб інформаційної безпеки, а саме виникли нові вектори загроз інформаційної безпеки і розширився спектр вразливостей для потенційних кібератак [1].

Кіберзагрози та збитки від кіберзлочинців вийшли на друге місце у світі після техногенних катастроф. Проблеми безпеки ускладнюються тим, що на сьогодні немає уніфікованих методів захисту інформації. Використання механізмів захисту, що успішно застосовуються в одній організації може категорично не підійти для іншої.

У березні 2018 року однією з гучних тем у світових ЗМІ став витік даних із найбільшої американської компанії Facebook. Користувачам соціальної мережі стало відомо, що без згоди та сповіщення передавано їх особисті дані британській фірмі Cambridge Analitica з комерційними цілями для обробки та аналізу. Цей інцидент привернув увагу громадськості до проблеми забезпечення конфіденційності користувацьких та корпоративних даних у сучасному цифровому світі.

Статистика подій однієї з найрозвиненіших цифрових країн світу запевняє, що витоку великої кількості даних є подією незвичайною. «Виток слід розглядати як високо ймовірну подію, ризик настання якої можна знизити за допомогою технічних та організаційних заходів, але виключити неможливо», – пояснюють фахівці інформаційної безпеки [3].

Експерти у сфері інформаційної безпеки вказують на необхідність зміни загального

методологічного підходу до забезпечення безпеки та підвищення надійності нових технологій. В якості альтернативи вони пропонують застосувати індивідуальний підхід до об'єктів захисту, який має на увазі вибір засобів забезпечення безпеки інформації з урахуванням конкретного сегменту та внесення своєчасного коригування.

Саме «індивідуалізація» та попереднє опрацювання захисту дає значно більш високу гарантію належного рівня цілісності, доступності та конфіденційності інформації в цифрових системах.

Людину, яка намагається порушити роботу інформаційної системи або отримати несанкціонований доступ до інформації, зазвичай називають комп'ютерним піратом (хакером). У своїх протиправних діях, спрямованих на оволодіння чужими секретами, зломщики прагнуть знайти такі джерела конфіденційної інформації, які давали б їм найбільш достовірну інформацію в максимальних обсягах з мінімальними витратами на її отримання. За допомогою різного виду хитрощів і безлічі прийомів і засобів підбираються шляхи та підходи до таких джерел. В даному випадку під джерелом інформації розуміється матеріальний об'єкт, який має певні відомості, що представляють конкретний інтерес для зловмисників або конкурентів.

Під загрозою безпеці інформації розуміються події або дії, які можуть призвести до спотворення, несанкціонованого використання або навіть руйнування інформаційних ресурсів керованої системи, а також програмних та апаратних засобів [2]. Інформаційна безпека включає:

– стан захищеності інформаційного простору, що забезпечує його формування та розвиток на користь громадян, організацій та держави;

– стан інфраструктури, при якому інформація використовується строго за призначенням і не впливає на систему при її використанні;

– стан інформації, при якому виключається або суттєво утруднюється порушення таких її властивостей, як конфіденційність, цілісність та доступність;

– економічну складову (структури управління в економічній сфері, включаючи системи збирання, накопичення та обробки інформації на користь управління виробничими структурами, системи загальноекономічного аналізу та прогнозування господарського розвитку, системи управління та координації в промисловості та на транспорті, системи управління енергосистем, централізованого постачання, системи прийняття рішення та координації дій у надзвичайних ситуаціях, інформаційні та телекомунікаційні системи);

– фінансову складову (інформаційні мережі та бази даних банків та банківських об'єднань, системи фінансового обміну та фінансових розрахунків).

Забезпечення інформаційної безпеки має починатися з виявлення суб'єктів відносин, що з використанням інформаційних систем. Спектр їх інтересів можна розділити на такі основні категорії: доступність (можливість за прийнятний час отримати необхідну інформаційну послугу), цілісність (актуальність та несуперечність інформації, її захищеність від руйнування та несанкціонованої зміни), конфіденційність (захист від несанкціонованого ознайомлення) [4].

Виходячи з вищевикладеного, у найбільш загальному вигляді інформаційна безпека може бути визначена як неможливість заподіяння шкоди властивостям об'єкта безпеки, що обумовлюються інформацією та інформаційною інфраструктурою. Поняття інформаційної безпеки у вузькому значенні цього слова передбачає:

– надійність роботи комп'ютера;
– збереження цінних даних;
– захист інформації від внесення змін до неї неуповноваженими особами;
– збереження таємниці листування в електронному зв'язку.

Безпека проявляється як неможливість завдання шкоди функціонуванню та властивостям об'єкта, або його структурним складовим.

Зупинимося на основних проблемах інформаційної безпеки, а також позначимо шляхи вирішення цих проблем під час цифрової трансформації.

Ще одним важливим напрямом у сфері інформаційної безпека є захист інформації. Мета роботи фахівців із захисту інформації – це забезпечення її конфіденційності, доступності та цілісності. Загалом, ці три ключові принципи інформаційної безпеки називають тріадою системи інформаційної безпеки [7], нижче розкриємо сенс цих понять.

Рис. Світові цифрові тренди (тріада системи інформаційної безпеки)

Confidentiality (з англ. «конфіденційність») – це властивість інформації бути закритою для неавторизованих осіб;

Integrity (з англ. «цілісність») – властивість збереження правильності та повноти даних;

Availability (з англ.«доступність») – властивість інформації бути доступною і готовою до використання за запитом авторизованого суб'єкта.

Особливу увагу необхідно приділити інцидентам інформаційної безпеки на об'єктах критичної інформаційної інфраструктури, це можуть бути як цільові атаки, так і техногенні катастрофи, фізичне викрадення активів та ін. У міру ускладнення атак нарощуються і засоби оборони (тобто інфраструктура інформаційної безпеки).

На цьому фоні все більшої популярності набирають системи SIEM (Security information and event management), основне завдання яких – це моніторинг корпоративних систем та аналіз подій безпеки в режимі реального часу, у тому числі з широким використанням комп'ютерних систем та глибокого машинного навчання (Deep learning) .

Великі технологічні компанії, які лідирують у галузі цифрової трансформації, набагато частіше за інших інтегрують свої продукти та засоби інформаційної безпеки у єдину архітектуру корпоративної безпеки. Треба відзначити, що в таких компаніях віддають перевагу стратегічному підходу та формуванню політики безпеки, що дозволяє:

– швидко виявляти загрози та оперативно реагувати на них;

– забезпечувати якісний захист інформаційних активів;

– мати прозоре виявлення загроз технологічне середовище.

Лідери цифрової трансформації, як правило, охочіше автоматизують процеси інформаційної безпеки в компанії, це набагато ефективніше за ручний моніторинг загроз і подій інформаційної безпеки, який застосовувався повсюдно до періоду цифрової трансформації. Позитивним прикладом такої автоматизації та комплексного підходу є запровадження SOC (Security Operations Center – центру забезпечення безпеки). Однак потрібно враховувати, що налаштування автоматизації всіх робочих процесів потребує більшого часу для тестування та необхідності залучення грамотних спеціалістів.

У результаті, можна виділити найкращі практики інформаційної безпеки, які можна

порекомендувати організаціям та установам під час процесу цифрової трансформації:

−побудувати єдину архітектуру безпеки, яка забезпечить централізоване управління IT-інфраструктурою та прозорість усіх подій інформаційної безпеки;

−розробити стратегію захисту корпоративної мережі та політику безпеки компанії;

−запровадити вбудовані засоби контролю відповідності стандартам та вимогам регуляторів;

−використовувати методи як превентивного, так і проактивного захисту.

Можна погодитися з фахівцями у сфері інформаційних технологій [5], що цифрову трансформацію не варто розглядати спрощено, лише як автоматизацію і комп'ютеризацію окремих процесів чи підрозділів підприємств, а слід розуміти як повне переосмислення методів ведення бізнесу, формування додаткових компетентностей, впровадження нових і реконструкцію існуючих бізнес-процесів, їх інтеграцію, як в межах підприємства, так і з зовнішніми контрагентами на засадах сучасних IT-технологій (хмарні обчислення, штучний інтелект, машинне навчання тощо).

Система захисту інформації, як і будь-яка система, повинна мати певні види власного забезпечення, спираючись на які вона виконуватиме свою цільову функцію [6]. З огляду на це система захисту інформації має:

– *правове забезпечення.*

Сюди входять нормативні документи, положення, інструкції, настанови, вимоги яких є обов'язковими в рамках сфери дії; організаційне забезпечення. Мається на увазі, що реалізація захисту інформації здійснюється певними структурними одиницями, такими як служба безпеки, служба режиму, служба захисту інформації технічними засобами та ін.

– *апаратне забезпечення.*

Передбачається широке використання технічних засобів, як захисту інформації, так забезпечення діяльності власне системи захисту інформації;

– *інформаційне забезпечення*.

Воно включає документовані відомості (показники, файли), що лежать в основі вирішення завдань, що забезпечують функціонування системи. Сюди можуть входити показники доступу, обліку, зберігання, так і системи інформаційного забезпечення розрахункових завдань різного характеру, пов'язаних з діяльністю служби забезпечення безпеки;

−*програмне забезпечення*.

До нього відносяться антивірусні програми, а також програми (або частини програм регулярного застосування), що реалізують контрольні функції під час вирішення облікових, статистичних, фінансових, кредитних та інших завдань;

– *математичне забезпечення*.

Передбачає використання математичних методів для різних розрахунків, пов'язаних з оцінкою небезпеки технічних засобів зловмисників, зон та норм необхідного захисту; лінгвістичне забезпечення. Сукупність спеціальних мовних засобів спілкування спеціалістів та користувачів у сфері захисту інформації;

– *нормативно-методичне забезпечення.*

Сюди входять норми та регламенти діяльності органів, служб, засобів, що реалізують функції захисту інформації, різноманітних методик, що забезпечують діяльність користувачів при виконанні своєї роботи в умовах жорстких вимог захисту інформації; ергономічне забезпечення. Сукупність засобів, що забезпечують зручність роботи користувачів апаратних засобів захисту інформації. Підбиваючи підсумки, варто зазначити, що проблема інформаційної безпеки в умовах цифровізації набуває особливої актуальності, а ті загрози, які породжує цифрова трансформація можуть бути успішно подолані лише взаємопов'язаною дією технічних, організаційних та економічних методів та засобів.

Список використаних джерел

1. Gorodianska L.V., Nosenko T.I. & Vember V.P. (2019) Neobanks operations and

security features. Problems of Infocommunications. *Science and Technology PIC S&T'2019*: 2019 IEEE International Scientific and Practical Conference 08-11 October 2019 (pp. 839-842). Kyiv. DOI: 10.1109/PICST47496.2019.9061268[in Ukrainian]
2. Городянська Л. & Цюкало Л. (2021). Інформаційна безпека суб'єктів малого підприємництва в умовах цифровізації. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*, (70), 105–114. https://doi.org/10.17721/2519-481X/2021/70-11
3. Информационная безопасность: Учебное пособие. Авторы: Ясенев В. Н., Дорожкин А. В., Сочков А. Л., Ясенев О. В. Под общей редакцией проф. Ясенева В. Н. Нижний Новгород: Нижегородский госуниверситет им. Н. И. Лобачевского, 2017. 198 с.
4. Інформатика та інформаційні технології у цивільній безпеці: Практикум Гусєва Л. В., Журавський М. М, Маляров М. В., Паніна О. О., Піксасов М. М. Харків: НУЦЗУ, 2015. 330 с.
5. Кузьомко В. М. Інформаційна безпека бізнесу в умовах цифрової трансформації економіки. URL: https://ir.kneu.edu.ua:443/handle/2010/36159
6. Ленков С. В., Перегудов Д. А., Хорошко В. А. Методы и средства защиты информации : монография в 2 т. / Киев : Арий, 2008. Т. 2 : Информационная безопасность / под ред. В. А. Хорошко. 343 с.
7. Україна 2030Е – країна з розвинутою цифровою економікою. *Український інститут майбутнього.* URL: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ НАВЧАННЯ УЧНІВ ВИГОТОВЛЕННЮ ВИШИТИХ ВИРОБІВ НА УРОКАХ ТРУДОВОГО НАВЧАННЯ

Вакуленко Надія Вікторівна
Полтавський національний педагогічний університет імені В. Г. Короленка

Анотація. *Розглядаються інформаційно-комп'ютерні технології, що використовуються на заняттях і дозволяють урізноманітнити навчальний матеріал на всіх етапах уроку, підвищити мотивацію учнів, їхню зацікавленість, сприяти більш міцному засвоєнню знань, формувати особистісні властивості та якості, що визначають художній розвиток учнів, озброїти їх знаннями, пов'язаними з розумінням мистецтва умінням висловлювати свої погляди, а також вирішувати проблему індивідуалізації навчання.*

Ключові слова: *інформаційна технологія, навчання учнів, технологія, трудове навчання, вишиті вироби.*

Сучасне інформаційне суспільство висуває нові вимоги до педагогічних працівників у питаннях застосування інформаційно-комп'ютерних технологій у процесі самостійного вилучення та представлення знань.

Інформатизація освітнього процесу – один із пріоритетних напрямків модернізації освіти, що включає в себе цілу низку таких важливих завдань [1], як:

–забезпечення освітніх установ комп'ютерною технікою та засобами комунікації;

–забезпечення шкіл електронними засобами навчання;

–автоматизація управлінської діяльності адміністрації шкіл;

–запровадження інформаційних технологій у навчальний процес шкіл;

–підготовка та підвищення кваліфікації вчителів щодо використання ІКТ в освітньому процесі.

Пошук підходів до побудови освітніх моделей, що ґрунтуються на можливостях інформаційних технологій, інтенсивно розвивається і є предметом діяльності багатьох