УДК 004.056.53:621.39 DOI: 10.31673/2412-4338.2024.016472

Ветлицька Олена Сергіївна
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID 0009-0002-6308-2325

Треньов Микита Георгійович
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID 0009-0002-8459-0599

ПРОБЛЕМИ КІБЕРСТІЙКОСТІ ІКТ-СИСТЕМ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Анотація. *Сучасний світ характеризується стрімким розвитком інформаційних технологій та зростанням значення кібербезпеки в бізнес-процесах компаній. У цьому контексті особливо актуальним стає забезпечення цілісної безпеки ІКТ-систем, які піддаються постійним зовнішнім та внутрішнім загрозам в умовах цифрової трансформації. Стратегічний підхід означає усунення розрізненості, розгортання узгоджених технологій і процесів та розробка єдиної інтегрованої архітектури безпеки, яка дозволяє забезпечувати захист на всіх рівнях організації систем ІКТ - від кінцевих точок IoT до мультихмарних інфраструктур. Такі організації дотримуються цієї стратегії набагато частіше, ніж їхні колеги на нижньому рівні, що може призвести до збільшення вразливостей і погіршення реакції на кібератаки. Високорівневі організації також частіше діляться інформацією про загрози у своїй компанії, адже це підвищує загальну обізнаність та готовність до протидії потенційним атакам.*

У організацій вищого рівня більше шансів переконатися, що їхні заходи безпеки працюють скрізь (локально, у хмарі, в IoT, на мобільних пристроях тощо). Оскільки поверхня атаки в організації збільшується разом із поширенням різних типів кінцевих точок і хмарних систем, застарілі інструменти безпеки іноді не встигають реалізувати свої функції. Вирішення цієї проблеми та забезпечення інтеграції інструментів в інфраструктуру значно покращує стан безпеки організації.

У статті розглянуто питання кіберстійкості систем ІКТ щодо загроз, які виникають у процесі цифрової трансформації. На основі глобальних статистичних досліджень компанії Fortinet виявлено базові тренди, що впливають на основні бізнес-процеси організацій, у яких відбувається цифрова трансформація. Визначено загрози кібербезпеки та показано їхню значущість для процесів цифрової трансформації. Надано практичні рекомендації щодо інтеграції систем кібербезпеки для формування єдиної архітектури безпеки організації.

Ключові слова: *цифрова трансформація, стійкість технічних систем, кіберстійкість, загрози цифрової трансформації, управління інформаційною безпекою, єдина архітектура безпеки.*

Vetlytska Olena
State university of information and communication technologies, Kyiv
ORCID 0009-0002-6308-2325

Trenov Mykyta
State university of information and communication technologies, Kyiv
ORCID 0009-0002-8459-0599

PROBLEMS OF CYBER RESILIENCE OF ICT SYSTEMS IN THE CONTEXT OF DIGITAL TRANSFORMATION

Abstract. *The modern world is characterized by the rapid development of information technology and the growing importance of cybersecurity in business processes of companies. Within this context, ensuring the*

comprehensive security of ICT systems becomes particularly relevant, as they are subject to constant external and internal threats in the conditions of digital transformation. A strategic approach implies the elimination of fragmentation, the deployment of aligned technologies and processes, and the development of a single integrated security architecture that allows for the protection at all levels of the organization's ICT systems - from IoT endpoints to multi-cloud infrastructures. Organizations that adhere to this strategy do so much more often than their lower-tier counterparts, which can lead to an increase in vulnerabilities and a deterioration in the response to cyberattacks. High-level organizations also share information about threats within their company more frequently, as this enhances the overall awareness and readiness to counter potential attacks.

Higher-level organizations are more likely to ensure that their security measures are effective everywhere (locally, in the cloud, in IoT, on mobile devices, etc.). As the attack surface in an organization increases with the proliferation of various types of endpoints and cloud systems, outdated security tools sometimes fail to perform their functions in time. Addressing this issue and ensuring the integration of tools into the infrastructure significantly improves the organization's security posture.

The article considers the issue of cyber resilience of ICT systems in relation to threats arising in the process of digital transformation. Based on Fortinet's global statistical research, the basic trends affecting the main business processes of organizations undergoing digital transformation are identified. Cybersecurity threats are identified and their significance for digital transformation processes is shown. Practical recommendations on the integration of cybersecurity systems to form a unified security architecture of the organization are provided.

***Keywords**: digital transformation, technical systems resilience, cyber resilience, digital transformation threats, information security management, unified security architecture.*

1. Вступ.

Перш ніж перейти до основної теми цієї статті, давайте визначимося з деякими поняттями, які, на наш погляд, є ключовими в цій роботі.

Фундаментальним поняттям у теорії технічних систем є їхня стійкість. Стосовно поняття "Стійкість - це здатність системи функціонувати в станах, близьких до рівноважного, в умовах постійних зовнішніх і внутрішніх дратівливих впливів".

В застосуванні до систем інформаційно-комунікаційних технологій (ІКТ), кіберстійкість – це здатність кіберсистеми, що працює за певним алгоритмом, досягати мети функціонування в умовах інформаційно-технічних впливів зовнішніх загроз за наявності внутрішніх вразливостей.

У низці наукових джерел (наприклад, [1]) визначено, що передвісником 4-ї промислової революції (Індустрії 4.0) є цифрова трансформація (ЦТ), якій також дається визначення. Цифрова трансформація - це процес інтеграції цифрових технологій в усі аспекти бізнес-діяльності та інфраструктуру суспільних відносин, що вимагає внесення докорінних змін у технології, культуру, фінансові операції і принципи створення нових продуктів і послуг [1]. Для максимально ефективного використання нових технологій та їх оперативного впровадження в усі сфери діяльності людини підприємства і бізнес повинні відмовитися від колишніх підвалин і повністю перетворити процеси та моделі роботи. Цифрова трансформація вимагає зміщення акцентів на периферію підприємств і підвищення гнучкості центрів обробки даних (ЦОД), а також хмарних обчислень, що підтримують периферію. Цей процес означає поступову відмову від застарілих технологій, обслуговування яких може дорого обходитися підприємствам, несе в собі зміну культури виробництва (перехід до Інтернету речей, IoT), яке в результаті підтримує прискорення процесів, що забезпечується ЦТ.

Разом з тим, ЦТ висуває абсолютно особливі виклики компаніям і породжує нові кіберзагрози для IT-систем, внаслідок чого більшість організацій у цих умовах перестає відповідати поточним вимогам щодо кіберстійкості. З цих позицій перейдемо до основної частини нашої роботи, в якій спробуємо дати сучасну інтерпретацію протистояння загрозам ІКТ з боку ЦТ.

2. Мета і задачі дослідження.

Метою дослідження є розгляд проблеми кіберстійкості в застосуванні до систем інформаційно-комунікаційних технологій. Завданнями статті у зв'язку із визначеною метою є:

а) розглянути поняття "кіберстійкість" та основні тенденції в процесі цифрової трансформації, визначити, що потрібно для забезпечення кіберстійкості систем інформаційно-комунікаційних технологій, відносно зовнішніх, а також внутрішніх загроз;

б) розглянути головні інформаційно-технологічні тренди, які впливають на основні бізнес-процеси компаній, за результатами статистичних досліджень, на основі цього дослідження визначити певні тенденції цифрової трансформації;

в) дослідити проблеми цифрової трансформації для стійкості систем інформаційно-комунікаційних технологій до кібератак, розглянути перелік атак, загроз і вразливостей, а також рекомендації щодо запобігання атак, ліквідації загроз і вразливостей цифрової трансформації.

3. Результати дослідження.

Відомо, що цифрова трансформація чинить значний вплив на технології: від прийняття рішень на основі даних до впровадження хмарних технологій, мобільності та вибухового розвитку Інтернету речей (IoT), але сам процес ЦТ виходить за рамки простого розгортання нових рішень. Під час ЦТ організації повинні переглянути сформовані бізнес-моделі та процеси для стимулювання інновацій і поліпшення результатів своєї діяльності. Саме спільне застосування цифрових технологій та інформаційних процесів дає права на переосмислення моделей бізнесу, а це - нелегке завдання.

Ефективна трансформація бізнес-процесів передбачає спільні зусилля всіх підрозділів за участю партнерів, клієнтів та інших зацікавлених сторін.

Імперативи цифрової трансформації вимагають докорінного переосмислення проблем безпеки ІКТ для досягнення головної мети: забезпечення кіберстійкості цих систем як щодо зовнішніх, так і внутрішніх загроз.

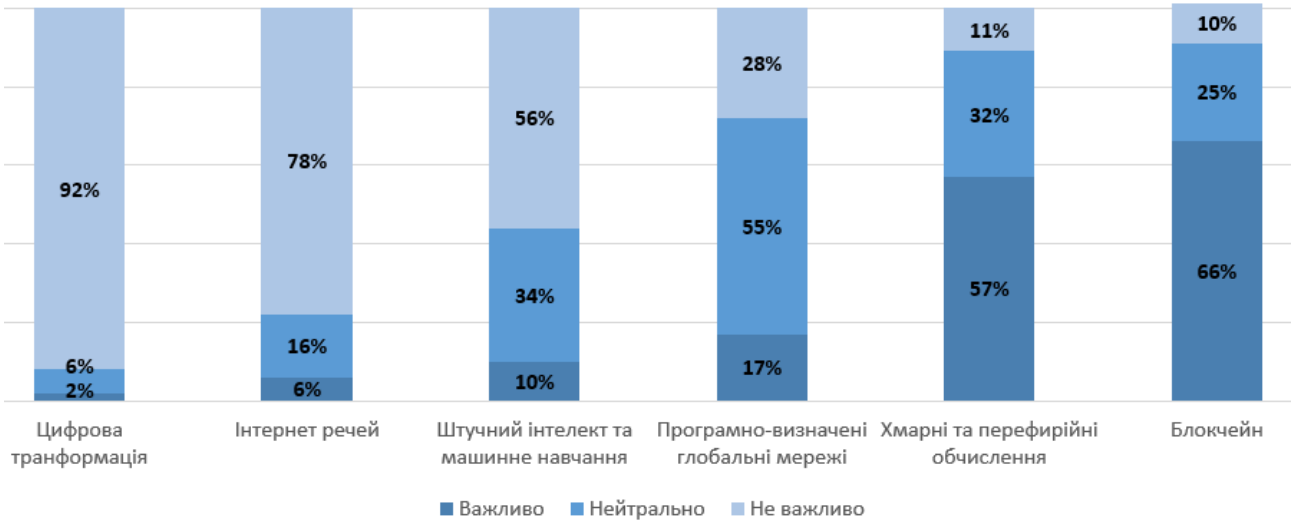

Рис. 1. Оцінка впливу сучасних IT-трендів на основні бізнес-процеси

Інтеграція бізнес-систем, інформаційних та операційних технологій, що дають змогу ухвалювати рішення на основі потоків даних, створює нові проблеми безпеки, оскільки ці повторно підключені системи також можуть збільшити збитки від атак на корпоративні мережі. Надалі система безпеки має стати цілісною і автоматизованою від самого початку, а не збиратися воєдино з плином часу з окремих програмно-технічних рішень.

Аналітикам і фахівцям з ІБ, щоб охопити вплив такого глобального процесу, як ЦТ, на кібербезпеку систем ІКТ, необхідно зібрати відповідну статистику.

Саме з цією метою компанія Fortinet випустила звіт про наслідки цифрової трансформації для безпеки [2]. Під час цього дослідження було опитано 300 керівників служб безпеки компаній (CISO/CSO) з чисельністю співробітників не менше 2500 осіб з різних галузей промисловості в Північній Америці, Європі, Азії та Австралії. Мета опитування - зібрати дані про перебіг цифрової трансформації в цих компаніях, а також виявити проблемні місця ЦТ.

За результатами цих статистичних досліджень, перш за все, розглянемо головні IT-тренди, що впливають на основні бізнес-процеси компаній (рис. 1).

На підставі цього дослідження було виявлено такі тенденції.

Тенденція 1: Цифрова трансформація є найвпливовішим трендом для бізнесу в останні 5 років.

З усіх опитаних фахівців, 92 % респондентів оцінили процес ЦТ як такий, що має "досить великий" або "надзвичайно великий" ефект для організації.

Друге і третє місце в рейтингу впливу на бізнес отримали дві тенденції, які часто вважаються елементами ЦТ: IoT (78 %), штучний інтелект (AI) і машинне навчання (56 %).

Далі перейдемо до оцінки впливу ЦТ на значущість кіберзагроз. На рис. 2. наведено графік значущості загроз кібербезпеці систем ІКТ.

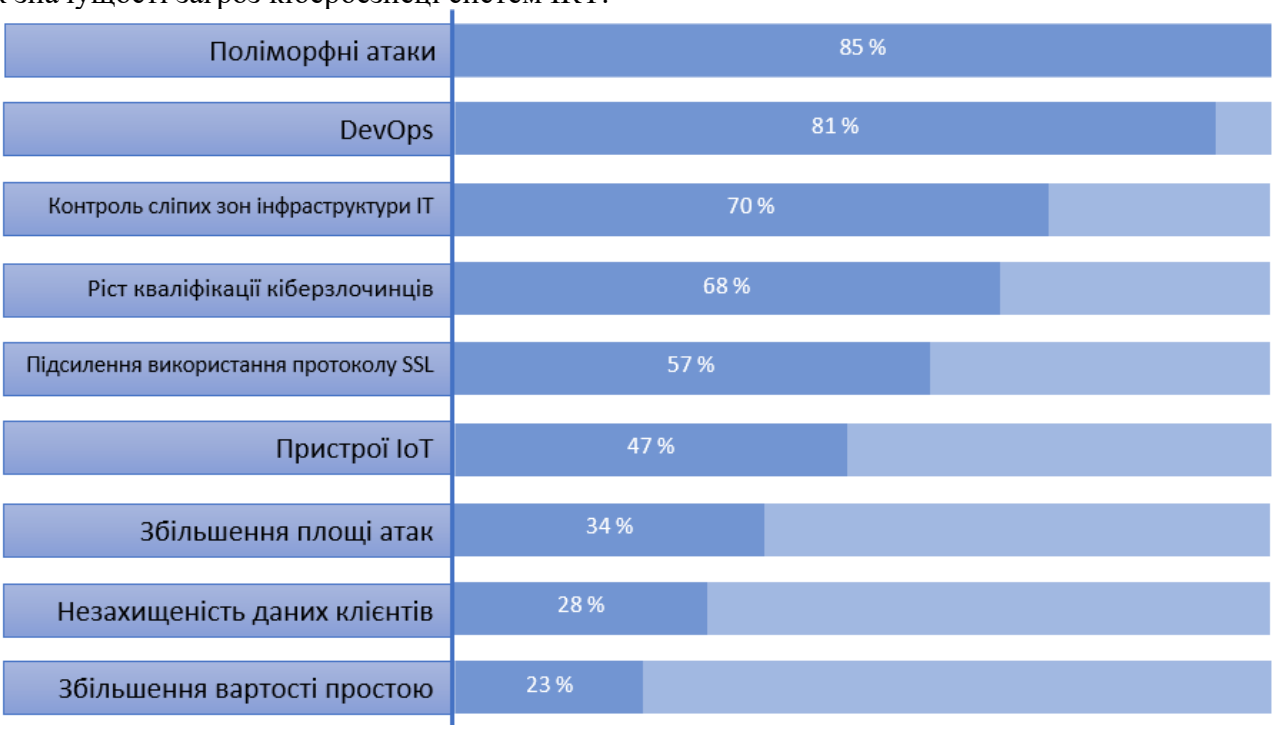

Рис. 2. Оцінка впливу ЦТ на значущість кіберзагроз

У той час як у багатьох статтях у галузевих ЗМІ та на IT-форумах організаційні питання та обмеження, які несуть у собі застарілі технології, обговорюються як найбільші проблеми для ЦТ, що частково вірно, фахівці з інформаційної безпеки в переважній більшості впевнені, що проблеми безпеки є найбільш значущими перешкодами для реалізації ЦТ. А саме, 85 % опитаних CISO/CSO (керівників та ІБ-фахівців у компаніях) оцінюють проблеми безпеки як такі, що мають "досить великий" або "надзвичайно великий" вплив на бізнес-процеси в організаціях. Крім того, друга найпоширеніша відповідь (56 %) пов'язана з дотриманням вимог галузевих регуляторів.

Керівники ІБ-департаментів особливу увагу приділяють двом джерелам ризику: зовнішньому і внутрішньому. Зростання поліморфних атак і загроз, які постійно трансформуються або змінюються, щоб уникнути виявлення, 85 % фахівців з ІБ оцінюють як "досить велику" або "надзвичайно велику" проблему [3]. Також слід звернути увагу (значення 81 % на рис. 2) на зростання негативного впливу технології DevOps, яка, на думку опитаних CISO/CSO, дає змогу вразливостям "прослизати" в корпоративну мережу разом з більш швидкими темпами розробки ПЗ, і ця тенденція останнім часом посилюється [4]. Обидві ці загрози потенційно можуть посилитися в міру того, як поверхня атаки стає складнішою у контексті ЦТ, що проходить у компанії ЦТ. З огляду на важливість наведених загроз для кібербезпеки, дамо розширене тлумачення цим небезпечним технологіям.

Поліморфізм полягає у формуванні коду шкідливої програми "на льоту", вже під час виконання, при цьому сама процедура, що формує код, також не повинна бути постійною і видозмінюється під час кожного нового зараження. У багатьох випадках зміна шкідливого коду досягається шляхом додавання операторів, які не змінюють сам алгоритм роботи програми (наприклад, оператор NOP). Постійна видозміна програмного коду шкідливої програми не дає змоги створити універсальну сигнатуру для даного зразка. Фахівці з кібербезпеки для протидії цьому методу успішно застосовують в антивірусному програмному забезпеченні такі технології, як евристичний аналіз та емуляцію.

Трохи зупинимося на такій популярній останнім часом в ІТ-компаніях технології, як DevOps. Методологія DevOps означає інтеграцію діяльності розробників і фахівців з обслуговування ПЗ, мереж і обладнання у командах і компаніях. "Модна" технологія є предметом особливої настороженості з боку фахівців ІБ, оскільки вона принципово змінила взаємини між розробниками софту, системними адміністраторами, службами технічної підтримки і кінцевими користувачами.

На рис. 3 наведено схему функціонування DevOps.

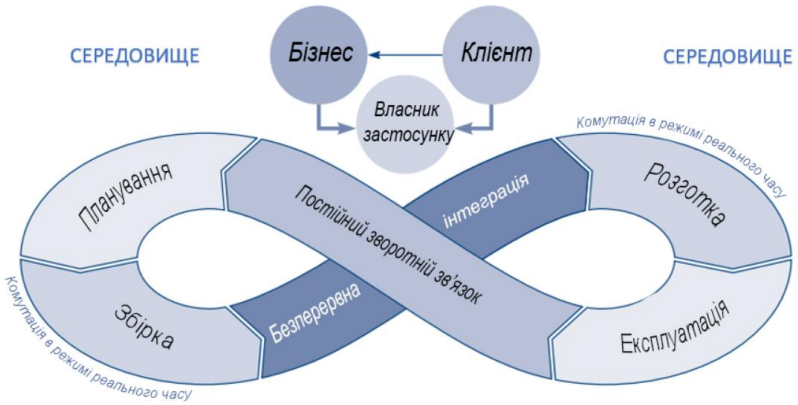

Рис. 3. Що таке DevOps

Ще одна серйозна проблема - відсутність повної видимості всіх зон і процесів для фахівців відділів безпеки (70 %), враховуючи дедалі складнішу обчислювальну інфраструктуру, яку представляє ЦТ. Ця проблема також може бути результатом спадщини неінтегрованих, багатопозиційних систем та ІТ-продуктів (що застосовувалися в оборонній промисловості). Для забезпечення безпеки складних, високорозвинених розподілених середовищ, що охоплюють віддалені філії, корпоративні центри обробки даних і гібридні хмари, департаменти безпеки повинні підтримувати найбільш повну видимість для виявлення аномальної поведінки систем і швидкої нейтралізації загроз.

Цифрова трансформація також посилила акцент на захист конфіденційності та більш високі вимоги до її дотримання. У міру того, як кібератаки стають дедалі більш витонченими і руйнівними, регулюючі органи встановлюють більш суворі правила і керівні принципи захисту персональної ідентифікаційної інформації (англ. Personally Identifiable Information, PII). У результаті, організації повинні пам'ятати про комплаєнс (англ. Compliance),

тобто про дотримання певних правил, і звертатися до найкращих у своєму класі сертифікованих продуктів, процесів і фахівців, щоб забезпечити належний рівень управління ризиками. Ще до початку ЦТ системи інформаційної безпеки на звичайному підприємстві за замовчуванням включали кілька розрізнених сховищ з локальними службами і розгорталися, як правило, у кількох хмарних сервісах з різними інструментами безпеки.

Стратегія ЦТ може призвести до ще більш складного середовища з ще більшою кількістю хмар і збільшенням кількості пристроїв IoT, багато з яких не були розроблені з урахуванням вимог кібербезпеки.

Таблиця 1

Зведений перелік атак, загроз і вразливостей ЦТ

№ з/п	Атаки, загрози та вразливості ЦТ	Значимість загроз, %	Рекомендації щодо виявлення та запобігання атакам, ліквідації загроз та вразливостей ЦТ
1	Поліморфні атаки	85	Впровадження SIEM та систем моніторингу на базі ШІ та глибокого машинного навчання (Deep Learning)
2	Загрози технології DevOps	81	Перехід на більш безпечну технологію DevSecOps
3	Уразливості «сліпих зон» інфраструктури IT-системи	70	Заходи для реалізації прозорості інфраструктури систем ІКТ, які належать до ЦТ
4	Зростання атакуючого потенціалу кіберзлочинців	68	Широке впровадження систем автоматизації та інтеграції ІБ інфраструктур систем ІТ, які належать до ЦТ
5	Широке використання протоколу SSL	57	Для зниження частки фішингових атак слід перейти на EV SSL сертифікати
6	Загрози та вразливості Інтернету речей (IoT)	47	Використання технології блокчейн для управління аутентифікацією, забезпечення неподільності інформації та працездатності ІТ-сервісів
7	Розширення простору реалізації загроз	34	Використання проактивних методів захисту інформації

Тенденція 2: Найбільш серйозний виклик для реалізації ЦТ - це безпека і стійкість систем до кібератак і відсутність прозорості ІТ-інфраструктури під час ЦТ.

Особливу увагу необхідно приділити інцидентам ІБ на об'єктах критичної інформаційної інфраструктури (КІІ); це можуть бути, як таргетовані атаки (англ. Advanced Persistent Threat, APT), так і техногенні катастрофи, фізичне викрадення активів та інші загрози. У міру ускладнення атак нарощуються і "засоби оборони" (тобто інфраструктура ІБ).

На цьому тлі дедалі більшої популярності набирають інтелектуальні системи управління кібербезпекою - SIEM (англ. Security Information and Event Management), основне завдання яких - моніторинг корпоративних систем і аналіз подій безпеки в режимі реального часу, зокрема з широким використанням систем штучного інтелекту (ШІ) і глибокого машинного навчання (англ. Deep Learning) [5].

Тенденція 3: Використання високоінтелектуальних систем для управління кібербезпекою.

Аналізуючи проблеми ЦТ для стійкості систем ІКТ до кібератак, наведемо ранжований у відсотках зведений перелік атак, загроз і вразливостей, а також рекомендації щодо запобігання атакам, ліквідації загроз і вразливостей ЦТ (див. таблицю).

Не всі організації далеко просунулися у впровадженні сучасних методів забезпечення безпеки, згаданих у [2]. Також потрібно врахувати, що компанія Fortinet проводила свої статистичні дослідження в основному серед так званих високорівневих компаній, а тому про стан кібербезпеки в організаціях середнього та низького рівнів можна тільки здогадуватися. Проєкти з інтеграції рішень безпеки, забезпечення наскрізної прозорості та автоматизації контролю відповідності все ще перебувають у стадії реалізації у 30-40 % організацій і завершені менш ніж в одній третині компаній. Такий факт, що багато з них перебувають у стадії розгортання, вказує на те, що організації швидко рухаються в спробах випереджати загрози, що розвиваються.

Тенденція 4: Великі обсяги інфраструктури ІКТ, як і раніше залишаються вразливими для різного роду кібератак.

За середніми оцінками фахівців CISO/CSO, близько 25 % інфраструктури не захищені від сьогоднішніх загроз безпеки. У міру розширення поверхні атаки застарілі архітектури безпеки часто не можуть масштабуватися для задоволення нових вимог. Навіть якщо точкові рішення розгорнуті для забезпечення деякого захисту, поширення розрізнених систем, що виникає в результаті цього, означає, що загальний профіль безпеки організації не може бути значно поліпшено.

Також зазначимо, що вразливості, які можна усунути за допомогою оновлень програмного забезпечення та виправлень, все ще залишаються потенційною проблемою для деяких організацій.

Таким чином, можна констатувати, що далеко не всі організації перебувають в однаковій мірі готовності до такого складного, а часом і тривалого процесу перетворень, яким є цифрова трансформація, а часом і тривалого процесу перетворень, яким є цифрова трансформація. Однак проривний розвиток інтелектуальних механізмів управління кібербезпекою, зокрема на основі ШІ, вселяють у нас надію на мінімізацію цієї рудиментарної тенденції в осяжній перспективі.

4. Висновки.

Організації високого рівня частіше інтегрують свої системи безпеки для формування єдиної архітектури безпеки. Стратегічний підхід означає усунення розрізненості та розгортання узгоджених технологій і процесів у всіх частинах систем ІКТ - від кінцевих точок IoT до мультихмарних інфраструктур. Такі організації дотримуються цієї стратегії набагато частіше, ніж їхні колеги на нижньому рівні. Високорівневі організації також частіше діляться інформацією про загрози у своїй компанії.

Одним із результатів розрізненості технологій і процесів є те, що весь обсяг аналітики загроз, доступний в організації, не використовується у всій інфраструктурі. Тільки найкращі фахівці служб ІБ звертають увагу на цю проблему.

В організацій вищого рівня більше шансів переконатися, що їхні заходи безпеки працюють скрізь (локально, у хмарі, в IoT, на мобільних пристроях тощо). Оскільки поверхня атаки в організації збільшується разом із поширенням різних типів кінцевих точок і хмарних систем, застарілі інструменти безпеки іноді не встигають реалізувати свої функції. Вирішення цієї проблеми та забезпечення інтеграції інструментів в інфраструктуру значно покращує стан безпеки організації.

Топ-компанії вбудовують засоби контролю відповідності для централізованого відстеження та звітності як за галузевими стандартами, так і за стандартами безпеки.

Галузі з жорстким регулюванням кілька років тому першими почали впроваджувати автоматизований контроль дотримання нормативних вимог. Останнім часом інші галузі

намагаються надолужити згаяне через потік нових правил і стандартів, величезних змін в інформаційній інфраструктурі та мінливого ландшафту загроз.

В організацій вищого рівня більше шансів мати наскрізну видимість у всіх середовищах, оскільки наскрізна видимість практично неможлива з розрізненими інструментами безпеки. Без цієї прозорості організації просто не можуть йти в ногу з сучасним ландшафтом загроз. У той час як визначення "наскрізної видимості" швидко розширюється, організації, які просунулися далі в цьому процесі, отримують найкращі результати. Топ-компанії частіше автоматизували більше половини своїх методів забезпечення безпеки.

Обсяг загроз, що спостерігаються сьогодні в більшості організацій, означає, що ручний моніторинг загроз і їх виправлення перетворилися з непродуктивної витрати часу персоналу на безглузду роботу. Однак повне налаштування автоматизації робочих процесів потребує часу та тестування. Організації, де рівень кібербезпеки вищий, просунулися далі шляхом автоматизації, ніж їхні менш успішні колеги.

Основні висновки нашого дослідження досить прості:

ЦТ - це домінуюча нині IT-тенденція на ринку ІКТ-технологій, а забезпечення безпеки та наростаючі кіберзагрози - найбільша перешкода на шляху до повноцінної цифрової трансформації.

Існують як внутрішні, так і зовнішні загрози безпеці, насамперед, - це поліморфні загрози та вразливості, які несе в собі використання DevOps.

Більшість компаній намагаються вибудувати адекватну структуру безпеки, що відповідає новим реаліям, які несе ЦТ.

Окремі результати дослідження, безумовно, можуть когось насторожити і змусити замислитися про доцільність проведення ЦТ, однак треба розуміти, що цифрова трансформація несе в собі й чималі плюси. Незважаючи на такі проблеми, як розширення поверхні атак, підвищена складність управління всіма елементами IT-інфраструктури та ландшафт складних загроз, який розвивається, передовим організаціям все-таки вдається запобігати руйнівним атакам. Ключовим моментом на цьому шляху є попереджувальний підхід до управління ризиками, який захищає від зловмисних атак і зломів. Зокрема, в організаціях, які дотримуються найкращих практик ІБ, рівень кібербезпеки набагато вищий, ніж у тих, які нехтують такими, і в них, як правило, не трапляється збоїв, втрат даних або порушень політик ІБ.

Якщо говорити коротко, до найкращих практик ІБ стосовно теми дослідження можна віднести:

- проектування такої архітектури безпеки організації, яка забезпечує прозорість і видимість усієї IT-інфраструктури та дає змогу здійснювати централізований контроль за нею;
- вироблення стратегії, що використовує інтеграцію для розповсюдженої автоматизації робочих процесів і обміну аналітичними даними про загрози всередині компанії.

Список використаних джерел

1. Гриценко В.І., Бажан Л.І. Цифрова трансформація економіки // Керуючі системи та машини. — 2017. — № 6. — С. 3-16.

2. Fortinet 2018 Security Implications of Digital Transformation Report [Електронний ресурс]. - Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/Fortinet-2018-Security-Implications-of-Digital-Transformation-Report.pdf (дата звернення: 14.04.2021).

3. Спінелліс, Діомідіс (січень 2003). «Надійна ідентифікація вірусів обмеженої довжини є NP-повною». Транзакції IEEE з теорії інформації. 49 (1): 280–4.

4. Що таке DevOps? Опис DevOps [Електронний ресурс]. - Режим доступу: https://www.guru99.com/what-is-devops.html

5. Когут Ю. І. Кібербезпека та ризики цифрової трансформації компаній: практичний посібник / Ю. І. Когут. – Київ: Консалтингова компанія «СІДКОН», 2021. 372 с.

6. Moshenchenko M., Zhurakovskyi B., Poltorak V., Bondarchuk A., Korshun N. Optimization Algorithms of Smart City Wireless Sensor Network Control // CEUR Workshop Proceedings, 2021, 3188, p. 32–42/

7. Shevchenko O., Bondarchuk A., Polonevych O., Zhurakovskyi B.,Korshun N. Methods of the objects identification and recognition research in the networks with the IoT concept support // CEUR Workshop Proceedings, 2021, 2923, p. 277–282

8. Malinov V., Zhebka V., Zolotukhina O., Franchuk T., Chubaievskyi V. Biomining as an Effective Mechanism for Utilizing the Bioenergy Potential of Processing Enterprises in the Agricultural Sector / CEUR Workshop Proceedings., 2023, 3421, p. 223–230

References

1. Hrytsenko V.I., Bazhan L.I. Digital transformation of the economy // Control systems and machines. - 2017. - No. 6. - P. 3-16.

2. Fortinet 2018 Security Implications of Digital Transformation Report [Electronic resource]. - Access mode: https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/Fortinet-2018-Security-Implications-of-Digital-Transformation-Report.pdf (accessed: 04/14/2021).

3. Spinellis, Diomidis (January 2003). "Reliable identification of viruses of bounded length is NP-complete". IEEE Transactions on Information Theory. 49 (1): 280-4

4. What is DevOps? Description of DevOps [Electronic resource]. - Access mode: https://www.guru99.com/what-is-devops.html

5. Cybersecurity and risks of digital transformation of companies: a practical guide / Y. Kohut - Kyiv: Sidcon Consulting Company, 2021. 372 c.

6. Moshenchenko M., Zhurakovskyi B., Poltorak V., Bondarchuk A., Korshun N. Optimization Algorithms of Smart City Wireless Sensor Network Control // CEUR Workshop Proceedings, 2021, 3188, p. 32–42

7. Shevchenko O., Bondarchuk A., Polonevych O., Zhurakovskyi B.,Korshun N. Methods of the objects identification and recognition research in the networks with the IoT concept support // CEUR Workshop Proceedings, 2021, 2923, p. 277–282

8. Malinov V., Zhebka V., Zolotukhina O., Franchuk T., Chubaievskyi V. Biomining as an Effective Mechanism for Utilizing the Bioenergy Potential of Processing Enterprises in the Agricultural Sector / CEUR Workshop Proceedings., 2023, 3421, p. 223–230