МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ZERO TRUST ARCHITECTURE У ЗАХИСТІ ОРГАНІЗАЦІЙНИХ IT-СИСТЕМ: ТЕОРІЯ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Андрій КОБИЛЯЦЬКИЙ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Андрій КОБИЛЯЦЬКИЙ
Ім’я, ПРІЗВИЩЕ

Керівник: Володимир ШУЛЬГА
д.і.н., професор Ім’я, ПРІЗВИЩЕ

Рецензент:

Київ 2026

ё

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2026 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Кобиляцькому Андрію Андрійовичу

(прізвище, ім’я, по батькові здобувача)

1.Тема кваліфікаційної роботи “Zero Trust Architecture у захисті організаційних ІТ-систем: теорія та практична реалізація”,

керівник кваліфікаційної роботи Володимир ШУЛЬГА, д.т.н., професор,

(Ім’я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20“ лютого 2026 р. №51

2.Строк подання кваліфікаційної роботи “12” травня 2026 р.

3.Вихідні дані до кваліфікаційної роботи: організаційні ІТ-системи, архітектура Zero Trust, технології контролю доступу, міжнародні стандарти кібербезпеки, наукова та технічна література.

4.Перелік питань, які мають бути розроблені:

4.1. Проаналізувати сучасні загрози організаційним ІТ-системам та обґрунтувати потребу в переході до архітектури Zero Trust.

4.2. Дослідити теоретичні засади, принципи та компоненти Zero Trust Architecture.

4.3. Вивчити інструменти практичної реалізації Zero Trust Architecture та розробити рекомендації щодо її впровадження в організації.

5.Перелік ілюстративного матеріалу: презентація PowerPoint, 8 рисунків і 5 аналітичних таблиць за темою дослідження.

6.Дата видачі завдання “05“ березня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкта, предмету, мети та завдань дослідження.	18.03.2026	
2.	Збір та аналіз літератури.	30.03.2026	
3.	Аналіз особливостей забезпечення безпеки інформаційних систем організації на базі технології Zero Trust.	08.04.2026	
4.	Дослідження основних характеристик технології Zero Trust та особливостей її застосування для забезпечення безпеки інформаційних систем організації.	15.04.2026	
5.	Вивчення інструментів і методів реалізації технології Zero Trust для забезпечення безпеки інформаційних систем організації.	22.04.2026	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2026	
7.	Оформлення роботи.	06.05.2026	
8.	Оформлення презентації.	11.05.2026	
9.	Отримання рецензії на роботу.	10.06.2026	
10.	Захист в ЕК.	__.06.2026	

Здобувач вищої освіти _____ Андрій КОБИЛЯЦЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Володимир ШУЛЬГА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ё

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Кобиляцький А.А. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Zero Trust Architecture у захисті організаційних IT-систем: теорія та практична реалізація"
Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач КОБИЛЯЦЬКИЙ Андрій у кваліфікаційній роботі проаналізував теоретичні засади Zero Trust Architecture, дослідив сучасні підходи до захисту організаційних IT-систем, вивчив інструменти практичної реалізації архітектури нульової довіри та розробив рекомендації щодо її впровадження.

КОБИЛЯЦЬКИЙ Андрій показав розуміння проблеми дослідження, бачення теоретичних і практичних напрямів її розв'язання, довів володіння методами наукового аналізу та проявив себе як організований, відповідальний виконавець.

Це дозволяє оцінити кваліфікаційну роботу здобувача КОБИЛЯЦЬКОГО Андрія на оцінку "добре" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Володимир ШУЛЬГА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____ 2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Кобиляцький А.А. допускається до захисту цієї роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну бакалаврську роботу

здобувача вищої освіти КОБИЛЯЦЬКИЙ Андрій
на тему “Zero Trust Architecture у захисті організаційних ІТ-систем: теорія та практична реалізація”

Актуальність. У сучасних умовах цифрової трансформації організаційні ІТ-системи функціонують у гібридних, хмарних і віддалених середовищах, де традиційна периметрова модель захисту вже не забезпечує достатнього рівня безпеки. Zero Trust Architecture передбачає постійну перевірку користувачів, пристроїв і запитів доступу, що дає змогу мінімізувати ризики несанкціонованого доступу, витоку даних і горизонтального переміщення зловмисників у мережі. З огляду на це тема кваліфікаційної роботи є актуальною та практично значущою.

Позитивні сторони.
1. У роботі досліджено теоретичні засади та принципи Zero Trust Architecture.
2. Розглянуто сучасні загрози організаційним ІТ-системам і підходи до контролю доступу.
3. Проаналізовано практичну реалізацію архітектури нульової довіри на базі рішення Xage.
4. Сформульовано рекомендації щодо впровадження Zero Trust Architecture в організації.

Недоліки.

Доцільно було б ширше висвітлити економічну оцінку впровадження Zero Trust Architecture та порівняти кілька вендорських платформ за єдиними критеріями ефективності.

Однак зазначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувач КОБИЛЯЦЬКИЙ Андрій заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____
підпис Ім’я, ПРІЗВИЩЕ

ё

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню Zero Trust Architecture у захисті організаційних ІТ-систем. Робота складається зі вступу, трьох розділів, висновків і переліку посилань. Ілюстративний матеріал містить 8 рисунків і 5 аналітичних таблиць.

Метою роботи є дослідження теоретичних засад Zero Trust Architecture та розроблення практичних рекомендацій щодо її реалізації в організаційних ІТ-системах.

Об'єктом дослідження є процес забезпечення кібербезпеки організаційних ІТ-систем.

Предмет дослідження – принципи, методи та інструменти реалізації Zero Trust Architecture у захисті організаційних ІТ-систем.

Методи дослідження. Для досягнення мети використано методи аналізу та синтезу, порівняння, класифікації, узагальнення, системного підходу, а також аналіз технічної документації та практик упровадження Zero Trust Architecture.

Як результат у роботі проаналізовано загрози організаційним ІТ-системам, розкрито принципи архітектури нульової довіри, досліджено підходи до контролю доступу, розглянуто практичну реалізацію на базі Xage та сформовано рекомендації щодо впровадження Zero Trust Architecture.

Галузь застосування. Результати дослідження можуть бути використані фахівцями з кібербезпеки, адміністраторами ІТ-інфраструктури та керівниками служб інформаційної безпеки під час проєктування й упровадження архітектури Zero Trust.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРБЕЗПЕКА, ОРГАНІЗАЦІЙНІ ІТ-СИСТЕМИ, ZERO TRUST ARCHITECTURE, НУЛЬОВА ДОВІРА, ZTNA, КОНТРОЛЬ ДОСТУПУ, БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ, МІКРОСЕГМИНТАЦІЯ, XAGE.

ABSTRACT

The qualification thesis is devoted to the study of Zero Trust Architecture in the protection of organizational IT systems. The thesis consists of an introduction, three chapters, conclusions, and references. The illustrative material includes 8 figures and 5 analytical tables.

The purpose of the thesis is to study the theoretical foundations of Zero Trust Architecture and to develop practical recommendations for its implementation in organizational IT systems.

The object of the research is the process of ensuring cybersecurity of organizational IT systems.

The subject of the research is the principles, methods, and tools for implementing Zero Trust Architecture in the protection of organizational IT systems.

Research methods. The thesis applies analysis and synthesis, comparison, classification, generalization, a systems approach, and analysis of technical documentation and practical Zero Trust implementation practices.

As a result of the research, threats to organizational IT systems were analyzed, the principles of Zero Trust Architecture were examined, access control approaches were studied, implementation based on Xage was considered, and practical recommendations for Zero Trust deployment were developed.

Field of application. The research results can be used by cybersecurity specialists, IT infrastructure administrators, and information security managers when designing and implementing Zero Trust Architecture.

Keywords: INFORMATION SECURITY, CUBERSECURITY, ORGANIZATION IT SYSTEM, ZERO TRUST ARCHITECTURE, ZTNA, ACCESS CONTROL, MULTI-FACTOR AUTHENTICATION, MICROSEGMENTATION, XAGE.

ë

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ZTNA - Zero Trust Network Access

ZTA – Zero Trust Architecture

ZTP – Zero Trust Platform

SIEM – Security Information and Event Management

MFA – Multi-Factor Authentication

NAC – Network Access Control

NGFW – Next-Generation Firewall

SASE – Secure Access Service Edge

SWG – Secure Web Gateway

IoT – Internet of Things

IPS – Intrusion Prevention System

ё

ВСТУП

Актуальність теми. У сучасних умовах цифрової трансформації організації дедалі частіше використовують хмарні сервіси, віддалений доступ, мобільні пристрої та розподілені інформаційні платформи. Через це класична периметрова модель захисту, яка ґрунтується на припущенні про довіру до внутрішньої мережі, втрачає ефективність. Zero Trust Architecture пропонує інший підхід: кожен користувач, пристрій, сервіс і запит на доступ мають постійно перевірятися незалежно від їхнього розташування. Така модель дозволяє зменшити площину атаки, обмежити горизонтальне переміщення зловмисників і підвищити стійкість організаційних ІТ-систем до сучасних кіберзагроз.

Мета роботи – дослідження теоретичних засад Zero Trust Architecture та розроблення практичних рекомендацій щодо її реалізації в захисті організаційних ІТ-систем.

Об’єкт дослідження – процес забезпечення кібербезпеки організаційних ІТ-систем.

Предмет дослідження – принципи, методи та інструменти реалізації Zero Trust Architecture у захисті організаційних ІТ-систем.

Для досягнення мети в роботі поставлено такі завдання:

1. Дослідити особливості захисту організаційних ІТ-систем на основі Zero Trust Architecture та визначити основні проблеми її впровадження в сучасних умовах.
2. Проаналізувати теоретичні засади, принципи та ключові складові Zero Trust Architecture у контексті захисту організаційних ІТ-систем.
3. Оцінити сучасні підходи, методи та практики забезпечення кібербезпеки, що застосовуються в межах Zero Trust Architecture.
4. Дослідити та обґрунтувати використання основних технологічних засобів реалізації Zero Trust Architecture, зокрема

багатофакторної автентифікації, механізмів управління доступом і перевірки довіреності пристроїв.

5. Розробити рекомендації щодо впровадження Zero Trust Architecture для підвищення рівня захищеності організаційних ІТ-систем.

Оцінити ефективність застосування Zero Trust Architecture для захисту організаційних ІТ-систем в умовах використання хмарних технологій, дистанційної роботи та мобільного доступу до корпоративних ресурсів.

Методи дослідження. Методологічною основою дослідження є аналіз наукових джерел, порівняння підходів до контролю доступу, класифікація кіберзагроз, системний аналіз архітектури Zero Trust, а також узагальнення практик упровадження технологічних рішень для захисту організаційних ІТ-систем.

Практичне значення одержаних результатів. За результатами дослідження розроблено структурований варіант реалізації Zero Trust Architecture та рекомендації щодо впровадження контролю доступу, багатофакторної автентифікації, мікросегментації, моніторингу подій безпеки й управління ризиками в організаційних ІТ-системах.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 25 лютого 2026 року.

ё

Розділ 1. ОСОБЛИВОСТІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

1.1. Дослідження основних загроз інформаційних систем організації

У сучасному інформаційному суспільстві, де цифрові технології стрімко проникають у всі сфери життя, питання кібербезпеки набуває особливої актуальності для громадян, підприємств і державних установ. Активний розвиток інформаційно-комунікаційних технологій супроводжується не лише появою нових можливостей, але й значним збільшенням кількості кіберзагроз та різновидів атак. Саме тому постійний моніторинг, дослідження та оцінювання актуальних ризиків є необхідною умовою ефективного захисту інформаційних ресурсів.

Кібербезпека охоплює комплекс організаційних, технічних і програмних заходів, спрямованих на захист комп'ютерних систем, серверного обладнання, мобільних пристроїв, мережевої інфраструктури та цифрових даних від несанкціонованого втручання, викрадення або пошкодження. Основною метою кіберзахисту є забезпечення конфіденційності, цілісності та доступності інформації, а також підтримання стабільного функціонування інформаційних систем.

Протягом останніх років сфера кібербезпеки істотно ускладнилася через швидкі темпи розвитку цифрових технологій і постійне вдосконалення методів, які використовують кіберзлочинці. Щодня виявляються нові вразливості програмного забезпечення та способи компрометації інформаційних систем, що створює додаткові ризики для користувачів, організацій і державних структур.

Розуміння сучасних кіберзагроз є важливою передумовою формування ефективної системи захисту інформації. Аналіз нових методів атак дозволяє організаціям завчасно впроваджувати заходи безпеки, удосконалювати політики захисту даних і підвищувати рівень обізнаності працівників щодо можливих ризиків. Водночас користувачі можуть покращувати власну цифрову безпеку

шляхом використання складних паролів, регулярного оновлення програмного забезпечення та обережного ставлення до підозрілих електронних повідомлень і вебресурсів.

Для ефективної протидії сучасним загрозам фахівці з інформаційної безпеки повинні постійно відстежувати нові тенденції у сфері кіберзлочинності, аналізувати вразливості та вивчати актуальні сценарії атак. Важливим є застосування комплексного підходу до захисту, який поєднує сучасні технологічні рішення, навчання персоналу та систематичний аналіз кіберзагроз. Крім того, результативна боротьба з кіберзлочинністю потребує тісної взаємодії між державними органами, приватним сектором та громадянами для оперативного обміну інформацією та вироблення спільних механізмів реагування.

Кіберзагрози можуть спричиняти суттєві економічні збитки як для окремих користувачів, так і для організацій. Одним із найбільш небезпечних наслідків є прямі фінансові втрати, що виникають у результаті викрадення коштів або отримання зловмисниками доступу до конфіденційної фінансової інформації. Такі інциденти нерідко супроводжуються необхідністю компенсації збитків, проведенням розслідувань та відновленням скомпрометованих систем.

Крім безпосередніх фінансових втрат, кіберінциденти можуть негативно впливати на безперервність бізнес-процесів. Наприклад, атаки із застосуванням програм-вимагачів часто блокують доступ до даних і критично важливих інформаційних ресурсів до моменту виконання вимог зловмисників. Це призводить до простоїв, зниження продуктивності та втрати прибутку. Додаткові витрати виникають у зв’язку з необхідністю відновлення працездатності систем і впровадженням додаткових механізмів захисту.

Вагомим фактором фінансових ризиків є також штрафні санкції та юридичні витрати, пов’язані з порушенням вимог щодо захисту інформації. У випадку витоку персональних даних або недотримання нормативних вимог організації можуть бути притягнуті до відповідальності та зазнати значних фінансових втрат. Окрім цього, додаткові витрати можуть виникати через

ё

необхідність залучення юридичних консультантів для врегулювання правових наслідків кіберінцидентів.

Не менш важливими є непрямі збитки, пов’язані з погіршенням ділової репутації та втратою довіри клієнтів. Якщо організація не забезпечує належний рівень захисту інформації та стає жертвою витоку даних або іншого інциденту, це може негативно позначитися на її іміджі. Наслідком часто стає скорочення клієнтської бази, зниження прибутковості та послаблення конкурентних позицій на ринку. Відновлення позитивної репутації після серйозного порушення безпеки зазвичай потребує значних фінансових і часових ресурсів.

Репутаційні наслідки кіберзагроз

Кіберінциденти здатні суттєво впливати на ділову репутацію організації. У разі витоку інформації або успішної кібератаки рівень довіри з боку клієнтів, партнерів та інших зацікавлених сторін може значно знизитися. Одним із ключових факторів, який формує ставлення користувачів до компанії, є впевненість у надійному захисті їхніх персональних даних.

Якщо організація не забезпечує належний рівень інформаційної безпеки, а конфіденційні відомості клієнтів стають доступними стороннім особам, це створює відчуття небезпеки та невпевненості. За таких умов клієнти можуть відмовитися від подальшої співпраці та обрати інші компанії, які гарантують вищий рівень захисту інформації. Крім того, суспільство може сприймати таку організацію як недостатньо компетентну або недбалу у питаннях кібербезпеки, що додатково погіршує її імідж.

Негативні наслідки поширюються не лише на взаємовідносини з клієнтами. Постачальники, ділові партнери та інвестори також можуть втратити впевненість у здатності компанії забезпечувати захист конфіденційних відомостей. Це нерідко призводить до припинення співпраці, скорочення інвестицій або відмови від нових партнерських проєктів, що негативно впливає на подальший розвиток підприємства.

Суттєву роль у формуванні громадської думки після кіберінциденту відіграють засоби масової інформації та реакція суспільства. Від того, наскільки

оперативно й прозоро компанія інформує про інцидент та вживає заходів для усунення його наслідків, залежить рівень довіри до неї. Несвоєчасна реакція, приховування деталей або недооцінка масштабів проблеми можуть викликати негативний суспільний резонанс і стати причиною тривалої репутаційної кризи.

У довгостроковій перспективі репутаційні втрати можуть мати не менш серйозні наслідки, ніж прямі фінансові збитки. Відновлення позитивного іміджу потребує значних ресурсів, а також тривалого часу для повернення довіри клієнтів і партнерів. Саме тому сучасні організації повинні приділяти особливу увагу розвитку систем кіберзахисту та мати чітко визначені процедури реагування на інциденти інформаційної безпеки.

Порушення конфіденційності інформації

Одним із найнебезпечніших наслідків кіберзагроз є порушення конфіденційності даних. Вплив таких інцидентів поширюється не лише на окремих користувачів, а й на підприємства, державні установи та суспільство загалом. У сучасному цифровому середовищі інформація стала одним із найцінніших ресурсів, тому її компрометація може спричинити значні негативні наслідки.

Передусім кіберзагрози можуть призвести до несанкціонованого доступу до персональних і конфіденційних відомостей. У результаті зловмисники отримують можливість використовувати викрадені дані для фінансового шахрайства, підробки документів або інших протиправних дій. Потерпілі можуть втратити доступ до банківських рахунків, зазнати фінансових збитків або зіткнутися з використанням їхніх персональних даних без дозволу. Такі події часто мають не лише матеріальні, а й психологічні наслідки для постраждалих осіб.

Серйозним ризикам піддаються також організації. У випадку витоку даних можуть бути скомпрометовані відомості про клієнтів, комерційні секрети, результати наукових розробок або інтелектуальна власність. Подібні інциденти негативно впливають на конкурентоспроможність підприємств, спричиняють фінансові втрати та можуть стати підставою для судових спорів. Особливо

ё

вразливими є малі та середні підприємства, які часто не мають достатніх ресурсів для впровадження комплексних засобів захисту.

Порушення конфіденційності також негативно впливає на рівень суспільної довіри до цифрових сервісів. Побоювання щодо безпеки особистих даних можуть змушувати користувачів обмежувати використання електронної комерції, онлайн-банкінгу, соціальних мереж та інших цифрових платформ. У результаті це стримує розвиток цифрової економіки та зменшує можливості для впровадження інноваційних технологій.

Таким чином, забезпечення конфіденційності інформації є одним із ключових завдань сучасної кібербезпеки. Ефективний захист персональних і корпоративних даних дозволяє мінімізувати ризики фінансових втрат, зберегти довіру користувачів та сприяти стабільному розвитку цифрового суспільства.

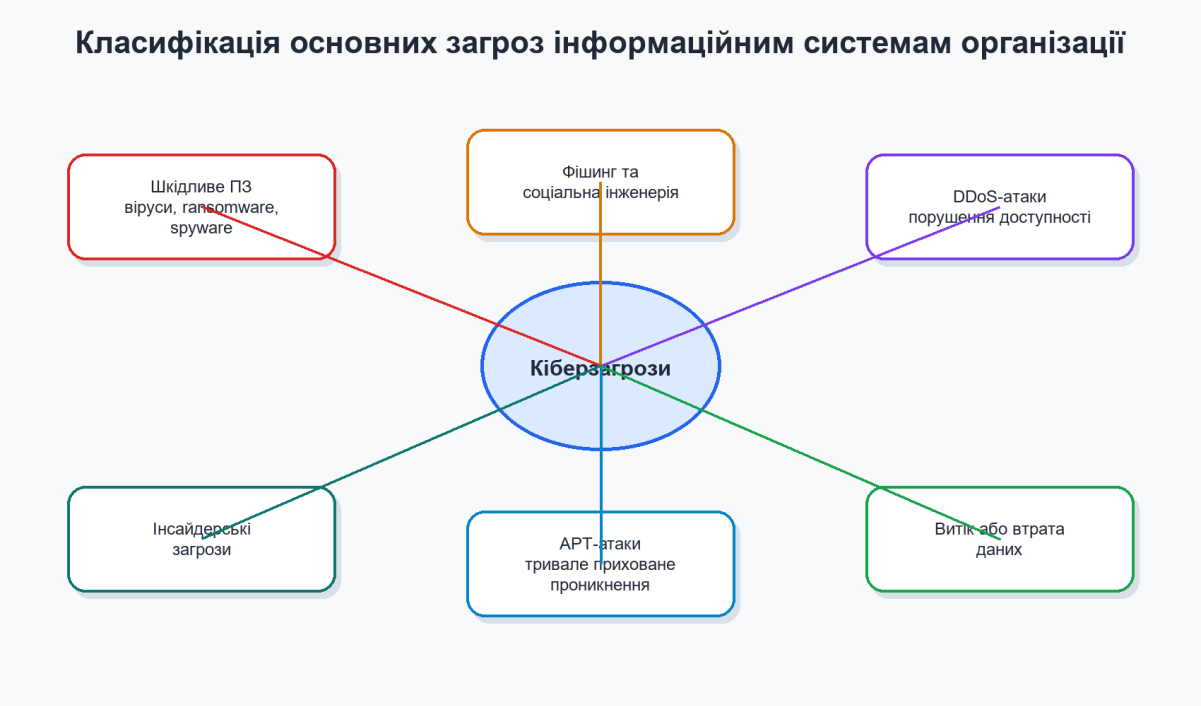

Рис. 1.1. Класифікація основних загроз інформаційним системам організації

Таблиця 1.1

Основні типи кіберзагроз та заходи їх мінімізації

Тип загрози	Прояв	Можливі наслідки	Заходи мінімізації
Шкідливе програмне забезпечення	Віруси, трояни, ransomware, spyware	Порушення доступності, витік або шифрування даних	Антивірусний захист, оновлення, резервне копіювання
Фішинг і соціальна інженерія	Підроблені листи, вебсторінки, дзвінки	Компрометація облікових записів, фінансові втрати	MFA, навчання персоналу, фільтрація пошти
DDoS-атаки	Перевантаження сервісів великою кількістю запитів	Недоступність сервісів і простої бізнес-процесів	Фільтрація трафіку, CDN, план реагування
Інсайдерські загрози	Зловживання правами доступу або помилки працівників	Витік даних, несанкціоновані зміни	Мінімальні привілеї, аудит, розподіл ролей
APT-атаки	Тривале приховане перебування в інфраструктурі	Шпигунство, викрадення критичних даних	SIEM, мікросегментація, аналіз поведінки

Джерело: сформовано автором.

1. Шкідливе програмне забезпечення

Шкідливе програмне забезпечення (Malware) являє собою сукупність програмних засобів, створених для завдання шкоди комп’ютерним системам, мережам або користувачам. До цієї категорії належать комп’ютерні віруси, мережеві черви, троянські програми, програми-вимагачі, шпигунське програмне забезпечення, рекламні модулі та інші небезпечні застосунки.

Поширення шкідливого програмного забезпечення може здійснюватися через вкладення електронної пошти, заражені вебресурси, завантаження програм із ненадійних джерел або використання вразливостей програмного забезпечення. Після проникнення до системи такі програми здатні викрадати конфіденційні дані, змінювати або знищувати файли, порушувати роботу операційної системи та відкривати несанкціонований доступ до мережевих ресурсів.

Для мінімізації ризику зараження необхідно використовувати сучасні антивірусні рішення, регулярно оновлювати програмне забезпечення та контролювати джерела отримання файлів і програм.

ё

2. Соціальна інженерія

Соціальна інженерія є одним із найпоширеніших методів кібератак, який ґрунтується на психологічному впливі на людину. Основною метою такого підходу є отримання конфіденційної інформації або спонукання користувача до виконання дій, що можуть поставити під загрозу безпеку інформаційної системи.

Зловмисники часто використовують довіру, неуважність або недостатню обізнаність людей. Вони можуть видавати себе за представників банківських установ, співробітників технічної підтримки, колег чи керівників організації. До найбільш поширених методів належать фішингові повідомлення, телефонні дзвінки із запитом конфіденційних даних, створення фальшивих вебсайтів і підроблених профілів у соціальних мережах.

Також застосовуються фізичні методи впливу, зокрема проникнення до захищених приміщень під виглядом співробітника або відвідувача, а також створення вигаданих сценаріїв для отримання необхідної інформації.

Наслідками атак соціальної інженерії можуть бути крадіжка особистих даних, фінансове шахрайство, зараження систем шкідливим програмним забезпеченням або отримання несанкціонованого доступу до корпоративних ресурсів. Ефективний захист передбачає регулярне навчання персоналу, використання багатофакторної автентифікації та підвищення рівня обізнаності користувачів щодо сучасних методів шахрайства.

3. Фішинг

Фішинг є різновидом кібершахрайства, за якого зловмисники імітують діяльність легітимних організацій або сервісів з метою отримання персональних даних користувачів. Найчастіше об’єктами викрадення стають паролі, реквізити банківських карток, логіни або інша конфіденційна інформація.

Для реалізації атак використовуються підроблені електронні листи, повідомлення в месенджерах або вебсторінки, які зовні практично не відрізняються від справжніх ресурсів. Отримані в результаті атаки дані можуть бути використані для викрадення коштів, доступу до облікових записів або здійснення інших протиправних дій.

З метою захисту від фішингових атак користувачам рекомендується уважно перевіряти адреси відправників, не переходити за сумнівними посиланнями та не вводити особисті дані на неперевірених вебресурсах.

4. Програми-вимагачі

Програми-вимагачі (Ransomware) належать до категорії шкідливого програмного забезпечення, основною функцією якого є блокування або шифрування інформації користувача з подальшою вимогою викупу за її відновлення.

Зараження системи найчастіше відбувається через фішингові повідомлення, завантаження заражених файлів або експлуатацію наявних уразливостей програмного забезпечення. Після успішного проникнення програма шифрує файли та відображає повідомлення з вимогою сплатити певну суму коштів, зазвичай у криптовалюті.

Подібні атаки можуть спричиняти значні фінансові збитки, втрату критично важливих даних та порушення функціонування організацій. Для зменшення ризиків рекомендується регулярно створювати резервні копії інформації, своєчасно встановлювати оновлення безпеки та уникати відкриття підозрілих вкладень.

5. Атаки типу «відмова в обслуговуванні»

Атака типу DoS (Denial of Service) спрямована на порушення нормальної роботи інформаційної системи шляхом перевантаження її ресурсів великою кількістю запитів або даних. У результаті сервер, вебсайт чи мережева інфраструктура стають недоступними для легітимних користувачів.

Такі атаки можуть здійснюватися шляхом масового надсилання мережевих запитів, використання програмних вразливостей або залучення ботнетів — мереж заражених пристроїв, які одночасно генерують значний обсяг трафіку.

Наслідком DoS-атак можуть бути зупинка бізнес-процесів, фінансові втрати та погіршення якості надання послуг. Для протидії таким загрозам організації повинні впроваджувати системи моніторингу трафіку, механізми фільтрації запитів та мати підготовлений план реагування на інциденти.

ё

6. Розширені стійкі загрози (APT)

Розширені стійкі загрози (Advanced Persistent Threats, APT) являють собою складні цілеспрямовані кібератаки, які зазвичай здійснюються висококваліфікованими групами зловмисників або державними структурами. Їхньою метою є тривале приховане перебування в інформаційній системі для отримання доступу до цінної інформації або здійснення шпигунської діяльності.

APT-атаки зазвичай реалізуються поетапно. Спочатку проводиться збір інформації про ціль, після чого виконується проникнення до мережі, закріплення в системі та подальше переміщення між її сегментами. Завершальним етапом є викрадення, зміна або знищення конфіденційних даних.

Для приховування своєї діяльності зловмисники використовують спеціалізоване шкідливе програмне забезпечення, вразливості нульового дня та методи соціальної інженерії. Основними цілями таких атак є державні органи, фінансові установи, оборонні підприємства та організації, що працюють із цінною науковою чи комерційною інформацією.

Ефективний захист від APT потребує впровадження багаторівневої системи безпеки, яка включає сегментацію мережі, суворий контроль доступу, постійний моніторинг подій безпеки, регулярний аналіз вразливостей та підвищення рівня кіберграмотності персоналу.

1.2. Аналіз підходів до забезпечення безпеки інформаційних систем

Кіберзагрози мають значний вплив на діяльність комерційних підприємств, державних установ, громадських організацій та окремих користувачів. Фахівці у сфері інформаційної безпеки та науковці постійно працюють над розробленням нових превентивних методів, технологій і засобів захисту, спрямованих на підвищення рівня кібербезпеки.

Серед сучасних викликів особливе місце посідають атаки із застосуванням програм-вимагачів, а також ризики, пов’язані з активним впровадженням хмарних сервісів. Додатковими факторами небезпеки виступають потенційні вразливості мереж п’ятого покоління (5G) та стрімкий розвиток Інтернету речей

(IoT), до складу якого входять розумні побутові пристрої та інші підключені до мережі системи.

Постійне зростання кількості кіберзагроз стимулює розвиток новітніх технологій захисту інформації. У зв’язку з цим особливого значення набувають інноваційні рішення, створені для протидії актуальним кіберризикам і забезпечення належного рівня захисту цифрових ресурсів.

Нижче розглянуто найбільш поширені сучасні технології у сфері кібербезпеки, їхні принципи функціонування та основні напрями практичного застосування. Такі рішення використовуються для захисту інформаційних систем від постійно змінюваних загроз і підтримання стабільної роботи інформаційної інфраструктури.

Поведінкова аналітика (Behavioral Analytics)

Поведінкова аналітика є технологією аналізу даних, яка дозволяє досліджувати особливості взаємодії користувачів із вебресурсами, мобільними застосунками, інформаційними системами та мережевим середовищем. Засоби поведінкового аналізу активно застосовуються спеціалістами з кібербезпеки для виявлення потенційних вразливостей і загроз.

Аналіз поведінкових шаблонів дає змогу своєчасно виявляти аномальні події та нетипові дії, які можуть свідчити про підготовку або реалізацію кібератаки. Наприклад, система здатна зафіксувати надмірно великий обсяг даних, що передається з окремого пристрою, що може бути ознакою несанкціонованої активності. Додатковими індикаторами можливих загроз є виконання операцій у незвичний час або нетипова послідовність дій користувача.

До основних переваг поведінкової аналітики належать можливість раннього виявлення потенційних атак, прогнозування майбутніх інцидентів та автоматизація процесів моніторингу й реагування на загрози.

Блокчейн (Blockchain)

Блокчейн являє собою різновид розподіленої бази даних, у якій інформація зберігається у вигляді взаємопов’язаних блоків, об’єднаних за допомогою криптографічних механізмів. Особливістю цієї технології є те, що внесені дані

ё

можуть накопичуватися, однак їх зміна або видалення практично неможливі.

У сфері кібербезпеки блокчейн використовується для підвищення рівня захищеності інформаційних систем і пристроїв, створення надійних протоколів безпеки та мінімізації ризику несанкціонованого доступу до баз даних. Завдяки криптографічному захисту та децентралізованій архітектурі значно ускладнюється можливість компрометації інформації.

Серед переваг блокчейну варто відзначити підвищення конфіденційності користувачів, зниження впливу людського фактора, забезпечення прозорості операцій та скорочення витрат завдяки відсутності потреби у залученні третіх сторін для підтвердження достовірності даних.

Крім того, технологія усуває проблему централізованого зберігання інформації. Дані розміщуються у розподіленій мережі вузлів, що робить систему більш стійкою до атак і значно зменшує ймовірність успішного втручання з боку зловмисників.

Хмарне шифрування (Cloud Encryption)

Використання хмарних сервісів сприяє підвищенню ефективності діяльності організацій, розширює можливості надання віддалених послуг та дозволяє оптимізувати фінансові витрати. Водночас зберігання інформації у хмарному середовищі може збільшувати ризик її компрометації. Для зниження таких ризиків застосовується технологія хмарного шифрування, яка передбачає перетворення даних у зашифрований формат до моменту їх передачі до хмарного сховища.

Для реалізації процесу шифрування використовуються спеціальні криптографічні алгоритми. Доступ до зашифрованої інформації можуть отримати лише авторизовані користувачі, які володіють відповідними ключами дешифрування. Такий підхід значно зменшує ймовірність несанкціонованого доступу до даних та їх витоку.

Фахівці у сфері кібербезпеки вважають хмарне шифрування одним із найбільш ефективних засобів захисту інформації. Використання цієї технології перешкоджає отриманню доступу до даних сторонніми особами, підвищує

рівень довіри користувачів до хмарних сервісів та сприяє дотриманню нормативних вимог щодо захисту інформації.

Контекстно-залежна безпека (Context-Aware Security)

Контекстно-залежна безпека є сучасною технологією кіберзахисту, що забезпечує прийняття більш обґрунтованих рішень щодо надання доступу до інформаційних ресурсів у режимі реального часу.

Традиційні механізми контролю доступу зазвичай базуються на принципі прийняття рішення за схемою «дозволити» або «заборонити». Такий підхід не завжди враховує всі обставини доступу та може призводити до блокування легітимних користувачів, що негативно впливає на продуктивність роботи.

На відміну від традиційних методів, контекстно-залежний захист використовує додаткові параметри для оцінювання рівня довіри до користувача. До таких параметрів належать час підключення, географічне розташування, характеристики пристрою, репутація вебресурсів та інші контекстні фактори. Аналіз цієї інформації дозволяє більш точно визначати правомірність запиту на доступ.

Перевагою контекстно-залежної безпеки є оптимізація процесів доступу до даних та підвищення зручності роботи для авторизованих користувачів. Разом із тим використання такого підходу потребує особливої уваги до питань конфіденційності персональної інформації.

Штучний інтелект (Artificial Intelligence, AI)

Технології штучного інтелекту активно застосовуються для виявлення, аналізу та запобігання кіберзагрозам. За допомогою алгоритмів штучного інтелекту спеціалісти з інформаційної безпеки можуть оперативно виявляти підозрілу активність і реагувати на потенційні інциденти.

Водночас кіберзлочинці також використовують інструменти на основі штучного інтелекту для реалізації більш складних атак. Зокрема, до таких технологій належать дипфейки — штучно створені зображення, відео та аудіоматеріали, які можуть переконливо імітувати реальних людей або події. Крім того, застосовуються методи змагального машинного навчання, спрямовані

ё

на введення систем штучного інтелекту в оману шляхом подання спеціально підготовлених даних.

Для протидії таким загрозам використовуються захисні системи штучного інтелекту, які дозволяють досліджувати поведінку інформаційних систем, аналізувати можливі сценарії атак та своєчасно виявляти шкідливу активність. Використання штучного інтелекту також сприяє вдосконаленню алгоритмів захисту та підвищенню стійкості моделей машинного навчання до зовнішніх впливів.

Розширене виявлення та реагування (Extended Detection and Response, XDR)

Розширене виявлення та реагування (XDR) є сучасною технологією кібербезпеки, призначеною для комплексного моніторингу, виявлення та нейтралізації загроз. На відміну від традиційних систем захисту кінцевих точок, XDR охоплює не лише пристрої користувачів, але й мережеву інфраструктуру, хмарні сервіси та інші компоненти інформаційного середовища.

Головною особливістю XDR є здатність об’єднувати дані з різних джерел у єдину систему аналізу. Це дозволяє формувати цілісне уявлення про події безпеки та оперативно виявляти складні багатовекторні атаки.

Технологія забезпечує високий рівень автоматизації процесів аналізу загроз, підтвердження інцидентів та кореляції подій. Завдяки цьому зменшується кількість хибних спрацювань, скорочується час реагування на атаки та підвищується ефективність роботи фахівців з кібербезпеки.

Manufacturer Usage Description (MUD)

Manufacturer Usage Description (MUD) — це стандарт, розроблений Інженерною робочою групою Інтернету (IETF) для підвищення рівня безпеки пристроїв Інтернету речей у домашніх мережах та середовищі малого бізнесу.

Пристрої IoT часто є потенційними цілями мережевих атак, наслідком яких можуть стати витік конфіденційної інформації або порушення працездатності обладнання. Водночас механізми їх захисту повинні залишатися доступними та економічно доцільними.

Використання стандарту MUD дозволяє визначати допустимі сценарії мережевої взаємодії пристроїв і таким чином обмежувати можливості для реалізації атак. Завдяки цьому підвищується рівень захищеності IoT-пристроїв від розподілених атак типу відмови в обслуговуванні (DDoS), а також зменшуються потенційні збитки у разі успішного проникнення зловмисників.

Zero Trust

Традиційні підходи до мережевої безпеки ґрунтувалися на принципі «довіряй, але перевіряй», який передбачав високий рівень довіри до користувачів, що перебувають усередині корпоративної мережі. Архітектура Zero Trust використовує інший підхід, сформульований принципом «ніколи не довіряй, завжди перевіряй».

Модель Zero Trust вимагає обов'язкової автентифікації та перевірки кожного користувача перед наданням доступу до інформаційних ресурсів або програмних сервісів організації.

Рис. 1.2. Еволюція моделей кіберзахисту від периметрової безпеки до Zero Trust

На відміну від традиційних систем, концепція нульової довіри не надає додаткових привілеїв користувачам лише через їхнє перебування в межах

ё

корпоративної мережі. Кожен запит на доступ перевіряється незалежно від місця його походження. Такий підхід дозволяє значно підвищити рівень захисту інформації та знизити ризик внутрішніх і зовнішніх загроз.

1.3. Аналіз моделей контролю доступу

Рис. 1.3. Моделі контролю доступу в інформаційних системах

Таблиця 1.3

Порівняння моделей контролю доступу

Модель	Основна ідея	Переваги	Обмеження
DAC	Права визначає власник ресурсу	Гнучкість і простота адміністрування	Висока залежність від дій користувача
MAC	Доступ задається рівнями секретності	Жорсткий контроль критичних ресурсів	Складність налаштування та низька гнучкість
RBAC	Права надаються відповідно до ролей	Зручність для організаційної структури	Ролі потребують постійного перегляду
ABAC	Рішення ґрунтуються на атрибутах і контексті	Точні політики доступу	Складність опису та супроводу політик
Zero Trust	Кожен запит перевіряється незалежно від розташування	Адаптивний контроль і мінімізація довіри	Потребує зрілої ідентифікації та моніторингу

Джерело: сформовано автором.

В умовах сучасних інформаційних систем надання необмеженого доступу до корпоративних ресурсів і сервісів становить серйозну загрозу для інформаційної безпеки. Практика показує, що кіберзлочинці можуть атакувати організації будь-якого масштабу незалежно від сфери діяльності. Одним із найбільш поширених способів компрометації інформаційних систем є отримання несанкціонованого доступу до легітимних облікових записів користувачів, що часто стає наслідком фішингових кампаній або викрадення облікових даних.

Для мінімізації подібних ризиків організації впроваджують механізми автентифікації та авторизації, які визначають порядок доступу до інформаційних ресурсів. Контроль доступу виступає одним із ключових елементів системи захисту, забезпечуючи визначення користувачів, процесів або програм, яким дозволено взаємодіяти з певними ресурсами та виконувати конкретні дії.

Під час розробки політик безпеки компанії враховують вимоги захисту інформації, особливості IT-інфраструктури та нормативно-правові вимоги. Варто зазначити, що механізми контролю доступу поширюються не лише на співробітників, а й на програмні компоненти, сервіси та автоматизовані процеси.

Сучасні технології керування доступом значно перевершують традиційні методи захисту. Використання смарт-карток, біометричних засобів і хмарних платформ забезпечує підвищення рівня безпеки, зручність адміністрування та підтримку віддаленої роботи. Такі рішення дозволяють автоматизувати управління користувачами, реалізовувати детальне розмежування прав доступу та інтегруватися з іншими компонентами системи безпеки для формування єдиного захисного середовища.

Основні моделі контролю доступу

Для регулювання взаємодії користувачів із ресурсами організації застосовуються різні моделі контролю доступу. Кожна з них визначає власні правила надання, зміни або відкликання дозволів і характеризується певним рівнем централізації, гнучкості та безпеки.

Обов'язковий контроль доступу (MAC)

ё

Модель Mandatory Access Control (MAC) базується на централізованому управлінні правами доступу та забезпечує один із найвищих рівнів захисту інформації. У межах цієї моделі всі рішення щодо доступу приймаються централізовано адміністраторами або власниками системи, тоді як звичайні користувачі не мають можливості змінювати або делегувати свої привілеї.

Доступ до ресурсів визначається за допомогою спеціальних міток безпеки, які присвоюються як користувачам, так і об’єктам інформаційної системи. Доступ дозволяється лише за умови відповідності рівнів класифікації та допуску.

Початково модель MAC була розроблена для військових і розвідувальних структур, однак сьогодні активно використовується в державному секторі, фінансових установах та інших організаціях, що працюють із критично важливою інформацією.

У рамках MAC широко застосовуються дві концептуальні моделі безпеки:

Модель Biba орієнтована на забезпечення цілісності інформації. Вона дозволяє користувачам нижчих рівнів доступу переглядати інформацію вищих рівнів, але обмежує можливість внесення змін до неї.

Модель Bell-LaPadula спрямована насамперед на забезпечення конфіденційності даних. Вона передбачає суворий контроль доступу відповідно до рівнів секретності та широко використовується в урядових і військових системах.

Переваги MAC:

- високий рівень централізованого контролю;
- чітке дотримання політик безпеки;
- ефективне розмежування доступу за допомогою міток безпеки.

Недоліки MAC:

- складність впровадження та адміністрування;
- обмеження співпраці між користувачами;
- значні витрати на підтримку актуальності політик і класифікацій.

Дискреційний контроль доступу (DAC)

Модель Discretionary Access Control (DAC) надає власникам ресурсів

можливість самостійно визначати, хто може отримати доступ до їхніх даних або сервісів. Для цього використовуються списки контролю доступу (ACL), які містять інформацію про дозволи для окремих користувачів або груп.

На відміну від MAC, модель DAC є більш гнучкою, оскільки дозволяє делегувати права доступу без необхідності централізованого погодження кожної зміни.

Переваги DAC:

- простота використання;
- висока гнучкість у налаштуванні дозволів;
- швидке надання доступу новим користувачам.

Недоліки DAC:

- підвищений ризик надлишкових привілеїв;
- складність централізованого контролю;
- можливість виникнення помилок через людський фактор.

Контроль доступу на основі ролей (RBAC)

Role-Based Access Control (RBAC) є однією з найпоширеніших моделей управління доступом у сучасних організаціях. Основна ідея полягає в тому, що права доступу призначаються не конкретним користувачам, а ролям, які відповідають їхнім посадовим обов'язкам.

Користувачі об'єднуються в групи залежно від функціональних завдань, а кожна роль отримує набір дозволів, необхідних для виконання відповідних робочих процесів. Завдяки цьому значно спрощується адміністрування доступу та процес підключення нових співробітників.

Переваги RBAC:

- висока масштабованість;
- автоматизація управління доступом;
- централізоване адміністрування політик;
- зниження ризику надмірних привілеїв.

Недоліки RBAC:

- складність впровадження в масштабних організаціях;

ё

- можливість дублювання ролей;
- необхідність постійного перегляду структури ролей.

Контроль доступу на основі правил (RuBAC)

Rule-Based Access Control (RuBAC) реалізує управління доступом на основі заздалегідь визначених правил та умов. Рішення про надання доступу приймається з урахуванням різних параметрів, таких як час, місцезнаходження користувача, тип пристрою або інші контекстні фактори.

Подібний підхід особливо ефективний для організацій, яким необхідно обмежувати доступ залежно від конкретних умов використання системи. Водночас налаштування та підтримка таких правил можуть потребувати значних технічних знань і часу.

Архітектура Zero Trust

Концепція Zero Trust є сучасним підходом до забезпечення інформаційної безпеки та базується на принципі «ніколи не довіряй — завжди перевіряй». На відміну від традиційних моделей, які головним чином зосереджуються на захисті мережевого периметра, Zero Trust виходить із припущення, що потенційна загроза може знаходитися як поза межами мережі, так і всередині неї.

У межах цієї архітектури кожна спроба доступу до інформаційних ресурсів розглядається як потенційно небезпечна та потребує перевірки незалежно від місця розташування користувача чи пристрою. Доступ надається лише після успішної автентифікації, авторизації та перевірки відповідності встановленим політикам безпеки.

Ключова ідея Zero Trust полягає в тому, що організація повинна діяти так, ніби її інфраструктура вже перебуває під загрозою компрометації. Завдяки цьому всі запити постійно аналізуються, а механізми захисту адаптуються до нових кіберризиків і змін у середовищі. Такий підхід суттєво зменшує ймовірність несанкціонованого доступу та підвищує загальну стійкість інформаційної системи до сучасних кібератак.

Висновки до розділу 1

У першому розділі визначено основні загрози організаційним ІТ-системам, розглянуто наслідки кіберінцидентів і проаналізовано моделі контролю доступу. Обґрунтовано, що традиційні периметрові підходи не забезпечують достатнього рівня захисту в умовах хмарних сервісів, віддаленої роботи та мобільного доступу, тому організаціям доцільно переходити до адаптивних моделей безпеки.

ё

Розділ 2. ТЕОРЕТИЧНІ ЗАСАДИ ZERO TRUST ARCHITECTURE У ЗАХИСТІ ОРГАНІЗАЦІЙНИХ ІТ-СИСТЕМ

2.1. Концепція Zero Trust: основи, принципи та ключові особливості

Архітектура Zero Trust: концепція, принципи та особливості впровадження

Перехід від класичних моделей мережевої безпеки до архітектури Zero Trust став одним із найважливіших напрямів розвитку сучасних систем кіберзахисту. Традиційний підхід базувався на припущенні, що всі користувачі та пристрої, які перебувають усередині корпоративної мережі, є довіреними, тоді як основна увага приділялася захисту зовнішнього периметра від потенційних загроз. Однак зі зростанням кількості кібератак, внутрішніх порушень безпеки та складності сучасних загроз такий підхід поступово втратив свою ефективність.

На відміну від традиційної моделі, концепція Zero Trust ґрунтується на принципі «ніколи не довіряти за замовчуванням і завжди здійснювати перевірку». Будь-який запит на доступ до інформаційних ресурсів розглядається як потенційно небезпечний незалежно від того, чи надходить він із внутрішньої мережі, чи із зовнішнього середовища. У результаті кожен користувач, пристрій або програмний компонент повинен пройти процедури перевірки перед отриманням доступу до даних або сервісів.

Рис. 2.1. Ключові принципи концепції Zero Trust

Архітектура нульової довіри забезпечує більш гнучкий та адаптивний підхід до захисту цифрових активів організації. Постійна перевірка ідентичності користувачів та застосування принципу мінімально необхідних привілеїв дозволяють значно скоротити потенційну поверхню атаки та знизити ризик несанкціонованого доступу. Крім підвищення рівня захисту даних, така модель сприяє безпечній роботі віддалених співробітників, підрядників та партнерів.

Важливою перевагою Zero Trust є однакове застосування політик безпеки до всіх суб'єктів мережі незалежно від їхнього місцезнаходження. Такий підхід допомагає протидіяти різноманітним видам атак, зокрема DDoS-атакам, соціальній інженерії та спробам внутрішнього компрометування систем. Завдяки високій адаптивності архітектура здатна оперативно реагувати на нові кіберзагрози та зміни IT-інфраструктури.

Основні принципи архітектури Zero Trust

Концепція Zero Trust побудована навколо ідеї повної відсутності довіри до будь-якого запиту на доступ. Замість захисту лише мережевого периметра увага приділяється контролю кожної взаємодії всередині інформаційного середовища.

Фундамент архітектури складають три ключові принципи:

ё

Явна перевірка доступу.

Кожен користувач, пристрій або програмний сервіс повинен пройти процедури автентифікації та авторизації перед отриманням доступу до ресурсів. Додатково враховуються контекстні параметри, зокрема рівень безпеки пристрою, його конфігурація та поточний стан.

Принцип мінімальних привілеїв.

Користувачам надаються лише ті права, які необхідні для виконання їхніх безпосередніх обов'язків. Такий підхід реалізується через механізми Just Enough Access (JEA) та Just-In-Time Access (JIT), що дозволяє мінімізувати ризики компрометації облікових записів.

Припущення про можливість компрометації.

Zero Trust виходить із того, що порушення безпеки можуть відбутися будь-якої миті. Саме тому особлива увага приділяється сегментації мережі, моніторингу активності та обмеженню переміщення зловмисника між сегментами інфраструктури.

Завдяки такому підходу організації можуть своєчасно виявляти потенційні загрози та зменшувати можливі наслідки інцидентів інформаційної безпеки.

Сім основних компонентів архітектури Zero Trust

Для ефективного функціонування архітектура нульової довіри спирається на сім взаємопов’язаних складових.

Ідентифікація користувачів.

Доступ до інформаційних ресурсів надається лише після успішного підтвердження особи користувача. Для цього широко використовуються механізми багатофакторної автентифікації.

Контроль безпеки пристроїв.

Усі пристрої, які підключаються до мережі, повинні відповідати встановленим вимогам безпеки, регулярно оновлюватися та перебувати під централізованим управлінням.

Сегментація мережі.

Мережеве середовище розподіляється на окремі сегменти, що дозволяє

локалізувати потенційні інциденти та контролювати переміщення трафіку між зонами.

Захист інформації.

Конфіденційні дані повинні бути захищені шляхом використання криптографічних механізмів як під час зберігання, так і під час передавання.

Моніторинг та реагування.

Постійний аналіз мережевої активності дає змогу оперативно виявляти підозрілі дії та швидко реагувати на кіберінциденти.

Політики безпеки.

Система правил доступу повинна постійно оновлюватися відповідно до поточних ризиків, змін бізнес-процесів та нових видів загроз.

Мінімізація привілеїв.

Кожен користувач або пристрій отримує лише той рівень доступу, який є необхідним для виконання конкретних функцій.

Переваги та труднощі впровадження Zero Trust

Запровадження архітектури нульової довіри забезпечує суттєве підвищення рівня кібербезпеки організації. Регулярна перевірка всіх запитів на доступ значно ускладнює реалізацію атак, спрямованих на компрометацію облікових записів або викрадення даних. Додатково підвищується ефективність управління вразливостями завдяки постійному контролю точок доступу та своєчасному усуненню ризиків.

Водночас впровадження Zero Trust пов’язане з певними труднощами. Організації часто стикаються з необхідністю модернізації існуючої інфраструктури, перегляду політик безпеки та інтеграції нових технологічних рішень. Окрім фінансових витрат, важливим аспектом є підготовка IT-фахівців та навчання персоналу роботі в новому середовищі.

Незважаючи на складність переходу, практика демонструє, що інвестиції в архітектуру нульової довіри виправдовують себе завдяки значному зменшенню кількості інцидентів безпеки та підвищенню рівня захисту корпоративних ресурсів.

ё

Сфери застосування Zero Trust

Архітектура нульової довіри ефективно використовується як у великих корпораціях, так і в невеликих організаціях. Особливо актуальною вона є для галузей, що працюють із конфіденційною інформацією, зокрема фінансового сектору, медичних установ, державних органів та науково-дослідних організацій.

Разом із тим принципи Zero Trust успішно застосовуються й у малому бізнесі, забезпечуючи масштабований механізм захисту, який може розвиватися одночасно зі зростанням компанії. Гнучкість архітектури дозволяє адаптувати її до будь-яких умов експлуатації та специфіки діяльності організації.

Критерії вибору платформи Zero Trust

Під час вибору платформи для реалізації концепції Zero Trust необхідно враховувати декілька важливих характеристик.

По-перше, рішення повинно підтримувати сучасні механізми керування ідентифікацією та доступом (IAM), включаючи багатофакторну автентифікацію та контекстно-орієнтовані політики доступу.

По-друге, важливу роль відіграють можливості мікросегментації, які дозволяють розділяти мережу на окремі захищені зони та обмежувати поширення потенційних загроз.

По-третє, система повинна забезпечувати повну прозорість мережевих процесів, надаючи засоби моніторингу, журналювання подій та аналітики в режимі реального часу.

Таким чином, архітектура Zero Trust є одним із найперспективніших напрямів розвитку сучасних систем кібербезпеки. Завдяки принципам постійної перевірки, мінімізації привілеїв та безперервного контролю вона забезпечує високий рівень захисту цифрових ресурсів організації та ефективно протидіє сучасним кіберзагрозам.

2.2. Архітектура Zero Trust в інформаційному середовищі

У процесі впровадження архітектури Zero Trust Architecture (ZTA) використовується низка взаємопов’язаних логічних компонентів, які можуть

функціонувати як у локальному середовищі організації, так і у хмарній інфраструктурі. Концептуальна модель, наведена на

демонструє основні елементи архітектури та принципи їхньої взаємодії. Варто зазначити, що ця схема відображає логічну структуру системи, а не конкретну технічну реалізацію.

У представленій моделі точка прийняття рішень (Policy Decision Point, PDP) поділяється на два окремі логічні модулі: механізм політики (Policy Engine, PE) та адміністратор політики (Policy Administrator, PA). Взаємодія між усіма компонентами здійснюється через площину керування (Control Plane), тоді як передача прикладних даних відбувається через площину даних (Data Plane).

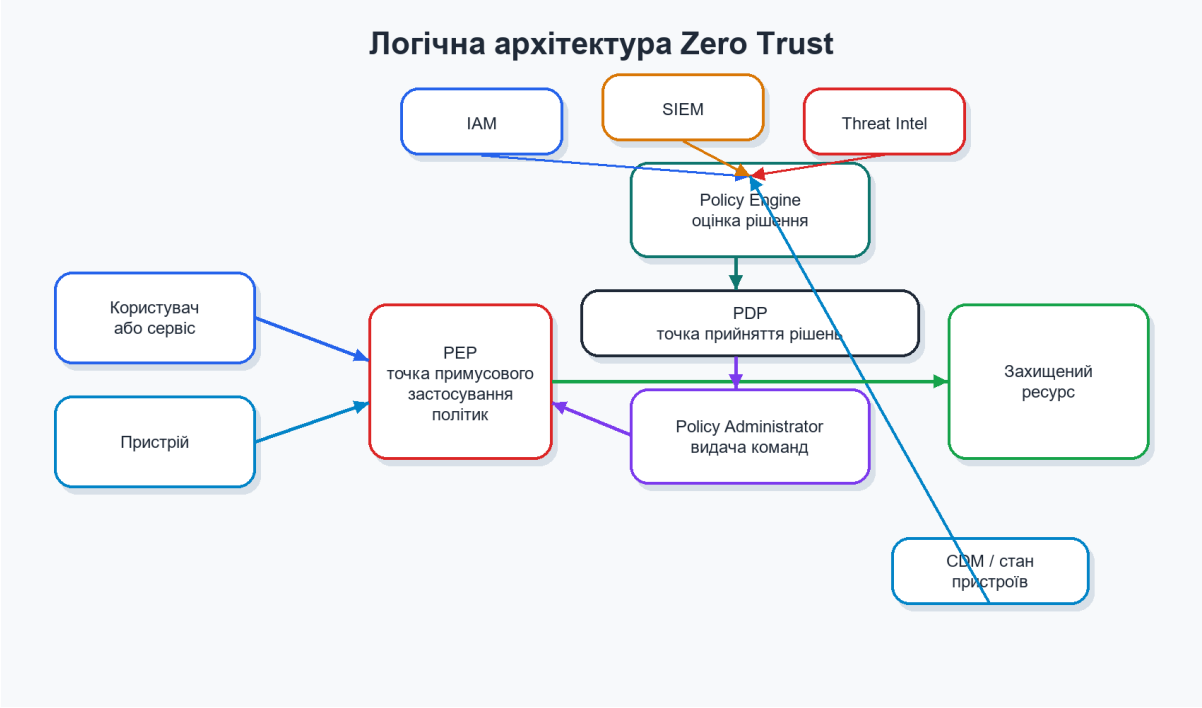

Рис. 2.2. Логічна архітектура Zero Trust

Опис основних компонентів Zero Trust Architecture

Механізм політики (Policy Engine, PE)

Механізм політики є центральним компонентом архітектури Zero Trust,

ё

який приймає остаточне рішення щодо надання або заборони доступу до певного ресурсу. Для формування рішення він використовує внутрішні політики безпеки підприємства, а також інформацію із зовнішніх джерел, таких як системи моніторингу стану активів, сервіси аналізу кіберзагроз та інші інформаційні платформи.

На основі отриманих даних PE виконує оцінку рівня довіри та визначає один із можливих результатів: дозволити доступ, відмовити в доступі або відкликати раніше надані права. Усі прийняті рішення реєструються та передаються адміністратору політики для подальшого виконання.

Адміністратор політики (Policy Administrator, PA)

Адміністратор політики відповідає за практичну реалізацію рішень, прийнятих механізмом політики. Основним його завданням є створення, підтримка або завершення каналу зв’язку між користувачем і ресурсом.

Крім цього, PA формує необхідні автентифікаційні атрибути, маркери доступу або тимчасові облікові дані, які використовуються під час встановлення сеансу взаємодії. Якщо доступ дозволено, адміністратор політики налаштовує відповідні компоненти системи для відкриття з’єднання. У випадку відмови або відкликання дозволу він ініціює його завершення.

У багатьох реалізаціях функції PE та PA можуть бути об'єднані в єдину службу, однак у концептуальній моделі вони розглядаються як окремі логічні елементи.

Пункт контролю виконання політик (Policy Enforcement Point, PEP)

PEP виконує функцію безпосереднього контролю мережевих взаємодій між суб'єктом та захищеним ресурсом. Він забезпечує запуск, супровід і завершення сеансів зв’язку відповідно до вказівок адміністратора політики.

Цей компонент може реалізовуватися як програмний агент на стороні користувача, як шлюз безпеки перед ресурсом або як окремий мережевий портал, який контролює весь вхідний та вихідний трафік. Саме через PEP здійснюється фактичне застосування політик доступу до корпоративних ресурсів.

За межами PEP розташовується довірена зона, де знаходяться інформаційні

ресурси підприємства, що підлягають захисту.

Додаткові джерела інформації для прийняття рішень

Окрім базових компонентів, архітектура Zero Trust використовує низку допоміжних систем, які забезпечують механізм політики актуальною інформацією для прийняття обґрунтованих рішень щодо доступу.

Система безперервної діагностики та усунення ризиків (CDM)

Дана система здійснює постійний моніторинг стану інформаційних активів організації. Вона збирає дані про версії операційних систем, рівень оновлень, наявність вразливостей та відповідність пристроїв встановленим вимогам безпеки.

Отримана інформація використовується для оцінки надійності пристрою, який ініціює запит на доступ до корпоративних ресурсів.

Система контролю відповідності нормативним вимогам

Цей компонент забезпечує дотримання організацією галузевих стандартів і законодавчих вимог у сфері інформаційної безпеки. До таких вимог можуть належати стандарти державного сектору, фінансової сфери, охорони здоров'я та інших критичних галузей.

На основі нормативних документів формуються внутрішні політики безпеки, що використовуються під час прийняття рішень про доступ.

Сервіси аналізу кіберзагроз

Джерела інформації про загрози надають актуальні відомості щодо нових вразливостей, шкідливого програмного забезпечення, компрометованих ресурсів та зафіксованих кібератак.

Інформація може надходити як із внутрішніх систем моніторингу, так і від зовнішніх постачальників аналітики кіберзагроз. Це дозволяє оперативно реагувати на нові ризики та коригувати політики доступу.

Журнали мережевої та системної активності

Системи журналювання збирають інформацію про дії користувачів, мережевий трафік, події безпеки та доступ до ресурсів. Аналіз цих даних забезпечує зворотний зв'язок щодо поточного стану захищеності інформаційної

ё

інфраструктури.

Політики доступу до даних

Політики доступу визначають набір правил, атрибутів та обмежень, які регламентують взаємодію користувачів із корпоративними ресурсами. Вони формуються відповідно до функціональних обов'язків працівників та бізнес-процесів організації.

Саме ці політики виступають базовою основою для процесів авторизації та контролю доступу.

Інфраструктура відкритих ключів (PKI)

PKI забезпечує створення, видачу та керування цифровими сертифікатами для користувачів, пристроїв, сервісів і програмних компонентів. Використання криптографічних сертифікатів дозволяє підвищити рівень довіри та безпеки процесів автентифікації.

Інфраструктура може бути як внутрішньою, так і інтегрованою з зовнішніми центрами сертифікації.

Система керування ідентифікацією (Identity Management System)

Система управління ідентифікацією відповідає за створення, зберігання та супровід облікових записів користувачів. Вона містить інформацію про ролі, атрибути доступу, закріплені пристрої та інші характеристики суб'єктів інформаційної системи.

Найчастіше такі системи інтегруються з каталогами LDAP, сервісами PKI та іншими механізмами автентифікації.

Система управління інформаційною безпекою та подіями (SIEM)

SIEM-платформа збирає та аналізує події безпеки з різних джерел інфраструктури. Отримані дані використовуються для виявлення підозрілої активності, формування звітності, вдосконалення політик безпеки та оперативного реагування на інциденти.

Завдяки централізованому аналізу подій SIEM значно підвищує ефективність функціонування архітектури Zero Trust та дозволяє своєчасно виявляти потенційні кіберзагрози.

2.3. Варіанти підходів до архітектури нульової довіри

Існує декілька підходів до впровадження архітектури Zero Trust Architecture (ZTA) в організаціях. Вони відрізняються набором використовуваних компонентів та джерелами формування політик безпеки. Незважаючи на відмінності в реалізації, усі підходи базуються на ключових принципах Zero Trust, проте можуть використовувати певні компоненти як основний механізм прийняття рішень щодо доступу. Повноцінна архітектура нульової довіри зазвичай поєднує елементи декількох моделей одночасно. До основних підходів належать удосконалене управління ідентифікацією, логічна мікросегментація та мережева сегментація.

Рисунок 2.3 – Підходи до впровадження архітектури Zero Trust

ё

Таблиця 2.3.

Порівняння підходів до реалізації Zero Trust Architecture

Підхід	**Ключовий механізм**	**Сфера застосування**	**Очікуваний результат**
Управління ідентичностями	IAM, MFA, життєвий цикл облікових записів	Користувачі, адміністратори, підрядники	Зменшення ризику компрометації доступу
Мікросегментація	Поділ мережі на ізольовані зони	Сервери, OT/IT-сегменти, критичні сервіси	Обмеження горизонтального переміщення
ZTNA	Доступ лише до конкретних застосунків	Віддалена робота, хмарні сервіси	Зменшення залежності від VPN
Поведінкова аналітика	Аналіз дій користувачів і пристроїв	SOC, SIEM, моніторинг інцидентів	Виявлення аномальної активності
Централізовані політики	Policy Engine і Policy Administrator	Управління доступом у розподіленому середовищі	Уніфіковане застосування правил безпеки

Джерело: сформовано автором.

Вибір конкретного варіанта залежить від особливостей діяльності організації, наявної IT-інфраструктури та вимог до безпеки. У деяких випадках певна модель є більш доцільною та простішою для впровадження, тоді як використання інших підходів може потребувати суттєвої перебудови бізнес-процесів і корпоративних мереж.

Використання розширеного управління ідентифікацією в ZTA

Одним із найпоширеніших способів побудови Zero Trust є модель, що базується на керуванні цифровими ідентичностями користувачів. У межах цього підходу саме ідентифікація суб'єкта виступає основою для формування політик доступу.

Політики безпеки створюються відповідно до ролей, атрибутів та прав конкретного користувача або сервісу. Головним критерієм доступу виступає набір привілеїв, призначених суб'єкту. Водночас на остаточне рішення можуть впливати й додаткові чинники, зокрема тип пристрою, його поточний стан безпеки, місцезнаходження користувача або інші параметри середовища.

У деяких випадках такі фактори можуть змінювати рівень довіри до

суб'єкта та впливати на обсяг дозволених дій, наприклад надавати лише частковий доступ до ресурсів або окремих наборів даних.

Подібні реалізації часто асоціюються з концепцією програмно-визначеного периметра (Software Defined Perimeter, SDP), яка активно використовує принципи програмно-визначених мереж (SDN) та мереж, орієнтованих на наміри (Intent-Based Networking, IBN).

У даній архітектурі адміністратор політики виконує роль мережевого контролера, який динамічно змінює конфігурацію мережі відповідно до рішень механізму політики. Запити користувачів надходять через точки контролю виконання політик (PEP), які перебувають під управлінням адміністратора політики.

Якщо така модель реалізується на прикладному рівні мережі (рівень 7 моделі OSI), найчастіше застосовується схема «агент–шлюз». У цьому випадку клієнтський агент та шлюз ресурсу формують захищений канал зв’язку, через який здійснюється взаємодія між користувачем і цільовим ресурсом. Аналогічні підходи можуть використовуватись також у хмарних середовищах, віртуальних мережах та інших спеціалізованих інфраструктурах.

Варіанти практичного розгортання архітектури

Усі компоненти Zero Trust є логічними сутностями і не обов'язково реалізуються окремими фізичними системами. Один сервер або сервіс може виконувати функції кількох логічних модулів, тоді як окремий компонент може складатися з декількох програмних чи апаратних елементів.

Наприклад, корпоративна інфраструктура відкритих ключів (PKI) може містити окремі сервіси для видачі сертифікатів користувачам та пристроям, проте використовувати єдиний кореневий центр сертифікації. У багатьох сучасних рішеннях Zero Trust функції Policy Engine та Policy Administrator часто інтегруються в один програмний продукт.

Вибір моделі розгортання залежить від архітектури підприємства, наявних інформаційних систем та особливостей бізнес-процесів.

Модель агент–шлюз

ё

У даному варіанті точка контролю виконання політики складається з двох частин. Перша розташовується на пристрої користувача у вигляді програмного агента, а друга знаходиться безпосередньо перед захищеним ресурсом та виконує функції шлюзу.

Агент перехоплює мережеві запити користувача та передає їх на перевірку. Шлюз забезпечує контроль доступу до ресурсу та пропускає лише ті з'єднання, які були авторизовані адміністратором політики.

У типовому сценарії співробітник використовує корпоративний ноутбук для підключення до внутрішньої системи підприємства. Запит надходить до агента, який передає його адміністратору політики. Після аналізу механізмом політики формується рішення щодо доступу.

Якщо запит схвалений, створюється захищений канал зв'язку між агентом та шлюзом. Для цього можуть використовуватися IP-адреси, мережеві порти, сеансові ключі шифрування та інші параметри безпеки. Після завершення роботи або виникнення інциденту безпеки з'єднання автоматично закривається.

Подібний підхід найбільш ефективний для організацій із централізованим управлінням пристроями та корпоративними ресурсами.

Модель анклавного шлюзу

Даний варіант є розвитком моделі агент–шлюз. Основна відмінність полягає в тому, що шлюз розташовується не перед кожним окремим ресурсом, а перед групою ресурсів або цілим сегментом інфраструктури.

Таким сегментом може бути локальний центр обробки даних, корпоративна хмара або група сервісів, що забезпечують виконання певного бізнес-процесу.

Подібна архітектура особливо корисна для захисту застарілих інформаційних систем, які не підтримують сучасні механізми інтеграції або API.

Перевагою підходу є можливість централізованого контролю доступу до великої кількості ресурсів. Водночас недоліком виступає менш деталізований контроль, оскільки шлюз захищає весь сегмент загалом, а не кожен окремий ресурс.

Модель порталу ресурсів

У цій архітектурі використовується єдина точка контролю доступу, яка виконує функції порталу для користувачів.

Портал може забезпечувати доступ як до одного ресурсу, так і до групи ресурсів, об'єднаних спільною бізнес-функцією. Прикладом може бути портал доступу до приватної хмарної інфраструктури або корпоративного дата-центру.

Головною перевагою моделі є відсутність необхідності встановлення спеціального програмного забезпечення на всі клієнтські пристрої. Це робить підхід зручним для реалізації політик BYOD та міжорганізаційної співпраці.

Однак через відсутність локального агента організація отримує менше інформації про стан кінцевого пристрою та може здійснювати його перевірку лише під час підключення до порталу. Крім того, така модель є більш вразливою до атак типу DoS або DDoS, тому шлюзові системи повинні мати високий рівень відмовостійкості.

Ізольоване середовище виконання програм

Ще одним різновидом архітектури агент–шлюз є використання ізольованих середовищ для запуску додатків.

У цьому випадку перевірені програми працюють у віртуальних машинах, контейнерах або інших ізольованих середовищах. Такий підхід дозволяє захистити критично важливі додатки навіть у разі компрометації основної операційної системи.

Доступ до ресурсів отримують лише ті програми, які працюють у захищеному середовищі та відповідають встановленим політикам безпеки.

Перевагою моделі є високий рівень ізоляції та захисту від шкідливого програмного забезпечення. Недоліком виступає складність адміністрування та необхідність постійної підтримки великої кількості ізольованих середовищ.

Алгоритм довіри

Центральним елементом архітектури Zero Trust виступає алгоритм довіри (Trust Algorithm, TA), який використовується механізмом політики для прийняття остаточного рішення щодо доступу.

ё

Алгоритм аналізує інформацію з різних джерел, включаючи політики безпеки, атрибути користувачів, характеристики пристроїв, поведінкові моделі та дані про актуальні кіберзагрози.

Основними джерелами даних для алгоритму є:

- запит на доступ до ресурсу;
- база даних користувачів та їх атрибутів;
- інформація про стан корпоративних активів;
- вимоги безпеки до конкретного ресурсу;
- дані систем аналізу кіберзагроз.

Кожному джерелу може бути призначена певна вага залежно від його важливості для організації. На основі комплексного аналізу формується рівень довіри до суб'єкта та приймається рішення щодо надання або відмови в доступі.

Після ухвалення рішення результат передається адміністратору політики, який налаштовує відповідні точки контролю виконання політик та забезпечує встановлення або завершення з’єднання. Крім того, адміністратор може ініціювати повторну автентифікацію користувача або достроково припинити сеанс у разі виникнення загроз безпеці чи завершення робочого процесу.Варіації алгоритму довіри

Існують різноманітні підходи до реалізації ТА. Розробники можуть по-різному визначати пріоритетність наведених вище чинників залежно від їхнього бачення важливості кожного з них. Також існують дві ключові характеристики, за допомогою яких можна розрізняти ТА. По-перше, це спосіб оцінювання факторів: як бінарних рішень або як зважених складових загального показника чи рівня довіри. По-друге, це спосіб аналізу запитів щодо інших запитів того самого суб’єкта, застосунку/служби або пристрою.

Критерії та бальна оцінка. ТА, що базується на критеріях, передбачає наявність набору визначених атрибутів, які мають бути виконані перед наданням доступу до ресурсу або дозволом на виконання певної дії (наприклад, читання чи запис). Такі критерії встановлюються підприємством і налаштовуються окремо для кожного ресурсу. Доступ або дія дозволяються лише за умови виконання всіх

встановлених вимог. Натомість ТА на основі бальної системи розраховує рівень довіри, використовуючи значення кожного джерела даних та вагові коефіцієнти, визначені підприємством. Якщо отриманий результат перевищує встановлений для ресурсу поріг, доступ надається або дія виконується.

У протилежному випадку запит відхиляється або права доступу обмежуються (наприклад, дозволяється лише перегляд файлу без можливості його редагування).

Одиничний та контекстний підходи. Одиничний ТА аналізує кожен запит окремо, не враховуючи попередню історію суб'єкта під час оцінювання. Такий підхід забезпечує швидше прийняття рішень, однак існує ризик, що атака залишиться непоміченою, якщо її дії не виходять за межі дозволеної ролі користувача. Контекстний ТА, навпаки, враховує нещодавню активність суб'єкта або мережевого агента під час перевірки запитів на доступ. Це вимагає від PE зберігання інформації про стан усіх суб'єктів і застосунків, проте значно підвищує ймовірність виявлення зловмисника, який використовує викрадені облікові дані та діє за нетиповим сценарієм для конкретного користувача.

Крім того, PE повинен отримувати інформацію про поведінку користувачів від PA та PEP, з якими взаємодіють суб'єкти під час роботи. Аналіз поведінкових моделей може застосовуватися для формування профілю допустимого використання, а відхилення від звичної поведінки можуть спричиняти додаткові перевірки автентифікації або блокування доступу до ресурсів.

Зазначені характеристики не обов'язково є взаємозалежними. Можна реалізувати ТА, який визначає рівень довіри для суб'єкта або пристрою та водночас оцінює кожен запит незалежно від попередніх. Проте контекстні ТА з бальною системою оцінювання забезпечують більш гнучке та деталізоване керування доступом, оскільки дозволяють оперативно адаптуватися до змінних умов і надавати актуальну оцінку надійності облікового запису значно швидше, ніж статичні політики, що змінюються адміністраторами вручну.

У ідеальному випадку алгоритм довіри ZTA має бути контекстним, хоча на практиці це не завжди можливо через обмеження наявної інфраструктури

ё

підприємства. Контекстний ТА здатний мінімізувати ризики у випадках, коли зловмисник діє в межах звичайних шаблонів доступу до скомпрометованого облікового запису або здійснює внутрішню атаку. Під час розроблення та впровадження алгоритмів довіри важливо знаходити баланс між рівнем безпеки, зручністю використання та економічною доцільністю. Постійні вимоги до повторної автентифікації користувача, поведінка якого відповідає типовим сценаріям його ролі та функціональних обов'язків, можуть негативно впливати на зручність роботи.

Наприклад, якщо працівник відділу кадрів зазвичай переглядає від 20 до 30 особових записів на день, контекстний ТА може сформувати попередження, коли кількість звернень раптово перевищить 100 записів. Аналогічно система може реагувати на спроби доступу поза межами звичайного робочого часу, що може свідчити про компрометацію облікового запису та викрадення інформації. Такі ситуації демонструють переваги контекстного підходу, який здатний виявити аномальну поведінку там, де одиничний ТА не помітить загрозу. Інший приклад — бухгалтер, який зазвичай працює з фінансовою системою вдень, але раптом намагається отримати доступ до неї вночі з невідомого місця.

Формування набору критеріїв або визначення вагових коефіцієнтів і порогових значень для кожного ресурсу потребує ретельного планування та тестування. На початковому етапі впровадження ZTA адміністратори можуть зіткнутися з ситуаціями, коли законні запити на доступ відхиляються через помилки конфігурації. Це зумовлює необхідність проходження етапу початкового налаштування системи. Для забезпечення дотримання політик без порушення бізнес-процесів може виникнути потреба у коригуванні критеріїв або ваг оцінювання. Тривалість такого періоду залежить від визначених підприємством показників ефективності та допустимого рівня помилкових відмов або необґрунтованих дозволів на доступ до ресурсів.

Компоненти мережі та середовища

У середовищі ZT має забезпечуватися логічне або фізичне розмежування потоків даних, які використовуються для адміністрування мережі, та потоків,

призначених для функціонування прикладних систем і сервісів. Зазвичай таке розділення реалізується через площину керування (control plane) та площину даних (data plane).

Площина керування використовується компонентами інфраструктури підприємства та постачальниками послуг для конфігурування й обслуговування активів, прийняття рішень щодо надання або блокування доступу до ресурсів, а також для створення маршрутів зв'язку між ресурсами. Площина даних призначена для фактичного обміну інформацією між програмними компонентами. Такий обмін може бути неможливим до моменту встановлення відповідного каналу через площину керування. Наприклад, PA та PEP можуть використовувати площину керування для створення маршруту між суб'єктом і корпоративним ресурсом, після чого застосунок або сервіс працюватиме через площину даних.

Вимоги до мережевої інфраструктури для підтримки ZTA

1. Корпоративні активи повинні мати базове мережеве підключення. Локальна мережа (LAN), незалежно від того, чи перебуває вона під контролем підприємства, забезпечує базову маршрутизацію та інфраструктурні сервіси, такі як DNS. Віддалені корпоративні активи можуть використовувати лише частину таких сервісів.

2. Підприємство повинно мати змогу ідентифікувати власні або керовані активи та визначати їхній поточний рівень захищеності. Для цього застосовуються корпоративні облікові дані, а не інформація, яку можна підробити, наприклад MAC-адреси.

3. Організація має забезпечувати моніторинг усього мережевого трафіку. Навіть якщо повна перевірка прикладного рівня недоступна для всіх пакетів, повинні реєструватися дані про їх проходження. Метадані з'єднань (адресати, час, ідентифікатори пристроїв тощо) використовуються для динамічного оновлення політик і підтримки процесу оцінювання доступу.

4. Доступ до корпоративних ресурсів має здійснюватися виключно через PEP. Ресурси не повинні приймати довільні підключення з Інтернету.

ë

Доступ надається лише після успішної автентифікації та авторизації клієнта через спеціально налаштовані канали. Такий підхід ускладнює проведення сканування мережі та DoS-атак. Водночас окремі елементи інфраструктури, наприклад DNS-сервери, можуть залишатися загальнодоступними.

5. Площини даних і керування повинні бути логічно відокремленими. PE, PA та PEP взаємодіють через спеціалізовану мережу керування, недоступну для звичайних корпоративних активів. Площина даних використовується лише для передачі прикладного трафіку.

6. Корпоративні активи повинні мати можливість підключатися до компонентів PEP, оскільки саме через них здійснюється доступ до ресурсів підприємства. Це може бути вебпортал, мережевий пристрій або програмний агент.

7. PEP є єдиним компонентом, який взаємодіє з адміністратором політик у межах бізнес-процесів. Усі корпоративні інформаційні потоки проходять через один або декілька PEP.

8. Віддалені корпоративні активи повинні мати прямий доступ до ресурсів підприємства без необхідності маршрутизації трафіку через корпоративну мережу. Наприклад, доступ до хмарної електронної пошти не повинен вимагати попереднього підключення через VPN.

9. Інфраструктура підтримки рішень щодо доступу в ZTA має бути масштабованою та здатною адаптуватися до змін навантаження. Компоненти PE, PA та PEP є критично важливими для функціонування бізнес-процесів, тому їхня недоступність або затримки можуть негативно вплинути на роботу організації.

Доступ корпоративних активів до певних ресурсів може обмежуватися відповідно до політик безпеки або інших факторів. Наприклад, мобільним пристроям може бути заборонено доступ до окремих ресурсів за межами країни розташування підприємства. Такі обмеження можуть залежати від географічного положення, типу пристрою або інших встановлених критеріїв.

У галузі кібербезпеки концепція Zero Trust Security вважається одним із найрезультативніших підходів, оскільки вона повністю відмовляється від

принципу довіри за замовчуванням. Модель Zero Trust Security використовує механізми керування ідентифікацією для захисту доступу користувачів до програмних систем та інфраструктури, виходячи з припущення, що потенційно ненадійні суб'єкти можуть перебувати як усередині корпоративної мережі, так і за її межами.

Виділяють п'ять основних практик впровадження Zero Trust Security в організаціях.

Багатофакторна автентифікація (MFA).

Для посилення захисту облікових записів рекомендується використовувати багатофакторну автентифікацію. Оскільки застосування лише паролів уже не забезпечує належного рівня безпеки, процес підтвердження особи може доповнюватися різними факторами автентифікації: інформацією, яку користувач знає, фізичними засобами, якими він володіє, або біометричними характеристиками. Такий механізм перевірки має поширюватися на всі категорії користувачів, зокрема звичайних і привілейованих співробітників, а також партнерів та клієнтів. Додаткові методи підтвердження особи є необхідними під час доступу до критично важливих даних або отримання розширених прав.

Перевірка пристроїв.

Кожен пристрій, який використовується для взаємодії з корпоративними ресурсами, повинен пройти реєстрацію та процедуру перевірки. Контроль ідентифікації має охоплювати всі кінцеві точки мережі. Використання систем управління мобільними пристроями дає змогу автоматизувати процес реєстрації сертифікатів і знизити витрати на адміністрування.

Забезпечення відповідності пристроїв політикам безпеки.

Пристрої повинні відповідати встановленим вимогам інформаційної безпеки, серед яких шифрування накопичувачів, актуальні версії антивірусного програмного забезпечення та своєчасне встановлення оновлень. Необхідно впроваджувати механізми моніторингу стану пристроїв і керування правилами доступу залежно від ролей або груп користувачів. Крім того, слід забезпечити автоматичне анулювання облікових даних пристрою у випадку його втрати,

ё

викрадення або блокування облікового запису користувача.

Принцип найменших привілеїв.

Надання доступу до ресурсів повинно здійснюватися лише в обсязі, необхідному для виконання посадових обов'язків. Адміністративні повноваження мають перебувати під постійним контролем, а доступ до критичних компонентів інфраструктури повинен бути максимально обмеженим. Цей принцип однаково стосується як адміністраторів, так і звичайних користувачів.

Використання адаптивних механізмів захисту.

Сучасні системи керування ідентифікацією застосовують технології машинного навчання для аналізу поведінки користувачів, пристроїв і програмних засобів. Наприклад, виявлення нетипових дій, таких як спроби доступу з незвичних географічних локацій або нових пристроїв, дає можливість динамічно коригувати рівень доступу та привілеїв відповідно до поточного рівня ризику.

Дотримання зазначених практик сприяє забезпеченню високого рівня захисту корпоративної інфраструктури та відповідає основним принципам концепції Zero Trust.

Zero Trust Access від Xage відкриває нові можливості для промислових підприємств, забезпечуючи оперативніше реагування на кіберінциденти та ефективнішу взаємодію між партнерами, постачальниками й іншими сторонніми організаціями. Водночас переваги віддаленого доступу не повинні супроводжуватися підвищенням рівня ризику. Кіберзловмисники регулярно використовують засоби віддаленого доступу для несанкціонованого проникнення до систем, викрадення конфіденційної інформації та поширення шкідливого програмного забезпечення. Саме тому рішення для віддаленого доступу повинні проєктуватися з урахуванням сучасних вимог безпеки та забезпечувати ефективний захист від подібних загроз [6].

Висновки до розділу 2

У другому розділі досліджено принципи Zero Trust Architecture, її логічні компоненти та основні підходи до впровадження. Показано, що ефективність архітектури нульової довіри забезпечується поєднанням багатофакторної автентифікації, мінімальних привілеїв, мікросегментації, постійного моніторингу та політик доступу, сформованих на основі контексту й оцінки ризику.

ё

Розділ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ZERO TRUST ARCHITECTURE У ЗАХИСТІ ОРГАНІЗАЦІЙНИХ IT-СИСТЕМ

3.1. Розгортання архітектури Zero Trust на базі рішення Xage

Традиційні підходи до забезпечення інформаційної безпеки та контролю доступу базуються на концепції мережевого периметра, відповідно до якої активи поділяються на довірені сегменти. У межах таких сегментів користувачам, програмам і пристроям автоматично надається певний рівень довіри та відповідні права доступу. Подібні зони можуть охоплювати тисячі пристроїв із різним функціональним призначенням та неоднаковою цінністю для організації. У разі компрометації навіть однієї робочої станції зловмисник може здійснювати горизонтальне переміщення мережею та отримувати доступ до значно важливіших і чутливіших ресурсів.

Модель безпеки Zero Trust розвиває традиційний підхід, забезпечуючи підвищений рівень захисту та водночас спрощуючи управління доступом. Архітектура Zero Trust Access (ZTA) розглядає цифрову ідентичність як основний периметр безпеки замість автоматичного надання довіри будь-якому об’єкта, який отримав доступ до певного сегмента мережі. Відповідно до принципів нульової довіри жоден користувач, програмний компонент чи пристрій не вважається надійним до моменту успішного проходження автентифікації та авторизації згідно з установленими політиками безпеки.

Для створення захищеного середовища використовуються цифрові ідентифікатори та облікові дані. Навіть після успішного підтвердження особи суб’єкту надається лише мінімально необхідний рівень доступу до ресурсів і тільки на період, необхідний для виконання конкретного завдання.

На відміну від традиційних механізмів ізоляції, таких як брандмауери та VPN, сучасні розподілені й масштабовані IT/OT-інфраструктури потребують рішень безпеки, заснованих на ідентифікації та реалізації принципів Zero Trust. Такий підхід поширюється не лише на користувачів і пристрої, а й на програмні

застосунки, сервіси та дані, які формують цифрову екосистему підприємства. Завдяки цьому організації можуть уникнути компромісів між функціональністю та безпекою, характерних для застарілих архітектур, що важко адаптуються до сучасних вимог.

Платформа Xage спрощує процес управління доступом, надаючи централізований механізм створення та застосування політик безпеки в межах усього середовища. Кожному користувачу, пристрою, програмі та інформаційному об’єкта присвоюється унікальний цифровий ідентифікатор, що забезпечує можливість реалізації детальних правил доступу та контролю їх виконання.

Додатково Xage підвищує рівень захищеності організації завдяки підтримці сучасних механізмів автентифікації та авторизації, включаючи складні паролі, багатофакторну автентифікацію (MFA) та інші засоби перевірки особи. Архітектура рішення побудована як високодоступна та відмовостійка мережа кібербезпеки, яку можна впровадити поверх наявної інфраструктури без необхідності заміни обладнання або модифікації мережевої топології.

Крім того, оскільки всі операції доступу до ресурсів контролюються та реєструються в захищеному середовищі Fabric, забезпечується повна видимість взаємодій між користувачами, програмами та технічними засобами в середовищі оперативних технологій (OT).

Сучасна інфраструктура підприємства може охоплювати виробничі майданчики, центри керування, центри обробки даних і хмарні платформи, між якими постійно відбувається взаємодія людей, програмних систем, пристроїв і даних. За таких умов важливо забезпечити можливість доступу до ресурсів без створення додаткових вразливостей для потенційних зловмисників. Традиційні інструменти захисту вже не забезпечують необхідного рівня деталізації контролю, тому виникає потреба у впровадженні сучасних рішень, здатних реалізовувати точкове управління доступом до окремих ресурсів і взаємодій [9].

Віддалений доступ на основі принципу Zero Trust

Починаючи від периферії мережі, архітектура Xage охоплює корпоративну

ё

IT-інфраструктуру, хмарні сервіси та всі взаємодії між ними. Платформа Fabric формує цілісне захищене середовище від кінцевих пристроїв до хмарних ресурсів, поєднуючи розширені можливості керування політиками безпеки та контролю доступу. Це дозволяє реалізувати безпечний віддалений доступ до корпоративних ресурсів без створення додаткових ризиків для інформаційної безпеки.

Xage забезпечує захищений віддалений доступ до середовищ оперативних технологій (OT) та надає можливість детального контролю взаємодії з виробничими активами на основі цифрової ідентичності. Рішення спрощує управління доступом і може замінювати або доповнювати традиційні засоби захисту, зокрема брандмауери, VPN та проміжні сервери (Jump Box), знижуючи складність адміністрування та експлуатаційні витрати.

Традиційно віддалений доступ до ресурсів OT надавався на рівні окремого майданчика або мережевого сегмента. У такому випадку користувач, який отримував доступ до одного ресурсу в межах зони, фактично міг взаємодіяти й з іншими системами, часто без належного журналювання та контролю виконуваних дій. У платформі Xage кожна спроба доступу проходить процедури автентифікації та авторизації, а для критично важливих активів додатково підтримується багатофакторна автентифікація на рівні окремого пристрою або сервісу.

Рішення Xage Zero Trust Remote Access надає такі можливості:

Рис. 3.1. Схема розгортання Zero Trust Access на базі Xage

Таблиця 3.1.

Етапи впровадження Zero Trust Architecture в організації

Етап	Зміст робіт	Результат
Інвентаризація активів	Визначення користувачів, пристроїв, застосунків і критичних даних	Сформована карта активів і залежностей
Оцінка ризиків	Виявлення загроз, вразливостей і критичних сценаріїв доступу	Пріоритети впровадження захисних заходів
Посилення ідентифікації	Упровадження MFA, IAM і принципу мінімальних привілеїв	Контрольований доступ користувачів
Мікросегментація	Поділ мережі та сервісів на ізольовані зони	Обмеження поширення атак
Моніторинг і аудит	Збір подій, аналіз поведінки, реагування на інциденти	Постійна перевірка стану безпеки

Джерело: сформовано автором.

– безпечне підключення через демілітаризовану зону OT (OT DMZ) із використанням проксі-серверів Xage та механізмів тунелювання, що підтримують різні протоколи зв’язку, зокрема SSH, HTTP/HTTPS, RDP, VNC, Modbus та інші;

– детальний контроль доступу на основі ролей та цифрових ідентичностей до конкретних активів, а не лише до мережевих сегментів або зон довіри;

ё

– автоматизоване застосування політик безпеки по всьому маршруту взаємодії без необхідності змінювати налаштування облікових записів, кінцевих пристроїв або мережевих екранів;

– завершення протоколів, керування сеансами та шифрування з'єднань безпосередньо на вузлах Xage, що унеможливлює прямий доступ до захищених ресурсів;

– інтегровані механізми контролю дій користувачів, включаючи обмеження окремих операцій відповідно до встановлених політик безпеки;

– постійний моніторинг сеансів роботи, запис дій користувачів та контроль виконуваних операцій;

– ведення захищених від модифікації журналів аудиту для всіх взаємодій та адміністративних дій;

– підтримку вимог галузевих стандартів і нормативних документів, зокрема NERC-CIP та IEC 62443;

– реалізацію безпечного доступу до спеціалізованих настільних застосунків, таких як FactoryTalk або RocLink, що дозволяє віддаленим спеціалістам працювати з клієнт-серверними ОТ-системами через контрольовані та захищені канали зв'язку, які забезпечують вищий рівень безпеки порівняно з традиційними VPN-рішеннями.

Таким чином, використання механізмів віддаленого доступу на основі принципу нульової довіри дозволяє значно підвищити рівень захисту виробничих та корпоративних ресурсів, забезпечуючи детальний контроль усіх взаємодій і мінімізуючи ризики несанкціонованого доступу.

Віртуальний операційний центр Xage

Віртуальний операційний центр Xage забезпечує можливість ефективної взаємодії між технічними спеціалістами незалежно від їхнього місцезнаходження. Рішення дозволяє локальним і віддаленим операторам працювати з однаковими наборами робочих екранів, застосунків та інформаційних ресурсів, що сприяє покращенню координації виробничих процесів.

Підтримка багатомоніторного режиму забезпечує відображення робочого середовища в конфігурації, максимально наближеній до реальних умов експлуатації. Це дозволяє підвищити ефективність роботи персоналу без зниження рівня інформаційної безпеки.

Основні можливості віртуального операційного центру включають:

– віддалене відображення декількох фізичних дисплеїв на пристроях користувачів незалежно від їх конфігурації;

– підтримку режимів перегляду та повноцінної взаємодії з можливістю виконання операцій відповідно до наданих повноважень;

– організацію спільного доступу до віддалених робочих станцій через браузер або окремі вікна відображення;

– централізоване управління віддаленими сеансами роботи;

– надання різних рівнів доступу без створення додаткових ризиків для систем оперативного управління (ОТ).

Таким чином, віртуальний операційний центр забезпечує безпечну співпрацю між спеціалістами різних виробничих майданчиків, зберігаючи контроль над критично важливими ресурсами підприємства.

Xage Insights та Xena AI Copilot

Платформа Xage Fabric включає аналітичний модуль Xage Insights та інтелектуального помічника Xena AI Copilot, створеного на основі сучасних технологій генеративного штучного інтелекту. Їхнє використання дозволяє

ё

значно покращити контроль безпеки, спростити адміністрування та підвищити ефективність управління доступом.

Xage Insights

Модуль Xage Insights забезпечує розширений моніторинг активності користувачів, пристроїв і програмних компонентів у межах корпоративного середовища. Інструмент надає детальну аналітичну інформацію, яка може бути використана для своєчасного виявлення потенційних загроз та вдосконалення політик безпеки.

Серед основних можливостей системи:

– виявлення облікових записів, для яких не активовано багатофакторну автентифікацію (MFA);

– пошук пристроїв і ресурсів, до яких не застосовуються політики доступу;

– аналіз активності користувачів та виявлення аномальної поведінки;

– оцінка рівня захищеності інфраструктури та визначення потенційних вразливостей;

– формування звітів щодо поточного стану безпеки організації.

Завдяки отриманим аналітичним даним адміністратори можуть оперативно виявляти прогалини в системі захисту та своєчасно впроваджувати необхідні заходи для їх усунення.

Xena AI

Xena є інтелектуальним помічником, який використовує алгоритми штучного інтелекту для аналізу подій безпеки та підтримки процесу прийняття рішень. Система дозволяє адміністраторам отримувати відповіді на запити природною мовою та формувати рекомендації на основі даних корпоративного середовища.

Можливості Xena включають:

– аналіз активності користувачів, пристроїв і сервісів;

– виявлення потенційних загроз та аномалій;

– оцінювання ефективності політик безпеки;

– автоматичне формування рекомендацій щодо підвищення рівня захисту;

– генерацію звітів для технічних фахівців і керівництва.

Завдяки глибокому аналізу шляхів доступу та поведінки користувачів Xena допомагає визначати критичні вектори атак і пропонує механізми їх усунення шляхом коригування політик безпеки.

Серед прикладів запитів, які можуть бути оброблені системою:

– визначення географічних локацій, з яких здійснювався доступ до корпоративних ресурсів;

– пошук підозрілої активності в інформаційних системах;

– виявлення політик, які потребують оптимізації;

– формування звітів щодо поточного стану захищеності інфраструктури;

– автоматизація адміністративних завдань, таких як активація MFA, блокування облікових записів або зміна паролів у Active Directory.

Використання Xena дозволяє підвищити ефективність роботи адміністраторів безпеки та скоротити час реагування на потенційні кіберзагрози.

Платформа Xage Fabri

Xage Fabric є високодоступною розподіленою платформою кібербезпеки, яка виступає основою всіх продуктів і сервісів компанії Xage. Її архітектура забезпечує реалізацію принципів Zero Trust та дозволяє організувати захищений доступ до ресурсів незалежно від місця їх розташування.

Платформа побудована на технології розподіленого реєстру, що забезпечує автоматичне розповсюдження критично важливих даних між вузлами системи. Для захисту інформації використовуються криптографічні механізми консенсусу, зокрема Shamir's Secret Sharing та Federated Byzantine Agreement, які унеможливлюють несанкціонований доступ до даних навіть у разі компрометації окремих компонентів.

Основними перевагами Xage Fabric є:

1. Збереження працездатності механізмів автентифікації, авторизації та контролю доступу навіть за відсутності підключення до глобальної мережі або

ё

корпоративної WAN-інфраструктури.

2. Автоматичне поширення політик безпеки та облікових даних між усіма вузлами без необхідності ручного дублювання інформації.

3. Використання розподіленого сховища облікових даних, що значно ускладнює їх компрометацію та викрадення.

4. Реалізація централізованого контролю доступу на основі цифрових ідентичностей для користувачів, пристроїв, програмних компонентів і даних.

5. Підтримка механізмів єдиного входу (SSO), багатофакторної автентифікації та інтеграції з Active Directory й іншими системами керування ідентифікацією.

Архітектура розгортання Xage Fabric

Архітектура Xage Fabric забезпечує захищену взаємодію між корпоративними користувачами, хмарними сервісами, віддаленими майданчиками та промисловими системами управління.

У верхньому рівні архітектури розташовані корпоративні центри обробки даних або приватні хмари. На цьому рівні здійснюється централізоване управління політиками безпеки через Xage Manager, інтеграція з LDAP та Active Directory, а також забезпечується взаємодія користувачів із серверами, робочими станціями та корпоративними застосунками.

Середній рівень представлений хмарними платформами та віддаленими майданчиками. Платформа підтримує інтеграцію з такими сервісами, як Azure, AWS та Oracle Cloud, забезпечуючи захищений доступ до вебзастосунків, віртуальних робочих столів і корпоративних сервісів.

Нижній рівень архітектури охоплює середовища оперативних технологій (OT), де оператори взаємодіють із системами SCADA, PLC та інженерними робочими станціями. Компоненти Xage забезпечують контроль доступу, автентифікацію та моніторинг усіх операцій у виробничій інфраструктурі.

Завдяки такій архітектурі організація отримує єдиний механізм управління доступом для IT-, OT- та хмарних середовищ.

Переваги використання Xage Fabric

Платформа Xage Fabric забезпечує комплексний підхід до управління доступом і захисту інформаційних ресурсів. Основні переваги рішення включають:

– реалізацію принципів нульової довіри для всіх взаємодій між користувачами, пристроями, програмами та даними;

– запобігання горизонтальному переміщенню зловмисників у мережі шляхом застосування MFA та автоматичної ротації облікових даних;

– використання динамічних рольових політик замість статичних правил мережевих екранів;

– підтримку безпечного локального та віддаленого доступу до ресурсів;

– впровадження багатофакторної автентифікації без необхідності зміни конфігурації наявних активів;

– централізоване управління цифровими ідентичностями для сучасних і застарілих систем;

– підтримку середовищ із кількома постачальниками сервісів ідентифікації;

– захищений обмін даними між компонентами IT-, OT- та хмарної інфраструктури;

– використання розподіленого сховища для журналів аудиту та операційних даних;

– автоматичне керування обліковими даними та їх ротацію для зниження ризику компрометації облікових записів.

Завдяки зазначеним можливостям платформа Xage Fabric забезпечує високий рівень безпеки, гнучке управління доступом і ефективний захист сучасних розподілених інформаційних систем [13].

3.2. Технологія забезпечення безпеки організації на базі рішення Xage Zero Trust

Нульовий довірчий доступ до прикладних систем інформаційної

ё

інфраструктури

Платформа Xage надає функціональність **Zero Trust Remote Access**, що забезпечує захищений віддалений доступ до клієнт-серверних застосунків, характерних для середовищ оперативного управління (OT), зокрема FactoryTalk, Studio5000 та інших. Такий підхід дозволяє усунути одну з ключових проблем кібербезпеки — безпечне підключення сторонніх користувачів, підрядників або пристроїв до корпоративної інфраструктури без ризику занесення шкідливого програмного забезпечення чи виконання несанкціонованих дій.

Технологія Zero Trust Remote Access забезпечує значно вищий рівень захисту порівняно з традиційними VPN-рішеннями.

Рис. 3.2. Захищений віддалений доступ і мікросегментація в архітектурі Xage Zero Trust

Принцип функціонування

Автентифікація користувача

Користувач проходить процедуру входу до Xage Fabric, після чого

формується захищене пряме з’єднання між його робочим пристроєм та вузлом нульової довіри (Zero Trust Enforcement Point) у середовищі Fabric. Такий вузол може бути розгорнутий у хмарній інфраструктурі, IT-середовищі, iDMZ або OT-сегменті.

Авторизація та формування тунелів Zero Trust

Після підтвердження прав доступу до необхідного периферійного ресурсу система автоматично створює захищені тунелі нульової довіри. Доступ надається виключно до визначених активів і мережевих протоколів відповідно до встановлених політик безпеки. Захист тунелів реалізується за допомогою цифрових підписів Fabric та багаторівневої багатофакторної автентифікації (MFA).

Робота з цільовими ресурсами

Користувач отримує можливість працювати з цільовою системою через відповідні клієнт-серверні застосунки безпосередньо зі свого пристрою. Водночас Xage Fabric забезпечує логічну ізоляцію пристрою від інших сегментів OT, IT та хмарної інфраструктури, запобігаючи поширенню потенційних загроз.

Основні переваги

- Усунення необхідності довіряти неконтрольованим пристроям, які підключаються до мережі.
- Використання захищених тунелів Zero Trust із суворо визначеними правилами доступу.
- Підтримка сегментації та ізоляції пристроїв від критично важливих компонентів мережі.
- Підвищення рівня захисту клієнт-серверних взаємодій у середовищах OT та IT.

Запропонований підхід дозволяє суттєво знизити кіберризики та гарантувати безпеку інфраструктури навіть за умови використання сторонніх пристроїв і зовнішніх підрядників.

Управління привілейованим доступом та доступом постачальників

Окрім механізмів віддаленого підключення, Xage надає можливості

ё

централізованого управління привілейованим доступом як для внутрішніх співробітників, так і для зовнішніх користувачів, включаючи доступ до промислових активів ICS, таких як SCADA-системи, ПЛК (PLC) та RTU.

Платформа дозволяє організувати контрольований доступ для працівників, постачальників, сервісних організацій та інших партнерів виключно до тих ресурсів, які необхідні для виконання їхніх функціональних обов'язків.

Функціональні можливості Xage включають:

- Оперативне створення облікових записів для внутрішніх та зовнішніх користувачів.
- Швидке впровадження політик мінімально необхідних привілеїв для будь-яких користувачів і ресурсів.
- Автоматичне блокування або деактивацію облікових даних, а також регулярну зміну паролів для запобігання використанню застарілих або скомпрометованих облікових записів.
- Надання тимчасового доступу третім сторонам лише на період виконання конкретних завдань.
- Моніторинг і запис сеансів роботи з можливістю подальшого аудиту.
- Автоматизоване виявлення облікових записів на керованих активах.
- Контроль і фільтрацію команд залежно від рівня привілеїв користувача.
- Використання API для отримання та керування обліковими даними.
- Автоматичну або ручну ротацію облікових даних.
- Підтримку широкого спектра платформ і систем, включаючи сервери, робочі станції, мережеве обладнання, бази даних, хмарні сервіси та клієнт-серверні застосунки.
- Детальне ведення журналів аудиту з можливістю інтеграції із SIEM та SOAR-рішеннями.

Єдиний вхід із підтримкою кількох постачальників ідентифікації (IdP)

Платформа Xage реалізує механізми єдиного входу (SSO) для корпоративних і виробничих ресурсів. Рішення підтримує як користувацькі

облікові записи, так і автентифікацію машин, сервісів та застосунків, що використовують промислові протоколи або працюють на віддалених майданчиках.

Ідентифікаційно-орієнтована архітектура SSO забезпечує безпечний та централізовано контрольований доступ користувачів, програм і пристроїв незалежно від структури сегментації мережі. Завдяки порталу SSO користувачам не потрібно вручну запам’ятовувати IP-адреси, мережеві порти, параметри підключення чи окремі облікові дані для кожного ресурсу.

Крім того, Xage підтримує федерацію служб ідентифікації між різними організаціями. Це дозволяє партнерам, які беруть участь у спільних проєктах, використовувати власні корпоративні облікові записи для доступу до спільних інформаційних ресурсів.

Система підтримує централізоване управління декількома постачальниками ідентифікаційної інформації (Identity Providers, IdP), що забезпечує інтеграцію різних систем керування ідентифікацією в єдиному середовищі.

Для об’єктів критичної інфраструктури Xage дозволяє створювати незалежні домени ідентифікації для різних рівнів мережі та окремих виробничих майданчиків. Такий підхід мінімізує ризик поширення наслідків компрометації корпоративних IT-облікових записів на OT-середовище та запобігає каскадному впливу інциденту між різними об’єктами інфраструктури.

Підтримка кількох IdP та протоколів автентифікації

Платформа забезпечує інтеграцію з кількома постачальниками ідентифікації та доменами Active Directory, які можуть належати до різних зон безпеки або мережевих сегментів. Підтримуються такі протоколи автентифікації, як LDAP, SAML та ADFS, що дозволяє адаптувати механізми перевірки особи відповідно до вимог конкретного середовища.

Приховування ресурсів до моменту автентифікації

Доступність інформації про активи та системи обмежується до моменту успішного проходження автентифікації. Як локальні, так і віддалені користувачі

ё

можуть отримати доступ до ресурсів лише після перевірки облікових даних у відповідному домені Active Directory та проходження багатофакторної автентифікації.

Локальна автентифікація при втраті зв'язку

Система забезпечує можливість локальної автентифікації користувачів через Active Directory локального майданчика навіть за відсутності зв'язку з центральною мережею. Це підвищує безперервність роботи та стійкість до мережевих відмов.

Багаторівнева багатофакторна автентифікація

Рішення підтримує використання різних методів MFA, включаючи безпарольну автентифікацію, апаратні токени та біометричні засоби підтвердження особи. Механізми MFA можуть застосовуватися на різних рівнях доступу та інтегруватися з різними постачальниками ідентифікаційної інформації, забезпечуючи гнучку та адаптивну модель захисту. Багатофакторна автентифікація (MFA)

Уніфікована багатофакторна автентифікація (MFA)

Xage усуває складнощі, пов'язані з впровадженням багатофакторної автентифікації в наявні інформаційні та виробничі середовища. Завдяки можливості інтеграції MFA практично з будь-якими пристроями та програмними системами платформа дозволяє поширити додаткові механізми автентифікації на всі корпоративні активи, забезпечуючи централізоване управління засобами захисту на основі цифрової ідентичності.

Архітектура рішення спеціально розроблена для сценаріїв використання в середовищах OT та IoT. Високонадійні механізми автентифікації та контролю доступу реалізуються безпосередньо на периферії мережі та продовжують функціонувати навіть у разі втрати зв'язку з центральними компонентами системи. Це дозволяє забезпечити багатофакторний доступ із мінімальними затримками навіть у мережах із нестабільним з'єднанням або при роботі з віддаленими об'єктами.

Основні можливості MFA для промислових та IoT-активів

- Реалізація комплексного контролю доступу на основі ідентифікації користувачів, пристроїв і застосунків.
- Застосування багатофакторної автентифікації до застарілих систем, які підтримують лише однофакторну автентифікацію або не мають її взагалі, включаючи SCADA-системи, ПЛК та RTU, за допомогою Xage Enforcement Point (XEP).
- Уніфікація та стандартизація механізмів MFA для всіх типів ресурсів: програмного забезпечення, робочих станцій, систем керування та мережевого обладнання.
- Гнучкий вибір і швидке переключення між різними методами підтвердження особи, включаючи апаратні ключі, смарт-картки, мобільні автентифікатори та інші засоби.
- Забезпечення відповідності галузевим і нормативним вимогам без необхідності модернізації або заміни наявних активів.
- Ведення повного аудиту взаємодії користувачів і машин із детальним журналюванням усіх подій.

Внутрішня сегментація мережі та міжмашинний контроль доступу

Традиційні механізми сегментації мережі, такі як VLAN, міжмережеві екрани та списки контролю доступу (ACL), характеризуються високою складністю впровадження та супроводу, а також не забезпечують належного контролю на рівні окремих пристроїв.

Технології Xage Zero Trust Segmentation та Microsegmentation дозволяють реалізувати детальну сегментацію середовища, у межах якої можуть бути визначені індивідуальні правила взаємодії для кожного користувача та кожного пристрою. Такий підхід значно знижує ризики горизонтального переміщення зловмисників (lateral movement) і реалізації атак типу Living off the Land (LotL).

На додаток до контролю доступу користувачів і застосунків, Xage використовує модель керування взаємодією між машинами на основі цифрових ідентифікаторів. Ідентичність пристрою формується на основі комбінації мережевих, системних і прикладних характеристик, включаючи IP-адресу, MAC-

ë

адресу, використовувані протоколи, версії програмного забезпечення, прошивки, апаратного забезпечення та інші параметри.

Після формування цифрових ідентифікаторів для окремих пристроїв або груп можуть створюватися політики взаємодії, які враховують розташування активу, часові обмеження, дозволені параметри обміну даними та функціональну роль пристрою в системі.

Додатково платформа підтримує наскрізне шифрування окремих потоків взаємодії, що дозволяє захищати лише необхідні комунікації без надмірного навантаження на інфраструктуру.

Переваги міжмашинного контролю доступу

- Деталізоване та динамічне управління взаємодією між пристроями без використання статичних правил.
- Формування цифрової ідентичності для всіх активів із можливістю виявлення підміни або несанкціонованих пристроїв.
- Автоматичне створення IPSec-тунелів для наскрізного шифрування взаємодії відповідно до політик безпеки.
- Виявлення та блокування спроб підробки повідомлень.
- Мінімальний вплив на технологічні процеси завдяки мікросекундному рівню затримок.
- Реалізація функцій сегментації та міжмережевого екранування без необхідності зміни структури підмереж.
- Підтримка принципів зонування та каналів зв’язку відповідно до вимог стандарту IEC 62443.

Xage Enforcement Point як альтернатива внутрішнім міжмережевим екранам

Xage Enforcement Point (XEP) виступає універсальною точкою застосування політик безпеки, яка за принципом «заборонено за замовчуванням» блокує доступ до всіх ресурсів, що знаходяться за нею.

XEP одночасно виконує функції шлюзу автентифікації, фільтрації мережевого трафіку та внутрішнього міжмережевого екрана сегментації.

Порівняно з традиційними брандмауерами рішення забезпечує ширші можливості внутрішньої сегментації при менших витратах на впровадження та адміністрування.

Компонент підтримує локальне управління обліковими записами, застосування політик доступу та роботу в режимі прозорого проксі-сервера безпеки. Також можливе програмно-кероване двонаправлене управління трафіком, що розширює функціональність традиційних діодів даних. XEP доступний як у вигляді апаратного пристрою, так і у віртуалізованому виконанні.

Zero Trust Data Exchange (ZTDE)

Механізм Zero Trust Data Exchange (ZTDE) забезпечує безпечний обмін даними між різними інформаційними платформами, організаціями, програмами та пристроями із гарантуванням автентичності, цілісності та конфіденційності інформації.

Рішення дозволяє організаціям організовувати захищений доступ до даних незалежно від місця їх розташування та кількості учасників взаємодії. Система захищає інформацію від несанкціонованих змін і забезпечує реплікацію даних разом із пов’язаними метаданими безпеки через Xage Fabric до всіх точок споживання.

Розподілена архітектура Fabric забезпечує надійну передачу даних типу «точка-точка» навіть у складних мережевих середовищах із нестабільним з’єднанням. Це дозволяє безпечно передавати інформацію між периферійними пристроями, центрами обробки даних і хмарними платформами.

Основні принципи ZTDE

Автентичність

Кожен інформаційний об’єкт підписується цифровим підписом із використанням унікального криптографічного ключа. Дані про походження та цифрові відбитки пристроїв зберігаються в Xage Fabric, що забезпечує підтвердження джерела походження інформації.

Цілісність

Для кожного набору даних формуються криптографічні хеші, які

ё

реплікуються в Fabric. Це дозволяє перевіряти цілісність інформації на будь-якому етапі її використання або передачі.

Конфіденційність і контроль доступу

Платформа підтримує детальне керування доступом на рівні пристроїв, застосунків, користувачів і потоків даних. Політики можуть враховувати тему повідомлення, часові параметри або навіть окремі значення даних.

Завдяки механізму захищеної реплікації Xage Fabric забезпечує наскрізний безпечний обмін інформацією між усіма компонентами екосистеми. Під час встановлення взаємодії між двома вузлами система автоматично створює зашифровані канали зв'язку без необхідності ручного налаштування.

Відповідність MITRE ATT&CK for ICS

Платформа MITRE ATT&CK for ICS є загальновизнаним галузевим стандартом опису тактик, технік і процедур (TTP), які використовуються кіберзловмисниками під час атак на промислові системи керування.

За даними виробника, платформа Xage Fabric забезпечує повне блокування або ефективне пом'якшення впливу понад 90 % технік і методів атак, представлених у матриці MITRE ATT&CK for ICS.

Інтеграція з партнерськими рішеннями

Xage підтримує інтеграцію з широким спектром технологічних партнерів для реалізації комплексної системи кіберзахисту, що охоплює запобігання атакам, виявлення загроз та реагування на інциденти.

Збагачення інвентаризації активів

Платформа може отримувати інформацію від систем виявлення активів, доповнюючи її даними про поведінку користувачів, права доступу та політики безпеки.

Виявлення аномалій та реагування на загрози

Інтеграція із системами аналізу аномалій забезпечує доступ до детальних журналів аудиту та телеметрії з усіх рівнів моделі Purdue, що дозволяє своєчасно виявляти приховані атаки та підозрілу активність у середовищах OT.

У разі виявлення загроз Xage може автоматично обмежувати права доступу

користувачів або пристроїв, які демонструють аномальну поведінку.

Адаптивний контроль доступу через інтеграцію з EDR/XDR

Платформа інтегрується з рішеннями класу EDR та XDR для автоматичного коригування політик доступу залежно від поточного рівня ризику.

Наприклад, якщо система виявлення фіксує підозрілу активність або взаємодію із відомими шкідливими ресурсами, Xage може автоматично звузити доступ відповідного пристрою, запобігаючи подальшому поширенню атаки.

Інтеграція з SIEM/SOAR

Xage веде детальний аудит усіх подій безпеки та дій користувачів і підтримує передачу журналів до платформ SIEM та SOAR. Це забезпечує централізований моніторинг, розслідування інцидентів та автоматизоване реагування на кіберзагрози.

3.3. Розроблення рекомендацій щодо захисту організаційних IT-систем на базі Zero Trust Architecture

Таблиця 3.2.

Матриця ризиків до та після впровадження Zero Trust Architecture

Ризик	Рівень до впровадження	Механізм Zero Trust	Очікуваний рівень після впровадження
Компрометація облікового запису	Високий	MFA, IAM, умовний доступ	Середній або низький
Горизонтальне переміщення в мережі	Високий	Мікросегментація, PEP, політики взаємодії	Низький
Надмірні привілеї користувачів	Середній	Least privilege, регулярний перегляд ролей	Низький
Неконтрольований віддалений доступ	Високий	ZTNA, доступ до конкретного ресурсу	Середній або низький
Несвоєчасне виявлення інцидентів	Середній	SIEM, журналювання, поведінкова аналітика	Низький

Джерело: сформовано автором.

На основі проведеного аналізу концепції Zero Trust, сучасних підходів до управління доступом та передових практик забезпечення інформаційної безпеки сформовано комплекс рекомендацій, спрямованих на підвищення рівня

ё

захищеності інформаційних систем організації.

1. Впровадження архітектури Zero Trust

Доцільно реалізувати модель нульової довіри (Zero Trust), яка передбачає постійну перевірку всіх користувачів, пристроїв та сервісів незалежно від їхнього розташування в мережі.

Основними заходами повинні стати:

- впровадження принципу мінімально необхідних привілеїв (Least Privilege Access), який забезпечує надання користувачам лише тих прав доступу, що необхідні для виконання службових обов'язків;
- застосування багатофакторної автентифікації (MFA) для всіх категорій користувачів, включаючи внутрішніх співробітників, адміністраторів і віддалених користувачів;
- використання адаптивних політик доступу, що враховують не лише облікові дані користувача, а й контекст підключення, поведінкові характеристики, стан пристрою та рівень ризику поточної сесії.

2. Розвиток системи керування цифровими ідентичностями

Для забезпечення централізованого контролю доступу рекомендується впровадити інтегровану систему управління ідентифікацією та доступом (IAM), яка підтримує взаємодію з різними постачальниками ідентифікаційних даних.

Зокрема, доцільно:

- забезпечити підтримку декількох Identity Provider (IdP);
- використовувати сучасні протоколи автентифікації та федерації ідентичностей, зокрема LDAP, SAML та ADFS;
- інтегрувати нові механізми управління доступом із наявною корпоративною інфраструктурою без необхідності масштабної модернізації існуючих систем.

3. Посилення захисту об'єктів критичної інфраструктури

Для мінімізації ризиків несанкціонованого доступу до критичних активів рекомендується впроваджувати захищені механізми віддаленого доступу на

основі принципів Zero Trust.

Основні заходи повинні включати:

- відмову від традиційних VPN-рішень на користь технологій Zero Trust Network Access (ZTNA);
- приховування інформації про ресурси до моменту успішної автентифікації користувача;
- використання Zero Trust Remote Access для доступу до клієнт-серверних застосунків середовищ операційних технологій (OT);
- застосування механізмів автоматичної ротації облікових даних та багаторівневого контролю доступу для запобігання горизонтальному поширенню атак у мережі.

4. Автоматизація процесів забезпечення безпеки

З метою оперативного виявлення та нейтралізації кіберзагроз доцільно впроваджувати інтелектуальні засоби аналізу та автоматизованого реагування.

Рекомендується:

- використовувати технології поведінкової аналітики та машинного навчання для виявлення аномальної активності користувачів і пристроїв;
- автоматизувати процеси моніторингу відповідності кінцевих пристроїв вимогам корпоративної політики безпеки;
- впроваджувати механізми адаптивного коригування політик доступу залежно від поточного рівня ризику.

5. Забезпечення безперервності функціонування систем безпеки

Для підвищення стійкості інформаційної інфраструктури до відмов мережевих компонентів рекомендується:

- забезпечити можливість локальної автентифікації користувачів через служби Active Directory навіть за відсутності зв’язку з центральними ресурсами;
- використовувати розподілені сховища для зберігання журналів аудиту, подій безпеки та облікових даних;
- впроваджувати механізми захисту критичних записів від

ё

несанкціонованої модифікації або видалення.

6. Підвищення рівня обізнаності персоналу

Ефективність сучасних систем захисту значною мірою залежить від рівня підготовки співробітників. У зв’язку з цим необхідно організувати комплексну програму навчання персоналу.

Доцільно передбачити:

- регулярне проведення навчань і практичних тренінгів із питань кібербезпеки;
- підготовку користувачів до роботи з багатофакторною автентифікацією та системами керування ідентичністю;
- проведення навчальних кібернавчань і симуляцій атак для відпрацювання процедур реагування на інциденти;
- періодичне оцінювання рівня обізнаності працівників щодо сучасних кіберзагроз.

Висновки до розділу 3

У третьому розділі розглянуто практичну реалізацію Zero Trust Architecture на базі рішення Xage, визначено етапи впровадження та сформовано рекомендації щодо захисту організаційних IT-систем. Запропонований підхід дає змогу обмежити доступ до критичних ресурсів, підвищити контроль за діями користувачів і зменшити ризик поширення кіберзагроз усередині мережі.

ВИСНОВКИ

У ході виконання роботи було проведено комплексне дослідження проблематики забезпечення безпеки інформаційних систем організацій на основі концепції Zero Trust. Визначено актуальні кіберзагрози, які впливають на функціонування сучасних інформаційних систем, а також обґрунтовано доцільність використання архітектури нульової довіри як одного з найбільш ефективних підходів до побудови комплексного кіберзахисту.

Виконано аналіз сучасних підходів до захисту інформаційних систем із використанням технологій Zero Trust. Встановлено, що ключовими компонентами таких рішень є багатофакторна автентифікація, адаптивне управління доступом на основі політик безпеки, мікросегментація мережі, безперервна перевірка ідентичності користувачів і пристроїв, а також застосування розподілених механізмів контролю доступу та аудиту подій.

Досліджено методи й інструменти впровадження концепції Zero Trust для захисту інформаційних ресурсів організації. Особливу увагу приділено сучасним платформам управління доступом, зокрема рішенням на базі технології Xage, які забезпечують комплексний захист користувачів, пристроїв, застосунків і каналів передачі даних незалежно від їх розташування в мережевій інфраструктурі.

Проаналізовано процес інтеграції технологій Zero Trust у корпоративне середовище. Визначено основні етапи впровадження механізмів безпечного доступу до інформаційних ресурсів із дотриманням вимог конфіденційності, цілісності та доступності даних. Показано, що використання принципу нульової довіри дозволяє суттєво знизити ризики несанкціонованого доступу, компрометації облікових записів та поширення кіберзагроз усередині корпоративної мережі.

Проведений аналіз підтвердив, що в умовах постійного зростання кількості та складності кіберзагроз організаціям необхідно переходити від традиційних периметрових моделей захисту до адаптивних підходів, заснованих на безперервній перевірці довіри. Ефективна реалізація концепції Zero Trust

ё

повинна охоплювати не лише механізми контролю доступу, але й засоби моніторингу поведінки користувачів і пристроїв, управління ризиками, автоматизації процесів реагування на інциденти та централізованого аудиту подій безпеки.

На основі результатів дослідження сформовано практичні рекомендації щодо впровадження технологій Zero Trust в організаціях. Запропоновано підходи до побудови багаторівневої системи автентифікації, централізованого управління цифровими ідентичностями, налаштування політик доступу та постійного моніторингу безпеки з метою мінімізації ризиків витоку інформації та реалізації кібератак.

Також визначено ключові напрями інтеграції архітектури Zero Trust у сучасні корпоративні IT-системи. Запропоновані підходи дозволяють забезпечити безпечну взаємодію працівників, які працюють у гібридному або віддаленому форматі, а також підвищити рівень захисту корпоративних ресурсів незалежно від місця підключення користувачів та використовуваних пристроїв.

Отже, впровадження технологій Zero Trust є важливим напрямом розвитку сучасних систем кібербезпеки та необхідною умовою забезпечення надійного захисту інформаційних активів організації. Використання принципів нульової довіри сприяє підвищенню стійкості інформаційної інфраструктури до сучасних кіберзагроз, зменшенню площини атаки та створенню безпечного середовища для функціонування цифрових сервісів і бізнес-процесів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kumar, I. (2023). Emerging Threats in Cybersecurity: A Review Article. International Journal of Applied and Natural Sciences, 1(1), 01–08. Retrieved from https://bluemarkpublishers.com/index.php/IJANS/article/view/2

2. New Technologies in Cybersecurity | Combatting the Latest Threats. Explore Cybersecurity Degrees and Careers | CyberDegrees.org. URL: https://www.cyberdegrees.org/resources/hot-technologies-cyber-security/

3. Exploring Access Control Models: Building Secure Systems in Cybersecurity.
Tripwire | Security and Integrity Management Solutions. URL: https://www.tripwire.com/state-of-security/exploring-access-control-models-building-secure-systems-cybersecurity (дата звернення: 30.10.2024).

4. Zero Trust Architecture: The Key to Modern Cybersecurity. *Trio Blog*. URL: https://www.trio.so/blog/zero-trust-architecture/

5. NIST Special Publication 800-207, Zero Trust Architecture, COMPUTER SECURITY, August 2020 URL: https://doi.org/10.6028/NIST.SP.800-207

6. Top 5 Best Practices for Implementing Zero Trust Security - DataGroupIT. DataGroupIT. URL: https://datagroupit.com/top-5-best-practices-for-implementing-zero-trust-security/

7. Xage Zero Trust Access. Xage Security. 2024 URL: https://info.xage.com/hubfs/Datasheets/Xage%20Zero%20Trust%20Access.pdf

8. Xage Security and Darktrace Partner to Enhance Zero Trust Protection for Commercial Critical Infrastructure Environments. Darktrace | Cyber security that learns you. URL: https://darktrace.com/news/xage-security-and-darktrace-partner-to-enhance-zero-trust-protection

9. Shield Your Enterprise with Zero Trust Access from Xage. Xage Security. URL: https://xage.com/zero-trust-access/

ë

10. Universal Zero Trust Network Access. Xage Security. URL:

11. Xage: Zero trust cybersecurity for IT, OT, and cloud. URL: https://xage.com/wp-content/uploads/2023/05/Xage-Zero-Trust-Data-Exchange.pdf?hsCtaTracking=78b2a2b1-6699-4a77-b034-22abbbcd4f46|322a397a-d05d-41c2-9f81-292ba926b3a0

12. Mastering MITRE ATT&CK for Enterprise with a Zero Trust Model. WHITEPAPER. Xage Security. 2024

13. Unified Zero Trust Access and Protection for Operational Technology (OT) and Cyber Physical Systems (CPS) WHITEPAPER. Xage Security. 2024

14. NIST Special Publication 800-207. *Zero Trust Architecture*. National Institute of Standards and Technology, 2020.

15. NIST Special Publication 800-53 Rev. 5. *Security and Privacy Controls for Information Systems and Organizations*.

16. ISO/IEC 27001:2022. *Information security, cybersecurity and privacy protection — Information security management systems*.

17. ISO/IEC 27002:2022. *Information security controls*.

18. Kindervag J. *Build Security Into Your Network's DNA: The Zero Trust Network Architecture*. Forrester Research, 2010.

19. Google. *BeyondCorp: A New Approach to Enterprise Security*. Google White Paper.

20. Microsoft Corporation. *Zero Trust Security Model Overview*. Official Documentation.

21. Cisco Systems. *Zero Trust Security Architecture White Paper*.

22. Gartner Research. *Zero Trust Network Access (ZTNA) Market Guide*.

23. ENISA. *Threat Landscape Report*. European Union Agency for Cybersecurity, 2024.

24. Cloud Security Alliance (CSA). *Zero Trust Guidance*.

25. NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology, 2024.

26. OWASP Foundation. *OWASP Top 10 Web Application Security Risks 2021*.

27. Zetter K. *Countdown to Zero Day: Stuxnet and the Launch of the World's First*

ë

Digital Weapon.

28. Anderson R. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.

29. Stallings W. *Network Security Essentials: Applications and Standards*. Pearson.

30. McClure S., Scambray J., Kurtz G. *Hacking Exposed: Network Security Secrets & Solutions*.

31. SANS Institute. *Zero Trust Implementation Guidance and Research Papers*.

32. IEEE Xplore Digital Library. *Research Papers on Zero Trust Architecture and Cybersecurity Models*.

33. ACM Digital Library. *Studies on Access Control and Zero Trust Security Models*.

34. IETF RFC 7258. *Pervasive Monitoring Is an Attack*.

35. IETF RFC 8446. *The Transport Layer Security (TLS) Protocol Version 1.3*.

36. NIST NCCoE. *Implementing a Zero Trust Architecture (SP 1800-35)*.

37. U.S. Department of Defense. *Zero Trust Reference Architecture*, 2022.

38. CISA. *Zero Trust Maturity Model*. Cybersecurity and Infrastructure Security Agency.

39. Verizon. *Data Breach Investigations Report (DBIR) 2024*.

40. CrowdStrike. *Global Threat Report 2024*.

41. Palo Alto Networks. *The State of Zero Trust Security Report*.

42. IBM Security. *Cost of a Data Breach Report 2024*.

43. MITRE Corporation. *ATT&CK Framework for Cyber Threat Intelligence and Modeling*.