КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.1029
УДК 004.056.53:004.75

Городицький Остап Іванович
студент кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID: 0009-0000-7785-5582
ostap.horodytskyi.kb.2024@lpnu.ua

Опірський Іван Романович
д.т.н., професор, завідувач кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

ПОКРОКОВИЙ ПІДХІД ДО ІМПЛЕМЕНТАЦІЇ ZERO TRUST У ГІБРИДНИХ АРХІТЕКТУРАХ КОРПОРАТИВНОЇ БЕЗПЕКИ

Анотація. У статті досліджуються можливості імплементації моделі Zero Trust (ZT) у організаціях з системою безпеки на основі периметру (Perimeter-Based). Описано зміни, які відбулись у останні роки та вплинули на системи корпоративної безпеки організацій. Обґрунтовані причини втрати актуальності моделі Perimeter-Based та її основні недоліки. Описано, чому організації все частіше обирають архітектуру Zero Trust для своїх систем інформаційної безпеки та які проблеми моделі Perimeter-Based вона вирішує. Наведено проблеми, з якими зазвичай стикаються організації у процесі імплементації моделі Zero Trust. Надано короткі відомості про модель нульової довіри. В тому числі описано її принципи, думки дослідників щодо неї та її впровадження. Досліджено особливості імплементації ZT у наявні системи безпеки організацій. Встановлено, що ефективна імплементація ZT потребує комплексного підходу, який складається з кількох кроків. Першими з них визначено аудит поточного стану інформаційної безпеки організації та оцінку ризиків, пов'язаних з активами організації. Ці заходи є підготовчими та мають за мету визначити область впровадження та пріоритетні потреби організації у Zero Trust. Наступним кроком визначено процес формування та реалізації політик безпеки. Основною частиною процесу імплементації встановлено безпосереднє впровадження функціоналів, які реалізують принципи Zero Trust. Він розпочинається із визначення плану імплементації, а саме того, які засоби захисту будуть впроваджені до конкретних компонентів системи та у якому порядку. Для оцінки ступеню повноцінності Zero Trust, було наведено приклад "моделі зрілості". Також було наведено функціонал, впровадження якого реалізує принципи нульової довіри, та взаємозв'язок між ним. В тому числі, описано проведення мікросегментації мережі, впровадження технологій MFA та систем IAM (Identity and Access Management), використання систем UEM та UDR для контролю пристроїв, а також SIEM для виявлення загроз та SOAR для автоматизації та координації системи. Як підсумок процесу імплементації обґрунтовано потреби у постійному перегляді та покращенні системи безпеки. Також розглянуто практичні приклади імплементації ZT, які доводять ефективність та актуальність переходу на Zero Trust. Результати дослідження мають практичне значення для демонстрації можливостей і переваг переходу на архітектуру безпеки Zero Trust, отримання розуміння складнощів, які виникають у процесі її імплементації, та визначення ефективного та фінансово доцільного способу здійснення даного процесу.

Ключові слова: Zero Trust, імплементація, методологія, покроковий підхід, архітектура безпеки, корпоративна безпека, оцінка ризиків, модель зрілості, мікросегментація, IAM, UEM, SIEM, SOAR, мережева безпека, інформаційна безпека.

ВСТУП

Останнє десятиліття суттєво змінило роль та значення інформаційних систем для комерційних та державних організацій. Якщо раніше вони зазвичай були допоміжною інфраструктурою для їх роботи, то зараз вони все частіше стають її основою. З кожним роком вони стають все більш комплексними, часто включаючи в себе кілька внутрішніх систем та використовуючи хмарні технології. Пандемія коронавірусу також внесла значні зміни у робочий процес організацій, зробивши популярними практики віддаленої роботи та BYOD (Bring Your Own Device).

Перелічені вище фактори суттєво змінили стан інформаційної безпеки організацій, в тому числі ускладнивши визначення меж систем або повністю їх стерши. Крім цього, атаки з кожним роком стають частішими та комплекснішими, що робить їх наслідки все більш масштабними. Історично класична модель безпеки на основі периметру (Perimeter-Based) різко почала втрачати свої позиції. Причинами цього стало те, що, з одного боку, вона перестала встигати адаптуватись до нових реалій, а з іншого, через її фундаментальні недостатки.

Першим недостатком є робота системи за принципом “фортеці”, у якій середовище розділяється на внутрішнє (довірене) та зовнішнє (недовірене) за допомогою мережевого захисного бар’єру. З цього принципу випливає кілька недостатків архітектури на основі периметру. По-перше, доступ у такій системі зазвичай надається за фактом присутності всередині системи, при чому часто у неконтрольованому обсязі. По-друге, через фокус на моніторингу зовнішнього середовища, підозрілий трафік та події безпеки всередині системи часто залишаються непоміченими. Сукупність даних аспектів призводить до ситуацій, коли зловмисник, непомітно проникнувши у систему, розпочинає процес так званого “подальшого руху”, який заключається у поступовому набутті все більших прав та привілеїв у системі, що призводить до катастрофічних наслідків.

Другим важливим недостатком, який став особливо помітним у останні роки, є невизначеність периметру системи при використанні у організації хмарних сервісів, практик віддаленої роботи та BYOD. За даних умов, периметр системи постійно змінюється, і визначення меж, які потрібно захищати, стає неможливим.

Третім недостатком є статичність системи. Зазвичай, у системах безпеки на основі периметру, політики безпеки та надання доступу є статичними, що в умовах постійних змін у роботі системи робить їх схильними до появи вразливостей через втрату актуальності. Сама система безпеки часто є слабко автоматизованою, що вимагає більшої залученості персоналу та ресурсів до процесу забезпечення безпеки організації, що є недоцільним як з точки зору ефективності реагування на інциденти, так і з

Враховуючи все це, значна частина організацій розпочала пошук нової моделі інформаційної безпеки, яка б:

1) Задовольняла потреби організації у безпеці та забезпеченні працездатності.
2) Усувала недоліки системи безпеки Perimeter-Based.
3) Могла адаптуватись до майбутніх викликів у сфері забезпечення інформаційної безпеки організації.

Значна частина організацій знайшла вирішення цих проблем у архітектурі безпеки Zero Trust (ZT). На сьогоднішній день, більшість організацій розпочинають побудову системи інформаційної безпеки саме за цією архітектурою.

Принципи Zero Trust є відповіддю на фундаментальні недостатки моделі Perimeter-Based. Ключовим принципом Zero Trust є відсутність довіри до будь-якого компоненту

системи. Система за замовчуванням вважає недовіреним як зовнішнє, так і внутрішнє середовище, що несе за собою необхідність постійно аналізувати обставини, за яких робляться запити для отримання доступу до ресурсів системи. Наступним є принцип найменших привілеїв, який передбачає контроль над наданням доступу до ресурсів у найменшій кількості на найменший проміжок часу, потрібних для виконання дії. Також, мережа у моделі ZT поділена за принципом мікросегментації, що в певній мірі є поділом системи на значно менші периметри та подальший їх захист. Усі наведені вище принципи створені для мінімізації або повного запобігання просуванню зловмисників по системі, шляхом жорсткого контролю над привілеями суб'єктів та максимального скорочення площі атаки.

Модель безпеки Zero Trust відкидає наявність довіреного середовища, тому їй не потрібне чітке визначення периметру системи, що робить дану модель не чутливою до його змін.

Zero Trust також передбачає динамічність компонентів системи безпеки. Це стосується як політик безпеки організації, так і механізмів прийняття рішень доступу та реагування на інциденти безпеки. Здатність системи безпеки автоматично реагувати та адаптуватись до змін умов у системі є однією із пріоритетних цілей у даній архітектурі.

Постановка проблеми. Zero Trust - це парадигма, яка постійно розвивається. Не існує єдиного представлення цієї моделі, що в свою чергу не надає можливості створення єдиного способу імплементувати Zero Trust у нову або існуючу систему безпеки.

Імплементація Zero Trust вимагає суттєвих змін у роботі корпоративної системи інформаційної безпеки та організації в цілому. Тому, у процесі переходу на модель Zero Trust, організації стикаються з багатьма труднощами. Першою з них є відсутність повного розуміння поточного стану інформаційної безпеки організації, що унеможливлює здатність прийняття правильних рішень у процесі імплементації.

Наступною проблемою є фінансова доцільність впровадження ZT у організаціях з обмеженими ресурсами. Особливо часто ця проблема виникає у малих та середніх компаніях. Початкова імплементація Zero Trust потребує великих інвестицій у технології, кваліфікований персонал та подальше керування системою. Тому виникає потреба у пріоритизації одних потреб та відмові від інших.

Крім того, організації часто стикаються з проблемами у процесі планування переходу на ZT, виборі потрібного функціоналу, платформ, інструментів, тощо.

Сукупність даних факторів суттєво ускладнює можливість успішної імплементації Zero Trust для майже будь-якої організації. Більшість організацій не мають кваліфікованих експертів з глибоким розумінням даної архітектури, які могли б зрозуміти конкретні потреби організації і впровадити потрібні контролі та відповідний функціонал для контролю їх застосування.

Це створює потребу в організації у єдиному документі всієї фундаментальної інформації про Zero Trust та створенні інструкції для її імплементації, в особливості у організації з застарілими системами інформаційної безпеки. Прикладом такого документу є стандарт NIST SP 800-207. Проте у ньому поверхнево описані підхід до самої імплементації, процес підготовки до неї, її планування, приклади функціоналів для забезпечення принципів Zero Trust, тощо.

Тому процеси підготовки організації до імплементації ZT, планування, впровадження функціоналів та організації і автоматизації потребують детальнішого опису.

Метою статті є запропонувати покроковий підхід до імплементації Zero Trust у наявні архітектури корпоративної безпеки, який надавав би організаціям можливість

підлаштовувати модель під власні умови та потреби з ціллю отримання максимально ефективного та фінансово доцільного результату.

Для досягнення даної мети потрібно:

1. Дослідити особливості процесу імплементації Zero Trust у організації з наявною системою корпоративної безпеки.
2. Визначити кроки, які повинна зробити організація під час цього процесу.
3. Надати інформацію про функціонал, який реалізує принципи Zero Trust.
4. Оцінити потенційну користь від впровадження ZT.

Аналіз останніх досліджень та публікацій. Згідно зі стандартом NIST SP 800-207, Zero Trust - це сукупність концепцій та ідей, створених для мінімізації невизначеностей у прийнятті точних рішень щодо надання доступу за принципом найменших привілеїв у інформаційних системах. У свою чергу, архітектура, або ж модель Zero Trust - це план організації щодо використання концепцій ZT та охоплення взаємозв'язків між компонентами системи, планування робочого процесу та політик доступу.

Zero Trust - це не єдина модель, а сукупність принципів для дизайну системи, які можуть бути використані для покращення стану безпеки.

Основними принципами Zero Trust є:

"Never trust, always verify": жодному компоненту системи не можна довіряти, навіть якщо він знаходиться всередині неї.

"Least privilege access": доступ повинен надаватись у мінімальній потрібній кількості на мінімальний потрібний проміжок часу.

"Assume breach": компоненти системи повинні за замовчуванням вважати, що всередині неї вже знаходяться зловмисники. Середовище системи повинне вважатись недовіреним, через що виникає потреба перевіряти кожен окремий запит.

Модель Zero Trust передбачає захист ресурсів організації, а не периметру її системи. Враховуючи принципи ZT, система повинна постійно оцінювати ризики, пов'язані з ресурсами, для того щоб ефективно надавати мінімальний доступ до них.

Попри достатню популярність теми Zero Trust у наукових дослідженнях, більшість публікацій на тему впровадження даної моделі у існуючі архітектури корпоративної безпеки не дають повного розуміння усіх аспектів цього процесу. А з урахуванням особливостей ZT, як концепції, яка продовжує активно розвиватись, можливість виокремлення найкращого підходу для імплементації цієї моделі залишається під сумнівом.

У нещодавніх дослідженнях на тему впровадження Zero Trust, більшість експертів вважають поетапність імплементації ключовим фактором для її успішності. Наприклад, Вайнберг та Коген зазначають, що для досягнення бажаного результату у процесі впровадження Zero Trust, потрібно розділити його на фази, розставивши пріоритети організації та створивши дорожню карту імплементації. Кожна фаза залежить від попередньої, а остаточний результат впровадження може бути оцінений тільки за роки роботи системи.

У дослідженнях також піднімається тема фінансової доцільності та повернення інвестицій при імплементації Zero Trust. Підкреслюється висока початкова вартість процесу та потреба у пошуку фінансування або відмови від певних потреб. Оладімеджі вважає, що "економічна модель" ZT повинна бути адаптованою під контекст організації, в тому числі під її розміри та потреби.

Також частою є тема інтероперабельності рішень Zero Trust. Дослідники бачать проблему у впровадженні рішень ZT від різних вендорів, надаючи перевагу цілісним та комплексним рішенням від одного. Вайнберг та Коген аргументують це складністю у

процесах впровадження і налагодження їх взаємодії та можливою появою “розривів” у безпеці, що створюватимуть для неї вразливості.

Цао та співавтори у своїй роботі на тему автоматизації та координування архітектури Zero Trust зазначають, що для архітектури ZT не вистачає уніфікованих політик, які б стандартизували підходи до автоматизації деяких процесів, наприклад, політик шифрування та специфікації коду. Наслідком цього є проблема гетерогенності даних, які постачаються системам моніторингу та реагування. Це веде за собою потребу у використанні різних механізмів обробки для різних даних, що призводить до зниження продуктивності.

Підсумовуючи проаналізовані дослідження та публікації, тематика імплементації Zero Trust є доволі частою у наукових дослідженнях, проте деякі аспекти даного процесу залишаються слабко висвітленими, що робить важчим його реалізацію.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Підхід до імплементації Zero Trust у існуючу архітектуру корпоративної безпеки

Перед переходом на модель безпеки Zero Trust, організація повинна впевнитись у своїй готовності до її імплементації як з технічної, так і з фінансової точки зору.

Очевидно, що перехід від Perimeter-Based до Zero Trust моделі безпеки навряд чи може бути здійснений одразу, тому його варто здійснювати поступово, з кількома перехідними періодами. Починати варто з менш важливих елементів системи, й після успішної конфігурації та вирішення проблем, що виникли у її процесі, переходити до більш важливих. Під час перехідних періодів, система буде у стані гібридної моделі безпеки, тому потрібно завчасно подбати про сумісність інструментів ZT та Perimeter-Based, які будуть взаємодіяти між собою в цей час. Також варто врахувати те, що імплементація ZT може стати доволі дороговартісною, що означає потребу оцінити фінансову доцільність процесу.

Рекомендованим є створення всередині організації окремої команди співробітників, які будуть займатись процесом імплементації. Якщо серед працівників немає експертів з відповідними навичками, доцільно запросити зовнішню команду або організацію, яка спеціалізується на цьому процесі.

Ідентифікація поточного стану інформаційної безпеки організації

Перед імплементацією конкретних рішень Zero Trust, організаціія повинна визначити свої потреби та область впровадження. Тому першим кроком стане ідентифікація поточного стану інформаційної безпеки організації, а саме:

1. **Ідентифікація активів організації.**

Цей процес включає в себе не лише їх лістинг, а й їх глибокий аналіз з використанням інструментів для класифікації активів на основі їхньої важливості та рівню ризику, пов’язаним з ними. Для зберігання зібраних знань використовують системи типу CMDB (Configuration Management Database).

2. **Ідентифікація критичних бізнес-процесів.**

Визначення бізнес-процесів, функціонування яких є пріоритетним для організації з точки зору функціонування організації та її безпеки.

3. **Отримання розуміння того, як працює мережевий трафік між компонентами системи.**

Документація того, як дані рухаються всередині мережі, визначення застосунків та сервісів, які взаємодіють з ними, характеру їхньої взаємодії. У цьому можуть допомогти

інструменти для аналізу трафіку, такі як WireShark, SolarWinds NetFlow Traffic Analyzer та інші. Проаналізувавши шляхи передачі даних, можна визначити потенційні вразливі точки системи. Це допоможе запровадити найефективніші контролі та засоби захисту ZT для запобігання втраті даних під час їхнього життєвого циклу.

4. **Інвентаризація пристроїв.**

Лістинг всіх пристроїв, які знаходяться у системі організації. Серед них повинні бути пристрої, якими володіє безпосередньо організація, та по можливості ті, якими володіють співробітники. Зокрема, це потрібно для контролю їхньої конфігурації та захищеності.

5. **Визначення дійових осіб.**

Розуміння всіх суб'єктів, які будуть вести діяльність у системі (співробітників, гостей системи, і тд.), їхніх прав доступу, обов'язків, тощо.

6. **Ідентифікація наявних засобів захисту.**

Виявлення та документація усіх технічних, програмних, фізичних та організаційних засобів захисту та їхнє оцінювання.

Проте цього не достатньо для повного й об'єктивного розуміння стану безпеки системи. Решту аспектів системи часто ігнорують, вважаючи їх аспектами поза межами аналізу (з англ. - out-of-band), за замовчуванням вважаючи їхню безпеку бездоганною, що призводить до хибної оцінки безпеки системи. Щоб запобігти цьому, спектр аналізу безпеки повинен бути розширений як на системному, так і на нижчих рівнях, і жоден аспект не повинен залишатись поза аналізом.

Такий аналіз покращує розуміння поточного стану архітектури системи, що у подальшому стане основою для нової архітектури Zero Trust.

Оцінка ризиків

Після отримання інформації про поточний стан інформаційної безпеки організації, наступним кроком стане оцінка ризиків. Її метою є визначення загроз, реалізація яких може призвести до найбільших збитків для організації, як у фінансовому, так і репутаційному плані. Оцінка ризиків є не менш комплексною за саму імплементацію Zero Trust, і потребує збору великої кількості інформації. Алгоритм цього процесу складається з наступних пунктів:

1) **Вибір підходу оцінки ризиків**

Для початку, слід визначити який підхід оцінки ризиків найбільше підходить під потреби компанії, специфіки її функціонування, тощо. Підходи варіюються в залежності від того, якому фактору приділяється найбільша увага (наприклад, Attack-Based, Threat-based, Control-Centric та інші). Відштовхуючись від цього, організація може обрати найбільш доцільний фреймворк методології оцінки ризиків. Одним з підходів є гібридний, який включає в себе комбінацію фреймворків для кращого аналізу конкретних аспектів оцінки ризиків. Саме його ми й використаємо у цій статті, комбінуючи такі фреймворки як MITRE ATT&CK та FAIR (Factor Analyzis of Information Risk).

2) **Ідентифікація та класифікація критичних активів та бізнес-процесів**

Основний обсяг роботи з ідентифікації та класифікації повинен бути зроблений на кроці визначення поточного стану інформаційної безпеки організації, тут ж потрібно глибше проаналізувати зв'язки та залежності бізнес-процесів та активів.

Для кожного бізнес-процесу потрібно визначити всі його залежності у системі, тобто зв'язки з іншими елементами системи які підтримують його функціонування. Такі елементи системи часто називають підтримуючими, або ж забезпечувальними функціями. До них можуть належати IT-інфраструктура, людські ресурси, ланцюги

постачання, тощо. Такий же аналіз потрібно провести для активів організації, а саме те, які бізнес-процеси вони підтримують, хто є їхнім власником і тд. На основі цієї інформації потрібно визначити, наскільки втрата кожного активу впливає на функціонування того чи іншого бізнес-процесу. Також варто врахувати не тільки прямий вплив, а й побічні наслідки, такі як судові стягнення та втрата репутації при втраті конфіденційних даних клієнтів.

Документація залежностей бізнес-процесів та активів надає можливість для подальшого аналізу загроз та вразливостей, які будуть наступними кроками в оцінці ризиків.

3) **Ідентифікація можливих загроз**

У наступному пункті потрібно визначити потенційні загрози та елементи системи, на які ці загрози можуть бути спрямовані. Для цього ми використаємо фреймворк MITRE ATT&CK. За допомогою нього потрібно визначити актуальні для організації загрози, їх частоту виникнення, типові тактики реалізації цих загроз, та визначити, наскільки реальним є їх застосування в контексті організації.

Одним з інструментів для структуризації отриманої інформації є ATT&CK Navigator, який дозволяє створювати матриці тактик реалізації загроз, які є актуальними для того чи іншого елементу системи.

4) **Виявлення вразливостей**

Основна ціль цього пункту - отримання розуміння того, як і наскільки активи та бізнес-процеси організації вразливі до реалізації загроз, визначених у попередньому пункті. Виявлення вразливостей включає в себе аналіз технологічних та організаційних практик організації на слабкості, які можуть бути використані з ціллю реалізації загроз.

З технічної сторони питання, виявлення вразливостей відбувається шляхом комплексної перевірки систем, мережевого трафіку та застосунків на вразливості до типових загроз. Фреймворк MITRE ATT&CK передбачає автоматизовану та ручну оцінку даних аспектів. Рекомендованими інструментами для автоматизованої оцінки є OPENVAS (комплексне сканування мережі), OWASP ZP (динамічне сканування веб-застосунків) та NMAP (сканування мережі за допомогою NSE скриптів). До способів ручного виявлення вразливостей належить пентестинг компонентів системи.

Не менш важливим є виявлення вразливостей у організаційних практиках організації. До них входять як неправильна організація роботи персоналу, наприклад, його недостатня освіченість в контексті загроз, так і прогалини у політиках доступу. За допомогою аналізу існуючих процедур та політик організації потрібно виявити їхні недостатки, які ведуть до потенційної реалізації загроз.

Після ідентифікації вразливостей, потрібно зв’язати їх з конкретними типами загроз, визначеними у пункті 3. Це дозволить глибокий аналіз кожної вразливості, що в свою чергу допоможе з більш точним їх оцінюванням.

5) **Кількісна оцінка ризиків**

Кількісну оцінку ризиків у цій методології ми проведемо за допомогою моделі обчислення ризиків FAIR, адже вона орієнтується на фінансові втрати, що допоможе визначитидоцільність впровадження кокретних рішень Zero Trust у систему організації.

Ризик у FAIR може обчислюватись за допомогою багатьох аспектів, проте ця модель є адаптивною, тому використання у обчисленні аспектів найглибших рівнів не є обов’язковим і потреби організації у наданні оцінки ризикам цілком можуть задовольнятись за допомогою основних аспектів, поданих на рисунку 1 нижче.

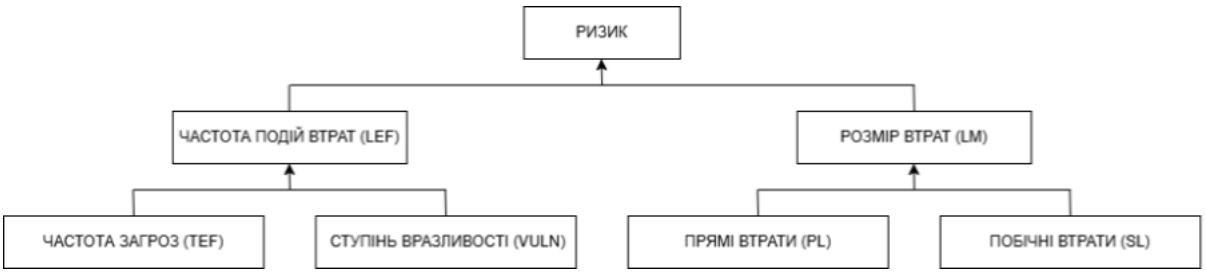

Рис. 1. Основні аспекти розрахунку ризиків у FAIR

Основними аспектами для обчислення ризику є частота подій втрат (Loss Event Frequency (LEF)) та розмір втрат (Loss Magnitude (LM)). Під поняттям частоти подій втрат йдеться про відношення кількості інцидентів, які призводять до втрат, до певного проміжку часу. Найчастіше береться відношення подій втрат/рік. Обчислення частоти подій втрат вимагає кількісної оцінки частоти загроз (Treat Event Frequency (TEF)) та ступеню вразливості активів та бізнес-процесів до них (Vulnerability (VULN)), які повинні бути проаналізовані у пункті 3 і 4 відповідно. Кількісний коефіцієнт TEF визначається як частота появи загрози на рік. VULN це характеристика частоти успішної реалізації загрози у межах від 0 до 1, де 0 означає що вразливості відсутні, а 1 - що атака успішна у 100% випадків.

Частота подій втрат обчислюється за формулою:

$$LEF = TEF \times VULN \quad (1)$$

Поняття розміру втрат ж є визначенням середніх фінансових втрат, з якими стикається організація внаслідок одного інциденту. Розмір втрат складається з прямих (PL) та побічних (SL) втрат і обчислюється як їхня сума. Приклади втрат наведені на таблиці 1.

Таблиця 1

Приклади фінансових втрат, яких може зазнати організація внаслідок інциденту

Прямі втрати	Побічні втрати
Втрати продуктивності, яка призводить до втрати прибутків	Судові витрати
Фінансові витрати на відновлення працездатності	Компенсації клієнтам
Фінансові витрати на розслідування інциденту	Втрати репутації
Фінансові витрати на відновлення пошкоджених активів	Втрати конкурентності

Кінцеве значення ризику обчислюється за формулою:

$$Risk = LEF \times LM \quad (2)$$

Пріоритезація ризиків та розробка плану їх зменшення

Після отримання числових значень всіх ризиків, організація повинна визначити свій план щодо управління ризиками. До цього пункту належить визначення допустимого рівня ризиків шляхом знаходження балансу між стратегічними цілями організації.

Надлишкові ризики повинні бути усунені внаслідок перегляду існуючих практик організації або впровадженням заходів безпеки Zero Trust. Для визначення доцільності імплементації того чи іншого засобу ZT, слід провести порівняння відношення приблизних фінансових витрат, потрбних для цього впровадження, до потенційного зниження суми ризиків.

Формування політик безпеки

Після отримання розуміння про принципи роботи системи та загрози для неї, наступним кроком є формування політик безпеки. Щоб відповідати принципам Zero Trust, вони повинні бути динамічними, тобто постійно змінюватись в залежності від змін у робочих процесах.

Політики доступу є ключовими для Zero Trust. Ефективна імплементація ZT потребує автоматизації процесу прийняття рішень щодо надання доступу до ресурсів організації. Тому організації варто розробити систему для реалізації цього процесу.

Політики доступу реалізуються за допомогою двох механізмів:

- **Механізм прийняття рішень політик (Policy Decision Point (PDP))**

Обробляє запити до ресурсів системи шляхом інтерпретації політик безпеки.

- **Механізм виконання рішень політик (Policy Enforcement Point (PEP))**

Виконує рішення, зроблені PDP, та здійснює моніторинг мережевого трафіку між суб'єктом та ресурсом.

PDP поділяється на два компоненти: адміністратора політик (Police Administrator (PA)) та двигун політик (Policy Engine (PE)). Адміністратор політик приймає політики від системи, зберігає та передає їх PDP. Двигун політик є "мозком" системи політики безпеки, що приймає рішення щодо запитів суб'єктів системи на основі алгоритму довіри (Trust Algorithm). Опрацьовуючи кожен запит, PE збирає дані про нього, а саме зміст запиту, інформацію про суб'єкта, що його здійснює, його роль та дозволи, патерн його дій, тощо. На основі цих даних визначається, задовольняти запит чи ні.

Рисунок 1 відображає копцептуальну модель взаємозв'язків логічних компонентів та їхньої взаємодії, згідно з NIST SP 800-207.

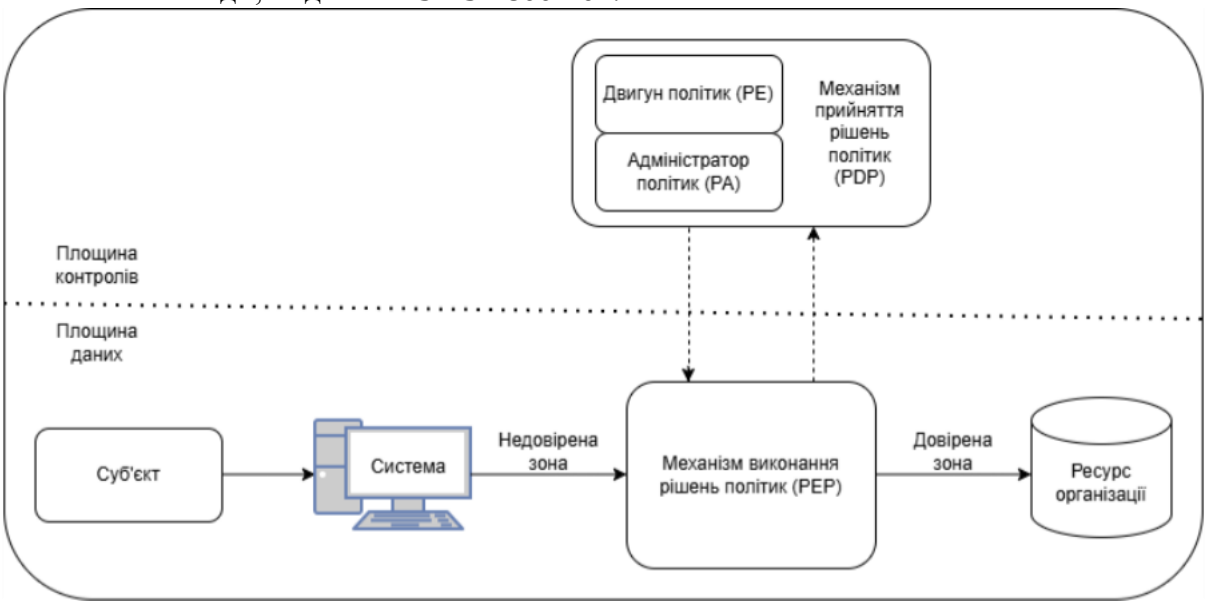

Рис. 2. Концептуальна модель взаємозв'язків компонентів системи надання доступу у архітектурі Zero Trust згідно з NIST SP 800-207

Далі організація повинна визначити, який підхід для обчислення алгоритму довіри вона використовуватиме у своїй системі.

Є два основні підходи в обчисленні алгоритму довіри для надання доступу:

–**На основі критеріїв:** Для отримання доступу до ресурсу, суб'єкт повинен задовольняти певні критерії, наперед визначені політикою доступу. Критерії доступу є динамічними й індивідуальними для кожного ресурсу.

–**На основі рейтингу довіри:** Для отримання доступу до ресурсу суб'єкт повинен мати певну кількість балів рейтингу. Рейтинг збільшується або зменшується на основі поведінки суб'єкта, таких як час автентифікації, кількість її спроб тощо.

Також алгоритми довіри поділяються на **одиночні** та **контекстуальні**. Одиночний алгоритм розглядає надання доступу тільки за поточним запитом, не враховуючи історію попередніх запитів суб'єкта. Його перевагою є швидші розрахунки, але суттєвим недоліком є можливість проведення атаки в межах прав доступу. Контекстуальний алгоритм розглядає не лище поточний, а й попередні запити суб'єкта, перевіряючи їх на підозрілі обставини. Це надає можливість більш динамічного та точного контролю доступу через свою адаптивність, проте потребує збору великої кількості даних про суб'єкт, його патерни поведінки, тощо. Для моделі Zero Trust контекстуальний алгоритм є значно кращим, проте алгоритми не є взаємовиключними, тому можлива їх комбінація в тому чи іншому вигляді.

Для розуміння роботи системи прийняття рішень, розглянемо приклад обробки запиту у системі з контекстуальним алгоритмом довіри на основі рейтингу.

Наприклад, о 22:40, фінансовий аналітик організації з домашнього ноутбука намагається отримати доступ до бази даних фінансових звітів. Система прийняття рішень бере до уваги наступну інформацію про запит:

Інформація про користувача:

- Права доступу користувача: відповідають мінімальним вимогам для доступу до ресурсу. Коефіцієнт довіри 1.0, Вага 0.2 - Рейтинг довіри +0.2.
- Активність: Користувач зазвичай не робить запити до ресурсів в неробочий час. Коефіцієнт довіри 0.2, Вага 0.1 - Рейтинг довіри +0.02.
- Мультифакторна автентифікація: пройдена з першої спроби. Коефіцієнт довіри 1.0, Вага 0.3 - Рейтинг довіри +0.3.
- Місцезнаходження: домашня адреса користувача. Коефіцієнт довіри 0.3, Вага 0.1 - Рейтинг довіри +0.03.

Рейтинг довіри користувача = 0.2 + 0.02 + 0.3 + 0.03 = 0.55

Інформація про пристрій:

- Пристрій не належить організації: Коефіцієнт довіри 0.1, Вага 0.1 - Рейтинг довіри +0.01.
- Конфігурація пристрою (версія ПЗ та застосунків, наявність антивірусу) відповідає більшості вимог організації: Коефіцієнт довіри 0.7, Вага 0.1 - Рейтинг довіри +0.07.
- Мережеве підключення: безпечне. Коефіцієнт довіри 1.0, Вага 0.1 - Рейтинг довіри +0.1.

Рейтинг довіри пристрою = 0.01 + 0.07 + 0.1 = 0.18

Інформація про ресурс:

- Мінімальне значення рейтингу довіри для доступу до ресурсу: 0.7.

Рейтинг довіри = 0.55 + 0.18 = 0.73 > 0.7 - Запит схвалено

Підсумовуючи, для реалізації системи прийняття рішень щодо політик безпеки, потрібно чітко сформулювати політики організації, реалізувати PDP та PEP, їхню взаємодію. Її ефективна взаємодія вимагає накопичення великої кількості даних про

систему, а саме інформації про суб'єкти, пристрої, активи системи, ресурси та розуміння загроз для них, тощо.

Впровадження заходів безпеки

Метою попередніх кроків було визначення нагальних потреб організації, які можуть бути вирішені за допомогою засобів захисту Zero Trust. Наступним кроком стане їх безпосереднє впровадження.

Для початку, потрібно розробити план імплементації, який повинен містити всю інформацію про засоби захисту, які планується запровадити, компоненти системи, щодо яких вони будуть впроваджені, почерговість імплементації, тощо. Стандарт NIST SP 800-207 рекомендує врахування наступних факторів при виборі засобів захисту Zero Trust, які будуть впроваджені у систему організації:

- Чи потрібно встановлювати засоби захисту на активи клієнтів? Використання у бізнес-процесах активів, які не належать організації або належать її партнерам, може нести за собою певні обмеження у робочому процесі.
- Чи працюватиме засіб захисту, якщо ресурси для бізнес-процесів повністю знаходяться у системі організації або за її межами? Розміщення ресурсів може впливати на вибір засобів захисту.
- Чи потребує цей засіб захисту логування взаємодій у системі для їх подальшого аналізу? Одним з ключових компонентів ZT є збір даних про перебіг процесів всередині системи, в тому числі для подальшого їх використання у Двигуні політик (PE).
- Чи засіб забезпечує підтримку різноманітних додатків, сервісів та протоколів?
- Чи засіб потребує змін у поведінці суб'єктів системи?

Відповіді на ці питання можна отримати за допомогою практичного моделювання одного з бізнес-процесів. Як уже згадувалось, починати імплементацію варто із менш важливих компонентів системи з ціллю отримання досвіду, виявлення можливих проблем з конфігурацією та запобіганню можливим ризикам для чутливих активів та системи в цілому.

Для планування та подальшої оцінки прогресу у процесі імплементації Zero Trust, використовують так звані "моделі зрілості", які відображають кроки, які організація повинна виконати для досягнення певного рівня повноцінності Zero Trust (зазвичай цільовим рівнем є ідеальний). Модель зрілості відображає прогрес імплементації у покращенні певних напрямків ZT. Напрямки, або ж "стовпи" визначають на захист яких компонентів системи орієнтована ZT.

Різні моделі зрілості розглядають різні стовпи. Наприклад, модель CISA, яка базується на NIST SP 800-207, розглядає 5 стовпів: Ідентичності, Пристрої, Мережі, Додатки і робочі процеси та Дані. Також між цими стовпами існують 3 наскрізні функції: Видимість та аналітика, Автоматизація та координація і Керування політиками. Модель зрілості від Microsoft бере за основу модель CISA і розглядає 6 стовпів, розділяючи Додатки та робочі процеси на два окремі стовпи. Модель DoD в свою чергу виділяє в CISA дві наскрізні функції, а саме Видимість та аналітику і Організацію та координацію, та розглядає їх як ще два стовпи.

Модель зрілості від компанії ATLAS Advisory, яка базується на основі NIST SP 800-27 та практичних випадках імплементації, не виділяє конкретних напрямків Zero Trust. Проте через свою фінансову орієнтованість, ми розглянемо її детальніше.

Модель від Atlas Advisory визначає шість рівнів зрілості ZT: Традиційний (Baseline), Початковий (Advanced Beginner), Розвинутий (Intermediate), Визначений (Advanced), Керований (Expert) та Оптимізований (Industry Leader). Традиційний рівень

зазвичай означає, що організація ще не розпочала імплементації Zero Trust. Оптимальний в свою чергу означає майже абсолютне забезпечення безпеки інформаційної системи організації за рахунок рішень ZT.

Характеристика кожного рівня описана на таблиці 2:

Таблиця 2

Характеристика рівнів повноцінності Zero Trust у моделі зрілості від ATLAS Advisory SE

Рівень зрілості	**Характеристика**
Традиційний	Безпека на основі периметру; широкий доступ до мережі після автентифікації; обмежена видимість системи; статичні політики безпеки; інструменти безпеки ізольовані між собою
Початковий	Базова сегментація мережі; мультифакторна автентифікація (MFA) до критично важливих застосунків; впроваджені інструменти виявлення пристроїв у мережі; контроль ідентичності привілейованих акаунтів; ручний збір логів
Розвинутий	Початкова мікросегментація; MFA до всіх застосунків; централізоване керування ідентичностями; впроваджена базова система SIEM; автоматичне сканування вразливостей
Визначений	Комплексна мікросегментація; адаптивна автентифікація на основі ризику; постійний контроль стану безпеки пристроїв; автоматизовані процеси реагування на загрози; аналітика поведінки користувачів та сутностей системи (UEBA)
Керований	Впровадженння моделі ZT до всіх ресурсів; постійна авторизація та верифікація; система виявлення та реагування на загрози на основі штучного інтелекту; інтегрована система координування безпеки (SOAR)
Оптимізований	Самовідновлювальна система безпеки; квантово-стійка криптографія; автономні операції безпеки, постійні покращення системи на основі розуміння загроз; реалізований підхід Security-as-code

Покращення зрілості Zero Trust відбувається за рахунок впровадження певного функціоналу, який реалізує принципи ZT. Він в свою чергу реалізується за допомогою використання певних технологій - інструментів, платформ та рішень, які реалізують функціонал. Наведемо приклади основних способів забезпечення роботи системи безпеки за принципами Zero Trust.

Мікросегментація є ключовим функціоналом моделі безпеки Zero Trust. Вона являє собою розбиття мережі на значно менші, ізольовані сегменти, кожен з яких має власні засоби захисту. Перевагами мікросегментації є обмеження площі потенційних атак, їхніх наслідків, та подальшого руху зловмисників по мережі.

За допомогою неї організація може покращити одразу кілька важливих компонентів системи безпеки. По-перше, вона покращує видимість та аналітику системи, дозволяючи ефективний моніторинг та керування взаємодіями між сегментами. Сегментація мережі на логічні компоненти дає детальніше розуміння трафіку між сегментами, що в свою чергу дозволяє виявлення аномальних подій. По-друге, це дає змогу покращити автоматизацію та координування системи, дозволивши ефективніше виявлення підозрілих дій та можливих загроз, які можуть бути непоміченими в загальній мережі.

Як згадувалось раніше, враховуюючи відстуність постійної довіри до будь-якого компоненту як ключовий принцип Zero Trust, виникає потреба у їх постійній перевірці перед наданням їм доступу до ресурсів організації. Тому впровадження ZT потребує використання системи **керування ідентичностями та їхньою авторизацією.** Даний функціонал складається із наступних компонентів:

1) Автентифікація користувача:

Однією з основ ZT є мультифакторна автентифікація (MFA) користувачів. Зазвичай вона містить у собі перевірку користувача за допомогою того, що він знає (пароль), має (смартфон, ID-карта, токен, тощо) та того, ким він є (біометрія). MFA не обов'язково повинна містити всі три фактори, допускається заміна паролів на посилену перевірку за допомогою фактору власності, наприклад криптографічних ключів.

Для того, щоб MFA відповідала принципам ZT, вона повинна бути контекстуальною та постійною. Під контекстуальністю мається на увазі її адаптивність до змін у системі та інтегрованість із політиками доступу. Постійність автентифікації означає періодичні вимоги повторної автентифікації користувача впродовж робочого процесу.

Для впровадження MFA доцільно використовувати такі стандартизовані платформи як OATH, FIDO2 та U2F.

2) Автентифікація пристроїв

Для автентифікації пристроїв також використовується мультифакторна автентифікація. Її фактори базуються на основі:

- **Сертифікатів.** Ідентичність пристрою підтверджується криптографічним сертифікатом. Їх на пристрій встановлює спеціальний персонал.
- **Постачальника.** Постачальник встановлює у пристрій спеціальне апаратне забезпечення, яке підтверджує його ідентичність. При додаванні цього пристрою у систему організації, для його подальшої ідентифікації система буде використовувати саме дані від постачальника, що покращує автоматизацію.
- **Характеристик пристрою.** Подібно до людської біометрії, ідентичність підтверджується унікальними характеристиками пристрою. Їх прикладом є фізичні характеристики каналу між пристроєм та автентифікатором.

Так само як і автентифікація користувачів, автентифікація пристроїв повинна бути контекстуальною та постійною.

3) Керування ідентичностями

Враховуючи те, що користувачі та пристрої можуть мати кілька ідентичностей, для керування ними використовують **системи керування ідентичностями та їх доступами** (Identity and Access Management (IAM) systems). Функція контролю доступу у цій статті вже була частково описана при реалізації політик доступу. Тому зараз ми сфокусуємось на керуванні ідентичностями у системі. Для цього використовують системи управління ідентичностями (Identity Management(IdM)), які збирають інформацію про ідентичності системи, їхню автентифікацію та використання. Системи IdM є ключовими для координації автентифікації ідентичностями між усіма функціоналами Zero Trust. Зазвичай вони складаються з трьох компонентів: постачальника послуг, ідентичності, яка робить запит до сервісу, та постачальника ідентичностей, який відповідає за створення, перевірку та зберігання ідентичностей системи.

Є кілька моделей систем управління ідентичностями - ізольовані, централізовані та федералізовані, які відрізняються між собою типом взаємодії між постачальником послуг та постачальником ідентичностей. У ізольованій моделі вони є однією сутністю. У централізованій всі постачальники послуг використовують одного постачальника ідентичностей, що дозволяє використовувати технологію Single Sign-On (SSO). Федералізована модель дозволяє постачальникам сервісів розпізнавати ідентичності від різних постачальників ідентичностей.

Розглянемо федералізовану модель детальніше. Її можна розширити, інтегрувавши в неї хмарні ідентичності системи, наприклад через Azure AD. Також вона підтримує

інтеграцію технології SSO. Через свою гнучкість, федеративна модель є оптимальним варіантом для моделі Zero Trust.

Рішення IAM інтегруються з різними технологіями й інструментами, щоб забезпечити захищену автентифікацію та авторизацію на рівні всієї організації. Наприклад, Microsoft рекомендує систему SAML для реалізації єдиного входу ідентичності у систему та OpenID Connect на основі OAuth 2.0 для перевірки ідентичностей.

Для загальної безпеки системи важливою є безпека кожного пристрою, що входить до неї. Тому, щоб відповідати принципам Zero Trust, політики доступу повинні брати до уваги стан безпеки пристроїв, які роблять запити в системі. Автентифікації пристроїв недостатньо для того, щоб вважати їх безпечними для роботи у мережі організації, тому виникає потреба у розширеному **контролі пристроїв**.

Процес перевірки стану безпеки пристроїв та їхньої відповідності до вимог для роботи у мережі називають валідацією пристроїв. Зазвичай він забезпечується за допомогою систем UEM (Unified Endpoint Management) та EDR (Endpoint Detection and Response). Вони контролюють відповідність конфігурації пристроїв системи до заданих вимог, їхню активність та допомагають організовувати робочий процес даних пристроїв. Зокрема, перевіряється така інформація як тип власності пристрою (належить він організації чи ні), версії програмного забезпечення, антивірусів та застосунків, тощо.

Системи UEM дозволяють організаціям власноруч налаштовувати і оновлювати ПЗ та застосунки на пристроях співробітників. Однією з захисних функцій є можливість віддаленого стирання даних або блокування пристрою при його викрадені. Крім того, вони дають можливість інвентаризувати пристрої системи. Провідними системами UEM є Microsoft Intune, VMware Workspace One та IBM Security MaaS360. В свою чергу, системи EDR фіксують підозрілу активність пристроїв та автоматично проводять їх обробку. Прикладом EDR є Microsoft Defender for Endpoint.

Видимість системи є наскрізною функцією Zero Trust, яка охоплює всі її напрямки. Тому для організації процесів виявлення загроз, реагування на них та їх подальшого аналізу виникає потреба у функціонуванні системи **моніторингу та аналітики системи.** Вона включає у себе збір усіх даних про події всередині системи та виявлення ознак загроз. Ефективна робота даного функціоналу потребує його інтегрування із системою IAM, яка надаватиме системам моніторингу та аналітики інформацію про всі події, пов’язані з автентифікаціями та доступами у системі.

Для реалізації даного функціоналу використовують системи SIEM (Security Incident and Event Management). Впровадження таких систем відбувається у три етапи. Першим є збір інформації про типові події безпеки у системі, тобто події, які мають ознаки певних загроз. Для цього системи SIEM доповнюються системами постійної діагностики та реагування (Continous Diagnostics and Mitigation (CDM) systems), які здійснюють збір інформації з пристроїв. Наступним етапом є надання системі розуміння конкретних зовнішніх загроз, наприклад, сигнатури типових атак. Останнім етапом є налаштування моніторингу та аналітики системи з метою забезпечення процесу аналізу подій безпеки та порівняння їх із ознаками конкретних загроз.

Завершенням забезпечення принципів Zero Trust є **автоматизація та координація системи**. Вона включає у себе використання програмного забезпечення та інструментів для автоматизації процесів всередині системи, знижуючи при цьому потребу у ручному керуванні нею. Особливо важливою автоматизація стає у ситуаціях, коли у системі водночас стається багато подій безпеки, і персонал не здатен їх обробити. Для

забепечення автоматизації та координування використовуються системи SOAR (Security Orchestration, Automation and Response). Між раніше згаданими системами SIEM та системами SOAR існує тісний зв'язок, адже саме SIEM виконує основний обсяг збору та обробки даних про події, які потім використовує SOAR. SOAR в свою чергу приймає рішення щодо реагування системи безпеки на інциденти та мінімізує їх наслідки за допомогою засобів захисту. Загалом, система автоматизації та координації є "мозком" системи безпеки, який керує функціонуванням решти компонентів системи.

Зараз SOAR та SIEM часто інтегруються між собою на рівні виробників даних систем. Провідними прикладами таких систем є Microsoft Sentinel та IBM Security QRadar.

Моніторинг та підтримка системи, її розширення

Певний період часу після імплементації Zero Trust, організації варто проводити повний моніторинг системи з метою оцінки її довгострокової роботоздатності. Під час нього потрібно задокументувати нові знання, які з'явились вже після початку роботи системі за принципами моделі ZT. До них належать додаткові відомості про поведінку компонентів системи та взаємодії між ними.

Також, для організації важливою є адаптація "культури Zero Trust" серед співробітників. Робочий процес у системах ZT може відрізнятись від того, що був раніше. Це може призвести до зменшення ефективності роботи працівників, що в свою чергу вплине на продуктивність організації. Щоб запобігти цьому, організації варто виділити час та ресурси на ознайомлення співробітників з особливостями роботи у системі ZT. Також варто сформувати певні політики щодо роботи у такій системі.

Очевидно, що навіть повна імплементація ZT у систему безпеки організації не може повністю і назавжди забезпечити її інформаційну безпеку. Організація не може зупинитись на імплементації, вона повинна постійно оновлювати та покращувати безпеку. У протилежному випадку, в певний момент система безпеки повністю втратить свою ефективність, після чого відновлення її функціонування стане набагато важчим та дороговартісним, ніж підтримка ZT від самого початку її впровадження.

Разом із розширенням системи, потрібно переглядати доцільність впровадження ZT у нові бізнес-процеси організації. Для цього потрібно постійно проходити цикл кроків імплементації, які були наведені у даній роботі, шукаючи способи покращити існуючу систему безпеки.

Практичний приклад імплементації

Раніше у статті ми розглядали модель зрілості від компанії ATLAS Advisory, яка займається забезпеченням інформаційної безпеки комерційних організацій по всій Європі, в тому числі імплементацією Zero Trust у застарілі системи безпеки організацій. На їхній практиці було кілька хороших прикладів зменшень фінансових втрат компаній шляхом впровадження засобів ZT, які ми зараз і розглянемо.

Випадок 1. Європейська фінансова установа (8500 працівників)

Установа поставила перед ATLAS Advisory ціль забезпечити роботу системи згідно з регламентом щодо цифрової стійкості фінансових установ ЄС DORA та директивою ЄС щодо правил кібербезпеки критичних секторів економіки NIS2. Також за мету було взято забезпечити безпеку віддаленої роботи працівників організації.

Після проведення початкового аудиту інформаційної безпеки установи, було виявлено, що практики організації мали кілька важливих недоліків, які не дозволяли безпечного віддаленого доступу співробітників. В першу чергу, віддалений доступ був організований на основі VPN, що було водночас дороговартісним та вразливим рішенням. Система керування ідентичностями представляла собою кілька ізольованих

систем, які не узгоджували . При аналізі роботи хмарних середовищ, було виявлено невідповідності з вимогами DORA та NIS2. Також у системі організації функціонувало 127 різних додатків, що суттєво ускладнювало їх контроль та загальну видимість системи.

Для вирішення даних проблем та досягнення поставлених цілей, у організації було впроваджено низку рішень Zero Trust. В першу чергу, за основу безпеки було взято стратегію Cloud-first Zero Trust від Zscaler, яка є об'єднанням концепцій пріоритезації у системі організації хмарних сервісів та концепції нульової довіри. Одним з недоліків такого підходу є підвищений ризик втрати даних, тому разом із ним було інтегровано систему запобігання втраті даних на базі платформи Microsoft Purview.

Для виправлення прогалин у керуванні ідентичностями всередині організації було впроваджено систему IAM на основі платформ OKTA та Thales SafeNet. Зокрема, в рамках цієї системи було впроваджено безпарольну мультифакторну автентифікацію на основі платформи FIDO2. Також, за допомогою модуля GRC від платформи ServiceNow, було запроваджено систему постійного моніторингу відповідності роботи системи вимогам DORA та NIS2.

Після 14 місяців роботи даної фінансової установи після імплементації рішень ZT, було проведено аналітику досягнутих результатів. В результаті неї визначено, що впровадження ZT принесло організації суттєві покращення як у технічних, так і у фінансових аспектах. У першу чергу слід відзначити, що були досягнуті ключові поставлені цілі, а саме досягнення повної готовності системи до безпечної віддаленої роботи працівників, а випадки порушень вимог DORA та NIS2 під час робочого процесу скоротились на 83%. Успішність фішингових атак знизилась на 96%. Також на 45% пришвидшено процес надання доступів, що підвищило продуктивність працівників та за деякими оцінками збільшило річний дохід організації приблизно на 890.000 євро на рік. Відмова від VPN та у організації віддаленої роботи дозволила скоротити витрати приблизно на 450.000 євро на рік.

Випадок 2. Мережа закладів надання медичних послуг (22000 працівників, 45 закладів)

Перед ATLAS Advisory SE було поставлено мету забезпечити захист даних клієнтів та медичного обладнання від зловмисників, у першу чергу від атак за допомогою програм-вимагачів (ransomware), що є частою проблемою для сфери діяльності організації. Такий інцидент нещодавно траплявся і у даній мережі закладів, що призвело до збитків на суму 1.8 мільйона євро. Також за мету було взято забезпечення відповідності роботи організації до вимог Загального регламенту захисту даних ЄС (GDPR).

Після проведення початкового аудиту, було визначено, що мережева архітектура організації є "плоскою", тобто у ній відсутня сегментація, що суттєво погіршує контроль над доступами користувачів та видимість у системі. Також було виявлено, що тисячі медичних пристроїв працюють на базі застарілих систем, що ускладнює їхню інтеграцію у системи EDR та SIEM. Надання доступів у організації надання доступів відбувається за допомогою паперових дозволів та документів, що очевидно є застарілим та сповільнює процеси отримання та скасування доступу для персоналу.

Для подолання проблеми "плоскості" мережі, у ній було проведено логічну сегментацію пристроїв. Сам доступ до мережі був забезпечений за принципами Zero Trust Network Access (ZTNA) на основі платформи Cisco ACI. Видимість у ній було покращено за допомогою платформи Forescout.

Задля впровадження системи надання доступу на основі ризиків, було впроваджено систему IAM на основі платформ Ping Identity та BeyondTrust.

Також для автоматизації систем реагування на інциденти безпеки * та координування системи було впроваджену систему Cortex XSOAR від компанії Palo Alto.

Як результат даних заходів, після 20 місяців роботи організації було досягнуто великого прогресу у досягеннні поставлених цілей. Статистика інцидентів, пов'язаних з витоком даних клієнтів та ransomware в середньому скоротилась із 2 до 0 та з 3 до 0 випадків на рік відповідно. Аудит відповідності робочого процесу до вимог GDPR показав результат 96% (для порівняння, до імплементації цей показник був 67%). З інших результатів, варто відзначити досягнення стовідсоткової видимості пристроїв у системі. Час реагування на інциденти безпеки в середньому скоротився з 45 до менш ніж 2 хвилин. Сама організація після імплементаціїї скоротила витрати на страхування інформаційної безпеки на 38%.

Крім цього, процес імплементації не призвів до зупинки надання послуг для клієнтів.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У даній роботі було розглянуто можливості імплементації моделі Zero Trust у організації з наявною архітектурою корпоративної безпеки. Враховуючи тенденції останніх років та свої фундаментальні недоліки, модель безпеки на основі периметру почала втрачати свою актуальність. Організації почали пошук нової моделі безпеки, яка б закривала прогалини моделі Perimeter-Based та водночас задовольняла власні потреби організацій. Більшість з них знайли вирішення цих завдань у концепції Zero Trust, тому вони розпочали перехід на дану архітектуру. Особливо активно такий перехід розпочався у останні 5 років, що доводить актуальність даної теми. Проте, після аналізу останніх досліджень було виявлено, що ця тема є ще недостатньо вивченою, у першу чергу через особливості Zero Trust, як парадигми, яка досі активно розвивається.

У роботі було досліджено та запропоновано методологію, яка могла б допомогти організаціям у процесі імплементації ZT. Наведено кроки, які варто здійснити, задля отримання максимально ефективного та фінансово доцільного результату.

Зокрема, було запропоновано гібридну методологію оцінки ризиків на основі фреймворків MITRE ATT&CK та FAIR, призначену для переведення загроз та вразливостей для активів організації у фінансовий еквівалент втрат з метою пріоритезації ризиків та їхнього подальшого зниження.

На кроці формування політик безпеки було описано концептуальну модель системи прийняття рішень надання доступу, в тому числі підходи до реалізації алгоритму довіри. Як приклад було наведено контекстуальне обчислення алгоритму довіри на основі рейтингу.

Основною частиною процесу імплементації було визначено впровадження заходів захисту Zero Trust. До нього відноситься планування процесу імплементації та безпосередня імплементація вибраних засобів захисту. Для полегшення оцінки повноцінності ZT було запропоновано орієнтуватись на "моделі зрілості" Zero Trust. Як приклад такої моделі було описано модель від компанії ATLAS Advisory з описом характеристик конкретних рівнів зрілості. Також у роботі було наведено приклади впровадження функціоналів, що реалізують принципи Zero Trust та взаємозв'язок між ними.

Після завершення процесу імплементації визначено потребу у подальшій підтримці та покращенні системи безпеки, а також проведення заходів, пов'язаних з адаптацією "культури Zero Trust" серед працівників організації.

Як приклад впровадження Zero Trust у існуючі системи безпеки організацій, було наведено реальний досвід від компанії ATLAS Advisory, який доводить те, що ця модель безпеки зараз є нагальною потребою, а не розкішшю для організацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. National Institute of Standards and Technology. (n.d.). *NIST Special Publication 800-207. Zero Trust Architecture.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (accessed 22.11.2025)
2. MITRE. (n.d.). *MITRE ATT&CK® framework.* https://attack.mitre.org/ (accessed 22.11.2025)
3. FAIR Institute. (2025). *FAIR 3.0. Factor Analysis of Information Risk.* https://www.fairinstitute.org/hubfs/Standards%20Artifacts/Factor%20Analysis%20of%20Information%20Risk%20%28FAIR%29%20Standard%20v3.0%20%28January%202025%29.pdf (accessed 22.11.2025)
4. Palo Alto Networks. (n.d.). *Asset discovery and prioritization.* https://docs.paloaltonetworks.com/best-practices/zero-trust-best-practices/zero-trust-best-practices/the-five-step-methodology/step-1-asset-discovery-and-prioritization (accessed 22.11.2025)
5. Papakonstantinou, N., Van Bossuyt, D., Linnosmaa, J., Hale, B., & O'Halloran, B. (2021). A zero trust hybrid security and safety risk analysis method. *Journal of Computing and Information Science in Engineering, 21,* 1–26. https://www.researchgate.net/publication/350440983_A_Zero_Trust_Hybrid_Security_and_Safety_Risk_Analysis_Method (accessed 22.11.2025)
6. Weinberg, A., & Cohen, K. (2024). Zero trust implementation in the emerging technologies era: A survey. *Complex Engineering Systems, 4.* https://www.researchgate.net/publication/384451867_Zero_trust_implementation_in_the_emerging_technologies_era_a_survey/citation/download (accessed 22.11.2025)
7. Oladimeji, G. (2024). A critical analysis of foundations, challenges and directions for Zero Trust security in cloud environments. *arXiv.* https://doi.org/10.48550/arXiv.2411.06139 (accessed 22.11.2025)
8. Cao, Y., Pokhrel, S., Zhu, Y., Doss, R., & Li, G. (2024). Automation and orchestration of Zero Trust architecture: Potential solutions and challenges. *Machine Intelligence Research, 21.* https://www.researchgate.net/publication/377719977_Automation_and_Orchestration_of_Zero_Trust_Architecture_Potential_Solutions_and_Challenges (accessed 22.11.2025)
9. Teerakanok, S., Uehara, T., & Inomata, A. (2021). Migrating to Zero Trust architecture: Reviews and challenges. *Security and Communication Networks.* https://www.researchgate.net/publication/351879191_Migrating_to_Zero_Trust_Architecture_Reviews_and_Challenges (accessed 22.11.2025)
10. Sunkara, G. (2025). Implementing Zero Trust architecture in modern enterprise networks. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, 17*(11). https://www.researchgate.net/publication/393185151_Implementing_Zero_Trust_Architecture_in_Modern_Enterprise_Networks (accessed 22.11.2025)
11. Sanchez Garcia, I., Mejia, J., & San Feliu, T. (2022). Cybersecurity risk assessment: A systematic mapping review, proposal, and validation. *Applied Sciences, 13*(395). https://www.researchgate.net/publication/366660649_Cybersecurity_Risk_Assessment_A_Systematic_Mapping_Review_Proposal_and_Validation (accessed 22.11.2025)
12. Olzak, T. (2025). Cybersecurity risk analysis and management. *ResearchGate.* https://www.researchgate.net/publication/389652223_Cybersecurity_Risk_Analysis_and_Management (accessed 22.11.2025)
13. Poirrier, A., Cailleux, L., & Clausen, T. (2025). Is trust misplaced? A Zero-Trust survey. *Proceedings of the IEEE,* 1–35. https://www.researchgate.net/publication/391001687_Is_Trust_Misplaced_A_Zero-Trust_Survey (accessed 22.11.2025)
14. Microsoft. (n.d.). *What is identity access management (IAM).* https://www.microsoft.com/uk-ua/security/business/security-101/what-is-identity-access-management-iam (accessed 22.11.2025)
15. Microsoft. (n.d.). *What is SOAR?* https://www.microsoft.com/uk-ua/security/business/security-101/what-is-soar (accessed 22.11.2025)

16. Cybersecurity and Infrastructure Security Agency. (n.d.). *CISA Zero Trust Maturity Model.* https://www.cisa.gov/zero-trust-maturity-model (accessed 22.11.2025)
17. Schneider, M. (2025). *Zero Trust Architecture: Complete implementation guide for enterprise organizations 2025.* ATLAS Advisory. https://atlas-advisory.eu/en/insights/zero-trust-architecture-guide (accessed 22.11.2025)
18. Phiayura, P., & Teerakanok, S. (2023). A comprehensive framework for migrating to Zero Trust architecture. *IEEE Access*, 1–1. https://www.researchgate.net/publication/368795473_A_Comprehensive_Framework_for_Migrating_to_Zero_Trust_Architecture (accessed 22.11.2025)
19. Abdelmagid, A., & Diaz, R. (2025). Zero Trust architecture as a risk countermeasure in small–medium enterprises and advanced technology systems. *Risk Analysis*, *45*, 2390–2414. https://www.researchgate.net/publication/390166384_Zero_Trust_Architecture_as_a_Risk_Countermeasure_in_Small-Medium_Enterprises_and_Advanced_Technology_Systems (accessed 22.11.2025)

.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023

Ostap Horodytskyi
Student of the Department of Information Protection
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0009-0000-7785-5582
ostap.horodytskyi.kb.2024@lpnu.ua

Ivan Opirskyy
Doctor of Technical Sciences, Professor, Head of the Department of Information Protection
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

STEP-BY-STEP APPROACH TO IMPLEMENTING ZERO TRUST IN HYBRID CORPORATE SECURITY SYSTEMS

Abstract. This article explores opportunities of implementing Zero Trust (ZT) model into organizations with Perimeter-Based security system. It describes changes that occurred in recent years and had an impact on organizations' corporate security systems. The reasons of the declining relevance of Perimeter-Based model and its shortcomings have been explained. Explained why organizations increasingly adopt Zero Trust in their information security systems and which problems of Perimeter-Based model it solves. Outlined problems that organizations usually encounter during ZT implementation. Presented brief overview of Zero Trust model. This includes a description of its core principles, experts' perspectives on the model, and considerations regarding its implementation. The specific features of implementing Zero Trust within organizations' existing security systems have been examined. It has been established that the effective implementation of Zero Trust requires a comprehensive, multi-step approach. The initial steps involve auditing the current state of an organization's information security and assessing the risks associated with its assets. These preparatory measures aim to define the scope of implementation and identify the organization's priority needs regarding ZT. The next step is defining and implementation of security policies. It has been established that the main part of implementation process is direct deployment of functionalities that enforce principles of Zero Trust. It begins with developing implementation plan, specifying which security measures will be applied to particular system components and in what sequence. To measure completeness of Zero Trust, an example of "maturity model" has been provided. Additionally, the functionalities whose implementation enforces the principles of Zero Trust, as well as the relationships between them, were presented. This also includes a description of network microsegmentation, the implementation of MFA technologies and IAM (Identity and Access Management) systems, the use of UEM and UDR solutions for device control, as well as SIEM for threat detection and SOAR for automating and coordinating the security system. As a conclusion of the implementation process, the necessity for continuous review and improvement of the security system has been substantiated. Practical examples of Zero Trust implementation have also been examined, demonstrating the effectiveness and relevance of transitioning to a Zero Trust architecture. The results may serve as practical demonstration of capabilities and benefits of transitioning to a ZT security architecture, to provide an understanding of the challenges encountered during its implementation, and define effective and cost-efficient approach to carry out this process.

Keywords: Zero Trust, implementation, methodology, step-by-step approach, security architecture, corporative security, risk assessment, maturity model, microsegmentation, IAM, UEM, SIEM, SOAR, network security, information security.

REFERENCES

1. National Institute of Standards and Technology. (n.d.). *NIST Special Publication 800-207. Zero Trust Architecture.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (accessed 22.11.2025)

2. MITRE. (n.d.). *MITRE ATT&CK® framework.* https://attack.mitre.org/ (accessed 22.11.2025)
3. FAIR Institute. (2025). *FAIR 3.0. Factor Analysis of Information Risk.* https://www.fairinstitute.org/hubfs/Standards%20Artifacts/Factor%20Analysis%20of%20Information%20Risk%20%28FAIR%29%20Standard%20v3.0%20%28January%202025%29.pdf (accessed 22.11.2025)
4. Palo Alto Networks. (n.d.). *Asset discovery and prioritization.* https://docs.paloaltonetworks.com/best-practices/zero-trust-best-practices/zero-trust-best-practices/the-five-step-methodology/step-1-asset-discovery-and-prioritization (accessed 22.11.2025)
5. Papakonstantinou, N., Van Bossuyt, D., Linnosmaa, J., Hale, B., & O'Halloran, B. (2021). A zero trust hybrid security and safety risk analysis method. *Journal of Computing and Information Science in Engineering, 21*, 1–26. https://www.researchgate.net/publication/350440983_A_Zero_Trust_Hybrid_Security_and_Safety_Risk_Analysis_Method (accessed 22.11.2025)
6. Weinberg, A., & Cohen, K. (2024). Zero trust implementation in the emerging technologies era: A survey. *Complex Engineering Systems, 4.* https://www.researchgate.net/publication/384451867_Zero_trust_implementation_in_the_emerging_technologies_era_a_survey/citation/download (accessed 22.11.2025)
7. Oladimeji, G. (2024). A critical analysis of foundations, challenges and directions for Zero Trust security in cloud environments. *arXiv.* https://doi.org/10.48550/arXiv.2411.06139 (accessed 22.11.2025)
8. Cao, Y., Pokhrel, S., Zhu, Y., Doss, R., & Li, G. (2024). Automation and orchestration of Zero Trust architecture: Potential solutions and challenges. *Machine Intelligence Research, 21.* https://www.researchgate.net/publication/377719977_Automation_and_Orchestration_of_Zero_Trust_Architecture_Potential_Solutions_and_Challenges (accessed 22.11.2025)
9. Teerakanok, S., Uehara, T., & Inomata, A. (2021). Migrating to Zero Trust architecture: Reviews and challenges. *Security and Communication Networks.* https://www.researchgate.net/publication/351879191_Migrating_to_Zero_Trust_Architecture_Reviews_and_Challenges (accessed 22.11.2025)
10. Sunkara, G. (2025). Implementing Zero Trust architecture in modern enterprise networks. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, 17*(11). https://www.researchgate.net/publication/393185151_Implementing_Zero_Trust_Architecture_in_Modern_Enterprise_Networks (accessed 22.11.2025)
11. Sanchez Garcia, I., Mejia, J., & San Feliu, T. (2022). Cybersecurity risk assessment: A systematic mapping review, proposal, and validation. *Applied Sciences, 13*(395). https://www.researchgate.net/publication/366660649_Cybersecurity_Risk_Assessment_A_Systematic_Mapping_Review_Proposal_and_Validation (accessed 22.11.2025)
12. Olzak, T. (2025). Cybersecurity risk analysis and management. *ResearchGate.* https://www.researchgate.net/publication/389652223_Cybersecurity_Risk_Analysis_and_Management (accessed 22.11.2025)
13. Poirrier, A., Cailleux, L., & Clausen, T. (2025). Is trust misplaced? A Zero-Trust survey. *Proceedings of the IEEE*, 1–35. https://www.researchgate.net/publication/391001687_Is_Trust_Misplaced_A_Zero-Trust_Survey (accessed 22.11.2025)
14. Microsoft. (n.d.). *What is identity access management (IAM).* https://www.microsoft.com/uk-ua/security/business/security-101/what-is-identity-access-management-iam (accessed 22.11.2025)
15. Microsoft. (n.d.). *What is SOAR?* https://www.microsoft.com/uk-ua/security/business/security-101/what-is-soar (accessed 22.11.2025)
16. Cybersecurity and Infrastructure Security Agency. (n.d.). *CISA Zero Trust Maturity Model.* https://www.cisa.gov/zero-trust-maturity-model (accessed 22.11.2025)
17. Schneider, M. (2025). *Zero Trust Architecture: Complete implementation guide for enterprise organizations 2025.* ATLAS Advisory. https://atlas-advisory.eu/en/insights/zero-trust-architecture-guide (accessed 22.11.2025)
18. Phiayura, P., & Teerakanok, S. (2023). A comprehensive framework for migrating to Zero Trust architecture. *IEEE Access*, 1–1.
19. Abdelmagid, A., & Diaz, R. (2025). Zero Trust architecture as a risk countermeasure in small–medium enterprises and advanced technology systems. *Risk Analysis, 45*, 2390–2414.