КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.22.179190
УДК 004.056

**Журавчак Даниїл Юрійович**
аспірант, асистент кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID 0000-0003-4989-0203
*danyil.y.zhuravchak@lpnu.ua*

**Глущенко Павло Костянтинович**
аспірант кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID 0000-0002-1262-5484
*pavlo.k.hlushchenko@lpnu.ua*

**Опанович Максим Юрійович**
аспірант кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID 0000-0002-2748-2965
*maksym.y.opanovych@lpnu.ua*

**Дудикевич Валерій Богданович**
доктор технічних наук, професор кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID 0000-0001-8827-9920
*valerii.b.dudykevych@lpnu.ua*

**Піскозуб Андріян Збігнєвич**
кандидат технічних наук, доцент кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID 0000-0002-3582-2835
*andriian.z.piskozub@lpnu.ua*

# КОНЦЕПЦІЯ НУЛЬОВОЇ ДОВІРИ ДЛЯ ЗАХИСТУ ACTIVE DIRECTORY ДЛЯ ВИЯВЛЕННЯ ПРОГРАМ-ВИМАГАЧІВ

**Анотація.** У цій науковій статті розглядається підхід до захисту Active Directory від загроз, пов'язаних з програмами-вимагачами, що стають все більш надзвичайно небезпечними для корпоративних інформаційних систем. Концепція «нульової довіри» в контексті Active Directory визначається як підхід, спрямований на виключення довіри зі структури системи безпеки та постійну перевірку користувача та його пристрою щодо відповідності налаштованим політикам безпеки, контексту та іншим параметрам. У статті розглядаються методи та інструменти, які дозволяють реалізувати концепцію нульової довіри в середовищі Active Directory, включаючи аналіз поведінки, моніторинг мережевого трафіку та використання розширених правил безпеки. Також досліджується важливість поєднання технологій обробки подій та штучного інтелекту для автоматизованого виявлення та реагування на аномальну активність. Результати дослідження вказують на можливість підвищення ефективності захисту Active Directory від загроз програм-вимагачів і забезпечення стійкості корпоративних мереж перед ними. Використання концепції нульової довіри може стати важливим кроком у забезпеченні кібербезпеки та збереженні надійності інформаційних ресурсів у сучасних підприємствах. Крім того, впровадження моделі нульової довіри в Active Directory узгоджується з розвитком ландшафту загроз. Оскільки атаки програм-вимагачів продовжують прогресувати, потреба в надійних заходах безпеки стає першорядною. Проактивний та адаптивний підхід Zero trust гарантує, що навіть якщо зловмисники порушують початковий захист, вони стикаються з додатковими рівнями перевірки, що робить бічне переміщення та витік даних набагато складнішим. В час, коли атаки програм-вимагачів можуть порушити бізнес-операції та скомпрометувати

конфіденційні дані, прийняття підходу нульової довіри в Active Directory є стратегічним переходом до більш безпечного та стійкого корпоративного IT-ландшафту.

**Ключові слова:** віруси-вимагачі; несанкціонований доступ; Active Directory; архітектура нульової довіри.

## ВСТУП

Сучасний світ неможливо уявити без цифрових технологій, що вбудовані в усі сфери життя — від освіти і медицини до бізнесу і розваг. Однак з розвитком цифрового простору зростає й кількість потенційних загроз для інформаційної безпеки. Однією з найбільш серйозних та актуальних проблем є програми-вимагачі, що мають на меті заблокувати доступ до системи або даних, а потім вимагають від користувача викуп за їх «відновлення».

Поточний стан досліджень у даній сфері продемонстрував багато методів боротьби з програмами-вимагачами, але не всі з них ефективні проти шкідливого програмного забезпечення, яке цільово атакує технології керування доступом, зокрема Active Directory. Active Directory (AD) від Microsoft є однією з найпоширеніших систем управління ідентифікацією та авторизацією в корпоративних мережах. Саме тому безпека AD має величезне значення для багатьох організацій.

Ця тема важлива, оскільки існує нагальна потреба в розробці нових та ефективних методів захисту AD від програм-вимагачів. Такі методи можуть запобігти значним втратам, які можуть виникнути в результаті атак. Дослідження таких методів є надзвичайно актуальним та важливим для інформаційної безпеки.

Основне питання, що ставиться в цій статті, полягає в тому, як можна використати концепцію нульової довіри для захисту AD від програм-вимагачів. Гіпотеза полягає у тому, що стратегія нульової довіри, яка передбачає неперервну верифікацію та перевірку всіх елементів системи, може значно підвищити ефективність захисту AD від шкідливого програмного забезпечення, або унеможливити потрапляння вірусів-вимагачів у корпоративну мережу взагалі.

**Постановка проблеми.** У цій роботі розглядається підхід до захисту Active Directory від загроз пов’язаних з вірусами-вимагачами на основі впровадження концепції «нульової довіри», що спрямований на виключення довіри зі структури системи безпеки. Так як концепція стає все більш популярною серед таких великих компаній як Microsoft, є доцільним дослідити поточні можливості впровадження та переваги даної концепції.

**Аналіз останніх досліджень і публікацій.** Макдональд, Г та інші, вказують на критичну роль Active Directory як основної системи ідентифікації та автентифікації, що робить її привабливою мішенню для кіберзлочинців [1]. Проблема полягає у тому, що багато традиційних систем безпеки не виявляють підозрілу активність, якщо вона відбувається в рамках дозволених прав користувача. Зловмисники використовують тактики, які оминають звичайні системи виявлення, зосереджуючись на крадіжці облікових даних, ескалації привілеїв та горизонтальному переміщенні. У відповідь на це, рішення для видимості ідентифікаторів та відповіді на інциденти ідентичності (IDR) запроваджуються для скорочення атак на поверхню шляхом виявлення вразливостей у контролері домену та захисту від крадіжки облікових даних.

Стефан Бавендієк. зосереджується на динамічному аналізі впливу програм-вимагачів на служби Active Directory у Windows Server [2]. Цікаво, що розглянуті варіанти програм-вимагачів не зупинили служби, але зашифрували важливі файли, що

зробило служби дисфункціональними. Це свідчить про те, що не лише безпосереднє блокування служб, але і шифрування важливих файлів може призвести до серйозних проблем в роботі AD.

**Мета статті.** Метою цієї статті є розробка та аналіз стратегії захисту Active Directory від програм-вимагачів, використовуючи концепцію нульової довіри.

**Об'єкт дослідження.** Об'єктом дослідження є корпоративні мережі, що використовують Active Directory від Microsoft для управління ідентифікацією та авторизацією користувачів.

**Предмет дослідження.** Предметом дослідження є вплив стратегії нульової довіри на ефективність захисту корпоративних мереж, що використовують Active Directory, від програм-вимагачів.

**Завдання дослідження:**

1. Описати теоретичні основи безпеки Active Directory; описати вектор атаки програм-вимагачів на AD; та описати концепції архітектури нульової довіри (ZTA) та її імплементації у патернах архітектури Active Directory.
2. Розробити методику використання концепції нульової довіри для виявлення та блокування програм-вимагачів в середовищі Active Directory.
3. Протестувати розроблену методику на реальних та емульованих атаках — зібрати дані.
4. Проаналізувати та оцінити ефективність розробленої методики.

Сформулювати висновки та рекомендації щодо можливості використання концепції нульової довіри для підвищення безпеки корпоративних мереж, що використовують Active Directory.

## ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Актуальність та важливість досліджуваної проблеми підтверджується численними науковими роботами та дослідженнями, присвяченими проблемам безпеки в корпоративних мережах, використанню Active Directory, концепції нульової довіри та захисту від програм-вимагачів. Однак, у світлі нових цифрових загроз, існує необхідність в постійному оновленні та розвитку підходів до захисту інформації.

Active Directory (AD) — це технологія від Microsoft, яка використовується для управління ідентифікацією та авторизацією користувачів в корпоративних мережах. AD забезпечує єдину точку входу для управління ідентифікацією, політиками безпеки, інтернет-протоколами та іншими компонентами мережі.

Концепція нульової довіри, або Zero Trust [3], базується на принципі «нікому не довіряти», незалежно від того, знаходиться користувач або пристрій у внутрішній мережі чи за її межами. Такий підхід означає, що а кожен запит до системи повинен проходити незалежну верифікацію, незалежно від джерела запиту. Програми-вимагачі — це шкідливе програмне забезпечення, що блокує доступ до системи або файлів користувача, а потім вимагає від користувача викуп за їх «відновлення». Вони можуть бути особливо шкідливими для корпоративних мереж, оскільки можуть блокувати доступ до критично важливих систем або даних. Взаємозв'язок між цими трьома елементами полягає в тому, що програми-вимагачі можуть атакувати корпоративні мережі, що використовують Active Directory для управління доступом. Тут може бути застосована концепція нульової довіри, що передбачає неперервну верифікацію та перевірку всіх елементів

системи, включаючи запити на доступ до ресурсів, що може допомогти виявити і заблокувати програми-вимагачі до того, як вони зможуть завдати шкоди.

Модель нульової довіри — це підхід до кібербезпеки, який за замовчуванням забороняє доступ до цифрових ресурсів організації та надає доступ лише автентифікованим користувачам до відповідних ресурсів на які у користувачів є права, незалежно від фізичної локації пристрою в мережі (периметру) чи його власність (корпоративний або приватний) [4]. Ця модель допомагає виявляти програми-вимагачі завдяки суворій перевірці особи кожної людини та пристрою, які намагаються отримати доступ до ресурсів, при кожному запиті. Вимагаючи автентифікації на кожному етапі, модель нульової довіри зменшує ймовірність несанкціонованого доступу та поширення програм-вимагачів у мережі. З точки зору виявлення програм-вимагачів, модель нульової довіри може доповнити існуючі заходи, забезпечуючи додаткові рівні безпеки. Наприклад, модель наголошує на моніторингу та аналізі мережевого трафіку для виявлення незвичної активності, яка може свідчити про потенційну атаку зловмисників. Завдяки постійній перевірці кожного етапу доступу та ретельному моніторингу будь-якої аномальної поведінки, модель Zero Trust підвищує шанси виявлення програм-вимагачів на ранніх стадіях ланцюжка знищення.

Крім того, акцент моделі Zero Trust на наданні мінімально необхідного доступу [5] для виконання конкретних завдань також сприяє виявленню програм-здирників. Обмежуючи привілеї користувачів і пристроїв, модель мінімізує потенційний вплив атаки зловмисників. Якщо користувач або пристрій з обмеженим доступом намагається виконати підозрілі дії або отримати доступ до файлів за межами дозволених повноважень, це може викликати сповіщення і спонукати до реагування для розслідування і зменшення загрози.

Поєднання моделі нульової довіри з іншими методами виявлення вимагачів, такими як статичний аналіз файлів, моніторинг аномалій виконання файлів і використання розширеного аналізу шкідливого програмного забезпечення, може забезпечити комплексний підхід до виявлення і нейтралізації атак вимагачів. Прийнявши модель нульової довіри, організації можуть підвищити свою здатність виявляти та реагувати на загрози з боку програм-вимагачів, зменшуючи потенційну шкоду, спричинену цими зловмисними атаками.

## МЕТОДИКА ДОСЛІДЖЕННЯ

Архітектура нульової довіри — це концепція безпеки, яка передбачає відсутність довіри до будь-якого користувача або пристрою, незалежно від їхнього місцезнаходження або мережевого підключення. Вона спрямована на захист чутливих ресурсів, таких як Active Directory (AD), шляхом впровадження суворого контролю доступу та постійного моніторингу і перевірки поведінки користувачів і пристроїв.

Що стосується захисту Active Directory від шкідливого програмного забезпечення, включаючи програми-вимагачі, модель нульової довіри може бути реалізована за допомогою наступних ключових принципів і компонентів[6]:

1. Керування ідентичностями та доступом (IAM): Впровадження надійних засобів управління ідентифікацією та доступом має вирішальне значення в архітектурі нульової довіри. Це передбачає використання багатофакторної автентифікації (MFA), доступу з найменшими привілеями та постійний моніторинг поведінки користувачів для виявлення будь-яких підозрілих дій.

2. Мікросегментація: Розділивши мережу на менші сегменти, або мікросегменти, організації можуть ізолювати та захистити критичні активи, такі як сервери AD. Це допомагає запобігти латеральному переміщенню шкідливого програмного забезпечення в мережі.
3. Безпека мережі та кінцевих точок: Розгортання передових рішень для захисту мережі і кінцевих точок, таких як брандмауери, системи виявлення вторгнень (IDS) і платформи захисту кінцевих точок (EDR), може допомогти виявити і заблокувати шкідливе програмне забезпечення до того, як воно зможе взаємодіяти з AD.
4. Поведінкова аналітика: Впровадження інструментів поведінкового аналізу може допомогти виявити аномальну поведінку користувачів, наприклад, незвичні шаблони входу або спроби доступу, які можуть вказувати на атаку зловмисників з вимогою викупу. Ці інструменти використовують алгоритми машинного навчання, щоб встановити базову поведінку для кожного користувача та виявити будь-які відхилення від неї.
5. Управління привілейованим доступом (PAM): Обмеження та моніторинг привілейованого доступу до серверів AD має вирішальне значення для запобігання атакам з вимогою викупу. Рішення PAM можуть забезпечити надійну автентифікацію, запис сеансів і моніторинг привілейованих дій в режимі реального часу.
6. Неперервний моніторинг та реагування на інциденти: Впровадження надійної системи моніторингу та реагування на інциденти має важливе значення для швидкого виявлення та реагування на атаки зловмисників. Це включає моніторинг мережевого трафіку в режимі реального часу, аналіз журналів і автоматизовані процеси реагування на інциденти.

Поєднуючи ці принципи та компоненти, організації можуть створити модель нульової довіри, спеціально розроблену для виявлення та усунення наслідків атак зловмисників у середовищі Active Directory.

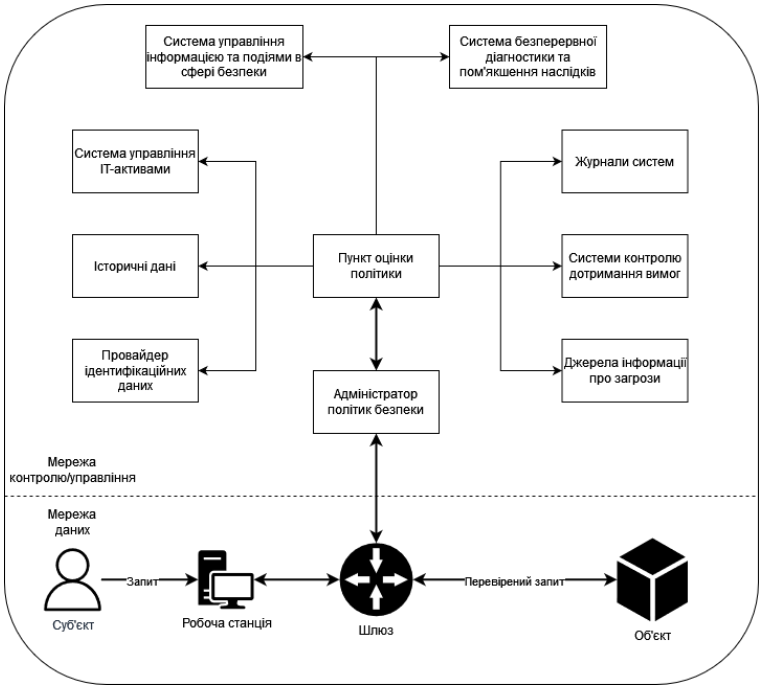


*Рис. 1. Схематичне зображення концепції безпеки AD з використанням ZTA*

Щоб розробити комплексну структуру для реалізації концепції нульової довіри в середовищах Active Directory для виявлення загроз, зокрема вірусів-вимагачів, нам потрібно розглянути кілька ключових компонентів і рекомендацій. Ось загальний план цієї концепції[7] – [9]:

1. Контроль доступу:
   a. Впроваджуйте детальний контроль доступу, заснований на принципі найменших привілеїв;
   b. Використовуйте контроль доступу на основі ролей (RBAC) для призначення дозволів користувачам і групам;
   c. Регулярно переглядайте та оновлюйте політики контролю доступу, щоб переконатися, що вони відповідають вимогам безпеки організації;
   d. Використовуйте рішення для управління привілейованим доступом (PAM) для жорсткого контролю адміністративного доступу.
2. Багатофакторна автентифікація (MFA):
   a. Увімкніть MFA для всіх облікових записів користувачів, включаючи привілейовані облікові записи;
   b. Використовуйте надійні методи автентифікації, такі як смарт-картки, біометричні дані або апаратні токени;
   c. Впроваджуйте адаптивну MFA, яка коригує рівень автентифікації на основі факторів ризику;
3. Моніторинг мережевого трафіку:
   a. Розгортання інструментів мережевого моніторингу для перехоплення та аналізу трафіку в середовищі Active Directory;
   b. Впровадити системи виявлення та запобігання вторгнень (IDPS) для виявлення та блокування зловмисної мережевої активності;
   c. Використовуйте сегментацію мережі для ізоляції критично важливих активів і обмеження бічного переміщення шкідливого програмного забезпечення.
4. Поведінкова аналітика:
   a. Впроваджуйте аналіз поведінки користувачів та організацій (UEBA) для виявлення аномальних моделей поведінки;
   b. Відстежуйте активність користувачів, підвищення привілеїв і запити на доступ, щоб виявити потенційні загрози зловмисного програмного забезпечення;
   c. Налаштуйте сповіщення та автоматичні відповіді на підозрілі дії, такі як блокування облікових записів або незвичний доступ до файлів.
5. Захист кінцевих точок:
   a. Впроваджуйте передові рішення для захисту кінцевих точок, які включають антивірусне програмне забезпечення, системи запобігання вторгненням на основі хостів (HIPS) та моніторинг цілісності файлів;
   b. Регулярно оновлюйте та виправляйте системи кінцевих точок для захисту від відомих вразливостей;
   c. Увімкніть білі списки додатків, щоб обмежити виконання несанкціонованого програмного забезпечення.
6. Реагування на інциденти:
   a. Розробіть план реагування на інциденти, специфічний для атак з вимогою викупу;

b. Встановіть чіткі процедури для виявлення, локалізації та ліквідації інфекцій, спричинених шкідливим програмним забезпеченням;
c. Регулярно тестуйте та оновлюйте план реагування на інциденти на основі уроків, винесених з попередніх інцидентів;

7. Постійний моніторинг та оцінка:
   a. Впровадити програму постійного моніторингу для відстеження ефективності системи нульової довіри;
   b. Регулярно переглядайте журнали, звіти та показники безпеки, щоб виявити потенційні слабкі місця або сфери для вдосконалення;
   c. Періодично проводьте тестування на проникнення та оцінку вразливостей, щоб забезпечити безпеку середовища Active Directory.

Важливо зазначити, що ця структура повинна бути адаптована до конкретних вимог і профілю ризиків організації. Необхідно регулярно оновлювати та коригувати її, щоб адаптуватися.

## ВПРОВАДЖЕННЯ КОНЦЕПЦІЇ НУЛЬОВОЇ ДОВІРИ У СЕРЕДОВИЩІ (AZURE) ACTIVE DIRECTORY

Впровадження концепції нульової довіри — безперервний процес, який включає широкий спектр процесів і технологій. Зважаючи на це, існують перевірені фреймворки, які полегшують впровадження даної концепції [10], [11].

Зокрема, план швидкої модернізації Microsoft (RAMP) розроблений, щоб допомогти вам швидко прийняти рекомендовану стратегію привілейованого доступу.

Мета полягає в застосуванні принципу найменших привілеїв до кожного рішення щодо доступу, дозволяючи чи забороняючи доступ до ресурсів на основі комбінації кількох контекстних факторів, а не лише однієї попередньої автентифікації. Щоб забезпечити максимальну вигоду, принципи Zero Trust повинні пронизувати більшість аспектів IT-екосистеми.

Кожен пункт у RAMP структуровано як ініціатива, яка відстежуватиметься та керуватиметься за допомогою формату, що базується на методології цілей та ключових результатів. Деякі пункти вимагають змін у процесах і знаннях та навичках людей, тоді як інші — простіші технологічні зміни. Багато з цих ініціатив включатимуть членів поза традиційним IT-відділом, яких слід залучати до прийняття рішень і впровадження цих змін, щоб забезпечити їхню успішну інтеграцію.

План містить наступні пункти[12]:

1. Відокремлення та керування привілейованими обліковими записами
   a. **Створення облікових записів екстреного доступу.** Він полягає у створення спеціальних акаунтів, щоб бути впевненим, що ви випадково не будете заблоковані в організації Active Directory у надзвичайній ситуації. Облікові записи екстреного доступу використовуються рідко та можуть завдати великої шкоди організації, якщо вони скомпрометовані, але їх доступність для організації також критично важлива для кількох сценаріїв, коли вони потрібні;
   b. **Визначення та категоризація привілейованих облікових записів.** Він полягає у визначенні всіх ролей та груп з високими привілеями, які вимагатимуть вищого рівня безпеки. Для них необхідно створити окремі окремі акаунти адміністраторів, надавши мінімальні необхідні права.

Після налаштування необхідних акаунтів, також, необхідно видалити облікові записи, які не є потрібними.

2. Покращення керування обліковими записами:
   a. **Впровадження та документування самостійного скидання пароля та комбіновану реєстрацію інформації безпеки.** Цей пункт полягає у налаштуванні самостійного скидання паролю завдяки чому, користувачі можуть скинути власні паролі після реєстрації. Комбінований досвід реєстрації інформації про безпеку забезпечує кращу взаємодію з користувачем, дозволяючи реєструватися для багатофакторної автентифікації і самостійного скидання пароля;
   b. **Захист облікових записів адміністратора.** Цей пункт вимагає, щоб усі привілейовані облікові записи використовували багатофакторну автентифікацію (MFA). Вона вимагається для всіх окремих користувачів, яким назавжди призначено одну або кілька ролей адміністратора. Також для більш надійного захисту необхідно впровадити використання методів входу без пароля, таких як ключі безпеки FIDO2 або Windows Hello в поєднанні з унікальними, довгими, складними паролями;
   c. **Блокування застарілих протоколів автентифікації для привілейованих облікових записів користувачів.** Слід заблокувати застарілі протоколи автентифікації, оскільки для них не можна застосувати багатофакторну автентифікацію. Якщо застарілі протоколи автентифікації ввімкнено, це може створити точку входу для зловмисників. Деякі застарілі програми можуть покладатися на ці протоколи, а організації можуть створювати окремі винятки для певних облікових записів. Ці винятки слід відстежувати та впроваджувати додаткові засоби моніторингу;
   d. **Створення процесу погодження програмного забезпечення.** Користувачів необхідно обмежити в можливості встановлювати стороннє програмне забезпечення і лише надавати дозволи, які ви вибираєте. Для програмного забезпечення, яке не відповідають цим критеріям, повинен існувати процес прийняття рішень централізовано командою адміністраторів безпеки та ідентифікації;
   e. **Моніторинг облікових записів та входів в систему.** Необхідно відстежувати маніпуляції з акаунтами користувачів та слідкувати за їхніми входами у систему, так як акаунти можуть бути скомпрометовані зовні так само, як і завжди існує внутрішня загроза;

**Розгортання робочих станцій адміністраторів.** Привілейовані облікові записи, такі як глобальні адміністратори (Global Administrators), повинні мати спеціальні робочі станції для виконання адміністративних завдань. Пристрої, на яких виконуються привілейовані завдання адміністрування, є ціллю зловмисників. Захист не лише облікового запису, але й робочих станцій має вирішальне значення для зменшення площі потенційної атаки. Це розділення обмежує їхню схильність до звичайних атак, як-от атак пов’язаних з електронною поштою

## ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У зв'язку із проведеним дослідженням, можемо дійти до наступних висновків:

- **Сутність Архітектури Нульової Довіри для Захисту Active Directory:** Здійснене дослідження акцентує увагу на необхідності архітектури нульової довіри для ефективного захисту ресурсів Active Directory. Практичне застосування принципів нульової довіри демонструє високу ефективність у протидії зловмисним програмам, включаючи програми-вимагачі;
- **Роль Керування Ідентичностями та Доступом:** Строге та централізоване керування ідентичностями та доступом виявилося вирішальним для забезпечення надійного захисту. Впровадження методів, таких як багатофакторна автентифікація та постійний моніторинг активності, створює додаткові бар'єри для незаконного доступу;
- **Ефективність Мікросегментації:** Стратегія мікросегментації сприяє ізоляції та захисту критичних компонентів мережі, зокрема серверів Active Directory, обмежуючи можливість неконтрольованого поширення зловмисного ПЗ;
- **Значення Розширених Засобів Безпеки Мережі:** Використання передових технологічних рішень для захисту мережі та кінцевих точок показало свою ефективність у виявленні та блокуванні шкідливих програм ще до інтеракції з Active Directory;
- **Потенціал Поведінкової Аналітики**: Інструменти поведінкового аналізу дозволяють з успіхом ідентифікувати аномальні патерни активності, що може бути попереджувальним знаком атаки;
- **Критична Роль Управління Привілейованим Доступом:** Стратегії управління привілейованим доступом є важливим засобом запобігання несанкціонованому доступу до критичних ресурсів Active Directory;
- **Необхідність Неперервного Моніторингу та Реагування на Інциденти:** Ефективні системи моніторингу та реагування на інциденти допомагають оперативно виявляти та ліквідовувати потенційні загрози, забезпечуючи високий рівень безпеки;

З урахуванням вищезазначеного, можна зробити висновок, що ефективний захист Active Directory від потенційних загроз та атак можливий за умови комплексного підходу до питань безпеки, який включає в себе застосування новітніх технологій та методів захисту, регулярне моніторинг та адаптація до змінюваних обставин.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. McDonald, G., et al. (2022). Ransomware: Analysing the Impact on Windows Active Directory Domain Services. *Sensors, 22, 953*. https://doi.org/10.3390/s22030953
2. Bavendiek, S. (2022). A zero trust security approach with FIDO2, preprint (Version 1) available at Research Square. https://doi.org/10.21203/rs.3.rs-2022891/v1
3. Stafford, V. (2020). *Zero trust architecture*. NIST special publication, 800, 207. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
4. Ward, R., & Beyer, B. (2014). *Beyondcorp: A new approach to enterprise security*. https://www.usenix.org/system/files/login/articles/login_dec14_02_ward.pdf
5. Spear, B., Cittadini, L., & Saltonstall, M. (2016). *Beyondcorp: The access proxy*. https://www.usenix.org/system/files/login/articles/login_winter16_05_cittadini.pdf

6. *Implementing a Zero Trust security model at Microsoft. Microsoft Insider Talk*. https://www.microsoft.com/insidetrack/blog/implementing-a-zero-trust-security-model-at-microsoft/
7. Zhuravchak, D., Dudykevych, V., & Tolkachova, A. (2023). Study of the Structure of the Endpoint Detection and Response Based on the Detection and Fighting of Ransom Virus Attacks. *Cyber security: education, science, technology, 3(19),* 69–82. https://doi.org/10.28925/2663-4023.2023.19.6982
8. Zhuravchak, D. (2021). Creating a System for Preventing the Spread of Ransomware Viruses Using the Python Programming Language and the Auditd Utility Based on the Linux Operating System. *Cyber security: education, science, technology, 4(12),* 108–116. https://doi.org/10.28925/2663-4023.2021.12.108116
9. D. Zhuravchak, et al. (2021). Ransomware Prevention System Design based on File Symbolic Linking Honeypots, *2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS),* 284–287, https://doi.org/10.1109/IDAACS53288.2021.9660913
10. *Zero trust: What it is, why you need it, and how to get started. Quest Blog.* https://blog.quest.com/zero-trust-what-it-is-why-you-need-it-and-how-to-get-started/
11. *Strengthening Active Directory security: 3 best practices for implementing a Zero Trust model. Quest Blog*. https://blog.quest.com/strengthening-active-directory-security-3-best-practices-for-implementing-a-zero-trust-model/
12. *Security rapid modernization plan. Microsoft Learn.* https://learn.microsoft.com/en-us/security/privileged-access-workstations/security-rapid-modernization-plan

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023

**Danyil Zhuravchak**
Postgraduate student, assistant of the Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID 0000-0003-4989-0203
*danyil.y.zhuravchak@lpnu.ua*

**Pavlo Hlushchenko**
Postgraduate student of the Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID 0000-0002-1262-5484
*pavlo.k.hlushchenko@lpnu.ua*

**Maksym Opanovych**
Postgraduate student of the Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID 0000-0002-2748-2965
*maksym.y.opanovych@lpnu.ua*

**Valerii Dudykevych**
Doctor of Sciences in Technology, professor of Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID 0000-0001-8827-9920
*valerii.b.dudykevych@lpnu.ua*

**Andrian Piskozub**
PhD, Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID 0000-0002-3582-2835
*andriian.z.piskozub@lpnu.ua*

# ZERO TRUST CONCEPT FOR ACTIVE DIRECTORY PROTECTION TO DETECT RANSOMWARE

**Abstract.** This scientific article explores the approach to protecting Active Directory from threats associated with ransomware, which are becoming increasingly perilous to corporate information systems. The concept of "zero trust" in the context of Active Directory is defined as an approach aimed at eliminating trust from the security framework and constantly verifying the compliance of users and their devices with configured security policies, context, and other parameters. The article delves into methods and tools that enable the implementation of the zero trust concept within the Active Directory environment, including behavior analysis, network traffic monitoring, and the utilization of advanced security rules. The importance of combining event processing technologies and artificial intelligence for automated detection and response to abnormal activity is also investigated. The research findings indicate the potential to enhance the effectiveness of protecting Active Directory from ransomware threats and ensuring the resilience of corporate networks against them. The adoption of the zero trust concept could be a significant step in ensuring cybersecurity and maintaining the reliability of information resources in modern enterprises. Furthermore, the implementation of the zero trust model within Active Directory aligns with the evolving threat landscape. As ransomware attacks continue to advance in sophistication, the need for robust security measures becomes paramount. Zero trust's proactive and adaptive approach ensures that even if attackers breach initial defenses, they encounter additional layers of scrutiny, making lateral movement and data exfiltration far more challenging. In an era where ransomware attacks have the potential to disrupt business operations and compromise sensitive data, the adoption of the zero trust approach within Active Directory represents a strategic shift towards a more secure and resilient corporate IT landscape.

**Keywords** ransomware; unauthorized access; Active Directory; zero-trust architecture.

## REFERENCES (TRANSLATED AND TRANSLITERATED)

1. McDonald, G., et al. (2022). Ransomware: Analysing the Impact on Windows Active Directory Domain Services. *Sensors, 22, 953*. https://doi.org/10.3390/s22030953
2. Bavendiek, S. (2022). A zero trust security approach with FIDO2, preprint (Version 1) available at Research Square. https://doi.org/10.21203/rs.3.rs-2022891/v1
3. Stafford, V. (2020). *Zero trust architecture*. NIST special publication, 800, 207. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
4. Ward, R., & Beyer, B. (2014). *Beyondcorp: A new approach to enterprise security*. https://www.usenix.org/system/files/login/articles/login_dec14_02_ward.pdf
5. Spear, B., Cittadini, L., & Saltonstall, M. (2016). *Beyondcorp: The access proxy*. https://www.usenix.org/system/files/login/articles/login_winter16_05_cittadini.pdf
6. *Implementing a Zero Trust security model at Microsoft. Microsoft Insider Talk*. https://www.microsoft.com/insidetrack/blog/implementing-a-zero-trust-security-model-at-microsoft/
7. Zhuravchak, D., Dudykevych, V., & Tolkachova, A. (2023). Study of the Structure of the Endpoint Detection and Response Based on the Detection and Fighting of Ransom Virus Attacks. *Cyber security: education, science, technology, 3(19)*, 69–82. https://doi.org/10.28925/2663-4023.2023.19.6982
8. Zhuravchak, D. (2021). Creating a System for Preventing the Spread of Ransomware Viruses Using the Python Programming Language and the Auditd Utility Based on the Linux Operating System. *Cyber security: education, science, technology, 4(12),* 108–116. https://doi.org/10.28925/2663-4023.2021.12.108116
9. D. Zhuravchak, et al. (2021). Ransomware Prevention System Design based on File Symbolic Linking Honeypots, *2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, 284–287, https://doi.org/10.1109/IDAACS53288.2021.9660913
10. *Zero trust: What it is, why you need it, and how to get started. Quest Blog.* https://blog.quest.com/zero-trust-what-it-is-why-you-need-it-and-how-to-get-started/
11. *Strengthening Active Directory security: 3 best practices for implementing a Zero Trust model. Quest Blog*. https://blog.quest.com/strengthening-active-directory-security-3-best-practices-for-implementing-a-zero-trust-model/
12. *Security rapid modernization plan. Microsoft Learn.* https://learn.microsoft.com/en-us/security/privileged-access-workstations/security-rapid-modernization-plan