ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ



«АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ»

Тези доповідей

29 жовтня
2026

м. Київ

Редакційна колегія:

Гайдур Г.І. – д.т.н., професор, завідувач кафедри Систем та технологій кібербезпеки Навчально-наукового інституту кібербезпеки та захисту інформації.

Зибін С.В. – д.т.н., професор, професор кафедри Систем та технологій кібербезпеки Навчально-наукового інституту кібербезпеки та захисту інформації.

Казмірчук С.В. - д.т.н., професор, професор кафедри Систем та технологій кібербезпеки Навчально-наукового інституту кібербезпеки та захисту інформації.

Гахов С.О. – к.військ.н., доцент, доцент кафедри Систем та технологій кібербезпеки Навчально-наукового інституту кібербезпеки та захисту інформації.

Марченко В.В. – д.ф., доцент кафедри Систем та технологій кібербезпеки Навчально-наукового інституту кібербезпеки та захисту інформації.

Рекомендовано до друку кафедрою Сиситем та технологій Державного університету інформаційно-комунікаційних технологійй (протокол № 4 від 02.11.2026 р.)

Актуальні проблеми кібербезпеки: Матеріали Всеукраїнської науково-практичної конференції (м. Київ, 29 жовтня 2026 року). Навчально-науковий інститут кібербезпеки та захисту інформації, Державний університет інформаційно-комунікаційних технологій. Київ, 2026. 388 с.

Збірник призначений для науковців, викладачів, докторантів, аспірантів і студентів закладів вищої освіти, фахівців з кібербезпеки та захисту інформації, працівників органів державної влади та місцевого самоврядування. Редакційна колегія не несе відповідальності за зміст матеріалів, що опубліковані у збірнику. Тези подані в авторській редакції та відображають персональну позицію учасників конференції.

Мохонько Діана
ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ. НОРМАТИВНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ 113
Стебловський Г.В., Земляков С.О.
ВАЖЛИВІСТЬ ЗАХИСТУ КІНЦЕВИХ ПРИСТРОЇВ НА ОСНОВІ ESET INSPECT & PROTECT 116
Гуленов І.В.
ПІДВИЩЕННЯ БЕЗПЕКИ VPN ЗА ДОПОМОГОЮ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ 120
Завгородня Євгенія Ярославівна
КІБЕРСТІЙКІСТЬ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ: УРОКИ АТАКИ INDUSTROYER2 ТА ПІДХІД НА ОСНОВІ NIST CSF 2.0 .. 123
Шимчук Г. В., Яцків П.О.,
КОНТЕКСТНА МОДЕЛЬ КЕРУВАННЯ ДОСТУПОМ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ ХМАРНИХ СЕРЕДОВИЩ 126
Шимчук Г. В., Яцків П.О.
АДАПТИВНИЙ ЗАХИСТ ІОТ-МЕРЕЖ НА ОСНОВІ ОЦІНКИ ДОВІРИ ПРИСТРОЇВ ТА ДИНАМІЧНОЇ МІКРОСЕГМЕНТАЦІЇ 129
Онопрієнко М.Ю
МЕТОДИ І ТЕХНОЛОГІЇ КІБЕРАТАК, ОРГАНІЗОВАНИХ ЗА ПІДТРИМКИ НАЦІОНАЛЬНИХ ДЕРЖАВ ТА ЗАСОБИ ПРОТИДІЇ ЇМ 132
Ланде Дмитро Володимирович, Кузьмінський Віктор Сергійович
ВИЛУЧЕННЯ ТРИПЛЕТІВ ПРО КІБЕРЗАГРОЗИ З ТЕКСТОВИХ ПОВІДОМЛЕНЬ ІЗ ГАРАНТОВАНОЮ МЕЖЕЮ ЧАСТКИ ПОМИЛОК 135
Четвертуха Н.Р., Отенко В.І.
ВИБІР ІНСТРУМЕНТУ ДИНАМІЧНОГО АНАЛІЗУ ДЛЯ ШКІДЛИВИХ ПРОГРАМ, ЯКІ ПРИХОВУЮТЬ СВОЮ ПОВЕДІНКУ 138
Опірський І.Р., Стефанків А.В.
МЕХАНІЗМИ ВІДБОРУ ОЗНАК СИГНАЛІВ У СИСТЕМАХ РАДІОЧАСТОТНОГО ФІНГЕРПРИНТИНГУ НА ОСНОВІ НЕЙРОННИХ МЕРЕЖ 141
Афонін М.В.
АКТУАЛЬНІ ПРОБЛЕМИ БЕЗПЕКИ ІНСТРУМЕНТІВ ВІДДАЛЕНОГО ДОСТУПУ В КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ 144
Гончаренко М.
ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ТА КЛАСИФІКАЦІЇ МЕРЕЖЕВИХ АТАК У ПРОМИСЛОВИХ МЕРЕЖАХ MODBUS TCP НА ОСНОВІ АЛГОРИТМУ XGBOOST 147
Ступченко А.О
ПОБУДОВА ЦЕНТРУ ОПЕРАЦІЙНОЇ БЕЗПЕКИ (SOC) ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ ОРГАНІЗАЦІЇ 150

Шимчук Г. В.,
старший викладач каф. КН,
ТНТУ ім. І. Пулюя,
Тернопіль, Україна
Яцків П.О.,
студент групи КТ-12,
ТНТУ ім. І. Пулюя,
Тернопіль, Україна

АДАПТИВНИЙ ЗАХИСТ ІОТ-МЕРЕЖ НА ОСНОВІ ОЦІНКИ ДОВІРИ ПРИСТРОЇВ ТА ДИНАМІЧНОЇ МІКРОСЕГМЕНТАЦІЇ

Запропоновано адаптивний підхід до захисту IoT-мереж, який поєднує інвентаризацію пристроїв, оцінювання їхнього поточного ризику та динамічну мікросегментацію. Для кожного пристрою враховуються стан автентифікації, актуальність програмного забезпечення, зовнішня експозиція, поведінкові відхилення та критичність функції. У модельному експерименті з 60 вузлами динамічне обмеження зв'язків та ізоляція підозрілих пристроїв зменшили середню кількість скомпрометованих вузлів з 30,87 до 3,25, тобто приблизно на 89,5 %.

Ключові слова: шлюз, мережа, IoT, SDN-контролер, MQTT-брокер, VLAN-сегментація

Захист Internet of Things ускладнюється значною неоднорідністю пристроїв, довгими життєвими циклами, обмеженими обчислювальними ресурсами та залежністю від хмарних сервісів і шлюзів. У межах однієї мережі можуть одночасно працювати камери, сенсори, контролери, шлюзи та пристрої попередніх поколінь із різним рівнем підтримки криптографії й оновлень. Компрометація одного вузла створює ризик латерального переміщення до інших компонентів, особливо якщо мережа побудована як великий довірений сегмент. CISA окремо звертає увагу на небезпеку публічно доступних пристроїв, конфігурацій за замовчуванням, застарілого ПЗ та зайвої експозиції сервісів в Інтернеті [1].

Базова рекомендація NIST для IoT полягає в тому, що продукт повинен мати набір технічних можливостей, які дозволяють організації ідентифікувати пристрій, керувати його конфігурацією, захищати дані, обмежувати логічний доступ, безпечно оновлювати ПЗ та отримувати інформацію про стан кібербезпеки [2]. У редакції NIST IR 8259 Rev. 1, опублікованій у 2026 році, додатково підкреслено необхідність закладати кібербезпеку в життєвий цикл IoT-продукту до його введення в експлуатацію [3]. Однак навіть за наявності цих можливостей статична VLAN-сегментація не реагує на зміну стану конкретного вузла: пристрій після компрометації часто продовжує мати ті самі мережеві права, що і до інциденту.

Метою роботи є розроблення адаптивного механізму, в якому мережеві дозволи IoT-пристрою визначаються не лише його постійною належністю до сегмента, а й актуальним рівнем довіри. Для кожного вузла формується профіль, що включає п'ять груп ознак: надійність автентифікації та унікальність облікових даних, актуальність прошивки й наявність відомих вразливостей, ступінь зовнішньої експозиції портів і сервісів, відхилення мережевої поведінки

від звичного профілю, критичність функції пристрою. Високий ризик за будь-якою критичною ознакою повинен мати пріоритет над середнім інтегральним балом, наприклад використання заводського пароля або несанкціоноване відкриття керуючого порту одразу переводить вузол у режим обмеження.

Запропоновано три стани політики. У стані «довірений» пристрій взаємодіє лише з визначеними сервісами: MQTT-брокером, локальним шлюзом, DNS/NTP та сервером оновлень. У стані «обмежений» забороняється peer-to-peer взаємодія з однотипними IoT-вузлами, скорочується перелік дозволених протоколів і підвищується деталізація журналювання. У стані «карантин» зберігається лише керований канал до системи моніторингу та, за потреби, сервера відновлення. Перехід між станами виконується policy engine на основі телеметрії, а реалізація правил можлива засобами SDN, ACL на комутаторах, host firewall або політиками програмно визначеної мережі.

Ключовою властивістю підходу є мікросегментація за мінімально необхідними потоками, а не за фізичним місцем пристрою. Камера не повинна мати прямого доступу до інших камер лише тому, що вони розміщені в одній VLAN, сенсор має передавати телеметрію брокеру, але не ініціювати з'єднання з контролером, контролер повинен приймати команди лише від авторизованого сервісу керування. Така структура обмежує радіус наслідків компрометації. Дослідження гнучкої Zero Trust архітектури для IIoT також демонструє практичну доцільність поєднання мікросегментації та програмно визначеного керування політиками для гетерогенних середовищ [4].

Для кількісної первинної оцінки виконано модельний експеримент. Побудовано мережу з 60 IoT-вузлів, поділених на чотири функціональні групи по 15 пристроїв. У статичному варіанті вузли одного сегмента могли безпосередньо взаємодіяти між собою, а шлюзи забезпечували міжсегментні зв'язки. В адаптивному варіанті кожен вузол мав лише необхідні службові зв'язки з локальним шлюзом і обмеженим набором сусідів, після виявлення підозрілої поведінки скомпрометований вузол ізолювався через два модельні такти. Моделювалося поширення компрометації впродовж десяти тактів із ймовірністю успішного переходу через дозволений зв'язок 0,1. Проведено 500 повторів із фіксованим початковим зерном генератора.

За статичної сегментації середня кількість вузлів, що встигали бути скомпрометованими, становила 30,87 із 60, стандартне відхилення – 13,45, в окремих прогонах компрометація охоплювала всі 60 пристроїв. За динамічної мікросегментації з автоматичною ізоляцією середнє значення становило 3,25 вузла, стандартне відхилення – 3,51, а максимальне – 19. Відносне зменшення середньої кількості скомпрометованих вузлів становило приблизно 89,5 %. Результат пояснюється двома механізмами: меншою кількістю дозволених ребер між пристроями та обмеженим часом, протягом якого ризиковий вузол залишається активним.

Модельний характер експерименту накладає суттєві обмеження: ймовірність поширення задавалася штучно, не враховувалися різні класи експлойтів, затримки реального SDN-контролера та можливі помилки

детектування. Тому числовий результат не слід переносити безпосередньо на виробничу IoT-мережу. Водночас експеримент показує структурний ефект мікросегментації: навіть недосконалий механізм виявлення має значно менше потенційних напрямів латерального переміщення, якщо взаємодія між пристроями спочатку обмежена принципом least privilege.

Для практичного впровадження пропонується починати з пасивної інвентаризації: визначити всі IoT-вузли, виробника, версію прошивки, відкриті порти, типові адреси призначення та нормальний обсяг трафіку. Далі формуються дозволені комунікаційні шаблони для кожного класу пристроїв. На другому етапі вводиться оцінка довіри без автоматичного карантину, щоб визначити частоту помилкових спрацювань. Після калібрування в автоматичний режим переводяться лише однозначні події: поява забороненого сервісу, зміна MAC/IP без реєстрації, спроби сканування, масові з'єднання з новими адресами, використання небезпечних облікових даних. Для legacy-пристроїв, які не підтримують сучасну автентифікацію, компенсувальним контролем має бути жорсткіша мережна ізоляція.

Для різних типів загроз механізм використовує різні комбінації ознак. Масове сканування або спроба поширення ботнету проявляються зростанням кількості нових адрес призначення та нетипових портів, такий вузол доцільно негайно відокремлювати від peer-to-peer потоків. Поява невідомого пристрою з підробленою або незареєстрованою ідентичністю повинна блокувати доступ до брокерів керування ще до накопичення поведінкової статистики. Для пристрою з простроченою прошивкою ризик може підвищуватися поступово: спочатку обмежується вихід в Інтернет, потім, якщо вразливість стає критичною, дозволяється лише канал оновлення. Таким чином, адаптивна політика поєднує реактивний контроль подій із профілактичним зменшенням поверхні атаки.

Отже, ефективний захист IoT потребує переходу від статичної сегментації до моделі, де довіра до пристрою змінюється відповідно до його поточного стану. Запропонований підхід поєднує інвентаризацію, поведінковий контроль, мінімально необхідні мережеві зв'язки та автоматичний карантин. Модельний експеримент показав суттєве зменшення потенційного масштабу компрометації порівняно зі статичною схемою. Подальші дослідження доцільно спрямувати на перевірку механізму в Mininet/Containernet або фізичному IoT-стенді, оцінювання затримки прийняття рішень і розроблення адаптивних порогів для різних класів пристроїв.

Перелік посилань:

1. Cybersecurity and Infrastructure Security Agency. Internet Exposure Reduction Guidance. 2025. URL: https://www.cisa.gov/resources-tools/resources/exposure-reduction.

2. Fagan M., Megas K., Scarfone K., Smith M. IoT Device Cybersecurity Capability Core Baseline. NIST IR 8259A. 2020. https://doi.org/10.6028/NIST.IR.8259A.

3. Fagan M., Megas K., Cuthill B., Marron J., Hoehn B. Foundational Cybersecurity Activities for IoT Product Manufacturers. NIST IR 8259 Rev. 1. 2026. https://doi.org/10.6028/NIST.IR.8259r1.

4. Zanasi C., Russo S., Colajanni M. Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. Ad Hoc Networks. 2024. Vol. 156. Art. 103414. https://doi.org/10.1016/j.adhoc.2024.103414.