Vol. 7, No. 1, 2025

DOI: https://doi.org/10.23939/csn2025.01.176

УДК 004.056

ДОСЛІДЖЕННЯ ВІДПОВІДНОСТІ ВИМОГАМ CYBER ESSENTIALS ДЛЯ СЕРТИФІКАЦІЇ КОМПАНІЇ

Т. Б. Крет, А. З. Піскозуб, П. В. Стасів

Національний університет "Львівська політехніка",
кафедра захисту інформації
E-mail: taras.b.kret@lpnu.ua, andriian.z.piskozub@lpnu.ua, pavlo.stasiv.kb.2024@edu.lpnu.ua

Розглянуто вимоги Cyber Essentials для забезпечення базових контролів безпеки, які необхідно запровадити для захисту від найпоширеніших кіберзагроз. Cyber Essentials є базовою схемою сертифікації з кібербезпеки, яку розробив уряд Великої Британії, яка діє з 2014 року та згідно якої було сертифіковано більше 100 тис. організацій. На відміну від міжнародного стандарту ISO 27001:2022, в якому реалізовано комплексний підхід до побудови системи менеджменту інформаційної безпеки, Cyber Essentials є базовим рівнем захисту від кіберзагроз, який будується на базі п'яти основних контролів.

Проаналізовано використання таких контролів Cyber Essentials, як брандмауери, безпечна конфігурація систем, управління оновленнями, контроль доступу користувачів та захист від шкідливого програмного забезпечення. Впровадження цих контролів дає змогу значно знизити ризик кібератак та зберегти конфіденційність даних.

Проведено порівняння двох рівнів сертифікації Cyber Essentials: Cyber Essentials, що базується на самооцінці організації, та Cyber Essentials Plus, який включає технічну перевірку IT-інфраструктури для підтвердження відповідності вимогам безпеки. Обидва рівні сертифікації потребують незалежної оцінки для того, щоб забезпечити об'єктивність та неупередженість процесу сертифікації, а також для підвищення довіри до отриманого сертифікату.

Ключові слова: аудит, сертифікація, вимоги, відповідність вимогам, кібербезпека, кіберзагрози, Cyber Essentials, Cyber Essentials Plus.

Вступ

У цифрову епоху, коли інформація є критично важливим активом, кібербезпека відіграє вирішальну роль у забезпеченні стабільності та успіху будь-якої організації. Актуальними залишаються дослідження в сфері кібербезпеки, які пов'язані з проблематикою впровадження вимог стандартів. З огляду на це розглянуто сертифікаційну схему Cyber Essentials, яке розробив уряд Великої Британії для захисту від кіберзагроз та допомоги організаціям підвищити рівень кібербезпеки. Питання відповідності вимогам Cyber Essentials є актуальним для багатьох організацій, які прагнуть підвищити рівень кібербезпеки та пройти незалежну сертифікацію. Проте процес впровадження цього стандарту може бути складним та потребувати відповідних ресурсів. Проаналізовано аспекти відповідності вимогам Cyber Essentials, проведено порівняння Cyber Essentials та Cyber Essentials Plus.

У Cyber Essentials визначено п'ять основних технічних контролів: брандмауери, безпечна конфігурація, управління оновленнями, контроль доступу користувачів та захист від шкідливого

програмного забезпечення. Безпечне налаштування обладнання та програмного забезпечення є основою кібербезпеки, адже слабкі місця в конфігурації можуть стати легким способом для проникнення зловмисників. Контроль доступу користувачів передбачає, що лише авторизовані особи мають мати доступ до конфіденційної інформації та систем, так мінімізуючи ризик внутрішніх загроз. Регулярне оновлення програмного забезпечення є критично важливим для усунення відомих вразливостей та захисту від нових кіберзагроз. Використання різних брандмауерів допомагає захистити внутрішню мережу організації від зовнішніх атак, фільтруючи трафік та блокуючи несанкціонований доступ. Нарешті, захист від шкідливого програмного забезпечення є необхідним для запобігання зараженню комп'ютерів вірусами, троянами та іншими шкідливими програмами. Детально розглянемо кожен з цих контролів та проаналізуємо їхнє значення, запропоновано рекомендації щодо їхнього успішного впровадження.

Огляд літературних джерел

Cyber Essentials широко застосовується у Великій Британії та відповідає сучасним вимогам в галузі кібербезпеки, оскільки пропонує простий та ефективний набір контролів, які допомагають організаціям будь-якого розміру захиститися від поширених кібератак [1]. На відміну від стандарту ISO 27001, сертифікація Cyber Essentials є значно простішою у впровадженні, оскільки зосереджується на п'яти ключових технічних контролях безпеки (брандмауери, безпечна конфігурація, управління оновленнями, контроль доступу користувачів, захист від шкідливого програмного забезпечення), які вважаються критично важливими для захисту від більшості кібератак. Cyber Essentials може слугувати основою для подальшого розвитку системи управління кібербезпекою в організації та її відповідності стандарту ISO 27001 [2].

Сертифікація Cyber Essentials, започаткована в червні 2014 року, невдовзі стала обов'язковою для деяких державних контрактів у Великій Британії, особливо тих, що передбачають роботу з конфіденційною та персональною інформацією [3]. У 2016 році створено Національний центр кібербезпеки Великої Британії (NCSC, National Cyber Security Centre), який забезпечує розробку стандартів, рекомендацій та є технічним органом Великої Британії з кібербезпеки. До 2019 року понад 15 000 сертифікатів Cyber Essentials видавалися щорічно, у 2022 році було видано 100 тис. сертифікатів.

NCSC співпрацює з IASME (Information Assurance for Small and Medium Enterprises), яка є сертифікаційною компанією з кібербезпеки та проводить перевірки відповідності вимогам Cyber Essentials [4]. У 2020 році IASME обрано єдиним партнером з надання послуг Cyber Essentials, замінивши попередню модель співпраці з п'яти партнерів.

У 2021 році розпочав роботу сервіс Cyber Essentials Readiness Tool, який допомагає оцінити поточний рівень кібербезпеки та працює як інтерактивний опитувальник по основних контролях Cyber Essentials [5]. Результатом роботи з Cyber Essentials Readiness Tool є індивідуальний план дій, який окреслює кроки, необхідні для підготовки до процесу сертифікації. У 2023 році започатковано діяльність Cyber Advisor, тобто радників-консультантів з кібербезпеки, які допомагають оцінити поточний стан кібербезпеки організації та впровадити технічні контролі відповідно до вимог Cyber Essentials [6]. З 2024 року почав діяти Knowledge Hub – джерело перевіреної та актуальної інформації про схему Cyber Essentials, зокрема останні оновлення, вказівки для окремих галузей і ресурси, які допоможуть у процесі сертифікації.

Сертифікація Cyber Essentials доступна у двох рівнях:

1. Cyber Essentials, який передбачає заповнення анкети самооцінювання. Організації відповідають на низку питань, що охоплюють співробітників, пристрої, місцезнаходження п'ять ключових контролів тощо. Відповіді має засвідчити член правління або особа, яка має аналогічні повноваження, після чого їх перевіряє незалежний оцінювач.

2. Cyber Essentials Plus передбачає технічну перевірку інформаційно-комунікаційних систем в організації. Базується на тих самих технічних контролях, що і Cyber Essentials, проте містить технічний аудит IT-інфраструктури для підтвердження фактичного впровадження.

Обидва рівні сертифікації Cyber Essentials - як базовий, так і Plus - передбачають самооцінювання, яке перевіряє незалежний експерт, але Cyber Essentials Plus додатково передбачає технічний аудит IT-систем для підтвердження відповідності вимогам безпеки.

Мета та постановка завдання

Ця стаття присвячена аналізу вимог відповідності стандарту Cyber Essentials, які застосовуються для побудови системи захисту інформації в організації. Метою дослідження є аналіз існуючих вимог до кібербезпеки, які ґрунтуються на основі вимог сертифікації Cyber Essentials та Cyber Essentials Plus.

Постановка завдання:

- проаналізувати вимоги Cyber Essentials;
- проаналізувати основні технічні контролі Cyber Essentials;
- порівняти відмінності у підходах Cyber Essentials та Cyber Essentials Plus;
- запропонувати рекомендації для реалізації відповідних вимог та технічних контролів.

Область застосування Cyber Essentials

Сертифікація Cyber Essentials може охоплювати як всю IT-інфраструктуру організації, так і визначений підрозділ. Межі області застосування (підрозділ бізнесу, мережа, фізичне розташування) мають бути узгоджені з органом сертифікації до початку оцінки. За допомогою поділу на підмножини можна визначити, які частини IT-інфраструктури будуть охоплені сертифікацією Cyber Essentials, а які – ні. Під вимоги стандарту потрапляють всі пристрої і програмне забезпечення в межах визначеної області застосування, які можуть приймати вхідні з'єднання та ініціювати вихідні з'єднання через інтернет, а також контролювати трафік між ними (рис.). Обов'язковою умовою є включення кінцевих пристроїв користувачів до області застосування.

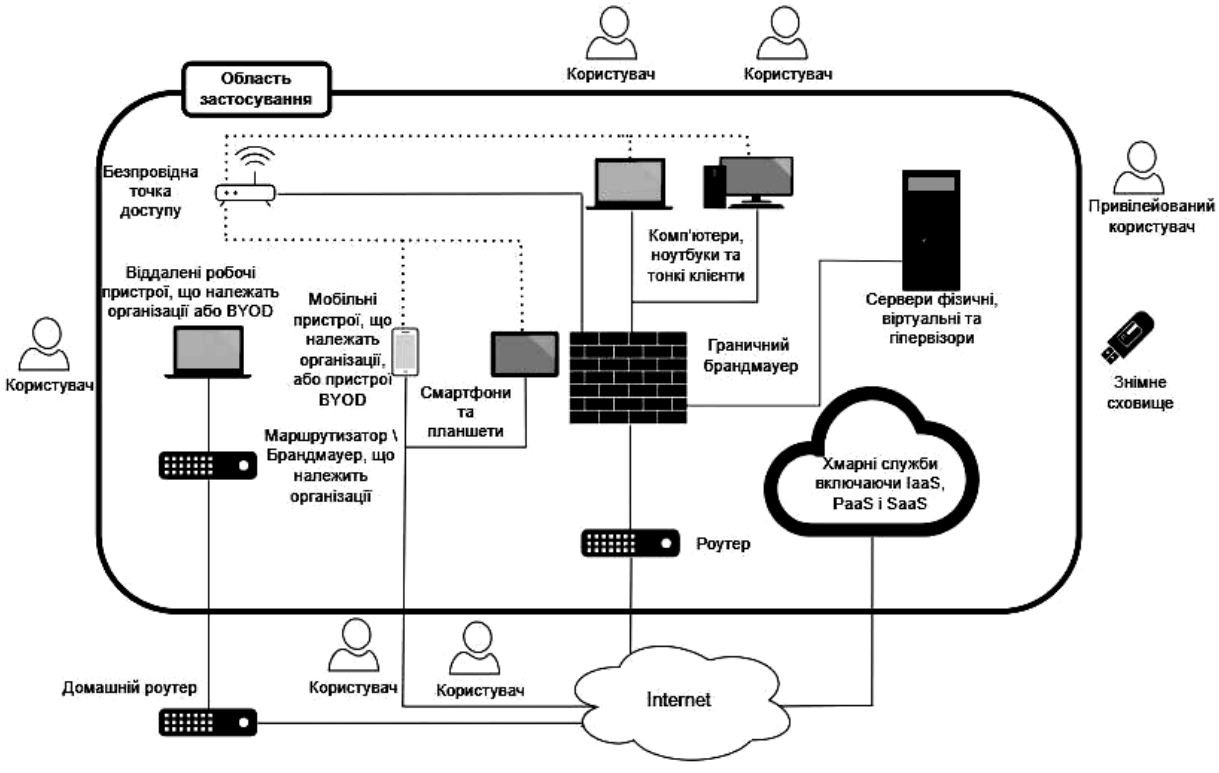

Рис. Область застосування Cyber Essentials до IT-інфраструктури

BYOD (Bring your own device) пристрої. Окрім мобільних або віддалених пристроїв, що належать організації, до області застосування вимог Cyber Essentials належать власні пристрої користувачів, які отримують доступ до даних або сервісів організації. Однак пристрої, які використовуються виключно для особистого спілкування (голосові та текстові застосунки) та двофакторної автентифікації, не підпадають під дію цих вимог. Традиційний підхід, коли компанія надає пристрої своїм співробітникам, забезпечує більшу однорідність і спрощує управління безпекою. Використання BYOD створює додаткові виклики, пов'язані з різноманітністю пристроїв та налаштувань. Для вирішення цих проблем необхідно розробити чіткі правила доступу до корпоративних ресурсів з використанням BYOD.

Робота з дому (робота за межами офісу організації або віддалена робота). Під час роботи з дому всі корпоративні пристрої та пристрої співробітників, що використовуються для виконання робочих завдань, підпадають під дію вимог Cyber Essentials. Якщо організація надає співробітнику маршрутизатор для домашнього інтернету, він також підлягає цим вимогам. В інших випадках необхідно забезпечити захист пристроїв співробітників за допомогою програмних брандмауерів. Якщо для роботи з дому використовується корпоративна VPN, то відповідальність за безпеку периметра мережі несе організація.

Безпровідні пристрої, зокрема безпровідні точки доступу, входять до області застосування Cyber Essentials, якщо вони можуть взаємодіяти з іншими пристроями через інтернет. Безпровідні пристрої не входять до області застосування Cyber Essentials, якщо атака зловмисника може бути здійснена лише в межах радіусу дії безпровідного сигналу або якщо вони є частиною маршрутизатора інтернет-провайдера в домашньому розташуванні.

Хмарні послуги. Якщо організація використовує хмарні послуги, такі як IaaS, PaaS та SaaS [7], вони підпадають під дію вимог Cyber Essentials. У табл. показано розподіл зон відповідальності (організації, провайдера, спільна) між організацією та провайдером хмарних послуг.

Відповідальність сторін вимогам безпеки

Вимога безпеки	IaaS	PaaS	SaaS
Брандмауери	Спільна	Спільна	Провайдер
Безпечна конфігурація	Спільна	Спільна	Спільна
Управління оновленнями	Спільна	Спільна	Провайдер
Контроль доступу користувачів	Організація	Організація	Організація
Захист від шкідливого програмного забезпечення	Спільна	Спільна	Провайдер

Якщо відповідальність за виконання певного заходу безпеки покладено на постачальника хмарних послуг, необхідно включити відповідні положення в договір. Постачальники хмарних послуг зазвичай публікують інформацію про свої заходи безпеки та посилаються на модель спільної відповідальності [8].

Облікові записи, що використовують треті особи. Облікові записи, що належать організації, підпадають під дію вимог Cyber Essentials, навіть якщо їх використовують треті особи (постачальник, підрядник тощо).

Пристрої, що використовують треті сторони. Пристрої кінцевих користувачів, власником яких є організація, які надані третій стороні, мають бути включені до дії вимог Cyber Essentials.

Вебзастосунки. Стандартні комерційні вебдодатки підлягають вимогам безпеки, тоді як власні розробки організації зазвичай не входять до сфери застосування. Фокус вимог безпеки

зосереджений на готових комерційних вебдодатках, а не на внутрішніх розробках. Найефективніший спосіб запобігти вразливостям в додатках – це дотримання найкращих практик розробки та тестування на проникнення відповідно до практики OWASP [9].

Технічні контролі

Під час сертифікації на відповідність Cyber Essentials перевіряється відповідність за п'ятьма технічними контролями:

1) брандмауери;
2) безпечна конфігурація;
3) управління оновленнями;
4) контроль доступу користувачів;
5) захист від шкідливого програмного забезпечення.

Управління активами не є окремим пунктом у переліку технічних контролів Cyber Essentials, але воно тісно пов'язане з усіма п'ятьма контролями і є невід'ємною частиною загальної стратегії кібербезпеки. Управління активами не обмежується лише потребами кібербезпеки, а охоплює різноманітні бізнес-функції, такі як IT-операції, фінанси та логістику [10]. Забезпечення узгодженості та інтеграції інформації про активи є критичним для успішного функціонування бізнесу [11, 12]. Управління активами – це не просто складання їх списків, а створення та підтримка надійної інформації про усі активи, яка необхідна для повсякденної роботи, прийняття рішень тощо.

Брандмауери

Кожен пристрій, під'єднаний до мережі "Інтернет", використовує набір мережевих служб, які дають змогу йому взаємодіяти з іншими пристроями та сервісами. Для мінімізації кібератак необхідно обмежити доступ до цих служб. Ефективним засобом для досягнення цієї мети є використання брандмауерів, які є програмно-апаратними рішеннями, та дозволяють фільтрувати вхідний і вихідний мережевий трафік на основі набору правил. Застосування брандмауерів дає змогу сегментувати мережу, контролювати доступ до ресурсів та запобігати несанкціонованому доступу. Брандмауер можна розділити на два типи:

- граничні брандмауери, які розміщуються на периметрі мережі та контролюють весь вхідний та вихідний трафік;
- програмні брандмауери, які встановлюються на окремих пристроях (наприклад, робочих станціях, серверах) і захищають саме цей пристрій.

Брандмауери аналізують кожен пакет даних, що проходить через них, порівнюючи його з набором правил. Якщо пакет відповідає правилам, він пропускається, в іншому випадку – блокується. Правила брандмауера можуть базуватися на різних критеріях, таких як вихідна/вхідна IP-адреса, порт, протокол та ін.

Вимоги Cyber Essentials, передбачені цим технічним контролем, застосовуються до граничних брандмауерів, настільних комп'ютерів, ноутбуків, маршрутизаторів, серверів, IaaS, PaaS, SaaS. У межах організації необхідно налаштувати захист кожного пристрою за допомогою брандмауера (або мережевого пристрою з функціями брандмауера). Більшість операційних систем вже мають вбудований програмний брандмауер, оптимізований для роботи з конкретною системою. Рекомендується використовувати саме його, оскільки він забезпечує надійний захист і не потребує додаткової конфігурації.

З огляду на вимогу Cyber Essentials для всіх брандмауерів (або мережевих пристроїв із функцією брандмауера) організація має:

- змінити адміністративні паролі, які встановлені за замовчуванням на надійні та унікальні або повністю вимкнути віддалений адміністративний доступ;
- заборонити доступ до адміністративного інтерфейсу, який використовується для керування конфігурацією брандмауера з інтернету, за винятком випадків, коли існує чітка та докумен-

тально підтверджена бізнес-необхідність, та інтерфейс захищений одним із таких засобів контролю як багатофакторна автентифікація або список дозволених IP-адрес, який обмежує доступ до невеликого діапазону довірених IP адрес у поєднанні з належним підходом автентифікації за паролем;

- блокувати за замовчуванням неавтентифіковані вхідні з'єднання;
- погодити та задокументувати усі вхідні брандмауерні правила з вказанням їх бізнес необхідності;
- видаляти або вимикати неактуальні правила брандмауера.

На всіх пристроях, що під'єднуються до незахищених мереж, таких як громадські Wi-Fi, обов'язково потрібно використовувати програмний брандмауер для додаткового захисту. Використання брандмауерів є необхідним елементом сучасної інформаційної безпеки. Застосування брандмауерів дає змогу значно знизити ризик кібератак та захистити інформаційні ресурси організації.

Безпечна конфігурація

Початкові конфігурації комп'ютерів та мережевих пристроїв зазвичай не є безпечними, часто стандартні налаштування містять слабкі місця, такі як:

- встановлений за замовчуванням загальновідомий пароль для облікового запису адміністратора або відсутність багатофакторної автентифікації;
- ввімкнені, але не використовувані облікові записи користувачів (наприклад, з адміністративними чи спеціальними привілеями);
- попередньо встановлені, але непотрібні програми або служби.

Ці налаштування за замовчуванням можуть дозволити зловмисникам отримати несанкціонований доступ до конфіденційної інформації. Однак застосовуючи технічні засоби контролю під час розгортання комп'ютерів та мережевих пристроїв, можна мінімізувати ці вразливості та захиститися від кібератак.

Cyber Essentials визначає такі вимоги безпечної конфігурації:

- блокувати та видаляти облікові записи користувачів, які зараз не використовуються;
- змінювати паролі до облікових записів, які встановлені за замовчуванням або які можна легко підібрати;
- блокувати та видаляти програмне забезпечення, яке не використовується, зокрема програми, системні утиліти та мережеві служби;
- вимикати усі налаштування, пов'язані з автозапуском, для уникнення несанкціонованого виконання шкідливого програмного забезпечення;
- забезпечувати автентифікацію усіх користувачів перед наданням доступу до сервісів та даних організації.

Для захисту пристроїв, які потребують фізичної присутності користувача, необхідно використовувати надійні методи автентифікації, такі як біометричні дані, паролі або PIN-коди. Для захисту від атак методом грубої сили потрібюно обмежити кількість спроб входу і блокувати пристрій після кількох невдалих спроб. У випадку використання облікових даних для розблокування пристрою мінімальна довжина пароля має становити не менше 6 символів. Якщо облікові дані використовуються також для автентифікації, необхідно застосовувати усі вимоги безпеки до паролів.

Управління оновленнями

Пристрій, на якому встановлено програмне забезпечення, може містити недоліки в безпеці, відомі як вразливості. Зловмисники активно використовують ці недоліки для атак. Важливо своєчасно встановлювати оновлення безпеки, які випускають виробники програмного забезпе-

чення, щоб захистити свої пристрої від кіберзагроз. Виробники програмного забезпечення регулярно випускають оновлення безпеки (патчі) для усунення виявлених вразливостей, ці оновлення можуть бути доступні негайно або за певним графіком.

У межах відповідності вимогам Cyber Essentials організація має:

- використовувати ліцензійне та підтримуване виробником програмне забезпечення;
- видаляти з пристроїв програмне забезпечення, яке більше не підтримується або не застосовується;
- використовувати функцію автоматичного оновлення програмного забезпечення (якщо є така можливість);
- встановлювати критичні оновлення безпеки, які усувають вразливості високого рівня, протягом 14 днів після їх випуску.

Контроль доступу користувачів

Вимоги Cyber Essentials зобов'язують організацію ретельно керувати правами доступу користувачів та надавати їм лише необхідні дозволи для виконання їхніх завдань. Ця вимога свідчить про необхідність впровадження принципу найменших привілеїв (principle of least privilege) в системі безпеки. Це означає, що кожен користувач повинен мати лише мінімальний набір прав, необхідний для виконання своїх обов'язків. Такий підхід дає змогу зменшити ризики, пов'язані з несанкціонованим доступом, оскільки навіть якщо зловмисник отримає доступ до облікового запису користувача, він матиме обмежені можливості для здійснення шкідливих дій.

Облікові записи з підвищеними правами становлять підвищений ризик для безпеки, якщо такі облікові записи будуть зламані, зловмисники зможуть завдати значної шкоди, наприклад викрадення даних, порушення бізнес-процесів та поширення атаки на інші пристрої в мережі. Облікові записи адміністратора мають значні права, такі як можливість внесення змін до операційної системи та керування іншими користувачами. Захист облікових записів адміністратора є критично важливим. Необхідно вжити всіх можливих заходів для захисту цих облікових записів від несанкціонованого доступу, включаючи використання багатофакторної автентифікації та принцип найменших привілеїв.

Організація має:

- мати процес створення та затвердження облікових записів користувачів;
- автентифікувати користувачів за допомогою унікальних облікових даних перед наданням доступу до програм або пристроїв;
- видаляти або деактивувати облікові записи користувачів, коли вони більше не потрібні;
- впроваджувати багатофакторну автентифікацію (MFA), де це можливо. Автентифікація до хмарних сервісів завжди має використовувати MFA;
- використовувати окремі облікові записи лише для виконання адміністративних дій (без доступу до електронної пошти, перегляду вебсторінок або інших стандартних дій користувача, які можуть піддавати адміністративні привілеї ризику);
- видаляти або деактивувати привілеї спеціального доступу, коли вони більше не потрібні (наприклад, коли співробітник змінює роль).

Захист від шкідливого програмного забезпечення

До шкідливого програмного забезпечення належать, зокрема, комп'ютерні віруси, хробаки, програми вимагачі. Потенційними джерелами розповсюдження шкідливого програмного забезпечення є шкідливі вкладення електронної пошти, завантаження, зокрема завантаження з магазинів додатків, пряма інсталяція несанкціонованого програмного забезпечення тощо.

Для захисту від шкідливого програмного забезпечення необхідно використовувати на всіх пристроях:

- антивірусне програмне забезпечення: має здійснюватися оновлення антивірусного програмного забезпечення та активне виявлення / блокування шкідливого програмного забезпечення, зокрема запобігання під'єднанню до шкідливих вебсайтів.
- список дозволеного програмного забезпечення: необхідно дозволяти виконання лише погодженого в компанії програмного забезпечення.

Відмінності між Cyber Essentials та Cyber Essentials Plus

Обидва рівні сертифікації Cyber Essentials - як базовий, так і Plus - передбачають самооцінювання, яке перевіряє незалежний експерт, але Cyber Essentials Plus додатково містить технічний аудит IT-систем для підтвердження відповідності вимогам безпеки.

Етапи сертифікації згідно базового підходу Cyber Essentials:

1. Заповнення анкети самооцінювання, яка охоплює п'ять ключових контролів безпеки:
- безпечне налаштування;
- контроль доступу користувачів;
- оновлення програмного забезпечення;
- міжмережеві екрани та маршрутизатори;
- захист від шкідливого програмного забезпечення.
2. Засвідчення відповідей, що здіснює член правління або особа, яка має аналогічні повноваження.
3. Перевірка відповідей, що здійсює незалежний оцінювач.

Етапи сертифікації згідно з Cyber Essentials Plus:

1) Виконання всіх вимог Cyber Essentials;
2) Технічний аудит інформаційно-комунікаційних систем організації;
3) Аудит проводить незалежний експерт, який безпосередньо перевіряє, чи дійсно впроваджені необхідні заходи безпеки на практиці.

Cyber Essentials та Cyber Essentials Plus є важливими інструментами для забезпечення кібербезпеки організацій будь-якого масштабу. Вибір між цими рівнями сертифікації залежить від потреб організації, її рівня ризику та доступних ресурсів. Проте в умовах постійного зростання кіберзагроз, впровадження будь-якого з цих стандартів є важливим кроком на шляху до забезпечення надійного захисту інформації та збереження конфіденційності даних.

Результати дослідження

Проведено комплексний аналіз стандарту Cyber Essentials, який є базовою схемою сертифікації з кібербезпеки, що розробив уряд Великої Британії. Cyber Essentials є базовим підходом для організацій будь-якого масштабу на шляху до забезпечення надійного захисту інформації та збереження конфіденційності даних в умовах зростання кіберзагроз.

У результаті дослідження було:

- проаналізовано основні вимоги стандарту, зокрема п'ять ключових технічних контролів: брандмауери, безпечна конфігурація систем, управління оновленнями, контроль доступу користувачів та захист від шкідливого програмного забезпечення;
- надано рекомендації щодо успішного впровадження п'яти ключових технічних контролів;
- проведено порівняльний аналіз двох рівнів сертифікації, виявлено їхні відмінності та особливості;
- визначено області застосування стандарту, зокрема використання власних пристроїв, роботу з дому, бездротові пристрої та хмарні послуги;
- запропоновано практичні рекомендації для компанії щодо впровадження вимог та технічних контролів Cyber Essentials.

Висновки

Проведено комплексний аналіз стандарту Cyber Essentials, який є базовою схемою сертифікації з кібербезпеки, яку розробив уряд Великої Британії. Актуальність дослідження зумовлена зростаючою кількістю кіберзагроз та необхідністю забезпечення базового рівня захисту для організацій будь-якого масштабу. Cyber Essentials, на відміну від більш комплексного стандарту ISO 27001, пропонує спрощений та ефективний підхід до захисту від найбільш поширених кібератак, зосереджуючись на п’яти ключових технічних контролях: брандмауери, безпечна конфігурація систем, управління оновленнями, контроль доступу користувачів та захист від шкідливого програмного забезпечення.

Детально розглянуто кожен з цих контролів, проаналізовано їхнє значення та надано рекомендації щодо успішного впровадження. Безпечне налаштування обладнання та програмного забезпечення визначено як основу кібербезпеки, оскільки слабкі місця в конфігурації можуть стати легким способом для проникнення зловмисників. Контроль доступу користувачів мінімізує ризик внутрішніх загроз, забезпечуючи доступ до конфіденційної інформації та систем лише авторизованим особам. Регулярне оновлення програмного забезпечення є критично важливим для усунення відомих вразливостей та захисту від нових кіберзагроз. Використання брандмауерів допомагає захистити внутрішню мережу організації від зовнішніх атак, а захист від шкідливого програмного забезпечення запобігає зараженню комп’ютерів вірусами та іншими шкідливими програмами.

Окрему увагу приділено порівнянню двох рівнів сертифікації Cyber Essentials: базового рівня, що базується на самооцінці організації, та рівня Plus, який передбачає технічну перевірку IT-інфраструктури для підтвердження відповідності вимогам безпеки. Обидва рівні сертифікації потребують незалежної оцінки для забезпечення об’єктивності та неупередженості процесу сертифікації, а також для підвищення довіри до отриманого сертифікату.

Охоплено питання застосування вимог Cyber Essentials до різних аспектів діяльності організації, таких як використання власних пристроїв (BYOD), робота з дому, бездротові пристрої та хмарні послуги. Підкреслено важливість чіткого визначення меж області застосування сертифікації та узгодження їх з органом сертифікації. Особлива увага приділяється розподілу відповідальності між організацією та провайдером хмарних послуг, а також питанням безпеки вебдодатків та управління активами.

Cyber Essentials є ефективним інструментом для забезпечення базового рівня кібербезпеки та підвищення кіберстійкості організацій. Стандарт пропонує чіткий та структурований підхід до захисту від найбільш поширених кіберзагроз, зосереджуючись на п’яти ключових технічних контролях. Вибір між рівнями сертифікації Cyber Essentials залежить від потреб організації, її рівня ризику та доступних ресурсів. Проте в умовах постійного зростання кіберзагроз впровадження будь-якого з цих стандартів є важливим кроком на шляху до забезпечення надійного захисту інформації та збереження конфіденційності даних.

Список літератури

1. *National Cyber Security Centre. URL: https://www.ncsc.gov.uk/ (дата звернення: 31.01.2025).*
2. *ISO/IEC 27001:2022 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги URL: https://www.iso.org/standard/27001 (дата звернення: 31.01.2025).*
3. *National Cyber Security Centre. 10 years of Cyber Essentials. URL: https://www.ncsc.gov.uk/files/10-years-of-Cyber-Essentials.pdf (дата звернення: 31.01.2025).*
4. *IASME. URL: https://iasme.co.uk/ (дата звернення: 31.01.2025).*
5. *National Cyber Security Centre. Cyber Essentials Readiness Tool Leaflet. URL: www.ncsc. gov.uk/files/ Cyber-Essentials-Readiness-Tool-Leaflet.pdf (дата звернення: 31.01.2025).*

6. National Cyber Security Centre. Cyber Essentials: Requirements for IT infrastructure. URL: https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-April-2023.pdf (дата звернення: 31.01.2025).

7. Khoma V., Abibulaiev A., Piskozub A., Kret T. Comprehensive Approach for Developing an Enterprise Cloud Infrastructure. CEUR Workshop Proceedings. 2024. Vol. 3654. Pp. 201–215.

8. Sisodia J., Khan M. Understanding the Shared Responsibilities Model in Cloud Services. ISACA Journal. 2022. Vol. 3. URL: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/understanding-the-shared-responsibilities-model-in-cloud-services (дата звернення: 31.01.2025).

9. Козловська М., Піскозуб А. Розробка ефективних заходів веб-безпеки для мережі шляхом проведення тестування на проникнення з використанням фреймворку OWASP. Ukrainian Information Security Research Journal. 2024. Vol. 26. No. 1. С. 101–110. Doi: https://doi.org/10.18372/2410-7840.26.18833.

10. Крет Т. Методика опису інформаційних активів організації при створенні системи менеджменту інформаційної безпеки. Комп'ютерні науки та інженерія : матеріали V Міжнародної конференції молодих вчених CSE-2011 (24–26 листопада 2011 р.) / Національний університет "Львівська політехніка". Львів : Видавництво Львівської політехніки, 2011. С. 342–343.

11. Гулак Н., Майстренко А. Автоматизація модуля інформаційних активів. Інформаційні технології та суспільство. Лип. 2024. 1 (12). 46- 50. Doi: https://doi.org/10.32689/maup.it.2024.1.6.

12. Badva P., Chowdhury P. D., Ramokapane K. M., Craggs B., Rashid A. Assessing Effectiveness of Cyber Essentials Technical Controls (ArXiv, abs/2406.15210). 2024. Doi: https://doi.org/10.48550/arXiv.2406.15210.

RESEARCH OF COMPLIANCE WITH CYBER ESSENTIALS REQUIREMENTS FOR COMPANY'S CERTIFICATION

T. B. Kret, A. Z. Piskozub, P. V. Stasiv

Lviv Polytechnic National University,
Department of Information Protection

This paper examines the Cyber Essentials requirements for ensuring basic security controls, which need to be implemented to protect against the most common cyber threats. Cyber Essentials is a foundational cybersecurity certification scheme developed by the UK government, which has been in operation since 2014 and under which more than 100,000 organizations have been certified. Unlike the international standard ISO 27001:2022, which implements a comprehensive approach to building an information security management system, Cyber Essentials is a basic level of protection against cyber threats, which is built based on five core controls.

This work analyzes the use of Cyber Essentials controls such as firewalls, secure system configuration, patch management, user access control, and malware protection. Implementation of these controls can significantly reduce the risk of cyberattacks and maintain data confidentiality.

This paper compares the two levels of Cyber Essentials certification: Cyber Essentials, which is based on an organization's self-assessment, and Cyber Essentials Plus, which includes a technical audit of the IT infrastructure to verify compliance with security requirements. Both certification levels require an independent assessment to ensure objectivity and impartiality in the certification process, as well as to increase confidence in the obtained certificate.

Keywords: audit, certification, requirements, compliance, cybersecurity, cyber threats, Cyber Essentials, Cyber Essentials Plus.