КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.1009
УДК 004.056:005.8:004.8

Полотай Орест Іванович
кандидат технічних наук, доцент, доцент кафедри управління інформаційною безпекою
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID: 0000-0003-4593-8601
orest.polotaj@gmail.com

Брич Тарас Богданович
кандидат технічних наук, доцент кафедри управління інформаційною безпекою
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID: 0000-0001-6853-1981
taras_brych@hotmail.com

Ткаченко Артур Мар'янович
викладач кафедри безпеки інформаційних технологій
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID: *0009-0009-6830-4741*
tkachenko.am14@gmail.com

Ящук Валентина Ігорівна
кандидат економічних наук, доцент, доцент кафедри управління інформаційною безпекою
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID: 0000-0003-2651-4918
valentina.lender@gmail.com

Федина Богдана Іванівна
кандидат технічних наук, доцент, доцент кафедри управління інформаційною безпекою
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID: 0000-0001-9487-2851
fedynabogdana@gmail.com

ІНТЕГРОВАНИЙ ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА ЗАСОБАМИ ЕТИЧНОГО ХАКІНГУ ТА ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Анотація. У статті було здійснено комплексний аналіз сучасних підходів до організації кібербезпеки на підприємствах, що дозволило не лише систематизувати наявні концепції управління інформаційною безпекою, а й виявити ключові тенденції, суперечності та проблемні аспекти у сфері технічного захисту інформації. Особливу увагу приділено співвідношенню між організаційними та технологічними складовими кіберзахисту, адже саме їхня неузгодженість часто стає причиною критичних вразливостей у корпоративних системах. Встановлено, що традиційні засоби захисту, орієнтовані переважно на превентивні заходи — зокрема, антивірусні рішення, міжмережеві екрани, системи контролю доступу — вже не здатні забезпечити повного рівня кіберстійкості в умовах динамічного розвитку кіберзагроз, зростання ролі соціальної інженерії та поширення цільових атак. Зазначене свідчить про необхідність переходу від реактивних моделей кіберзахисту до проактивних стратегій, у яких виявлення потенційних ризиків передує їх реалізації. Обґрунтовано важливість етичного хакінгу як інструмента активного виявлення вразливостей інформаційних систем до того, як ними можуть скористатися зловмисники. Етичний хакінг дозволяє підприємству оцінювати реальний рівень захищеності своїх інформаційних активів у максимально наближених до реальних умовах, що робить його одним із найефективніших засобів незалежного аудиту безпеки. На основі проведеного аналізу доведено, що інтеграція офенсивних методів тестування безпеки з технічними засобами захисту створює синергетичний ефект, завдяки якому досягається глибше розуміння слабких місць системи, підвищується оперативність реагування на потенційні загрози, а процес управління ризиками

стає більш гнучким і адаптивним. Взаємодія офенсивних практик з інструментами моніторингу (IDS/IPS, SIEM), криптографічними системами та засобами резервного копіювання сприяє формуванню замкненого циклу інформаційного захисту. Розроблена концептуальна модель інтеграції етичного хакінгу в систему технічного захисту інформації демонструє можливість поєднання превентивних, детекційних і реактивних механізмів у єдиному циклі безперервного вдосконалення кіберзахисту. Такий підхід базується на принципах динамічної адаптації, де результати тестів на проникнення безпосередньо впливають на налаштування та розвиток технічних засобів захисту. У результаті формується система, здатна до самонавчання та постійного оновлення відповідно до нових векторів атак. Це забезпечує не лише підвищення рівня кіберстійкості, а й оптимізацію використання ресурсів підприємства, оскільки превентивне виявлення загроз значно дешевше, ніж ліквідація наслідків інцидентів. Очікуваними перевагами впровадження інтегрованого підходу є суттєве підвищення рівня довіри до інформаційної інфраструктури підприємства, посилення репутаційної стійкості на ринку, зменшення ризиків несанкціонованого доступу та втрати даних. Крім того, такий підхід сприяє удосконаленню процесів внутрішнього аудиту безпеки, формуванню єдиної корпоративної політики управління інформаційними ризиками та розвитку культури відповідального ставлення до питань кіберзахисту на всіх рівнях організаційної структури. Важливо й те, що інтеграція етичного хакінгу стимулює підвищення кваліфікації персоналу, сприяє розвитку внутрішньої експертизи з безпеки та створює передумови для довгострокового підвищення конкурентоспроможності підприємства в цифровому середовищі.

Ключові слова: кібербезпека, етичний хакінг, технічний захист інформації, офенсивне тестування, кіберстійкість підприємства, інформаційна безпека, моделювання загроз, вразливість систем, аудит безпеки, інтегрована система захисту, превентивні заходи, моніторинг кіберзагроз, управління ризиками, тестування на проникнення, концептуальна модель кіберзахисту.

ВСТУП

Сучасні підприємства дедалі більше залежать від інформаційних технологій, що зумовлює потребу у створенні надійних систем кіберзахисту. З розвитком цифрової економіки та впровадженням автоматизованих систем управління значно зростає кількість кіберзагроз, які можуть спричинити витік конфіденційної інформації, фінансові збитки та порушення стабільності бізнес-процесів. Тому питання комплексного забезпечення кібербезпеки набуває стратегічного значення для кожного підприємства.

Інтеграція засобів технічного захисту інформації з методами етичного хакінгу створює нову парадигму захисту, що поєднує превентивні, аналітичні та реактивні заходи. Такий підхід дозволяє не лише виявляти та усувати вразливості, але й формувати динамічну систему безпеки, здатну адаптуватися до нових видів загроз.

З кожним роком спостерігається зростання кількості кібератак на підприємства різних галузей, незалежно від їхнього масштабу та форми власності. Зловмисники використовують дедалі складніші методи атак – від соціальної інженерії до цілеспрямованих проникнень у корпоративні мережі. Традиційні системи безпеки, орієнтовані лише на технічні засоби, вже не забезпечують достатнього рівня захисту.

У зв’язку з цим актуальним стає застосування інтегрованого підходу, що поєднує технічні, організаційні та аналітичні аспекти кіберзахисту. Особливе місце в такій системі займає етичний хакінг – інструмент, який дозволяє імітувати дії зловмисників для виявлення потенційних вразливостей ще до їхнього використання у реальних атаках. Поєднання етичного хакінгу з системами технічного захисту інформації забезпечує підвищення ефективності управління ризиками та зміцнення стійкості підприємства до кіберзагроз.

Постановка проблеми. Попри активне впровадження сучасних систем безпеки, більшість підприємств не мають цілісної стратегії захисту інформації, що враховує як технічні, так і проактивні методи тестування безпеки. Застосування технічних засобів без належного аудиту, моніторингу та регулярного тестування створює ілюзію захищеності, тоді як вразливості залишаються невиявленими.

Проблема полягає у відсутності інтегрованого підходу до забезпечення кібербезпеки, який би поєднував традиційні засоби технічного захисту (шифрування, фільтрацію, контроль доступу) з інструментами етичного хакінгу (penetration testing, vulnerability assessment, red teaming). Саме така інтеграція дозволяє створити замкнений цикл управління безпекою, де виявлення, оцінка та усунення загроз є безперервним процесом.

Таким чином, проблема полягає у відсутності на підприємствах цілісної системи кібербезпеки, яка б інтегрувала технічні засоби захисту інформації з практиками етичного хакінгу, що дозволяють виявляти та усувати вразливості ще до моменту їх експлуатації зловмисниками. Недостатня взаємодія між технічними, організаційними та аналітичними компонентами безпеки призводить до фрагментарності заходів, що знижує ефективність протидії сучасним кіберзагрозам.

У межах цієї статті передбачається розглянути сутність інтегрованого підходу до забезпечення кібербезпеки підприємства, проаналізувати можливості поєднання засобів технічного захисту інформації з методами етичного хакінгу, визначити переваги такого підходу, а також запропонувати модель його практичної реалізації.

Аналіз останніх досліджень і публікацій. Останні роки позначені інтенсивним зростанням досліджень у сфері етичного хакінгу (penetration testing, red-teaming), автоматизації тестів безпеки та інтеграції цих практик у корпоративні процеси управління інформаційною безпекою. З’являються систематичні огляди інструментів і фреймворків для пентестінгу, а також праці, що формалізують автоматизований підхід до тестування [3].

Паралельно зростає увага до інтеграції аналітики та AI у засоби виявлення загроз і в автоматизацію частини атак/тестування (зокрема — для прискорення і масштабування pentest/red team активностей). Разом з тим, автори підкреслюють етичні й технічні ризики такої інтеграції [5].

На рівні стандартів і практичних рекомендацій помітна консолідація підходів: ISO/IEC 27001 та супутні керівництва, а також документовані вказівки ENISA, все частіше вказують на необхідність регулярного тестування, оцінювання вразливостей та поєднання превентивних і реактивних заходів [4].

З останніх публікацій можна зробити такі висновки:

1. Ефективність пентестингу і red-teaming – численні огляди та емпіричні роботи підтверджують, що систематичні аудитні заходи (penetration testing, threat-led PT, red teaming) виявляють критичні вразливості, які пропускають автоматичні сканери, й покращують готовність організації до інцидентів. Разом з тим їхня результативність залежить від якості планування, зв’язку з процесами реагування та регулярності проведення [7].

2. Автоматизація vs. ручні методи – тренд на автоматизовані інструменти пентестингу (і навіть формалізацію PT-процедур) прискорює тестування й знижує витрати, але повністю замінити експертний аналіз наразі не може, особливо в частині складних логічних і соціальних векторів атак [1].

3. Фреймворки і вимірювання – застосування таких фреймворків, як MITRE ATT&CK, стає стандартною практикою для структурування сценаріїв атак у red-team

заходах і для зіставлення виявлених технік з існуючими контролями. Це сприяє кращому зв'язку офенсивних тестів із процесами ризик-менеджменту [6].

4. Політика, стандарти та комплаєнс — дослідження показують, що кампанії з пентестингу набувають більшої цінності, коли вони інтегровані в ISMS (ISO/IEC 27001) і в широку політику управління доступом, моніторингу і реагування. Таке поєднання підвищує ймовірність усунення знайдених вразливостей; і навпаки, «розрізнені» тестування часто не мають довготривалого ефекту [2].

У сучасних наукових дослідженнях, присвячених етичному хакінгу та технічному захисту інформації, спостерігається низка прогалин і суперечностей. Попри велику кількість публікацій, більшість із них зосереджуються на окремих аспектах кібербезпеки – технічних або організаційних, тоді як комплексний інтегрований підхід розглядається недостатньо. Бракує емпіричних робіт, які б оцінювали ефективність поєднання етичного хакінгу та технічних засобів захисту в реальному корпоративному середовищі, а також досліджень, що аналізують економічну доцільність таких рішень. Недостатньо уваги приділяється питанням етики, законодавчого регулювання та захисту персональних даних при проведенні етичного хакінгу. Крім того, у науковій літературі бракує методологічних рекомендацій щодо інтеграції результатів пентестів у систему управління інформаційною безпекою підприємства, що створює розрив між теорією та практикою побудови ефективної системи кіберзахисту.

Мета статті. Метою дослідження є обґрунтування та розроблення інтегрованого підходу до забезпечення кібербезпеки підприємства, який поєднує засоби технічного захисту інформації з методами етичного хакінгу. Такий підхід спрямований на створення ефективної, гнучкої та адаптивної системи інформаційної безпеки, здатної своєчасно виявляти, оцінювати та нейтралізовувати потенційні загрози. Для досягнення поставленої мети передбачається:

– проаналізувати сучасні підходи до організації кібербезпеки на підприємствах;

– визначити роль і можливості етичного хакінгу у виявленні вразливостей інформаційних систем;

– дослідити принципи функціонування технічних засобів захисту інформації та їхню взаємодію з офенсивними методами тестування безпеки;

– запропонувати концептуальну модель інтеграції етичного хакінгу в систему технічного захисту інформації підприємства;

– оцінити очікувані переваги впровадження такого підходу для підвищення рівня кіберстійкості організації.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Сучасна практика організації кібербезпеки на підприємствах ґрунтується на поєднанні декількох взаємодоповнювальних парадигм і технологічних стеків, що разом формують цілісну систему захисту інформаційних активів. До основних підходів належать: (1) фреймворки управління ризиками (risk-based frameworks), які систематизують процеси і пріоритизацію заходів; (2) принципи «захисту в глибину» (defense-in-depth) – багатошарова організація контролів; (3) архітектура Zero Trust – «нікому не довіряй за замовчуванням»; (4) використання модулів виявлення й реакції (SIEM/XDR/SOAR) та (5) інтеграція офенсивних практик (penetration testing, red-teaming, MITRE ATT&CK) у операційну модель безпеки. Кожен із цих підходів має свої методологічні основи, переваги та обмеження, а їхнє комбіноване застосування сьогодні розглядається як найефективніша стратегія захисту підприємства [14].

Фреймворки управління ризиками – зокрема NIST CSF та ISO/IEC 27001 [8] – задають структурований підхід до ідентифікації, оцінки, пом'якшення та моніторингу ризиків. Вони пропонують набір функцій і процесів (наприклад: ідентифікація, захист, виявлення, реагування, відновлення), які підприємство адаптує під власний контекст і вимоги комплаєнсу; ці стандарти також слугують основою для планування внутрішніх політик і процедур. Використання risk-based підходу дозволяє пріоритетизувати ресурси на ті активи й вектори, які мають найбільший вплив на бізнес-цілі.

Концепція «захисту в глибину» (defense-in-depth) підкреслює потребу багатошарових контролів: фізичних, технічних та організаційних. Ідея полягає в тому, що жоден окремий засіб не є достатнім – якщо один шар буде пробитий, інші стримуватимуть поширення інциденту або зменшуватимуть його наслідки. На практиці це реалізується через поєднання мережевих фаєрволів, сегментації, контролю доступу, шифрування, моніторингу та процедур реагування.

Архітектура Zero Trust (ZTA) набирає популярності як модель для середовищ із хмарними сервісами та віддаленою робочою силою [10]. Головні принципи ZTA – постійна перевірка ідентичності, найменший привілей (least privilege), мікросегментація та оцінка контексту доступу – дозволяють мінімізувати ризики, пов'язані з компрометацією облікових записів чи внутрішніми загрозами. Впровадження Zero Trust вимагає реформи ідентифікаційних процесів, контролю доступу та архітектури мережі, але дає змогу точніше контролювати доступ до ресурсів у гетерогенних IT-ландшафтах.

Сучасні операційні платформи безпеки поєднують централізоване збирання логів і кореляцію подій (SIEM) [11] з розширеним виявленням і реагуванням (XDR) та автоматизацією оркестрації реакцій (SOAR). Така комбінація забезпечує швидше виявлення інцидентів, скорочення часу на аналіз та часткове або повне автоматизоване застосування захисних дій. Однак ефективність цих рішень залежить від налаштування, якості телеметрії та інтеграції з процесами інцидент-менеджменту.

Офенсивні практики – penetration testing, vulnerability assessment, threat-led penetration testing, red-teaming – стають невід'ємною частиною сучасних програм безпеки: вони дозволяють емітувати реальні сценарії атак, виявляти логічні та процесні вразливості, які пропускають автоматизовані сканери, та оцінювати готовність організації до інцидентів. Фреймворки на кшталт MITRE ATT&CK дають спільну «мову» для моделювання атак і зіставлення виявлених технік із існуючими контролями, що спрощує пріоритизацію заходів. Інтеграція результатів офенсивних дій у цикл виправлення вразливостей і навчання персоналу підвищує загальну кіберстійкість.

Разом із тим, практична реалізація описаних підходів зустрічає низку складнощів. До ключових обмежень належать: складність інтеграції різнорідних інструментів і стандартів, брак кваліфікованих кадрів у SOC/Blue Team, потреба в значних ресурсах для повноцінного впровадження Zero Trust або SOAR, а також юридичні й етичні питання при проведенні масштабних офенсивних тестів (особливо коли тести зачіпають персональні дані або зовнішні сервіси). Оцінка ефективності (ROI) інтегрованих заходів також залишається неточною через дефіцит довготривалих емпіричних досліджень. Унаслідок цього практичні архітектури часто адаптують вибір підходів під наявні ресурси, ризиковий профіль підприємства та вимоги регуляторів.

Отже, сучасні підходи до організації кібербезпеки на підприємствах формують багаторівневу екосистему, що поєднує стандарти управління ризиками, концептуальні архітектури (defense-in-depth, Zero Trust), технологічні платформи для виявлення й реагування та практики етичного хакінгу. Основна теоретична передумова дослідження полягає в тому, що тільки інтегроване, адаптивне поєднання цих компонентів – із

чіткими процесами інтерпретації результатів тестів, пріоритизації виправлень і зворотного зв'язку на рівні ISMS – може забезпечити сучасний рівень кіберстійкості підприємства.

На рисунку 1 показано компоненти інтегрованого підходу організації кібербезпеки на підприємствах.

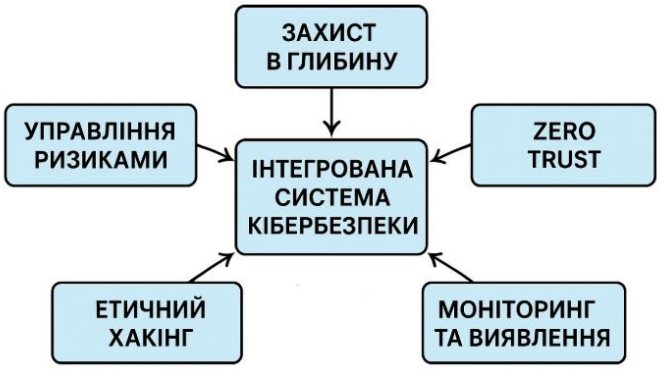

Рис. 1. Компоненти інтегрованого підходу організації кібербезпеки на підприємствах

Етичний хакінг, або тестування на проникнення (penetration testing), є одним із найважливіших інструментів у сучасній системі кіберзахисту підприємства. Його роль полягає у виявленні слабких місць інформаційних систем до того, як ними скористаються зловмисники. На відміну від злочинного хакінгу, етичний передбачає легальні та контрольовані дії, спрямовані на підвищення безпеки, а не на її порушення.

Основна цінність етичного хакінгу полягає у можливості реалістичного моделювання кібератак у контрольованих умовах. Це дозволяє оцінити фактичну ефективність існуючих технічних і організаційних засобів захисту. Застосування етичного хакінгу допомагає підприємствам виявити не лише технічні вразливості (наприклад, у вебсерверах, мережевих протоколах чи програмному забезпеченні), а й організаційні недоліки, такі як слабка політика паролів, неправильна конфігурація систем чи низька обізнаність персоналу.

Методи етичного хакінгу включають різні типи тестувань: чорну скриньку (black box) – без попереднього знання системи, сіру скриньку (gray box) – із частковим доступом до внутрішніх даних, та білу скриньку (white box) – із повною інформацією про систему. Такий підхід забезпечує всебічну перевірку безпеки, охоплюючи як зовнішні, так і внутрішні ризики [13].

Важливо, що результати етичного хакінгу дають змогу сформувати реалістичну карту ризиків і розробити практичні рекомендації для їхнього усунення. Крім того, регулярне проведення таких перевірок сприяє підвищенню рівня кіберстійкості підприємства та дозволяє дотримуватися вимог міжнародних стандартів (ISO/IEC 27001, NIST SP 800-115 тощо).

Таким чином, етичний хакінг відіграє стратегічну роль у системі інформаційної безпеки, виконуючи функцію активного моніторингу й попередження кіберзагроз. Його інтеграція в загальну систему технічного захисту забезпечує не лише своєчасне виявлення вразливостей, а й формує культуру безпеки, засновану на принципах проактивного захисту.

ISSN 2663 - 4023

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Принципи функціонування технічних засобів захисту інформації базуються на забезпеченні цілісності, конфіденційності та доступності даних, що становлять основу інформаційної безпеки підприємства. До складу таких засобів входять апаратні, програмні та програмно-апаратні компоненти, призначені для попередження несанкціонованого доступу, виявлення вторгнень, контролю інформаційних потоків і запобігання витокам даних. Їхнє функціонування ґрунтується на кількох ключових принципах: багаторівневості, ізоляції, аутентифікації, криптографічного захисту, моніторингу подій та управління доступом.

Зокрема, системи контролю доступу реалізують розмежування прав користувачів відповідно до ролей і політик безпеки. Засоби криптографічного захисту (шифрування, електронний підпис, сертифікація ключів) забезпечують цілісність і достовірність даних під час їх передавання та зберігання. Мережеві екрани (firewall), системи виявлення та запобігання вторгненням (IDS/IPS), а також системи захисту від витоків інформації (DLP) утворюють основу технічного периметру безпеки підприємства. Вони працюють у комплексі, створюючи багаторівневий бар'єр для зовнішніх і внутрішніх загроз.

Взаємодія технічних засобів захисту з офенсивними методами тестування (етичний хакінг, пентест, Red Team-атаки) є важливим елементом побудови інтегрованої системи безпеки. Офенсивні методи дозволяють перевірити ефективність технічних засобів на практиці, імітуючи дії реальних зловмисників. У процесі тестування фахівці з кібербезпеки аналізують, як системи реагують на спроби проникнення, обходу міжмережевих екранів, підбору паролів, ін'єкцій чи атак типу «людина посередині».

Результати таких перевірок дають змогу оцінити стійкість технічних засобів, визначити їхню реакцію на різні типи загроз і розробити рекомендації для вдосконалення конфігурації, політик доступу та процедур моніторингу. Таким чином, офенсивні методи виступають інструментом зворотного зв'язку у системі захисту, дозволяючи постійно вдосконалювати її ефективність і адаптувати до нових кіберзагроз.

Отже, поєднання технічних засобів захисту з активним тестуванням безпеки створює динамічну модель кіберзахисту, у якій превентивні, виявляючі та реактивні механізми функціонують у взаємозв'язку, забезпечуючи комплексний контроль над інформаційними ризиками.

В таблиці 1 показаний взаємозв'язок між технічними засобами захисту інформації та офенсивними методами тестування безпеки.

Таблиця 1

Взаємозв'язок між технічними засобами захисту інформації та офенсивними методами тестування безпеки

Перелік технічних засобів і заходів	Характеристика	Взаємодія з офенсивними методами тестування	Організаційна ланка підприємства, де застосовується	Ефект та позитивні моменти від поєднання
Мережеві екрани (Firewall)	Контролюють вхідний і вихідний трафік, блокують несанкціоновані з'єднання	Під час пентесту перевіряється ефективність фільтрації, виявлення слабких правил або обхід фаєрволу	IT-відділ, служба інформаційної безпеки	Виявлення помилок у налаштуванні, підвищення рівня сегментації мережі

Системи виявлення та запобігання вторгненням (IDS/IPS)	Аналізують мережевий трафік для виявлення атак у реальному часі	Тестування дозволяє перевірити, чи реагує система на реальні атаки, чи здатна розпізнати нові типи загроз	Центр моніторингу безпеки (SOC)	Підвищення точності виявлення, зниження кількості хибних спрацьовувань
Антивірусні та EDR-системи	Захищають кінцеві пристрої від шкідливого ПЗ та підозрілої активності	Red Team-тестування перевіряє, чи здатні антивірусні агенти виявляти складні сценарії атак	Робочі станції, сервери, IT-підтримка	Виявлення прогалин у сигнатурах і поведінкових алгоритмах захисту
Системи управління доступом (IAM)	Забезпечують ідентифікацію, автентифікацію та авторизацію користувачів	Офенсивне тестування перевіряє слабкі паролі, механізми багатофакторної автентифікації, політики прав доступу	Усі підрозділи підприємства, зокрема адміністративні	Зміцнення політики доступу, запобігання ескалації привілеїв
Криптографічні засоби (SSL/TLS, VPN, шифрування)	Забезпечують захищений обмін даними та конфіденційність інформації	Тестування на проникнення виявляє слабкі алгоритми або неправильну конфігурацію сертифікатів	Серверна інфраструктура, корпоративна мережа	Посилення захисту комунікацій, усунення вразливостей у шифруванні
Системи резервного копіювання та відновлення	Забезпечують збереження критичних даних у разі інцидентів	Етичний хакер оцінює, чи можливий несанкціонований доступ до резервних копій	IT-відділ, служба з управління даними	Підвищення надійності резервування, запобігання компрометації архівів
Системи запобігання витокам інформації (DLP) [12]	Контролюють пересилання даних поза межі мережі	Під час Red Team-тестів перевіряється, чи може обійтися контроль даних або приховане пересилання файлів	Адміністративний персонал, бухгалтерія, HR-відділ	Покращення правил контролю даних, зменшення ризику витоків
SIEM-системи (моніторинг і кореляція подій)	Збирають та аналізують події безпеки з різних джерел	Офенсивні дії дозволяють перевірити, наскільки швидко система реагує на інциденти	Центр кібербезпеки (SOC)	Підвищення рівня видимості інцидентів, оптимізація процедур реагування

Сучасні підприємства стикаються з постійно зростаючою кількістю кіберзагроз, серед яких шкідливе програмне забезпечення, фішингові атаки, внутрішні витоки даних та інші види кібератак. Одним із ключових викликів у забезпеченні безпеки інформаційних систем є не тільки застосування традиційних технічних засобів захисту, але й активне виявлення потенційних вразливостей у режимі, максимально

наближеному до реальних умов атаки. Саме у цьому контексті інтеграція етичного хакінгу з системами технічного захисту стає необхідною складовою підвищення кіберстійкості організації.

Розроблення концептуальної моделі інтеграції етичного хакінгу дозволяє структурувати процеси взаємодії між активними методами тестування безпеки та традиційними технічними заходами. Без такої моделі існує ризик дублювання зусиль, неефективного використання ресурсів або пропуску критичних вразливостей. Модель дозволяє:

– систематизувати підходи до проведення етичного хакінгу в контексті загальної стратегії інформаційної безпеки;

– визначити, на якому етапі впровадження технічних засобів доцільно проводити офенсивне тестування;

– забезпечити зворотний зв'язок між результатами тестування та оновленням політик і засобів захисту;

– підвищити адаптивність системи безпеки до нових кіберзагроз.

Концептуальну модель інтеграції етичного хакінгу в систему технічного захисту інформації підприємства можна представити у вигляді детальної таблиці 2:

Таблиця 2

Концептуальна модель інтеграції етичного хакінгу в систему технічного захисту інформації підприємства

Компонент моделі	Опис / Характеристика	Завдання та цілі	Взаємодія з технічними засобами	Результат / Ефект
Аудит існуючих технічних засобів захисту	Оцінка наявних систем контролю доступу, мережевих бар'єрів, антивірусів, резервного копіювання тощо	Виявлення слабких місць та "сліпих зон" у захисті	Технічні засоби працюють як превентивний бар'єр; аудит визначає їх ефективність	Формування початкової бази для інтеграції етичного хакінгу, виявлення критичних вразливостей
Визначення сфер застосування етичного хакінгу	Планування тестів на проникнення, оцінки безпеки додатків, мереж, соціального інжинірингу	Розробка сценаріїв офенсивного тестування для різних елементів системи	Проводяться тестування, які перевіряють реальну ефективність технічного захисту	Виявлення реальних слабких місць, підготовка рекомендацій щодо удосконалення захисту
Інтеграція процесів тестування та технічного захисту	Циклічна взаємодія офенсивного тестування і технічних засобів захисту	Забезпечити постійний контроль і коригування налаштувань захисту	Тестування дає дані для оптимізації налаштувань мережевих бар'єрів, систем контролю доступу, антивірусів	Адаптивна система безпеки, яка швидко реагує на нові загрози
Механізми документування та зворотного зв'язку	Фіксація результатів тестування, рекомендацій, протоколів змін	Створення прозорої системи обліку вразливостей та внесених змін	Технічні засоби та результати тестів документуються, звіти формують базу для оновлень	Відстеження динаміки вразливостей, контроль ефективності заходів, планування додаткових дій

Проактивне навчання та підвищення обізнаності персоналу	Використання результатів етичного хакінгу для навчання співробітників	Формування культури безпеки, зменшення людського фактору ризику	Персонал дотримується політик доступу, реагує на загрози, інтегруючи поведінку з технічними засобами	Людський фактор стає активним елементом безпеки, зниження ризику соціальних атак
Цикл постійного удосконалення	Компонент, який об'єднує всі етапи в замкнений цикл	Забезпечує адаптивність системи до нових загроз	Всі результати тестувань та налаштування технічних засобів передаються на повторний аудит та нове тестування	Система безпеки постійно еволюціонує, підвищується кіберстійкість підприємства

Пропонована концептуальна модель включає кілька взаємопов'язаних елементів:

1. Аудит існуючих технічних засобів захисту

Перед інтеграцією етичного хакінгу проводиться оцінка наявних систем контролю доступу, мережевих бар'єрів, антивірусних програм, систем резервного копіювання та інших технічних засобів. Мета цього етапу — визначити потенційні "сліпі зони", які можуть стати цілями для зловмисників.

2. Визначення сфер застосування етичного хакінгу

На цьому етапі формуються завдання для команд етичних хакерів: проведення тестів на проникнення (penetration testing), перевірка стійкості веб-додатків, оцінка безпеки внутрішніх мереж, соціальний інжиніринг тощо. Важливо, щоб ці заходи були скоординовані з політиками технічного захисту та не порушували функціонування систем.

3. Інтеграція процесів тестування та технічного захисту

Основна ідея моделі полягає у циклічній взаємодії: технічні засоби захисту виконують превентивну роль, а етичний хакінг постійно перевіряє їхню ефективність. Результати тестувань автоматично або напівавтоматично коригують налаштування засобів захисту, оновлюють політики доступу та пріоритети моніторингу.

4. Механізми документування та зворотного зв'язку

Всі проведені тестування та внесені зміни документуються у формі звітів, рекомендацій та протоколів. Ця документація дозволяє відстежувати еволюцію безпекової системи, визначати тенденції появи нових вразливостей та планувати додаткові технічні або організаційні заходи.

5. Проактивне навчання та підвищення обізнаності персоналу

Концептуальна модель передбачає використання результатів етичного хакінгу для навчання працівників: від розпізнавання соціальних атак до дотримання політик безпечного користування корпоративними системами. Це забезпечує комплексний підхід, де людина стає додатковим рівнем захисту.

Впровадження концептуальної моделі інтеграції етичного хакінгу в систему технічного захисту інформації підприємства створює багаторівневий, проактивний та адаптивний підхід до забезпечення кібербезпеки. Очікувані переваги такого підходу можна оцінити у кількох основних напрямках:

1. Підвищення ефективності виявлення вразливостей

Етичний хакінг дозволяє імітувати дії реальних зловмисників, перевіряючи як технічні засоби захисту, так і політики безпеки на підприємстві. Це дозволяє виявляти

слабкі місця, які могли залишитися непоміченими під час стандартного аудиту, та оперативно усувати їх.

2. Прискорення реагування на нові загрози

Завдяки циклічній взаємодії між тестуванням та технічними засобами захисту, організація отримує оперативну інформацію про потенційні загрози і може швидко адаптувати захисні механізми. Такий підхід зменшує час між появою вразливості і її усуненням, що критично для сучасного динамічного кіберсередовища.

3. Оптимізація використання ресурсів технічного захисту

Інтеграція етичного хакінгу дозволяє більш точно визначати, які технічні засоби та налаштування є критично важливими, а де можна знизити навантаження без втрати безпеки. Це забезпечує ефективніше використання фінансових та технічних ресурсів підприємства.

4. Підвищення обізнаності та кіберкультури серед персоналу

Результати етичного хакінгу використовуються для навчання працівників і формування у них відповідальної поведінки щодо інформаційної безпеки. Це зменшує ризики, пов’язані з людським фактором, наприклад, успішними соціальними атаками чи ненавмисними порушеннями політик безпеки.

5. Формування адаптивної та стійкої системи безпеки

Циклічний характер інтегрованої моделі забезпечує постійне вдосконалення захисних механізмів у відповідь на нові загрози. Організація отримує можливість не лише реагувати на інциденти, а й проактивно запобігати їм, що суттєво підвищує загальну кіберстійкість.

6. Зменшення ризиків фінансових та репутаційних втрат

Виявлення та усунення вразливостей до того, як ними скористається зловмисник, знижує ймовірність витоків даних, простоїв у роботі систем та негативного впливу на репутацію підприємства.

7. Підвищення довіри партнерів і клієнтів

Організація, яка застосовує інтегрований підхід до кібербезпеки, демонструє високий рівень професіоналізму у захисті інформації. Це сприяє зростанню довіри з боку бізнес-партнерів, клієнтів та регуляторів.

Таким чином, впровадження інтегрованого підходу створює синергійний ефект: поєднання технічного захисту та етичного хакінгу забезпечує не лише превентивний захист, а й постійне підвищення ефективності системи безпеки, що є ключовим фактором підвищення кіберстійкості сучасного підприємства.

Інтеграція етичного хакінгу в систему технічного захисту інформації дозволяє:

– підвищити рівень виявлення та усунення вразливостей;
– скоротити час реагування на нові загрози;
– оптимізувати використання технічних ресурсів захисту;
– сформувати проактивну культуру безпеки в організації;
– створити адаптивну систему, здатну швидко реагувати на динамічні зміни у кіберсередовищі.

Таким чином, концептуальна модель інтеграції етичного хакінгу не лише доповнює традиційні технічні заходи захисту, а й створює замкнений цикл постійного удосконалення системи кібербезпеки підприємства, забезпечуючи стійкість організації перед сучасними кіберзагрозами.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Проведене дослідження доводить, що ефективна система кібербезпеки підприємства не може будуватися виключно на основі технічних засобів захисту інформації. У сучасних умовах, коли атаки стають дедалі складнішими й динамічнішими, практика етичного хакінгу виступає необхідним елементом комплексного підходу до кіберзахисту. Саме поєднання офенсивних і захисних методів забезпечує глибше розуміння реального стану інформаційної безпеки підприємства.

Аналіз існуючих підходів показав, що етичний хакінг дозволяє виявляти не лише технічні, а й організаційні вразливості, які неможливо виявити стандартними засобами моніторингу. Це свідчить про його важливу роль у формуванні проактивної моделі безпеки, орієнтованої на постійне вдосконалення захисних механізмів.

Водночас результати дослідження підтверджують, що інтеграція етичного хакінгу в систему технічного захисту інформації підвищує рівень кіберстійкості підприємства завдяки циклічному процесу тестування, виявлення, аналізу та усунення вразливостей. Такий підхід забезпечує адаптивність системи безпеки до змін зовнішнього середовища і зменшує ризики внутрішніх порушень.

Важливим висновком є те, що поєднання технічних засобів захисту (IDS/IPS, DLP, SIEM, криптографічних протоколів тощо) з практиками етичного хакінгу створює не конкуренцію, а взаємодоповнювальну синергію, у якій результати офенсивного тестування безпосередньо сприяють удосконаленню технічних систем і політик безпеки.

Таким чином, інтегрований підхід до кіберзахисту має розглядатися не як окремий проект, а як постійна стратегія управління інформаційними ризиками, що охоплює технологічні, організаційні та людські аспекти безпеки.

Перспективи подальших досліджень полягають у кількох напрямах:

створення методики кількісної оцінки ефективності інтеграції етичного хакінгу у корпоративні системи безпеки;

розроблення моделей автоматизованого управління процесами офенсивного тестування;

дослідження можливостей застосування штучного інтелекту для імітації дій етичного хакера та прогнозування потенційних векторів атак;

формування освітніх і сертифікаційних програм, спрямованих на розвиток компетенцій з інтегрованої кібербезпеки серед фахівців підприємств.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Skandylas, C., & Asplund, M. (2025). *Automated penetration testing: Formalization and realization*. https://www.sciencedirect.com/science/article/pii/S0167404825001439
2. Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). *The ISO/IEC 27001 information security management standard: How to extract value from data in the IT sector*. *Sustainability*, *15*(7), 5828. https://www.mdpi.com/2071-1050/15/7/5828
3. Adam, H. M., Widyawan, W., & Putra, G. D. (2023). *A review of penetration testing frameworks, tools, and application areas*. In *2023 IEEE 7th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)* (pp. 319–324). IEEE.
4. ISO/IEC. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. https://www.iso.org/standard/27001
5. Parambil, M. M. A., Rustamov, J., Ahmed, S. G., Rustamov, Z., Awad, A. I., Zaki, N., & Alnajjar, F. (2024). *Integrating AI-based and conventional cybersecurity measures into online higher education settings: Challenges, opportunities, and prospects*. https://www.sciencedirect.com/science/article/pii/S2666920X24001309

6. Yulianto, S., Soewito, B., Gaol, F. L., & Kurniawan, A. (2024). *Enhancing cybersecurity resilience through advanced red-teaming exercises and MITRE ATT&CK integration: A paradigm shift in cybersecurity assessment*. https://www.sciencedirect.com/science/article/pii/S2772918424000432
7. Zhang, W., Xing, J., & Li, X. (2025). *Penetration testing for system security: Methods and practical approaches*. *arXiv preprint*. https://arxiv.org/html/2505.19174v1
8. Kukharska, N. P., Semeniuk, S. A., & Polotai, O. I. (2025). *Key aspects of the updated ISO/IEC 27002:2022 standard*. *Modern Information Protection*, (2), 76–87.
9. Lukianenko, T. Yu., Ponochovnyi, P. M., & Lehominova, S. V. (2022). *A methodology for detecting network intrusions and signs of computer attacks based on an empirical approach*. *Modern Information Protection*, 2(50), 15–21.
10. Polotai, O. I. (2025, June 11–12). *Zero trust architecture: A new security standard for corporate enterprise networks*. In *Information Society: Technological, Economic and Technical Aspects of Development* (Vol. 100, pp. 17–20). Ternopil.
11. Polotai, O. I., & Dovhanyk, S. (2020, March 16–22). *SIEM systems as an element of event analysis and management in CSOC*. In *All-Ukrainian Scientific and Practical Online Conference "Automation and Computer-Integrated Technologies in Production and Education: State, Achievements, Prospects of Development"* (pp. 60–61). Cherkasy: Bohdan Khmelnytsky National University of Cherkasy.
12. Polotai, O. I., & Puzyr, A. O. (2024). *Analysis and implementation of tools for preventing confidential information leakage in enterprises: A case study of DLP systems*. *Bulletin of Lviv State University of Life Safety*, (30), 134–144.
13. Tkachenko, A. M., Ivanusa, A. I., & Brych, T. B. (2025). *Development of an automated vulnerability scanning program for web applications*. In *Information and Analytical Support for the Activities of Security and Defense Sector Bodies of Ukraine: Scientific and Practical Conference* (pp. 37–40). Lviv: Lviv State University of Internal Affairs.
14. Tkachuk, R. L., Ivanusa, A. I., Yashchuk, V. I., Maslova, N. O., & Tkachenko, A. M. (2025). *Methods and models of information security and cybersecurity management in higher education institutions*. *Bulletin of Lviv State University of Life Safety: Collection of Scientific Papers*, (31), 101–116.
15. Toliupa, S., Pliushch, O. H., & Parkhomenko, I. I. (2020). *Construction of attack detection systems in information networks based on neural network structures*. *Cybersecurity: Education, Science, Technique*, 2(10), 169–181.
16. Chychkarov, Ye., Zinchenko, O., Bondarchuk, A., & Asieieva, L. (2023). *Feature selection method for intrusion detection systems using an ensemble approach and fuzzy logic*. *Cybersecurity: Education, Science, Technique*, 1(21), 234–251.

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

Orest Polotai
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department of Information Security Management
Lviv State University of Life Safety, Lviv, Ukraine
ORCID ID 0000-0003-4593-8601
orest.polotaj@gmail.com

Taras Brych
Candidate of Technical Sciences,
Associate Professor of the Department of Information Security Management
Lviv State University of Life Safety, Lviv, Ukraine
ORCID ID 0000-0001-6853-1981
taras_brych@hotmail.com

Artur Tkachenko
Lecturer of the Department of Information Security Management
Lviv State University of Life Safety, Lviv, Ukraine
ORCID ID *0009-0009-6830-4741*
tkachenko.am14@gmail.com

Valentina Yashchuk
Candidate of Economic Sciences, Associate Professor,
Associate Professor of the Department of Information Security Management
Lviv State University of Life Safety, Lviv, Ukraine
ORCID ID 0000-0003-2651-4918
valentina.lender@gmail.com

Bohdana Fedyna
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department of Information Security Management
Lviv State University of Life Safety, Lviv, Ukraine
ORCID ID 0000-0001-9487-2851
fedynabogdana@gmail.com

INFORMATION THREATS AND METHODS OF ENSURING SECURITY IN MODERN ONLINE GAMES

Abstract. The article provides a comprehensive analysis of modern approaches to organizing cybersecurity at enterprises, which allowed not only to systematize existing concepts of information security management, but also to identify key trends, contradictions and problematic aspects in the field of technical information protection. Particular attention is paid to the relationship between organizational and technological components of cyber protection, since it is their inconsistency that often causes critical vulnerabilities in corporate systems. It has been established that traditional means of protection, focused mainly on preventive measures - in particular, antivirus solutions, firewalls, access control systems - are no longer able to provide a full level of cyber resilience in the conditions of dynamic development of cyber threats, the growth of the role of social engineering and the spread of targeted attacks. This indicates the need to transition from reactive models of cyber protection to proactive strategies, in which the identification of potential risks precedes their implementation. The importance of ethical hacking as a tool for actively identifying vulnerabilities in information systems before they can be exploited by attackers is substantiated. Ethical hacking allows an enterprise to assess the real level of security of its information assets in conditions as close to real-world as possible, which makes it one of the most effective means of independent security auditing. Based on the analysis, it is proven that the integration of offensive security testing methods with technical protection tools creates a synergistic effect, which allows for a deeper understanding of the system's weaknesses, increases the speed of response to potential threats, and makes the risk management process more flexible and adaptive. The interaction of offensive practices with monitoring tools (IDS/IPS, SIEM), cryptographic systems, and backup tools contributes to the formation of a closed information protection cycle. The developed conceptual model for integrating

ethical hacking into the technical information protection system demonstrates the possibility of combining preventive, detection, and reactive mechanisms in a single cycle of continuous improvement of cyber protection. This approach is based on the principles of dynamic adaptation, where the results of penetration tests directly affect the configuration and development of technical protection tools. As a result, a system is formed that is capable of self-learning and constant updating in accordance with new attack vectors. This ensures not only an increase in the level of cyber resilience, but also optimization of the use of enterprise resources, since preventive threat detection is much cheaper than eliminating the consequences of incidents. The expected benefits of implementing an integrated approach are a significant increase in the level of trust in the enterprise's information infrastructure, increased reputational stability in the market, reduction of risks of unauthorized access and data loss. In addition, this approach contributes to the improvement of internal security audit processes, the formation of a unified corporate information risk management policy and the development of a culture of responsible attitude to cyber security issues at all levels of the organizational structure. It is also important that the integration of ethical hacking stimulates staff training, promotes the development of internal security expertise and creates the prerequisites for long-term improvement of the enterprise's competitiveness in the digital environment.

Keywords: cybersecurity, ethical hacking, technical information protection, offensive testing, enterprise cyber resilience, information security, threat modeling, system vulnerability, security audit, integrated protection system, preventive measures, cyber threat monitoring, risk management, penetration testing, conceptual model of cyber protection.

REFERENCES

1. Skandylas, C., & Asplund, M. (2025). *Automated penetration testing: Formalization and realization*. https://www.sciencedirect.com/science/article/pii/S0167404825001439
2. Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). *The ISO/IEC 27001 information security management standard: How to extract value from data in the IT sector*. *Sustainability, 15*(7), 5828. https://www.mdpi.com/2071-1050/15/7/5828
3. Adam, H. M., Widyawan, W., & Putra, G. D. (2023). *A review of penetration testing frameworks, tools, and application areas*. In *2023 IEEE 7th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)* (pp. 319–324). IEEE.
4. ISO/IEC. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. https://www.iso.org/standard/27001
5. Parambil, M. M. A., Rustamov, J., Ahmed, S. G., Rustamov, Z., Awad, A. I., Zaki, N., & Alnajjar, F. (2024). *Integrating AI-based and conventional cybersecurity measures into online higher education settings: Challenges, opportunities, and prospects*. https://www.sciencedirect.com/science/article/pii/S2666920X24001309
6. Yulianto, S., Soewito, B., Gaol, F. L., & Kurniawan, A. (2024). *Enhancing cybersecurity resilience through advanced red-teaming exercises and MITRE ATT&CK integration: A paradigm shift in cybersecurity assessment*. https://www.sciencedirect.com/science/article/pii/S2772918424000432
7. Zhang, W., Xing, J., & Li, X. (2025). *Penetration testing for system security: Methods and practical approaches*. *arXiv preprint*. https://arxiv.org/html/2505.19174v1
8. Kukharska, N. P., Semeniuk, S. A., & Polotai, O. I. (2025). *Key aspects of the updated ISO/IEC 27002:2022 standard*. *Modern Information Protection*, (2), 76–87.
9. Lukianenko, T. Yu., Ponochovnyi, P. M., & Lehominova, S. V. (2022). *A methodology for detecting network intrusions and signs of computer attacks based on an empirical approach*. *Modern Information Protection*, 2(50), 15–21.
10. Polotai, O. I. (2025, June 11–12). *Zero trust architecture: A new security standard for corporate enterprise networks*. In *Information Society: Technological, Economic and Technical Aspects of Development* (Vol. 100, pp. 17–20). Ternopil.
11. Polotai, O. I., & Dovhanyk, S. (2020, March 16–22). *SIEM systems as an element of event analysis and management in CSOC*. In *All-Ukrainian Scientific and Practical Online Conference "Automation and Computer-Integrated Technologies in Production and Education: State, Achievements, Prospects of Development"* (pp. 60–61). Cherkasy: Bohdan Khmelnytsky National University of Cherkasy.

12. Polotai, O. I., & Puzyr, A. O. (2024). *Analysis and implementation of tools for preventing confidential information leakage in enterprises: A case study of DLP systems*. *Bulletin of Lviv State University of Life Safety*, (30), 134–144.
13. Tkachenko, A. M., Ivanusa, A. I., & Brych, T. B. (2025). *Development of an automated vulnerability scanning program for web applications*. In *Information and Analytical Support for the Activities of Security and Defense Sector Bodies of Ukraine: Scientific and Practical Conference* (pp. 37–40). Lviv: Lviv State University of Internal Affairs.
14. Tkachuk, R. L., Ivanusa, A. I., Yashchuk, V. I., Maslova, N. O., & Tkachenko, A. M. (2025). *Methods and models of information security and cybersecurity management in higher education institutions*. *Bulletin of Lviv State University of Life Safety: Collection of Scientific Papers*, (31), 101–116.
15. Toliupa, S., Pliushch, O. H., & Parkhomenko, I. I. (2020). *Construction of attack detection systems in information networks based on neural network structures*. *Cybersecurity: Education, Science, Technique*, 2(10), 169–181.
16. Chychkarov, Ye., Zinchenko, O., Bondarchuk, A., & Asieieva, L. (2023). *Feature selection method for intrusion detection systems using an ensemble approach and fuzzy logic*. *Cybersecurity: Education, Science, Technique*, 1(21), 234–251.