УДК 004.056:378 DOI: 10.31673/2409-7292.2026.036112

Сиропятов Олександр Арсенович
доцент кафедри кібербезпеки та програмного забезпечення
Національний університет «Одеська політехніка», Одеса, Україна
ORCID: 0000-0002-2880-8111
E-mail: o.a.syropiatov@op.edu.ua

Тимошенко Лідія Миколаївна
доцент кафедри кібербезпеки та програмного забезпечення
Національний університет «Одеська політехніка», Одеса, Україна
ORCID: 0000-0002-2606-4358
E-mail: l.m.timoshenko@op.edu.ua

Агаджанян Олена Василівна
доцент кафедри кібербезпеки та програмного забезпечення
Національний університет «Одеська політехніка», Одеса, Україна
ORCID: 0000-0001-8302-6940
E-mail: o.v.ahadzhanian@op.edu.ua

ВІД ФОРТЕЦІ ДО ЕКОСИСТЕМИ: НОВА ПАРАДИГМА КІБЕРБЕЗПЕКИ УНІВЕРСИТЕТУ (ТОЧКА ЗОРУ ОДЕСЬКОЇ ПОЛІТЕХНІКИ)

У статті обґрунтовано необхідність переходу від класичної периметральної моделі інформаційної безпеки («фортеці») до концепції екосистеми кібербезпеки університету. Університет розглядається як відкрита соціотехнічна екосистема, еволюційною метою якої є спіральний цикл генерації та передачі знань. Систематизовано реальні кіберзагрози, які цілеспрямовано руйнують фази цього циклу. Запропоновано чотирирівневу архітектуру екосистеми кібербезпеки: організаційно-нормативний (з чітким розмежуванням відповідальності), процесно-орієнтований (динамічні профілі безпеки на базі Context-Aware Zero Trust), техніко-аналітичний (комплекс інтелектуального моніторингу з AI-driven SIEM) та антропогенно-освітній (формування «розподіленого імунітету»). Доведено, що центральним суб'єктом формування та аудиту екосистеми має виступати профільна кафедра кібербезпеки. Концептуальну модель описано через ресурсне обґрунтування на прикладі інфраструктури Одеської політехніки, що показало її високу практичну реалізованість та економічну доцільність. Розроблено систему кількісних індикаторів та план пілотної експлуатації для емпіричної верифікації архітектури. Обґрунтовано, що подальша імплементація цієї моделі має потенціал трансформувати кіберзахист із статті витрат та формального комплаєнсу на драйвер наукового лідерства, експорту аналітики та рівноправної міжнародної інтеграції.

Ключові слова: екосистема кібербезпеки, спіральний цикл знань, кіберстійкість, інтелектуальний моніторинг, динамічні профілі безпеки, система кількісних індикаторів, Одеська політехніка.

Вступ та формулювання проблеми

Екосистема – це функціональна єдність живих організмів та середовища їх існування. Термін уведений у науковий обіг англійським ботаніком Артуром Тенслі у 1935 році [1]. У класичному розумінні – це сукупність організмів, умов їх існування та взаємозв'язків між ними, що утворюють цілісну систему. Міжсистемний підхід дозволяє виділити фундаментальні властивості екосистем, незалежні від природи їх компонентів, що створює підстави для побудови аналогії між біологічними та складними соціальними системами [2].

Університет є характерним прикладом соціальної екосистеми. У запропонованій інтерпретації університет розглядатимемо не як закриту організацію з лінійними бізнес-процесами, а відкрите середовище, еволюційною метою якого є спрямована еволюція знань [3]. Реалізація даної мети концепції/парадигми має забезпечуватися спіральним циклом отримання, відбору, збереження, передачі та створення знань [4]. Стан університетської екосистеми визначається структурою спектра її діяльності та балансом складових. Однак внутрішня стійкість екосистеми постійно перевіряється зовнішнім середовищем. Сьогодні процеси еволюції знань та обміну ресурсами об'єктивно опосередковані цифровим середовищем. Інформаційно-телекомунікаційні системи є не просто інструментом, а нервовою та операційною системою університету. І сучасні кіберзагрози еволюціонували від простого

пошкодження інфраструктури до цілеспрямованого впливу на критичні бізнес-процеси. Актуальність розгляду цього питання підтверджується стратегічними пріоритетами державної політики України. Проте класична парадигма інформаційної безпеки (ІБ), що спирається на захист периметра та статичних масивів даних, є недостатньою. Виникає критичний розрив між вимогами держави, характером реальних кіберзагроз і обмеженістю класичних інструментів.

Рішенням цього завдання є трансформація підходів до захисту університету через концепцію екосистеми кібербезпеки. У даному контексті під екосистемою кібербезпеки розумітимемо інтегровану соціотехнічну модель, в якій організаційні, технологічні та освітні заходи захисту інформації об'єднані в єдиний контур управління ризиками, що забезпечує стійкість критичних бізнес-процесів університету. Центральним суб'єктом формування, супроводу та оперативного управління цією екосистемою виступає кафедра кібербезпеки, наявність якої у структурі більшості сучасних університетів робить запропоновану модель практично масштабованою та економічно ефективною.

Мета роботи – розробка теоретико-методологічних основ та архітектури екосистеми кібербезпеки університету для забезпечення його кіберстійкості, безперервності критичних процесів та захисту інформаційних ресурсів в умовах сучасних кіберзагроз.

Для досягнення поставленої мети вирішуються такі завдання:

1) розкрити сутність університету як соціальної екосистеми та формалізувати параметри її внутрішньої стійкості (спіральний цикл, спектр та операційний контур);

2) виявити та систематизувати реальні кіберзагрози та специфічні вразливості, що виникають у вузлах взаємодії екосистеми із зовнішнім цифровим середовищем;

3) проаналізувати відповідність поточної практики кіберзахисту вимогам держави та обґрунтувати необхідність переходу до екосистемної моделі з чіткою ієрархією відповідальності;

4) сформувати архітектурні принципи екосистеми кібербезпеки університету, що інтегрують технічні, організаційні та кадрові заходи навколо профільної кафедри кібербезпеки.

Основна частина

Університет як соціальна екосистема: сутність, структура, джерела вразливості

Традиційне управління закладом вищої освіти спирається на моделі, запозичені з корпоративного менеджменту: університет розглядається як організація з чіткими межами, ієрархією та лінійними бізнес-процесами. Такий підхід працює для опису адміністративної діяльності, але втрачає пояснювальну силу, коли йдеться про головний продукт університету – знання.

Знання постійно трансформуються і взаємодіють із зовнішнім середовищем. Тому університет доцільно розглядати як соціальну екосистему - відкрите середовище, де суб'єкти, інфраструктура та інформаційні ресурси перебувають у стані безперервного обміну з зовнішнім світом [2, 3].

Еволюція знань структурована у вигляді спірального циклу – безперервного процесу, який складається з чотирьох паралельних фаз [4]:

– залучення – імпульс системи ззовні: моніторинг наукового та освітнього контексту, залучення абітурієнтів і дослідників, інтеграція зовнішніх ідей;

– верифікація – фільтрація та фіксація: експертна оцінка, peer-review, систематизація, збереження в інституційній пам'яті (репозитарії, бази даних), перетворення інформаційних потоків на структуроване знання;

– сенсова інтеграція – вбудовування знання в суб'єктів: освітній процес, менторство, перетворення зовнішньої інформації на внутрішні компетенції та навички конкретних людей;

– еволюційний синтез – генерація нового: фундаментальні та прикладні дослідження, патентування, створення інновацій; це фаза, де екосистема створює нові сутності, які змінюють саму систему.

© Сиропятов О.А., Тимошенко Л.М., Агаджанян О.В. Від фортеці до екосистеми: нова парадигма кібербезпеки університету (точка зору Одеської політехніки). Сучасний захист інформації, 3(67), 25–36. https://doi.org/10.31673/2409-7292.2026.036112

Ключова властивість цього циклу – спіральність. Важливо, що всі чотири фази працюють паралельно і безперервно. Зупинка або деформація будь-якої фази руйнує весь цикл.

Спіральний цикл живиться ресурсами, які розподілені між ключовими доменами. Сукупність цих доменів утворює спектр екосистеми:

– освітній домен – якість викладання, оновлення навчальних програм;

– науковий домен – глибина досліджень, публікаційна активність, грантова підтримка;

– кадровий домен – залучення, утримання та розвиток талантів;

– управлінсько-ресурсний домен - ефективність розподілу фінансів, інфраструктури, гнучкість адміністрування;

– культурно-ціннісний домен – академічна доброчесність, етика, довіра, ідентичність.

Стан екосистеми визначається балансом спектра. Якщо один домен гіпертрофований за рахунок іншого (наприклад, наукові показники за рахунок академічної доброчесності або управлінської гнучкості), система втрачає цілісність. Узгоджена взаємодія всіх доменів забезпечує стійкість та адаптивність [5-7].

Реальне втілення еволюції вимагає створення операційного контуру – сукупності адміністративних та організаційних процесів, які фізично забезпечують життєдіяльність екосистеми. Він складається з шести ключових кроків:

1. Актуалізація та аудит освітньо-професійних стандартів (забезпечує фазу верифікації);

2. Інфраструктурне та ресурсне забезпечення (живить управлінсько-ресурсний домен);

3. Організація набору та формування контингенту (реалізує фазу залучення);

4. Безпосередня реалізація освітнього процесу (є ядром фази сенсової інтеграції);

5. Відтворення та розвиток науково-педагогічних кадрів (забезпечує безперервність кадрового домену);

6. Здійснення наукової та інноваційної діяльності (втілення фази еволюційного синтезу).

Внутрішня стійкість університетської екосистеми - це її здатність зберігати цілісність та напрямок еволюції. Вона забезпечується безперервністю спірального циклу, збалансованістю спектра та синхронізацією операційного контуру. Університет за своєю природою відкритий, і саме на стику його внутрішніх процесів із зовнішнім цифровим середовищем формуються такі системні вразливості [8, 9]:

– у вузлах між фазами циклу (ризики викривлення, витоку або блокування даних);

– у точках контакту доменів спектра із зовнішнім середовищем (інтеграція з державними реєстрами, хмарними сервісами, міжнародними базами);

– в операційних вузлах (організація набору, актуалізація програм, наукові дослідження).

Класичні інструменти кібербезпеки (захист периметра, антивіруси) не бачать цих процесів, бо вони працюють на рівні мережевих пакетів, а не на рівні бізнес-логіки університету [10]. Тому виникає критичний розрив між характером загроз і можливостями захисту, що обґрунтовує необхідність трансформації підходів до екосистеми кібербезпеки.

Систематизація реальних кіберзагроз і архітектурна криза системи кіберзахисту

Сьогодні кіберзагрози у вузлах екосистеми університету реальні. Сучасний університет є високоцифровим середовищем, де фази спірального циклу та кроки операційного контуру реалізуються через ІТС. Зовнішні кіберзагрози б'ють у конкретні цифрові вузли екосистеми:

1. Загрози фазі залучення та кроку 3 (організація набору): масштабні DDoS-атаки на портали вступу та інтегровані бази даних (наприклад, ЄДЕБО); фішингові кампанії, націлені на абітурієнтів для крадіжки їхніх цифрових ідентичностей. Наслідок: технічний зрив вступної кампанії, компрометація персональних даних;

2. Загрози фазі верифікації та кроку 2 (інфраструктура та пам'ять): атаки програм-здирників та вайперів на інституційні репозитарії, бібліотечні БД та сервери електронного документообігу. Наслідок: шифрування і знищення пам'яті, зупинка експертної фільтрації;

3. Загрози фазі сенсової інтеграції й кроку 4 (освітній процес): компрометація облікових записів викладачів та студентів у системах управління навчанням; несанкціоноване втручання

© Сиропятов О.А., Тимошенко Л.М., Агаджанян О.В. Від фортеці до екосистеми: нова парадигма кібербезпеки університету (точка зору Одеської політехніки). Сучасний захист інформації, 3(67), 25–36. https://doi.org/10.31673/2409-7292.2026.036112

в бази даних для підміни оцінок або навчальних матеріалів. Наслідок: порушення цілісності освітнього процесу, втрата академічної доброчесності;

4. Загрози фазі еволюційного синтезу та кроку 6 (наукова діяльність): цільові APT-атаки на науково-дослідні сервери та підключене лабораторне обладнання (IoT); промислове шпигунство через вразливості в ланцюгах постачання. Наслідок: крадіжка інтелектуальної власності, знищення «сирих» наукових даних.

Попри зростання складності кібератак поточна модель кіберзахисту в університетах є фрагментарною, реактивною та позбавленою контексту і характеризується недоліками:

1. Відсутність єдиного контексту та аналізу. Кіберзахист розподілений між підрозділами. Якщо стається інцидент (наприклад, DDoS на LMS під час сесії), IT-фахівці фіксують «перевантаження каналу» і «закривають тікет». Вони не аналізують цей інцидент як цілеспрямований удар по фазі сенсової інтеграції, який паралізує операційний контур;

2 Реактивність замість проактивності. Дії зводяться до «гасіння пожеж». Пост-аналіз обмежується технічним звітом для IT-відділу, без вироблення стратегічних рішень для керівництва щодо захисту бізнес-процесів;

3. Формальне виконання вимог. Заходи безпеки впроваджуються для проходження аудитів. Антивіруси та фаєрволи встановлені, але вони не бачать логічних аномалій (наприклад, коли зловмисник, отримавши легальний доступ через фішинг, повільно копіює наукові дані протягом місяців).

Сучасне законодавство України висуває жорсткі вимоги до університетів. Закон № 4336-IX [11] та Постанова КМУ № 712 [12] зобов'язують розробляти цільові профілі безпеки та проходити авторизацію з безпеки своїх ІТС. Постанова КМУ № 1281 [13] вимагає обов'язкового проведення інструктажів та тренінгів з кібергігієни. Постанова КМУ № 276 [14] та Закон № 4336-IX регламентують взаємодію з національною системою реагування (CERT-UA) та залучення міжнародної допомоги. Проблема полягає в тому, як університети інтерпретують ці вимоги. Цільовий профіль безпеки (згідно з Постановою № 712) розробляється для статичної ІТС (наприклад, «Сервер бази даних бібліотеки»). Держава дає університету інструмент для захисту процесів, а університет використовує його для захисту «заліза». Кібергігієна (Постанова № 1281) перетворюється на формальну лекцію «для галочки», а не на інтегрований процес формування стійкості суб'єктів екосистеми. Взаємодія з CERT-UA часто обмежується технічним пересиланням логів, без аналізу того, як отримані дані про загрози впливають на захищеність конкретних фаз Спірального циклу. Держава вимагає стійкості, але класична університетська ІБ-структура не здатна її забезпечити через відсутність аналітичного контуру, що пов'язує кіберінциденти з місією університету.

Подолання цього розриву вимагає трансформації фрагментарної ІБ-служби в екосистему кібербезпеки. Це не створення «чергової надбудови», а зміна самої архітектури захисту, де кібербезпека стає невід'ємною властивістю процесів еволюції знань. Тоді екосистема кібербезпеки вирішує поточні системні проблеми університету таким чином:

1. Контекстно-орієнтований захист бізнес-процесів. Замість розробки профілів безпеки для окремих серверів, екосистемний підхід передбачає розробку профілів для захисту фаз спірального циклу. Наприклад, профіль для LMS фокусується не лише на доступності сервера, а на цілісності облікових записів викладачів та незмінності навчальних матеріалів (захист сенсової інтеграції);

2. Єдиний аналітичний контур та предиктивне реагування. Впроваджується центр моніторингу (SOC/SIEM), який корелює мережеві події з бізнес-логікою університету. Якщо система фіксує аномальну активність у науковому репозитарії, вона ідентифікує це як потенційну APT-атаку на фазу еволюційного синтезу, ініціюючи протокол реагування з інформуванням CERT-UA;

3. Подолання кризи розмитої відповідальності та формування управлінського контуру. Класична модель створює хибну парадигму, де IT-служба несе відповідальність за всі

© Сиропятов О.А., Тимошенко Л.М., Агаджанян О.В. Від фортеці до екосистеми: нова парадигма кібербезпеки університету (точка зору Одеської політехніки). Сучасний захист інформації, 3(67), 25–36. https://doi.org/10.31673/2409-7292.2026.036112

кіберінциденти, тоді як керівники навчально-наукових підрозділів усуваються від питань безпеки. Екосистема вирішує цю проблему через чіткий розподіл ролей: IT-служба відповідає за інфраструктуру, керівники підрозділів – за кібергігієну й захист даних у своїх доменах, а кафедра кібербезпеки виступає незалежним стратегічним аудитором та оператором SOC;

4. Трансформація кібергігієни у механізм «розподіленого імунітету». Вимоги Постанови № 1281 трансформуються з формальних лекцій у контекстні тренінги. Викладач вчиться захищати свій курс у LMS, науковець - безпечно працювати з новими науковими даними. Це формує «розподілений імунітет» екосистеми, де кожен суб'єкт здатний локалізувати загрозу на своєму рівні;

5. Відкриття доступу до міжнародної допомоги та грантових програм. Це можливість, яка відкривається виключно при переході до концепції екосистеми. Міжнародні партнери (ЄС, НАТО, ENISA) інвестують у стійкі дослідницькі хаби. Наявність діючої екосистеми кібербезпеки, де поєднані навчальний процес, практика та наукові дослідження, автоматично трансформує університет зі «споживача чужих рішень» на «розробника технологій кіберстійкості», що дозволяє залучати ресурси за Постановою № 276;

6. Безперервна адаптивність та еволюційний зворотний зв'язок. Дані, отримані від CERT-UA, результати розслідування внутрішніх інцидентів та нові загрози, виявлені на кіберполігоні, автоматично стають вхідними даними для навчання ML-моделей та оновлення навчальних дисциплін. Система не лише реагує на загрози, а еволюціонує разом з ними.

Отже, систематизація реальних кіберзагроз доводить, що університет більше не може захищатися методом «фортеці». Тільки трансформація в екосистему кібербезпеки, де державні вимоги інтегровані безпосередньо у захист спірального циклу, а управлінський контур чітко розмежовує відповідальність бізнес-оунерів, технічних виконавців та незалежних аудиторів, здатна забезпечити безперервність, стійкість та суверенітет університету.

Архітектура та алгоритм функціонування екосистеми кібербезпеки

Отже, класична модель інформаційної безпеки не здатна забезпечити стійкість університету як соціальної екосистеми. Агресор атакує не сервери, а критичні бізнес-процеси. У зв'язку з цим у роботі пропонується концепція екосистеми кібербезпеки університету - інтегрованої соціотехнічної моделі, в якій організаційні, технологічні, освітні та аналітичні заходи об'єднані в єдиний контур управління ризиками. Ключовим драйвером адаптивності цієї моделі виступає застосування технологій штучного інтелекту (ШІ) та машинного навчання (МН), а центром координації та супроводу – кафедра кібербезпеки.

Багаторівнева архітектура екосистеми будується на чотирьох взаємопов'язаних рівнях (рис. 1). Фундаментом цієї архітектури є чіткий розподіл ролей, який усуває конфлікт інтересів та розмивання відповідальності.

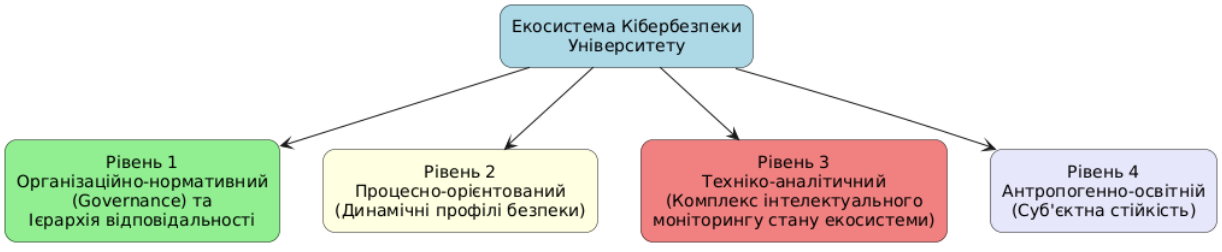

Рис. 1. Архітектура екосистеми

Рівень 1. Організаційно-нормативний та ієрархія відповідальності

Відповідно до ст. 51 Закону України № 4336-IX [11], архітектура вимагає створення підрозділу з кіберзахисту. В умовах, коли університет вже має профільну кафедру кібербезпеки, створення дублюючого адміністративного апарату є недоцільним. Тому центр формування, супроводу та оперативного управління екосистемою покладається на кафедру кібербезпеки. Впроваджується така ієрархія:

© Сиропятов О.А., Тимошенко Л.М., Агаджанян О.В. Від фортеці до екосистеми: нова парадигма кібербезпеки університету (точка зору Одеської політехніки). Сучасний захист інформації, 3(67), 25–36. https://doi.org/10.31673/2409-7292.2026.036112

1. Ректор – несе остаточну відповідальність за кіберстійкість університету, затверджує стратегію та забезпечує її ресурсне підкріплення;

2. Завідувач кафедри кібербезпеки (уповноважений заступник) - виступає стратегічним архітектором, незалежним аудитором та керівником кібернетичного контуру. Саме він розробляє та постійно вдосконалює стратегію кіберстійкості університету відповідно до змін у законодавстві, еволюції кіберзагроз та специфіки бізнес-процесів. Має права оперативного втручання у будь-який підрозділ у разі виявлення загроз та організаційно не залежить від IT-служби, що унеможливлює конфлікт інтересів за принципом «сам себе не перевіряє»;

3. Керівники інститутів, кафедр та служб – зберігають повну персональну відповідальність за кібергігієну, захист даних та дотримання політик безпеки у своїх доменах. Виступають «першою лінією оборони» та бізнес-власниками критичних процесів;

4. Співробітники та здобувачі освіти – активні суб'єкти захисту, інтегровані в розподілену мережу кіберстійкості (формування «розподіленого імунітету» екосистеми).

На рівні мережевої інфраструктури та технічного забезпечення розподіл такий:

1) керівник IT-служби університету – відповідає за стратегічний розвиток, проєктування, створення та підтримку локальних мереж інститутів, кафедр і загально-університетських сервісів (забезпечує технічний контур), приймає до виконання вимоги технічних політик безпеки мережі університету та рекомендації кафедри кібербезпеки щодо забезпечення кіберзахисту локальних мереж, створює необхідні технічні умови для безперервного моніторингу й аудиту безпеки підпорядкованих йому мереж;

2) керівник кіберполігону (SOC) – підпорядковується безпосередньо завідувачу кафедри кібербезпеки, забезпечує безперервний моніторинг, аналіз телеметрії, регулювання інцидентів та формування технічних політик безпеки мережі університету.

Рівень 2. Процесно-орієнтований (динамічні профілі безпеки)

Згідно з Постановою КМУ № 712 [12], університети зобов'язані розробляти цільові профілі безпеки. Інновація екосистеми полягає у зміщенні фокусу: профілі створюються не для статичних IT-активів, а для вузлів спірального циклу.

Застосування ШІ трансформує ці профілі в адаптивні моделі. ML-алгоритми аналізують історичний базис та контекст, автоматично змінюючи рівень довіри і заходи захисту в реальному часі, що реалізується через:

– контекстну DLP-політику: інтеграція ML із системою управління грантами дозволяє не блокувати передачу «сирих» наукових даних перед дедлайном звітності, а динамічно застосовувати криптографічне маркування та посилений телеметричний моніторинг сесії;

– мікросегментацію IoT/OT: поведінковий аналіз (UEBA) формує унікальний базис для лабораторного обладнання, миттєво ізолюючи скомпрометований VLAN без зупинки роботи інших приладів та навчальних класів;

– поведінкову біометрію: аналіз патернів роботи в адміністративних реєстрах (ЄДЕБО, ERP) виявляє компрометацію легальних облікових записів за аномаліями введення даних ще до моменту внесення деструктивних змін.

Рівень 3. Техніко-аналітичний (комплекс інтелектуального моніторингу стану екосистеми)

Фундаментом рівня є відмова від фрагментарного збору логів на користь створення єдиного аналітичного простору. Архітектура рівня базується на формуванні комплексу інтелектуального моніторингу, який структурно складається з трьох інтегрованих частин:

1. Периферія (розподілені аналітичні БД): сукупність усіх локальних аналітичних баз даних та сховищ телеметрії, що функціонують у локальних мережах інститутів, кафедр та наукових лабораторій. Забезпечує первинну фіксацію стану відповідно до технічних політик кафедри кібербезпеки та інфраструктурної підтримки IT-служби;

2. Центральний вузол агрегації (SIEM-ядро): єдиний аналітичний хаб, куди в режимі реального часу надходять та нормалізуються масиви даних з периферійного ешелону (на

основі уніфікованого переліку подій аудиту [15] та стандартів NIST SP 800-53 [16-17]). SIEM-система виступає «нервовим вузлом» екосистеми;

3. Інтелектуальний шар обробки (AI/ML-моделі): обробку агрегованого масиву телеметрії здійснюють алгоритми машинного навчання та поведінкового аналізу (UEBA). «Сирий» масив подій трансформується у контекстну картину загроз, що дозволяє виявляти складні, приховані аномалії (наприклад, повільний витік інтелектуальної власності або латеральне переміщення зловмисника).

Рівень 4. Антропогенно-освітній (суб'єктна стійкість)

Інновація екосистемного підходу полягає у зміні парадигми: людина розглядається не як загроза, а як перша лінія оборони. Замість пасивного "інформування" впроваджується механізм формування розподіленого імунітету екосистеми. Це реалізується через два інструменти:

1. Контекстна кібергігієна: впроваджуються рольові тренінги, адаптовані під конкретні бізнес-процеси (викладач захищає курс у LMS, науковець – грантові дані, співробітник деканату – реєстри ЄДЕБО);

2. Змагальні моделі навчання (CTF – Capture The Flag): суб'єкти залучаються до активної протидії загрозам через гейміфіковані сценарії, що моделюють реальні атаки на інфраструктуру університету. Формується культура «кіберстійкості через практику».

Алгоритм функціонування та реагування на інциденти (кібернетичний контур)

Функціонування екосистеми описується безперервним алгоритмом. Кафедра кібербезпеки виступає архітектором та модератором цього контуру, а кіберполігон – його операційним ядром:

1) збір телеметрії та ідентифікація: SOC кіберполігону агрегує події аудиту. ШІ-алгоритми здійснюють автоматичну попередню обробку та фільтрацію «інформаційного шуму»;

2) контекстна кореляція та оцінка впливу: алгоритми МН виконують семантичне зіставлення відфільтрованих подій із моделлю бізнес-процесів університету, пріоритезуючи їх за впливом на критичні операційні кроки;

3) ізоляція та нейтралізація: керівник кіберполігону ініціює протокол реагування. Кафедра кібербезпеки, використовуючи права оперативного втручання, координує дії з IT-службою без зупинки критичних академічних процесів. Відповідальність за локалізацію інциденту у своєму підрозділі залишається за керівником інституту/кафедри;

4) інтеграція та зворотний зв'язок: обмін інформацією з CERT-UA. Відповідно до вимог Закону № 4336-IX [11], отримані дані про нові вектори атак автоматично трансформуються в оновлення цільових профілів безпеки та донавчання (retraining) ML-моделей.

Запропонована архітектура та алгоритм вирішують фундаментальну проблему розриву між технічними інцидентами та місією університету. Чітка ієрархія, де кафедра кібербезпеки виступає незалежним аудитором з правами оперативного втручання, а керівники структурних підрозділів зберігають відповідальність за свої домени, забезпечує баланс між централізованим контролем та розподіленою стійкістю. Застосування на рівнях 2-3 AI дозволяє екосистемі перейти від реактивного «гасіння пожеж» до предиктивного захисту бізнес-процесів.

Апробація та валідація архітектури на базі інфраструктури університету

Ключовою перевагою запропонованої моделі є те, що вона не вимагає створення «з нуля» дорогих інфраструктурних надбудов. Оскільки Одеська політехніка, як практично всі сучасні університети мають у своїй структурі кафедру кібербезпеки або профільний інститут, ця модель є масштабованою. До ключових активів належать такі:

1) профільна кафедра кібербезпеки та студенти спеціальності F5 (центральний координатор екосистеми);

2) інститут інформаційної безпеки, радіоелектроніки та телекомунікацій;

3) кіберполігон (в дослідній експлуатації, ядро SOC);

4) система змагальних CTF-ігор;

5) власний захищений месенджер та поштовий сервіс.

Згідно з архітектурою (рівень 3), екосистема потребує потужного аналітичного центру - Комплексу інтелектуального моніторингу стану екосистеми. Кіберполігон університету, підпорядкований кафедрі кібербезпеки, виступає фізичним та логічним ядром цього комплексу, реалізуючи дві критичні функції:

– функція пісочниці (периферійний ешелон): на полігоні розгортаються віртуальні копії критичних вузлів екосистеми. Тут відпрацьовуються сценарії APT-атак та DDoS, що дозволяє безпечно тестувати динамічні профілі безпеки (вимога Постанови № 712 [12]) до їх впровадження в продуктивне середовище;

– функція моніторингу (центральний вузол агрегації та інтелектуальний шар): кіберполігон стає ядром університетського SOC. Студенти старших курсів та викладачі кафедри, об'єднані у внутрішню групу ASINT (Advanced Security Intelligence), під безпосереднім керівництвом науковців кафедри кібербезпеки здійснюють моніторинг подій аудиту, пентестинг власних систем та первинне реагування на інциденти.

Кафедра кібербезпеки формує технічні політики безпеки мережі, а IT-служба університету забезпечує інфраструктурну підтримку та технічні умови для безперервного моніторингу підпорядкованих їй мереж. Такий розподіл ролей усуває конфлікт інтересів (кафедра контролює, IT-служба виконує) та забезпечує системність управління кібербезпекою на технічному рівні.

Сьогодні технології штучного інтелекту та машинного навчання є обов'язковою умовою виживання та забезпечення стійкості екосистеми кібербезпеки. Проте «сліпе» впровадження універсальних рішень не враховує унікальної специфіки університету. Тому реалізація рівнів 2 та 3 вимагає глибокої кастомізації ML-моделей через синергію кількох профільних структур:

1) Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій;

2) Інститут штучного інтелекту (консультант): відіграє рекомендаційну та експертну роль, його фахівці забезпечують методологічну підтримку: пропонують оптимальні архітектурні рішення для впровадження моделей ШІ, адаптують їхні математичні параметри під наявну обчислювальну інфраструктуру університету та надають рекомендації щодо інтеграції передових алгоритмів в існуючі засоби кіберзахисту;

3) Кафедра кібербезпеки: безпосередня розробка, тонке налаштування та навчання ML-моделей здійснюються кафедрою кібербезпеки за активною участю студентів та аспірантів, де кафедра знає специфіку бізнес-процесів та перетворює рекомендації ШІ на працюючі інструменти захисту.

Кіберполігон виступає джерелом синтетичних та реальних датасетів, на яких кафедра валідує ці моделі. Такий розподіл ролей забезпечує глибоку інтеграцію фундаментальної науки, прикладної кібербезпеки та освітнього процесу, перетворюючи студентів на реальних розробників засобів захисту для власного університету.

Розглянемо валідацію антропогенно-освітнього рівня: диференційована кібергігієна та гейміфікація навчання. Постанова КМУ №1281 [13] вимагає проведення систематичних тренінгів з кібергігієни. Інновація екосистемного підходу полягає у впровадженні диференційованої, рольово-орієнтованої моделі кібергігієни, що реалізується через механізми:

1) вибірково-орієнтований підхід: замість масових лекцій екосистема формує цільові групи (викладачі, науковці, адміністративний персонал, студенти, керівники), кожна з яких отримує контекстну програму, прив'язану до їхніх реальних бізнес-процесів та часових інтервалів (наприклад, тренінги для науковців перед дедлайнами грантової звітності);

2) гейміфікація через CTF: щоб перетворити формальну вимогу на реальний інструмент формування «розподіленого імунітету», впроваджуються змагальні моделі навчання. CTF-змагання адаптуються під різні рівні підготовки та базуються на реальних інцидентах,

зафіксованих SOC університету. Це перетворює навчання з «обов'язкового заходу» на «цікавий виклик».

Для захисту Операційного контуру від інсайдерських загроз та фішингу університет впроваджує власний захищений месенджер та поштовий сервіс з жорсткою аутентифікацією. Це створює ізольований комунікаційний периметр, який різко знижує «поверхню атаки». Кафедра кібербезпеки здійснює незалежний аудит логів доступу та правил маршрутизації.

Наявність власної екосистеми кібербезпеки відкриває шлях до реалізації вищого рівня еволюції – еволюційного синтезу в сфері кіберзахисту. Це виводить університет на новий рівень глобальної суб'єктності:

1. Науковий центр з превентивної кібербезпеки: створюється на базі кіберполігону та кафедри кібербезпеки. Університет остаточно переходить від статусу споживача чужих рішень до статусу їхнього розробника;

2. Аналітичний хаб для глобальних розробників: унікальні масиви телеметрії та даних про кібератаки, які генеруються кіберполігоном та SOC, перетворюють університет на цінного донора даних. Аналітичний центр стає джерелом для валідації та навчання міжнародних систем кіберзахисту, відкриваючи шлях до співпраці з глобальними вендорами;

3. Рівноправне партнерство з провідними університетами світу: відповідно до Постанови КМУ № 276 [14], наявність діючої екосистеми є обґрунтуванням для участі у міжнародних програмах (ЄС, НАТО, ENISA). Проте головний здобуток – це вихід на рівноправне партнерство з провідними світовими університетами. Університет стає співрозробником стандартів кіберстійкості та експортером аналітичних моделей у сфері AI для кібербезпеки.

Для переходу від концептуального моделювання до емпіричної верифікації запропонованої архітектури розроблено систему кількісних індикаторів кіберстійкості (Key Performance Indicators – KPI). Ця система дозволить провести структуровану валідацію моделі під час пробної експлуатації на базі інфраструктури Одеської політехніки. Система KPI побудована відповідно до чотирирівневої архітектури, фаз спірального циклу еволюції знань та вимог нормативних документів (Закон України № 4336-IX, Постанови КМУ №, № 1281).

Індикатори ефективності екосистеми поділено на п'ять змістовних груп.

1. Операційні показники реагування на інциденти (рівень 3) відображають швидкість та якість роботи Комплексу інтелектуального моніторингу (SOC/SIEM):

– Mean Time to Detect (MTTD) – середній час виявлення загрози;

– Mean Time to Respond / Contain (MTTR / MTTC) – час на реакцію та локалізацію;

– Mean Time to Recover (MTTRec) – час на відновлення критичного бізнес-процесу;

– Incident Detection Rate (IDR) – частка проактивно виявлених загроз (до реалізації шкод);

– False Positive Rate (FPR) – рівень хибних спрацювань AI-моделей.

2. Захист бізнес-процесів (рівень 2 спіральний цикл) оцінюють цілісність фаз еволюції знань:

– Phase Protection Effectiveness – ефективність захисту конкретних фаз (залучення, верифікація, сенсова інтеграція, еволюційний синтез);

– Data Integrity Violation Rate – кількість інцидентів, пов'язаних з викривленням або витоком академічних/наукових даних;

– Availability of Critical Systems – доступність критичних вузлів (LMS, репозитарії, ЄДЕБО).

3. Антропогенна стійкість (рівень 4) – індикатори сформованого «розподіленого імунітету»:

– Phishing Click Rate – відсоток співробітників та студентів, які взаємодіють з фішинговими імітаціями;

– Training Effectiveness Rate – динаміка покращення навичок після рольових тренінгів;

– CTF Participation & Success Rate – залучення до змагальних моделей кібергігієни.

4. Ефективність управління та комплаєнс (рівень 1):

– Vulnerability Remediation Rate – швидкість усунення вразливостей за рекомендаціями кафедри кібербезпеки;

– Compliance Score – рівень відповідності вимогам Постанов КМУ № 712 та № 1281.

5. Стратегічні показники:

– Cyber Resilience Maturity Score – рівень зрілості екосистеми (0-5 балів, за адаптованою шкалою NIST).

Для підтвердження практичної реалізованості моделі пропонується поетапний план впровадження на базі Одеської політехніки:

1. Підготовчий етап (1-3 місяці): аудит поточного стану та формування базової лінії значень KPI;

2. Впровадження ключових елементів (4-8 місяців): розгортання кіберполігону як ядра SOC, інтеграція Context-Aware Zero Trust профілів, запуск SIEM та диференційованих CTF-тренінгів;

3. Моніторинг та збір телеметрії (протягом 6 місяців): безперервний збір даних у реальному середовищі;

4. Аналіз результатів та ітерація: порівняння цільових показників з базовою лінією, донавчання ML-моделей та коригування політик безпеки.

Університет має необхідну ресурсну базу для старту пілоту: профільну кафедру кібербезпеки, кіберполігон, Інститути інформаційної безпеки, штучного інтелекту та досвід участі CTF-змагань, що робить цей план економічно обґрунтованим.

Таблиця 1

Очікувані результати пілотної валідації екосистеми кібербезпеки

KPI	Базова лінія (орієнтовно)	Цільове значення після пілоту	Очікувана зміна
MTTD	12–24 години	< 1 година	−90 % і більше
MTTR (Respond)	36–72 години	< 6 годин	−85 % і більше
Phishing Click Rate	15–20 %	< 5 %	−70 % і більше
Availability критичних систем	96–98 %	> 99,5 %	+2–3 %

Успішна валідація запропонованої моделі на базі Одеської політехніки дозволить підтвердити її практичну реалізованість, економічну доцільність та готовність до масштабування на інші заклади вищої освіти України. Результати пілоту стануть емпіричною основою для подальших наукових досліджень та вдосконалення екосистеми кібербезпеки.

Отже, концептуальна валідація та ресурсне обґрунтування на прикладі Одеської політехніки підтверджують практичну реалізованість запропонованої моделі. Інтеграція існуючих активів дозволяє сформувати повноцінний контур кіберстійкості без критичних капітальних інвестицій.

Чітке закріплення за кафедрою кібербезпеки ролі центрального координатора та незалежного аудитора забезпечує системність управління. Запропонована методика кількісної валідації (KPI) та план пілотної експлуатації створюють надійний інструментарій для емпіричного доказу ефективності екосистеми. Модель відповідає вимогам держави та має потенціал перетворити кіберзахист зі статті витрат на драйвер міжнародного визнання та наукового лідерства.

Висновки

1. Доведено, що класична модель інформаційної безпеки, спрямована на ізольований захист IT-активів («фортеця»), є архітектурно неспроможною в умовах сучасних кіберзагроз. Запропоновано та обґрунтовано перехід до екосистемної моделі, де об'єктом захисту свиступають фази Спірального циклу еволюції знань та кроки операційного контуру.

© Сиропятов О.А., Тимошенко Л.М., Агаджанян О.В. Від фортеці до екосистеми: нова парадигма кібербезпеки університету (точка зору Одеської політехніки). Сучасний захист інформації, 3(67), 25–36. https://doi.org/10.31673/2409-7292.2026.036112

2. Вирішено проблему «розмитої відповідальності». Запропонована ієрархія чітко розмежовує ролі: IT-служба забезпечує інфраструктурний контур; керівники підрозділів несуть персональну відповідальність за кібергігієну у своїх доменах; а профільна кафедра кібербезпеки виступає незалежним стратегічним аудитором, архітектором та оператором SOC, що унеможливлює конфлікт інтересів.

3. Показано, що виживання екосистеми вимагає відмови від статичних правил на користь динамічних профілів та комплексу інтелектуального моніторингу. Синергія між кафедрою кібербезпеки Інституту ІБРТ та Інститутом штучного інтелекту дозволяє створювати високоточні інструменти захисту без критичних капітальних інвестицій у сторонні рішення.

4. Вимоги держави щодо кібергігієни трансформовано з формального комплаєнсу в механізм формування «розподіленого імунітету». Через впровадження диференційованої рольової кібергігієни та CTF-моделей, кожен суб'єкт екосистеми перетворюється на активний сенсор та першу лінію оборони.

5. Дослідження інфраструктури Одеської політехніки довело, що запропонована архітектура не вимагає створення дорогих надбудов «з нуля». Наявність профільної кафедри, кіберполігону, Інституту ШІ та CTF-платформи створює матеріально-технічний фундамент для імплементації моделі. Це підтверджує її економічну доцільність, масштабованість на інші ЗВО та здатність задовольнити вимоги держави.

6. Для переходу від концептуального моделювання до практичного впровадження розроблено систему кількісних індикаторів кіберстійкості, охоплюючи операційні, бізнес-орієнтовані, антропогенні та стратегічні метрики. Запропоновано поетапний план пілотної експлуатації на базі Одеської політехніки, який дозволить емпірично підтвердити ефективність переходу від реактивного захисту до предиктивної екосистеми.

7 Успішна імплементація запропонованої моделі створить фундаментальні передумови для генерації масивів телеметрії та аналітичних моделей. Це відкриє перспективи для набуття університетом статусу data provider для глобальних вендорів, створення нукового центру з превентивної кібербезпеки та виходу на рівноправне партнерство з провідними світовими університетами. Отже, кіберзахист має потенціал перетворитися зі статті витрат на потужний драйвер міжнародного визнання, наукового лідерства та залучення грантової допомоги.

Подальші розвідки будуть зосереджені на безпосередній інженерній імплементації та емпіричному тестуванні розроблених KPI під час пілотної експлуатації, аналізі ML-моделей на базі кіберполігону Одеської політехніки, а також на розробці уніфікованих математичних моделей для оцінки кіберстійкості фаз спірального циклу в умовах інтеграції з національною (CERT-UA) та європейською (ENISA) системами обміну телеметрією загроз.

Перелік посилань

1. Tansley A. G. The use and abuse of vegetational concepts and terms. Ecology.1935. Vol. 16, No. 3. P. 284-307.

2. Ostrom E. A general framework for analyzing sustainability of social-ecological systems. Science. 2009. Vol. 325, No. 5939. P. 419-422.

3. Etzkowitz H., Leydesdorff L. The dynamics of innovation: from National Systems and "Mode 2" to a Triple Helix of university-industry-government relations. Research Policy. 2000. Vol. 29, No. 2. P. 109-123.

4. Nonaka I., Takeuchi H. The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation. New York: Oxford University Press, 1995. 284 p.

5. McElroy M. W. The New Knowledge Management: Complexity, Learning, and Sustainable Innovation. Butterworth-Heinemann, 2003. 320 p.

6. Linkov I., Eisenbies J. R., Disch C., et al. Cyber-resilience: a framework for managing cyber risks. Journal of Cyber Security and Information Systems. 2018. Vol. 1, No. 1. Pp. 1-12.

7. Bodeau D. K., Graubart R., & Rosoff A. Cyber Resilience for Systems and Organizations. MITRE Corporation, 2017.

8. Alberts C. J., McQuaid D. Cybersecurity Engineering: Managing Risk and Resilience. SEI, 2010.

9. Rajkumar R., Lee I., Sha L., Stankovic J. Cyber-physical systems: the next computing revolution. Proceedings of the 47th Design Automation Conference. 2010. Pp. 731-739.

10. Linkov I., Bates M. E., Trump B. D., et al. Cyber-resilience and digital immunity in complex systems. Environment Systems and Decisions. 2020. Vol. 40. Pp. 1-10.

11. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. Відомості Верховної Ради України. 2025. № 35, ст. 134.

12. Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем : Постанова Кабінету Міністрів України від 18.06.2025 № 712. Офіційний вісник України. 2025. № 57, ст. 3921.

13. Про затвердження Порядку проведення інструктажів та систематичних тренінгів щодо кібергігієни : Постанова Кабінету Міністрів України від 08.10.2025 № 1281. Офіційний вісник України. 2025. № 87, ст. 6055.

14. Про утворення Міжвідомчої робочої групи з питань залучення міжнародної допомоги для забезпечення кібербезпеки та кіберстійкості держави : Постанова Кабінету Міністрів України від 08.03.2024 № 276. Офіційний вісник України. 2024. № 28, ст. 1803.

15. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Cognitive Warfare: The Battle for the Brain. NATO CCDCOE Publications, 2021.

16. National Institute of Standards and Technology (NIST). Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5). Gaithersburg, MD: NIST, 2020.

17. Перелік подій аудиту, що підлягають реєстрації (Додаток А до Політики AU, на основі НД ТЗІ 3.6-006-24 та NIST SP 800-53r5). Внутрішній регламент організації. 2024.

Oleksandr Syropyatov
Associate Professor, Department of Cybersecurity and Software
Odesa Polytechnic National University, Odesa, Ukraine
ORCID: 0000-0002-2880-8111
E-mail: o.a.syropiatov@op.edu.ua

Lidiia Tymoshenko
Associate Professor, Department of Cybersecurity and Software
Odesa Polytechnic National University, Odesa, Ukraine
ORCID: 0000-0002-2606-4358
E-mail: l.m.timoshenko@op.edu.ua

Olena Ahadzhanyan
Associate Professor, Department of Cybersecurity and Software
Odesa Polytechnic National University, Odesa, Ukraine
ORCID: 0000-0001-8302-6940
E-mail: o.v.ahadzhanian@op.edu.ua

FROM FORTRESS TO ECOSYSTEM: A NEW PARADIGM OF UNIVERSITY CYBERSECURITY (THE POINT OF VIEW OF ODESSA POLYTECHNIC)

The article substantiates the need to transition from the classical perimeter model of information security ("fortress") to the concept of a university cybersecurity ecosystem. The university is considered as an open socio-technical ecosystem, the evolutionary goal of which is a spiral cycle of knowledge generation and transfer. Real cyber threats that purposefully destroy the phases of this cycle are systematized. A four-level architecture of the cybersecurity ecosystem is proposed: organizational-normative (with a clear demarcation of responsibility), process-oriented (dynamic security profiles based on Context-Aware Zero Trust), technical-analytical (complex of intelligent monitoring with AI-driven SIEM) and anthropogenic-educational (formation of "distributed immunity"). It is proved that the central subject of ecosystem formation and audit should be the specialized department of cybersecurity. The conceptual model is described through resource justification on the example of the infrastructure of Odessa Polytechnic, which showed its high practical feasibility and economic feasibility. A system of quantitative indicators and a pilot operation plan for empirical verification of the architecture have been developed. It is substantiated that further implementation of this model has the potential to transform cyber security from an item of expenditure and formal compliance to a driver of scientific leadership, export of analytics and equal international integration.

Keywords: cybersecurity ecosystem, spiral knowledge cycle, cyber resilience, intelligent monitoring, dynamic security profiles, system of quantitative indicators, Odesa Polytechnic.

Надійшла до редакції (Received): 08.07.2026
Прийнята до друку (Accepted): 08.09.2026
Опубліковано онлайн (Available online): 15.09.2026

© Сиропятов О.А., Тимошенко Л.М., Агаджанян О.В. Від фортеці до екосистеми: нова парадигма кібербезпеки університету (точка зору Одеської політехніки). Сучасний захист інформації, 3(67), 25–36. https://doi.org/10.31673/2409-7292.2026.036112