ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС
Матеріали Міжнародної науково-практичної конференції
2

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

Одеса
2025

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)
Є 24

Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 16.05.2025 р.)

За загальною редакцією ***С. В. Ківалова***

Є 24 **Європейські орієнтири розвитку України: нові виміри у воєнний час** : у 2 т. : матеріали Міжнар.наук.-практ. конф. (Одеса, 16 травня 2025 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2025. – Т. 2. – 716 с.
ISBN 978-617-8430-61-0

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири України: нові виміри у воєнний час» містять результати наукових досліджень і практичних напрацювань вчених, фахівців і військовослужбовців, здійснені в умовах повномасштабної війни. У збірнику представлено як теоретичні, так і емпіричні дослідження у галузях філософії, загальної теорії держави і права, історії права, сучасних соціально-політичних процесів, соціології та психології.

Особливу увагу приділено аналізу загроз національній безпеці в конституційному, міжнародному та європейському правовому контекстах, а також питанням трудового, соціального, земельного, аграрного та екологічного права. Окремі розділи присвячено функціонуванню економіки та підприємництва в умовах євроінтеграції.

У збірнику також розглянуто проблематику цифрової трансформації, захисту інформації та кібербезпеки в умовах воєнного часу, методику викладання іноземних мов, перекладознавство, лінгвістику і журналістику. Висвітлено наукові здобутки в адміністративному, фінансовому, морському та митному праві, реформуванні судової системи, діяльності прокуратури, правоохоронних органів та адвокатури. Окремо проаналізовано питання кримінального права, кримінального процесу, кримінології, криміналістики, судової експертизи, медико-психологічного забезпечення правосуддя, а також аспекти цивільного, сімейного, господарського права, інтелектуальної власності та патентного судочинства. Розглянуто також актуальні питання діяльності бібліотек у закладах вищої освіти та фізичної підготовки здобувачів вищої освіти.

Збірник адресовано науковцям, викладачам, здобувачам вищої освіти, а також практикам у галузях права, економіки, соціології, політології, психології, філології, журналістики та кібербезпеки.

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)

Відповідальний за випуск ***М. Р. Аракелян***

ISBN 978-617-8430-61-0

СЕКЦІЯ 22. ІНФОРМАТИЗАЦІЯ ТА ЦИФРОВІЗАЦІЯ СУСПІЛЬСТВА В ЕПОХУ СТРІМКОГО РОЗВИТКУ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

СЕКЦІЯ 23. КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

СЕКЦІЯ 23.
КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

Керівник секції: *завідувач кафедри кібербезпеки, доктор економічних наук, професор Горбаченко Станіслав Анатолійович*
Секретар секції: *доцент кафедри кібербезпеки, кандидат технічних наук, доцент Кухаренко Сергій Вікторович*

Горбаченко Станіслав Анатолійович
Національний університет «Одеська юридична академія», завідувач кафедри кібербезпеки, доктор економічних наук, професор

ЗАСТОСУВАННЯ МЕТОДОЛОГІЇ SCRUM У ВИРІШЕННІ ЗАДАЧ КІБЕРБЕЗПЕКИ

Сучасні суб'єкти підприємництва здебільшого шукають інноваційні підходи, засоби та інструменти, які дозволять не лише оперативно реагувати на загрози, але й системно вдосконалювати механізми підтримки та захисту бізнес-процесів. Одним із таких підходів є Scrum – методологія, що зародилася в сфері розробки програмного забезпечення, але поступово знаходить своє місце і у сфері кібербезпеки завдяки своїй гнучкості та орієнтації на командну взаємодію [1].

Перша інформація про методологію Scrum з'явилася у 1990-х роках. Фахівці відразу побачили у вказаній методології відповідь на потребу в гнучкому управлінні проєктами, коли традиційні методи, такі як «водоспад», виявилися занадто громіздкими для динамічних середовищ [2]. У свою чергу Scrum базується на ітеративному підході, де робота розбивається на короткі цикли – спринти, що тривають від одного до чотирьох тижнів. І у кожному спринті команда прагне досягти конкретного результату, який можна оцінити та вдосконалити. У центрі Scrum стоять принципи прозорості, регулярного перегляду прогресу та адаптації до змін, що робить його привабливим для сфер, де швидкість реакції відіграє ключову роль. Саме такою сферою, на перший погляд, і є кібербезпека.

Однак, концептуально кібербезпека відрізняється від розробки програмного забезпечення, адже загрози постійно еволюціонують, і передбачити їхню природу, форму чи точний час появи майже неможливо. Відтак робота в сфері кіберзахисту вимагає залучення спеціалістів із різних напрямів – від аналітиків, які досліджують вразливості, до інженерів, які впроваджують захисні рішення і, навіть фахівців з управління персоналом, які проводять тренінги з кібергігієни для співробітників.

Критичність часу додає ще більше складності вирішенню питань кібербезпеки, адже затримка в реагуванні на інцидент може призвести до серйозних наслідків, таких як втрата даних чи репутації. Усе це робить традиційні підходи менш ефективними, тоді як Scrum пропонує інструменти для швидкої адаптації та поступового вдосконалення.

На практиці застосування Scrum у кібербезпеці дозволяє командам оперативно реагувати на нові загрози завдяки коротким циклам роботи. Регулярні зустрічі, такі як щоденні стендапи, забезпечують чітке розуміння того, що відбувається в проєкті, а огляди спринтів дають змогу оцінити досягнутий прогрес. Гнучкість методології проявляється в можливості швидко переглядати пріоритети завдань залежно від актуальних ризиків, а ретроспективи сприяють аналізу попереднього досвіду та вдосконаленню процесів. Особливо цінною є здатність Scrum об'єднувати зусилля різних спеціалістів, адже кібербезпека – це завжди командна гра, де успіх залежить від злагодженої взаємодії [3].

Проте адаптація методології Scrum до завдань кібербезпеки не обходиться без ризиків та труднощів. Адже вказані завдання часто носять реактивний характер – наприклад, відповідь на інцидент чи термінове усунення вразливості, що ускладнює планування спринтів. У деяких галузях, таких як фінанси чи охорона здоров'я, діють суворі регуляторні вимоги, які можуть суперечити гнучкому підходу Scrum. До того ж, результат роботи в кібербезпеці не завжди є конкретним продуктом – це може бути підвищення рівня захисту чи зниження ризиків, що важко виміряти в рамках традиційного інкременту. Усе це вимагає від команд творчого підходу до використання методології, зберігаючи її основні принципи, але адаптуючи їх до реалій завдань кібербезпеки.

Проте, можна стверджувати, що на практиці застосування Scrum у сфері кібербезпеки вже продемонструвало певну цінність в реальних організаціях, які стикалися з конкретними загрозами та успішно адаптували означену методологію для їхнього подолання. Одним із таких випадків є діяльність компанії JPMorgan Chase, яка у 2019 році зіткнулася зі сплеском фішингових атак на своїх клієнтів [4]. Щоб протистояти цій проблемі, команда кібербезпеки вирішила скористатися Scrum для створення та впровадження нової системи захисту. На старті проєкту керівник визначив амбітну мету – скоротити кількість успішних атак на 50% за 3 місяці. У процесі роботи команда сформувала беклог, який включав аналіз типових фішингових повідомлень, розробку вдосконалених фільтрів для електронної пошти та підготовку внутрішньої кампанії з підвищення обізнаності співробітників. Спринти тривалістю 2 тижні дозволили спочатку зібрати дані про атаки та протестувати початкові ідеї, а потім перейти до впровадження перших захисних механізмів. Регулярні огляди показали, що деякі фільтри потребували доопрацювання через нові тактики зловмисників, і команда оперативно скоригувала підхід. Вже через 2 місяці рівень успішних атак знизився на 40%, а до кінця третього спринту

ціль була повністю досягнута, що стало значним проривом у захисті клієнтських даних.

Ще один приклад пов'язаний із компанією Cloudflare, технологічним лідером у сфері хмарних рішень, яка у 2020 році працювала над посиленням захисту своїх клієнтів від атак типу DDoS. Команда кібербезпеки Cloudflare застосувала Scrum, щоб швидко розробити та впровадити нові механізми протидії. Робота розпочалася з оцінки вразливостей їхньої інфраструктури: під час першого спринту інженери провели стрес-тестування серверів і виявили потенційні слабкі місця в обробці трафіку [5]. Наступний спринт був присвячений розробці системи автоматичного перенаправлення шкідливого трафіку на спеціальні поглинаючі вузли. Щоденні стендапи допомагали вирішувати технічні складнощі, такі як налаштування алгоритмів фільтрації, а ретроспектива після другого спринту підказала, як пришвидшити процес тестування завдяки автоматизації. У підсумку через 6 тижнів Cloudflare вдалося суттєво підвищити стійкість своєї платформи, що дозволило уникнути перебоїв у роботі для мільйонів користувачів під час масованої хвилі атак, яка сталася незабаром після завершення проєкту.

Третій випадок стосується дій Агентства з кібербезпеки та захисту інфраструктури США (CISA) під час реагування на атаку SolarWinds у 2020 році, коли хакери скомпрометували численні державні установи. CISA використала Scrum для координації зусиль у кризовій ситуації. Перший спринт зосередився на локалізації загрози: аналітики відстежували джерело атаки через аналіз логів, а інженери ізолювали уражені сегменти мережі, щоб зупинити подальше поширення. Наступний етап передбачав відновлення систем і впровадження тимчасових захисних рішень, таких як оновлення конфігурацій брандмауерів. Незважаючи на надзвичайний тиск, щоденні зустрічі дозволяли уникати хаосу та дублювання завдань, а гнучкість Scrum дала змогу швидко переорієнтуватися, коли стало зрозуміло, що атака зачепила значно більше систем, ніж вважалося спочатку. Інцидент вдалося нейтралізувати за 2 тижні, а ретроспектива допомогла сформулювати стратегію профілактики, яка згодом була застосована для захисту інших державних установ.

Вищевказані приклади демонструють, як методологія Scrum адаптується до різноманітних викликів кібербезпеки. Короткі цикли роботи дозволяють командам швидко оцінювати результати й коригувати плани, а акцент на командній взаємодії забезпечує ефективність навіть у найскладніших умовах. Звісно, методологія не вирішує всіх проблем автоматично і потребує врахування унікальних особливостей кожного підприємства чи організації, однак здатність поєднувати швидкість із системним підходом робить її ефективним інструментом у боротьбі з кіберзагрозами. У майбутньому, коли кіберзагрози стануть ще більш витонченими, цей підхід, ймовірно, набуватиме дедалі більшого поширення, допомагаючи підприємствам та організаціям випереджати зловмисників і зберігати безпеку в цифровому просторі.

Список використаних джерел:

1. Храпкін О., Кіндрат О., Чопей Р. Управління проєктами в іт-галузі: методики, інструменти та керування ризиками. *Економіка та суспільство*. 2023. № 55. URL: https://doi.org/10.32782/2524-0072/2023-55-110

2. Scrum&Agile: що це таке та кому може знадобитися? URL: https://budni.robota.ua/career/scrum-agile (дата звернення: 02.04.2025).

3. Нефьодов Л. І., Філь Н. Ю. Модель вибору Scrum-майстра із застосуванням нечітких множин. *Вісник Харківського національного автомобільно-дорожнього університету*. 2022. Вип. 97. С. 16–23.

4. Pabin M. How the Finance Industry is Shaped by Technology – A Corporate Experience. *Finance Undergraduate Honors Theses*. 2023. URL: https://scholarworks.uark.edu/finnuht/9 (дата зверення: 05.04.2025).

5. Величко С. В. Засоби та механізми протидії ddos-атакам. *Інформаційне суспільство: проблеми та перспективи :* матеріали VII Всеукраїнської науково-практичної конференції (м. Одеса, 20 травня 2022 р.) / відп. ред. Н. І. Логінова. Одеса, 2022. С. 97-99.

Ключові слов: scrum, кібербезпека, регуляторні вимоги, захист даних, аналіз вразливостей.
Keywords: scrum, cybersecurity, regulatory requirements, data protection, vulnerability analysis.

Соколов Артем Вікторович
Національний університет «Одеська юридична академія»,
професор кафедри кібербезпеки, доктор технічних наук, професор
Радуш Володимир Вячеславович
Національний університет «Одеська політехніка»,
аспірант кафедри кібербезпеки та програмного забезпечення

МЕТОД НЕДВІЙКОВОГО АФІННОГО ПЕРЕТВОРЕННЯ ДЛЯ ПІДВИЩЕННЯ КРИПТОГРАФІЧНОЇ ЯКОСТІ S-БЛОКІВ

Одним із ключових елементів симетричних криптографічних алгоритмів є S-блоки, від криптографічної якості яких значною мірою залежить стійкість усієї системи до відомих атак, зокрема диференціального та лінійного криптоаналізу. Основними критеріями криптографічної якості S-блоків виступають:

1. Нелінійність;
2. Строгий лавинний критерій (Strict Avalanche Criterion, SAC);
3. Критерій бітової незалежності (Bit Independence Criterion, BIC);
4. Імовірність лінійної апроксимації (Linear Approximation Probability, LAP);
5. Імовірність диференціальної апроксимації (Differential Approximation Probability, DAP);
6. Кореляційна незалежність вихідних та вхідних векторів S-блоку.