**УДК 681.32:007.5**
**DOI: 10.15587/1729-4061.2019.169527**

# Розробка методології побудови системи безпеки інформації в корпоративній науково-освітній системі в умовах автономності університету

**С. П. Євсеєв, В.О. Алексієв, С. М. Балакірева, Є. В. Пелешок, О. В. Мілов, О. В. Петров, О. В. Раєвнєва, Б. П. Томашевський, І. Я. Тишик, О. В. Шматко**

*Розвиток обчислювальних засобів і технологій корпоративних мереж розширило спектр освітніх та інформаційних послуг в корпоративних науково-освітніх мережах (КНОС). Такі мережі відносяться до критичних кібернетичних інформаційних систем (ККІС), побудованих на основі моделей відкритих мереж. Такий підхід на початку 80-х років XX ст. не розглядав необхідність побудови системи безпеки, що не дозволяє забезпечити певний рівень безпеки від сучасних гібридних загроз. Перехід на автономність управління університетами в усьому світі висуває вимоги до забезпечення необхідної якості обслуговування (QoS) клієнтів КНОС. До користувачів КНОС відносяться адміністрація університету, професорсько-викладацький склад, студенти та персонал, який обслуговує освітняні процеси в ЗВО. Одним з головних критеріїв QoS є безпека інформації. Однак загального підходу до побудови комплексного захисту інформації в КНОС, яка забезпечувала необхідний рівень безпеки немає.*

*В основу методології запропонована концепція синтезу синергетичної моделі загроз на ККІС, удосконалених моделей інфраструктури КНОС, порушника, оцінки поточного стану інформаційної безпеки (ІБ) і вдосконаленого методу інвестицій в ІБ КНОС. Показано, що базис синергетичної моделі становить трирівнева модель стратегічного управління безпекою, яка забезпечує отримання синергетичного ефекту в умовах одночасної дії загроз інформаційній безпеці, кібербезпеці і безпеці інформації. На відміну від відомих такий підхід забезпечує визначення якісно нових і невідомих до цього емерджентних властивостей системи безпеки інформації з урахуванням коштів використаних на її створення. Застосування методології на практиці за рахунок розробки та впровадження нових рішень забезпечення послуг безпеки дозволяє забезпечити необхідний рівень безпеки інформації в КНОС. Запропоновані механізми послуг безпеки інформації будуються на гібридних криптосистемах на основі крипто-кодових конструкцій зі збитковими кодами*

*Ключові слова: корпоративна науково-освітня система, класифікатор загроз безпеки, система забезпечення інформаційної безпеки*

## 1. Вступ

У сучасних умовах розвиток Інтернет-технологій та обчислювальної техніки призвели до революційних змін в секторі освіти. Об'єднання інформаційних та комп'ютерних мереж університетів сформували єдиний інформаційний та кібернетичний простір, який інтегрував усі складові освітняного процесу надання послуг, сформував корпоративні інформаційно-освітняні системи (КНОС), які істотно розширили спектр освітняних послуг університетів. Як наслідок, суттєво трансформувалися і загрози на інформаційні ресурси КНОС. Загрози набули ознак гібридності. Від суто загроз інформаційної, кібернетичної безпеки та безпеки інформації прояви ознак гібридності почали мати місце унаслідок одночасного впливу на об'єкт захисту – інформаційні ресурси в КНОС, за рахунок виникнення явища синергізму [1, 2]. Суттєвим недостатком Інтернет-технологій є використання відкритих систем, що з самого початку їх розробки не передбачало створення систем захисту інформації. Крім цього поширення освітняних і наукових послуг, використання КНОС для створення наукових досліджень, величезні бази персональних даних створюють умови зростання кіберзагроз в останні десятиліття. Корпоративні інформаційно-освітні системи відносяться до критичних кібернетичних інформаційних систем (ККІС). які будуються на принципах відкритих систем (модель ISO/OSI), тому інформаційну безпеку в КНОС слід розглядати в контексті загальних питань безпеки інформаційних систем з опорою на відповідні законодавчі акти Для об'єктивної оцінки поточного стану інформаційної безпеки ККІС необхідно розглядати сучасні загрози на всі складові безпеки інформації: інформаційну безпеку (ІБ), кібербезпеку (КБ) та безпеку інформації (БІ). [3]. Однак відповідних документів в галузі освіти не існує, що не дозволяє своєчасно корегувати політику безпеки університету. Крім цього, КНОС використовуються в умовах автономії управління університетами, що накладає додаткові завдання на адміністрацію в умовах дії сучасних гібридних загроз.

В умовах автономії ЗВО, як і будь-яка організація, має свою систему управління, що складається з сукупності суб'єктів та об'єктів управління, підсистем та комунікацій між ними, а також процесів, що забезпечують ефективне функціонування організації. Не виключенням є й організаційна автономія ЗВО. Так, об'єктом управління виступають внутрішня організаційна структура ЗВО та управлінські рішення, що стосуються її зміни та приймаються у відповідності до законодавчої бази та статуту ЗВО.

Суб'єктами системи управління організаційною автономією ЗВО є керівні органи та структурні підрозділи ЗВО, що задіяні у процесі формулювання правил функціонування ЗВО і регулювання його організаційної структури. Зокрема, це ректор (керівник) ЗВО та заступники керівника (проректори з науково-педагогічної роботи), Вчена рада ЗВО, Наглядова рада ЗВО, конференція трудового колективу ЗВО та юридичний відділ ЗВО. Для виконня функцій адміністрування, ведення електронного документообігу, якісного надання освітняних послуг КНОС повинна забезпечити безпеку інформаційних

ресурсів (ІР) в умовах зростання можливостей сучасних загроз, відсутності вимог ругуляторів і законодавчів актів, необхідних підрозділів ІБ.

**2. Аналіз літературних даних та постановка проблеми**

Відомо, що методологічний базис будь-якій галузі безпеки являє собою ключові компоненти самої теорії безпеки та ґрунтується на методах і моделях, необхідних і достатніх для дослідження проблеми безпеки та вирішення практичних задач відповідного призначення. Так, нині в галузі інформаційної безпеки існує достатньо велика кількість методологій. Зокрема проведено аналіз методологій, які пов'язані з розробленням наукового базису для синтезу наступних систем безпеки. В роботі [4] для побудови методології безпеки використовуються синтез та аналіз диференціально-ігрових моделей та методів моделювання процесів кібернападу на державні інформаційні ресурс. Однак такій підхід потребує потужних обчислювальних засобів в умовах он-лайн використання. В [5] розроблена оцінка рівня захищеності державних ресурсів від соціотехнічних атак, але авторами не враховуються ознаки синергізма та гібридності сучасних загроз. оцінювання шкоди національній безпеці у сфері охорони державної таємниці [6]. В роботі [7] розглянуті питання побудови та застосування безпечних бездротових сенсорних мереж з випадковими параметрами мережі, але не врахована специфіка критичних кібернетичних інформаційних систем до яких відноситься КНОС. В [8] розглянутий захист державних інформаційних ресурсів, однак автори не враховують загрози на окремі складові безпеки, взаємозв'язок між загрозами та елементами інфраструктури КНОС. Аналіз стану комплексу технічного захисту інформації розглянутий в роботі [9], ризиків дерева ідентифікаторів державних інформаційних ресурсів в роботі [10]. В роботі [11] розглянута методологія побудови систем виявлення аномалій породжених кібератаками. В роботі [12] – методологія систем аналізу та оцінки ризиків втрат інформаційних ресурсів. Комплексний захист людини та соціальних груп від негативного інформаційно-психологічного впливу розглянутий в [13]. Методологія адаптивних систем оцінювання ризиків безпеки ресурсів інформаційних систем розглянута в [14]. Проведений аналіз запропонованих методологій в [8–14] показав, що автори використовують тільки окремі складові безпеки інформаційних ресурсів, як правило інформаційну безпеку, не враховують взаємозв'язок між інформаційними активами, елементами інформаструктури відповідних обчислювальних мереж/систем, можливість комплексування та ознаки гібридності загроз на складові безпеки [15–17]. Тому розглянуті методології потребують кардинального перегляду в частині, що стосується створення методологічного базису для побудови системи забезпечення ІБ інформації в КНОС як України в цілому, так і світу зокрема.

В [18] розглянуті методологічні засади щодо забезпечення безпеки в корпоративних мережах з використанням стандартних системних платформ і операційних систем в умовах підвищення потенційного ризику для безпеки критичної інфраструктури. Однак запропоновані практичні рішення не враховують комплексування сучасних загроз, не тільки між собою, а також з

використанням методів соціальної інженерії. Такий підхід не дозволяє своєчасно реагувати на модифікацію загроз. В роботах [19, 20] розглянуті методології побудови системи безпеки для критичних систем в умовах зростання кіберзагроз на індустриальні системи контролю [19] та критично важливих інфраструктур [20]. Однак автори не враховують гібридність загроз, і розглядають тільки кіберзагрози, що не дозволяє забезпечити корегування деструктивних заходів на протидію сучасним загрозам на ІБ та елементи систем захисту інформації.

В роботі [21] розглянута методологія підготовки вхідного набору даних для подальшого аналізу з використанням методів машинного навчання для компрометації секретного ключа алгоритму ECC на основі ризику витоку інформації по боковому каналу процесора. В роботах [22, 23] розглянуті питання забезпечення безпеки в умовах сучасних кіберзагроз на об'єкти кіберфізичних систем (CPS) та Інтернет речей (IoT) на програмному рівні. Однак використання фізичних каналів витоку інформації дозволяє отримати доступ до ресурсів даних систем. В роботі [24] розглянута методологія оцінки безпеки для аналізу безпеки критично важливих служб, розгорнутих в хмарних середовищах. Методологія пропонує гнучкість в тому сенсі, що оцінки безпеки на основі політик можуть бути визначені на основі вимог користувача, відповідних стандартів, політик і рекомендацій. Однак запропонований підхід не враховує гібридність сучасних загроз, можливість отримання ключових даних систем захисту через витік інформації по боковому каналу процесорів апаратних засобів в хмарних середовищах. В роботі [25] пропонується класифікатор сучасних загроз для кіберфізичних систем на основі побудови дерева атак. Однак запропонований підхід не враховує комплексування загроз для отримання синергетичного ефекту при дії на окремі механізми безпеки.

В роботі [26] проведені дослідження факторів, які впливають на інформованість інформаційної безпеки персоналу, запропоновані інтерпретації кейсів з використанням декількох методів збору даних. Крім цього автори стверджують, що культура та інформованість підвищує рівень безпеки в корпоративної мережі університету. В роботі [27] розглянуті питання відсутності відповідних законодавчих актів та освітніх програм щодо створення системи безпеки в корпоративних мережах ЗВО. В роботі [28] пропонується використання різних видів змагань серед студентів з питань ІБ, що в свою чергу вимагає ретельної підготовки до їх проведення. Однак запропоновані в роботі заходи спрямовані на підвищення рівня інформаційної грамотності суспільства і є доповненням до комплексної системи захисту інформації (КСЗІ). В роботі [29] представлені результати дослідження розробки методу та математичної моделі аутентифікації суб'єктів у електронному інформаційному освітньому середовищі університетів (EIEEU). Однак запропонований метод забезпечує тільки послугу автентичності, і потребує "доповнення" механізмами конфіденційності, доступності та цілісності в умовах сучасних гібридних загроз. В роботі [30] запропонована модель системи управління ІБ автоматизованих систем обробки даних критичного застосування. Модель дозволяє оцінити рівень ризику для ІБ та забезпечує підтримку прийняття

рішень про протидію несанкціонованому доступу до інформації. Однак модель не враховує синергізм загроз на всі складові безпеки: ІБ, КБ, БІ, тому її використання не дозволяє отримати емерджентні властивості при використанні КСЗІ в КНОС.

Виходячи з аналізу [15–32] можна стверджувати, що одним з пріоритетних напрямків підвищення рівня ІБ інформації в КНОС є побудова системи безпеки на основі використання методів і засобів захисту інформації постквантової криптографії від нападу гібридних загроз на складові безпеки: ІБ, КБ, БІ.

В роботі [17] розглянута методологія побудови безпеки в банківському секторі в умовах синергізму сучасних загроз, що дозволяє будувати комплексні систему захисту інформації, які дозволять забезпечити необхідний рівень ІБ. Крім цього, запропонований в [17] підхід э універсальним і може використовуватись з деякими уточненнями для будь-якої критичної кібернетичної системи, тому візьмемо цій підхід за основу.

Таким чином, в умовах гібридизації та комплексування загроз на складові безпеки: ІБ, КБ, БІ нині існує об’єктивне протиріччя між високими вимогами практики до забезпечення певного рівня захисту інформації в КНОС та недосконалістю, а подекуди й відсутністю дієвих науково обґрунтованих методологічних засад її забезпечення.

### 3. Мета і завдання дослідження

Метою дослідження є розроблення відповідної методології побудови системи забезпечення інформаційної безпеки інформації в корпоративних інформаційно-освітніх системах.

Для досягнення мети були поставлені такі завдання:

– провести аналіз системи управління організаційною автономією ЗВО;

– розробити Концепцію побудови синергетичної моделі загроз безпеці інформаційних ресурсів корпоративної науково-освітньої системи;

– сформулювати методологію побудови системи безпеки інформації в корпоративній науково-освітній системі в умовах автономності університету.

### 4. Аналіз системи управління організаційною автономією університетом

Організаційна автономія закладу вищої освіти (ЗВО) є компонентою інституційної автономії та покликана створити передумови для комерціалізації знань, розвитку внутрішніх академічних структур, реалізації стратегічних управлінських рішень шляхом забезпечення незалежного створення та функціонування організаційної структури управління ЗВО, впровадження дієвих механізмів реалізації управлінських технологій.

Сфера організаційної автономії охоплює формування загальних правил функціонування ЗВО та регулювання його організаційної структури, а саме: обрання, призначення та звільнення керівних осіб та інших органів управління внутрішніми структурами ЗВО; визначення терміну перебування на посадах керівників та підписання з ними контрактів; створення та ліквідація внутрішніх структурних підрозділів та відокремлених підрозділів ЗВО.

Структура системи управління інституційною автономією (СОУІА) університету має наступний кортежний вигляд:

$$IA^{унів} = \left\langle AA^{унів}, OA^{унів}, KA^{унів}, ФA^{унів} \right\rangle,$$

де $IA^{унів}$ – інституційна автономія університету; $AA^{унів}$ – академічна автономія; $OA^{унів}$ – організаційна автономія; $KA^{унів}$ – кадрова автономія; $ФA^{унів}$ – фінансова автономія. Структура СОУІА має складноструктурований вид за умови, що охоплює всі організаційні підрозділи університету на різних рівнях управління зі складним характером взаємовідносин між ними. На рис. 1 наведено Узагальнена організаційна структура управління академічною автономією ЗВО.


Рис. 1. Узагальнена організаційна структура управління академічною автономією ЗВО

Проведений аналіз рис. 1 показав, що для забезпечення управління ЗВО в умовах автономії необхідно використовувати КНОС, яка повинна забезпечувати необхідний рівень якості надання послуг QoS в умовах зростання потреб в Інтернет-ресурсах КНОС в цілому та її окремим підрозділам. для забезпечення.

Таким чином в основі системи управління корпоративної мережі ЗВО повинні лежати такі принципи:

– суміщення адміністрування окремих функціональних підсистем (питання ефективності не може вирішуватися поза розгляду питання живучості мережі, а питання безпеки без обліку ефективності та живучості (іншими словами, при зміні рівня безпеки, наприклад, змінюється і ефективність, що має бути враховано);

– централізоване/розподілене адміністрування, припускає, що основні завдання адміністрування повинні вирішуватися з центру (основний фрагмент мережі); вторинні завдання (наприклад, в рамках віддалених фрагментів) засобами управління окремих підсистем на основі веб-застосунків з забезпеченням безпеки відповідних інформаційних ресурсів КНОС;

– в рамках керуючої системи повинні бути реалізовані функції системи автоматичного управління документообігом та автономією ЗВО на основі веб-застосунків та центру сертифікації ключів (ЦСК). З метою підвищення оперативності реакції системи управління на особливо важливі події, в системі повинна реалізуватися автоматична обробка особливо важливих впливів на елементи КНОС;

– в рамках системи безпеки повинна бути реалізована запропонована трьохрівнева модель безпеки на основі Концепції стратегічного управління наданням послуг освіти в ЗВО України, адаптивне управління безпекою з адекватною зміною відповідних подій (наприклад, система виявлення атак може блокувати локальний порт в разі атаки типу “відмова в обслуговуванні”);

– для підвищення ефективності і надійності системи управління необхідно передбачити експертну систему – систему “підказок” для вироблення управляючих впливів на різні події на основі штучного інтелекту та нейронних мереж.

## 5. Розробка концепції побудови синергетичної моделі загроз безпеці інформаційних ресурсів корпоративної науково-освітньої системи

Невід’ємною частиною корпоративної освітньої системи (інформаційно-освітньої системи (ІОС) освітніх установ є соціальні мережі, портали яких містять персональні дані мільйонів користувачів, тим самим, представляючи собою величезні онлайн-директорії, які при бажанні доступні кожному [18, 19]. У сучасному ЗВО зберігається і обробляється величезна кількість різних даних, які пов’язані не тільки із забезпеченням навчального процесу, а й з науково-дослідними та проектно-конструкторськими розробками, персональні дані студентів і співробітників, службова, комерційна та інша конфіденційна інформація [33]. Однак концептуальна стратегія, політики і процедури забезпечення безпеки інформаційних активів, що циркулюють і що

зберігаються в КНОС, відсутні на законодавчому рівні. В роботі [33] запропонована модель процесу надання освітніх послуг, основою якої є процесний підхід, що забезпечує застосування в організації системи процесів разом з їх визначенням та взаємодіями, а також управління ними. Перевагою даного підходу є безперервність управління на стику окремих процесів в рамках системи процесів управління автономією, а також їх комбінації і взаємодії. Разом з тим, в Україні залишається пострадянське бюрократичне державне управління, що є на один з найважливіших чинників широкого поширення корупції. Спираючись на функціонал трирівневої моделі стратегічного набору типового підприємства [17] з метою розроблення концептуальних засад забезпечення безпеки інформаційних ресурсів (ІР) КНОС запропонована концепція побудови синергетичної моделі загроз безпеці ІР КНОС, яка базується на трирівневій стратегії управління безпекою ІР КНОС і умовах організаційного управління автономією ЗВО. *Перший рівень* описує загальну корпоративну стратегію ЗВО та його функціональні стратегії. Корпоративна стратегія визначає перспективи розвитку та сприяє виконанню основної місії ЗВО. На цьому рівні відповідно до синергетичного підходу розглядається загальна концепція безпеки інформаційних технологій КНОС і формуються цілі і завдання забезпечення кібербезпеки (КБ), а також визначається стан безпеки ІР:

$$S^{KRES} = \left\{ S_1^{KRES}, S_2^{KRES}, ..., S_m^{KRES} \right\},$$

де $S_i^{KRES} \in \left\{ S^{KRES} \right\}, (i = \overline{1,m})$ – стан безпеки ІР в КНОС.

Функціональні стратегії одного рівня мають горизонтальні зв'язки і узгоджуються на рівні цілей, з подальшою деталізацією на наступному рівні стратегічного набору.

На *другому рівні* формується корпоративна стратегія безпеки ІР:

$$\left\{ RR^{KRES} \right\} = \left\{ R_{BI} \right\} \cup \left\{ OV_{BI} \right\} \cup \left\{ IU_{BI} \right\},$$

де $\left\{ RR^{KRES} \right\}$ – множина вимог регуляторів, яка включає вимоги до безпеки ІР – $\left\{ R_{BI} \right\}$, що визначені у міжнародних і національних стандартах; множина оцінок ступеня виконання вимог безпеки $\left\{ OV_{BI} \right\}$ та множина попереднього підсумкового рівня відповідності безпеки ІР $\left\{ IU_{BI} \right\}$. Також визначаються цілі та завдання основних бізнес-процесів, пов'язаних із захистом персональних даних. Корпоративна стратегія безпеки описує, яким чином слід керувати і координувати зусилля за різними аспектами безпеки. Стратегія розвивається у формі функціональних стратегій: фінансової економічної, фізичної та інформаційну безпеку (ІБ).

На *третьому рівні* проводиться деталізація функціональних стратегій другого рівня стратегічного набору, формується корпоративна стратегія безпеки

інформації. Серед основних напрямків захисту доцільно виділити кадрову безпеку, фізичну безпеку, мережеву та безпеку інформації (БІ). На цьому рівні визначається відповідність між застосованими технічними засобами захисту інформації (ТЗЗІ) та загрозами ІБ, КБ, БІ на безпеку ІР:

$$OPZ^{KRES} = \sum_{i=1}^{k} OPZ_i,$$

де $OPZ_i$ – узагальнений показник рівня захищеності КНОС, що дозволяє оцінити рівень відповідності ТЗЗІ вимогам регуляторів. Стратегія безпеки ІР є важливою функцією керівництва ЗВО і повинна формуватися його керівництвом на основі методів експертних оцінок.

Для формування послуг безпеки в умовах організаційного управління автономією з урахуванням результату аналізу [33–36] пропонується використовувати запропоновану Концепції забезпечення безпеки в корпоративної науково-освітньої системи університету на основі веб-технологій. Структурна схема Концепції наведена на рис. 2. Основними елементами комплексної системи безпеки для забезпечення послуг автентифікації користувачів КНОС ЗВО та цілісності даних сервер LDAP та Центр сертифікації ключів.

На першому рівні для забезпечення освітніх Концепції побудови синергетичної моделі загроз безпеці ІР КНОС для забезпечення автентичності користувачів, їх авторизації та ідентифікації пропонується використовувати сервер LDAP.

Для забезпечення цілісності та автентичності даних на другому рівні пропонується використовувати Центр сертифікації ключів системи “Шифр-X.509”. Криптографічним ядром системи “Шифр-X.509” є програмний виріб “Шифр+” (бібліотеки криптографічних перетворень), який має дійсний позитивний експертний висновок Державної служби спеціального зв’язку та захисту інформації України. На третьому рівні Концепції побудови синергетичної моделі загроз безпеки інформаційних ресурсів корпоративної науково-освітньої мережі пропонується використовувати програмні застосунки щодо забезпечення антивірусної безпеки, атак на мережевому та транспортному рівнях.

Запропонована концепція ґрунтується на синергетичному підході до вибору найбільш ефективних напрямків досягнення поставлених цілей безпеки ІР з урахуванням величини ризику на кожному рівні моделі управління організаційною автономією ЗВО.

## 6. Формулювання методології побудови системи безпеки інформації в корпоративній науково-освітній системі в умовах автономності університету

На основі синтезу моделей, запропонованих в роботі [17], сформуємо методологічні принципи побудови системи забезпечення ІБ та оцінки поточного стану ІБ КНОС, які наведені на рис. 3. Спираючись на відомий

підхід до побудови методологій [4–14, 18–20, 23, 24] в статті пропонується принципово нова методологія побудови системи забезпечення ІБ ІР КНОС. Методологія містить чотири етапи (рис. 4–7):

1) визначення ймовірності впливу загроз ІБ, КБ, БІ на інформаційну безпеку ІР в КНОС;

2) визначення узагальненого показника рівня ІБ ІР в КНОС;

3) оцінювання ефективності інвестицій в ІР в КНОС;

4) побудова інтегрованих механізмів забезпечення конфіденційності, цілісності, автентичності та вірогідності БІн в А ІР в КНОС.

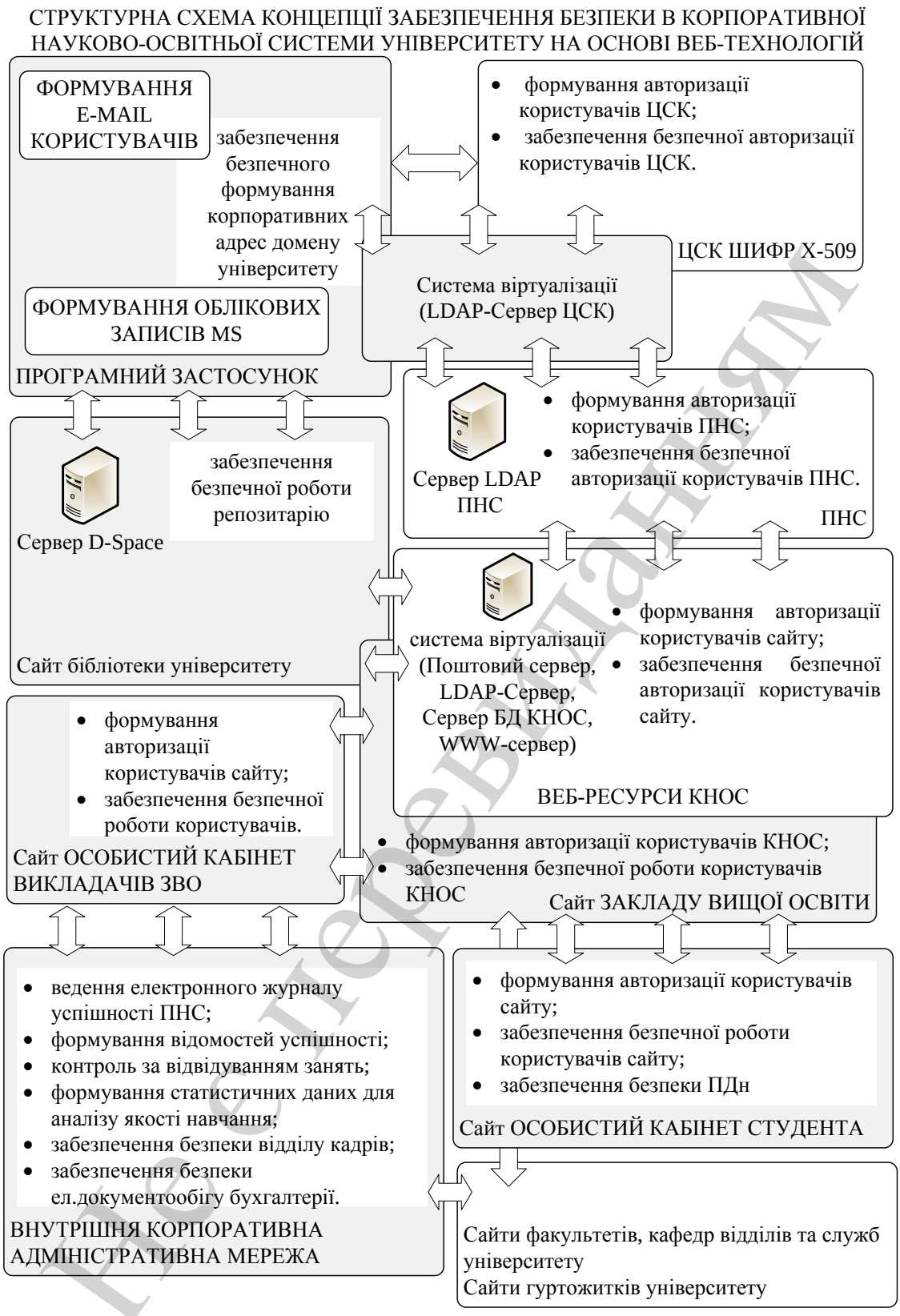


Рис. 2. Структурна схема Концепції забезпечення безпеки в КНОС університету на основі веб-технологій

**Узагальнений класифікатор загроз**

узагальнена синергетична загрози: $W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \bigcup W_{synerg}^{KB} \bigcup W_{synerg}^{BI}$

з урахуванням її гібридності: $W_{synerg}^{\text{hybrid } C,I,A,Au} = W_{synerg}^{C} \bigcap W_{synerg}^{\text{I}} \bigcap W_{synerg}^{A} \bigcap W_{synerg}^{Au}$.

**Удосконалена модель інфраструктури КНОС**

$$G^{KRES} = \{\{O^{KRES}\}, \{L^{KRES}\}, \{I_A\}\},$$

де $O^{KRES}$ – множина об'єктів середовища, що описують елементи КНОС та їх приналежність до рівнів ієрархії КНОС;
$L^{KRES}$ – множина зв'язків між елементами інфраструктури КНОС.

**Сінергітична модель загроз**

$$GR^{KRES} = \left\{\left\{DF^{KRES}\right\}, \left\{T_{risk}\right\}, \left\{T_P\right\}, \left\{T_U\right\}, \left\{VH\right\}\right\},$$

де $DF^{KRES} = \left\{V^{NS}, V^{AS}\right\}$, $T_{risk}$ – якісний показник ризику; $T_p$ – множина визначень ймовірності реалізації хоча б однієї загрози $j$-му активу; $T_U$ – множина визначень величини збитку від реалізації загрози $u_i$; $VH$ – множина деструктивного стану елементів КНОС

**Удосконалена модель зловмисника**

$$G_{IA}^{KRES} = \left\{aid_i, pur_i, T_{IA}, S_{\max_i}, pr_j, MS_i^{KRES}\right\}$$
$$\forall i \in n, \forall j \in m$$

де $aid_i \in \left\{aid\right\}$ – ідентифікатор зловмисника; $pur_i \in \left\{pur_i\right\}$ – мета зловмисника;
$T_{IA}$ – час успішної реалізації загрози;
$S_{\max_i}$ – ймовірний збиток системи;

$MS_i^{KRES} = \left\{ms_i\right\}_{i=1}^{N_{MS^{KRES}}}$ – рекомендації щодо виявлення, реагування ТЗЗІ,
$N_{MS^{KRES}}$ – кількість рекомендацій

**Удосконалена модель оцінки захищеності**

$$G_{OZ}^{KRES} = \left\{\begin{matrix}\left\{I_A\right\}, \left\{O^{KRES}\right\}, \left\{DF^{KRES}\right\}, \left\{RR^{KRES}\right\}, \\ \left\{SZ^{KRES}\right\}, \left\{ROZ^{KRES}\right\}, \left\{UZ_r^{KRES}\right\}\end{matrix}\right\},$$

де $\left\{I_A\right\}$ – множина елементів інформації;
$\left\{O^{KRES}\right\}$ – множина елементів ієрархії КНОС;
$\left\{DF^{KRES}\right\}$ – множина джерел загроз безпеці;
$\left\{RR^{KRES}\right\}$ – множина вимог регуляторів; $\left\{SZ^{KRES}\right\}$ – множина ТЗЗІ;
$\left\{ROZ^{KRES}\right\}$ – дані обліку оцінки захищеності КНОС; $\left\{UZ_r^{KRES}\right\}$ – рівень захищеності КНОС.

**Визначення узагальненого показника рівня захищеності КНОС**

$$OPZ^{KRES} = \sum_{i=1}^{k} OPZ_i \text{ , } UZ^{KRES} = \begin{cases} \text{високий, якщо } OPZ^{KRES} = 3; \\ \text{середній, якщо } 1 \le OPZ^{KRES} \le 3; \\ \text{низький, якщо } OPZ^{KRES} = 0. \end{cases}$$



Рис. 3. Синтез моделей методології побудови системи безпеки в КНОС

Аналіз рис. 3 показав, що синергетичний підхід до оцінки ефективності функціонування комплексних засобів захисту інформації дозволяє комплексування загрози, їх вплив на елементи інфраструктури та лінії зв'язку в КНОС, а також прогнозувати деструктивні заходи з протидії різним типам зловмисників.

*Етап 1. Визначення ймовірності впливу загроз ІБ, КБ, БІ на безпеку ІР на основі класифікатора загроз.*

Крок 1. 1. Формування метричних коефіцієнтів загроз експертами за послугами безпеки

$w^j = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K} w_{ik}^j$, де $w_{ik}^j$ – значення метричного коефіцієнта, виставленого *k*-м експертом для *i*-ї загрози *j*-ї послуги безпеки; *N* – кількість загроз; *K* – кількість експертів

Крок 1. 2. Формування ідентифікаторів загроз за складовими класифікатора

Крок 1. 3. Вибір вагових коефіцієнтів $\alpha_i$, які визначають появу *i* загрози

Крок 1. 4. Визначення реалізації кожної *i*-ї загрози з урахуванням імовірності прояву атаки: $w_i^j P_i^j = \frac{1}{K} P_i^j \sum_{k=1}^{N} w_{ik}^j$.

Крок 1. 5. Визначення реалізації виникнення декількох загроз для обраної послуги: $W_{synerg}^{C} = \sum_{i=1}^{M} w_i^C \alpha_i^C$, $W_{synerg}^{I} = \sum_{i=1}^{M} w_i^I \alpha_i^I$, $W_{synerg}^{A} = \sum_{i=1}^{M} w_i^A \alpha_i^A$, $W_{synerg}^{Au} = \sum_{i=1}^{M} w_i^{Au} \alpha_i^{Au}$

Крок 1. 6. Визначення сумарної загрози за складовими безпеки:

$$W_{synerg}^{IB} = \sum_{i=1}^{N}\left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}\right)\alpha_i,\ W_{synerg}^{KB} = \sum_{i=1}^{N}\left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}\right)\alpha_i,$$

$$W_{synerg}^{BI} = \sum_{i=1}^{N}\left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}\right)\alpha_i$$

Крок 1. 7. Визначення узагальненої синергетичної загрози на ІР:

$$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \cup W_{synerg}^{KB} \cup W_{synerg}^{BI}$$

Крок 1. 8. Визначення узагальненої синергетичної загрози з урахуванням її гібридності:

$$W_{synerg}^{\text{hybrid}\,C,I,A,Au} = W_{synerg}^{C} \cap W_{synerg}^{\text{I}} \cap W_{synerg}^{A} \cap W_{synerg}^{Au}.$$

Рис. 4. Етап 1. Визначення ймовірності впливу загроз ІБ, КБ, БІ на безпеку ІР на основі класифікатора загроз

Одержані за результатами аналізу комплексування загроз дані поступають на 3-й рівень моделі стратегічного управління банком для їх узагальнення при оцінюванні достатності технічних засобів захисту ІР в КНОС.

*Етап 2. Визначення залежностей між елементами інфраструктури КНОС, інформаційними активами, загрозами ІБ, КБ, БІ та ТЗЗІ на основі удосконаленої моделі інфраструктури КНОС, синергетичної моделі загроз, удосконалених класифікатора загроз та моделі зловмисника*

Крок 2. 1. Визначення зв'язку між інформаційними активами ІР $\{I_A\}$ та елементами інфраструктури КНОС: $A^{KRES}=\left\|a_{ij}^{KRES}\right\|$.

Крок 2.2. Визначення зв'язку між інформаційними активами $\{I_A\}$ й об'єктами середовища: $IO^R=\left\|IO_{il}^R\right\|$, де $IO_{il}^R$ – відображає наявність і тип зв'язку між *i*-м інформаційним активом та *l*-м об'єктом середовища КНОС.

Крок 2. 3. Визначення комплексування множини загроз. Для отримання синергетичного ефекту підвищення рівня захищеності ІР необхідно враховувати комплексування загроз: $DF^{KRES}=\{V^{NS}\}\cup\{V^{AS}\}$,
де $\{V^{AS}\}=\{V^{ASBI}\}\cap\{V^{ASIB}\}\cap\{V^{ASKB}\}$.

Крок 2. 4. Визначення ціни повного ризику всіх активів ІР КНОС. Ціна повного ризику дорівнює сумі цін ризику всіх активів:

$$R_{повн}=\sum_{i=1}^{n}R_j$$

Крок 2. 5. Визначення ймовірності реалізації хоча б однієї загрози для кожного активу ІР КНОС: $p_{rj}=1-\prod_{i=1}^{m}\left(1-pr_{ij}\right)$

Крок 2. 6. Визначення зв'язку між джерелами загроз і елементами КНОС: $A^{DF}=\left\|a_{ij}^{DF}\right\|$.

Рис. 5. Етап 2. Визначення залежностей між елементами інфраструктури КНОС, інформаційними активами, загрозами ІБ, КБ, БІ та ТЗЗІ

Кожен механізм захисту ІР в КНОС $SZ_i \in \{SZ^{KRES}\}$ характеризується вектором, де $T_{SZ}$ – тип засоби захисту, $T_V$ – час впровадження, $C_{SZ}$ – вартість. Таким чином, це дозволяє провести дослідження можливості "перекриття" наявними в КСЗІ технічними засобами забезпечити "протистояння" сучасним загрозам.

*Етап 3. Визначення узагальненого показника рівня захищеності ІР в КНОС на основі удосконаленої моделі.*

Крок 3. 1. Визначення зв'язку між загрозами і ТЗЗІ:

$$A^{DFSZ} = \left\| a_{ij}^{DFSZ} \right\|, \text{ при цьому } \forall j \in \{I_A\}, \text{ а } \forall i \in \{DF_i\}.$$

$$\left\| A^{DF} \right\| = \begin{cases} 1, \text{ якщо для } j\text{-го інформаційного актива існують } i \text{ загрози,} \\ 0, \text{ якщо для } j\text{-го інформаційного актива не існують } i \text{ загрози.} \end{cases}$$

Крок 3. 2. Визначення множини вимог регуляторів $\{RR^{KRES}\}$

$$\{RR^{KRES}\} = \{R_{BBI}\} \cup \{OV_{BBI}\} \cup \{IU_{BBI}\}$$

Крок 3.3. Визначення узагальненого показника рівня захищеності КНОС, який дозволяє оцінити рівень відповідності ТЗЗІ вимогам регулятора:

$OPZ^{KRES} = \sum_{i=1}^{k} OPZ_i$, де $k$ – кількість окремих показників безпеки

На підставі отриманих даних системі присвоюється один із трьох рівнів захищеності $UZ^{KRES} = \{\text{низький, середній, високий}\}$ відповідно до правила:

$$UZ^{KRES} = \begin{cases} \text{високий, якщо } OPZ^{KRES} = 3; \\ \text{середній, якщо } 1 \le OPZ^{KRES} \le 3; \\ \text{низький, якщо } OPZ^{KRES} = 0. \end{cases}$$

Рис. 6. Етап 3. Визначення узагальненого показника рівня захищеності ІР в КНОС на основі удосконаленої моделі

Проведений аналіз методів та механізмів безпеки в умовах гібридності та синергизму сучасних загроз [2, 15, 16, 21, 25–36] показав, що для забезпечення основних послуг безпеки (конфіденційності, цілісності, автентичності) використовуються криптографічні алгоритми. Однако в умовах сучасного розвитку обчислювальної техніки доцільно використовувати інтегровані механізми, які дозволяють одним механізмом забезпечувати кілка послуг. До таких механізмів відноситься крипто-кодові конструкції Мак-Елиса та Нідеррайтера. Які дозволяють забезпечити конфіденційність та цілісність інформації на основі несиметричної

криптосистеми, завадостійкість шляхом використання завадостійких кодів, та швидкість криптоперетворень на рівні швидкодії симетричних блокових шифрів.

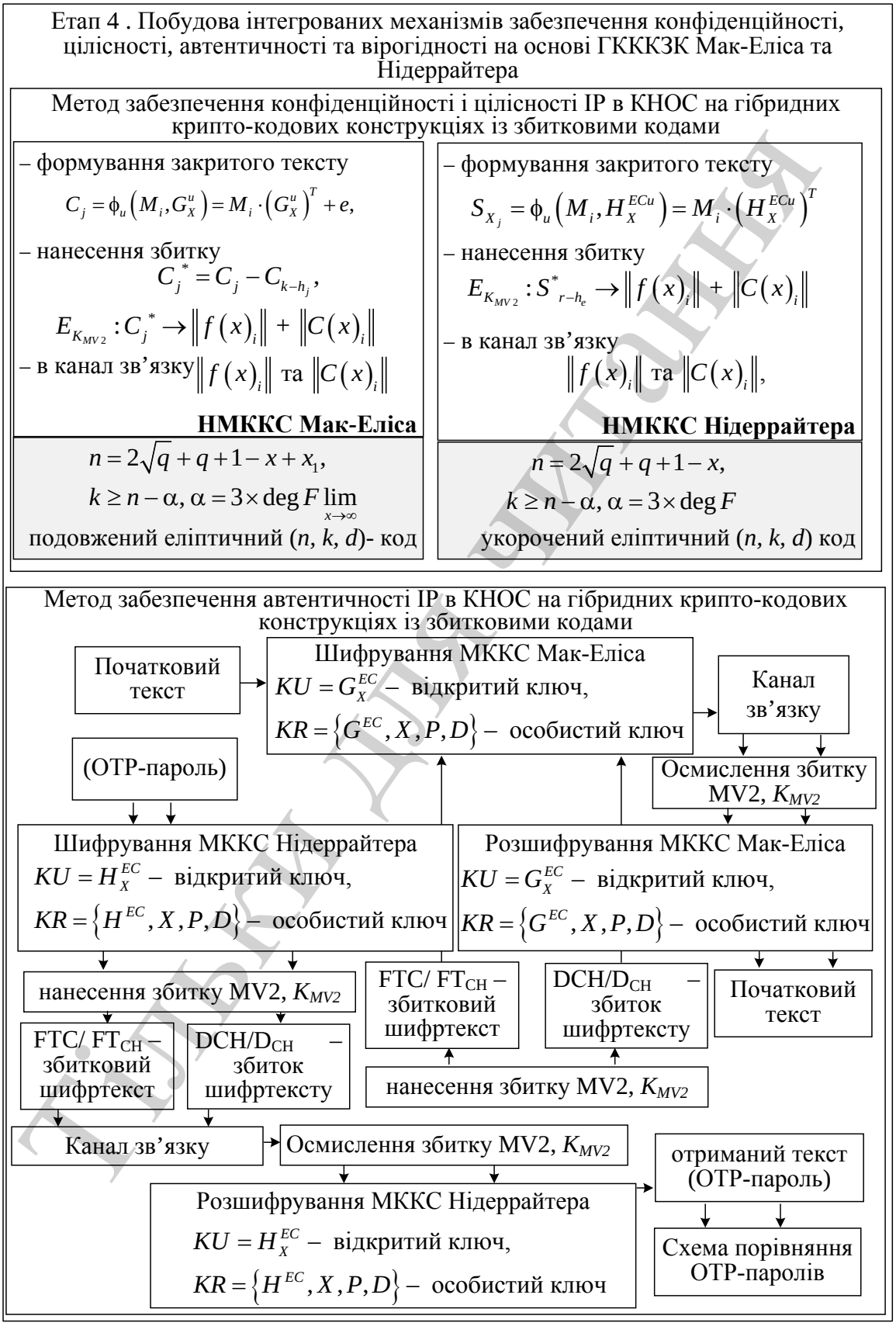


Рис. 7. Етап 4. Побудова інтегрованих механізмів безпеки та вірогідності

На четвертому етапі використовуються гібридні крипто-кодові конструкції на основі збиткових кодах, які розглянуті в роботах [37, 38].

Використання гібридних крипто-кодових конструкцій на збиткових кодах дозволяє збільшувати кількість токенів автентифікатору, використовувати дві несиметричні крипто-кодові системи, два/чотири канали передачі збиткового тексту автентифікатору і збитку. Масштабованість програмного модуля шляхом зміни параметрів МНККС Нідеррайтера і/або Мак-Еліса, в залежності від висунутих вимог до комунікаційних каналах КНОС, забезпечує його програмну реалізацію в мобільних гаджетах і сумісність з протоколами, що використовуються для передачі даних в Інтернет і мобільних мережах.

Такий підхід дозволяє забезпечувати масштабованість елементів інфраструктури КНОС, використовувати нові програмні застосунки щодо покращення надання освітніх послуг в умовах автономії ЗВО.

**7. Проведення експерименту на основі запропонованої методології.**

Для оцінки запропонованих рішень методолгічних засад щодо побудови системи безпеки ІР в КНОС проведемо експеримент.

Вихідними даними є *Type* – тип інформаційного активу, описується множиною базових значень *Type*={*SD, PID, RrD, ST, StO, Ol, YI, PD*}, де *SD* – наукові дані; *PID* – платіжні документи; *KrD* – кредитні документи; *ST* – дослідницька таємниця; *StO* – статистичні звіти; *Ol* – загальнодоступна інформація; *YI* – керівна інформація; *PD* – персональні дані. $A^K$ – конфіденційність; $A^C$ – цілісність; $A^D$ – доступність; $A^A$ – автентичність; $C_Y$ – безперервність – властивості інформації, які необхідно забезпечувати.

На основі запропонованого класифікатору в роботі [17] визначемо можливі загрози на КНОС, які наведені в табл. 1.

Таблиця 1
Перелік загроз на КНОС

| ID загрози | Зміст |
|---|---|
| 04.02.03.01 | Загроза фізичного старіння апаратних компонентів |
| 03.02.04.04 | Загроза відмови підсистеми забезпечення температурного режиму |
| 04.04.04.04 | Загроза несанкціонованого використання системних і мережевих утиліт |
| 02.04.01.03 | Загроза підміни програмного забезпечення |
| 04.02.03.01 | Загроза поширення “поштових хробаків” |
| 04.01.02.02 | Загроза форматування носіїв інформації |
| 04.01.02.02 | Загроза подолання фізичного захисту |
| 03.01.04.05 | Загроза підміни суб’єкта мережевого доступу |
| 03.01.04.05 | Загроза підміни довіреної користувача |
| 03.01.04.01 | Загроза підміни бездротового клієнта або точки доступу |
| 02.02.03.03 | Загроза пошкодження системного реєстру |
| 02.03.02.03 | Загроза перезавантаження апаратних і програмно-апаратних засобів обчислювальної техніки |

| ID загрози | Зміст |
|---|---|
| 02.03.02.05 | Загроза некоректного використання функціоналу програмного забезпечення |
| 03.01.03.02 | Загроза доступу до локальних файлів сервера за допомогою URL |
| 03.02.04.03 | Загроза впливу на програми з високими привілеями |

З урахуванням синергізму та гібридності сучасних загроз в табл. 2 наведені результати оцінки цих властивостей.

Таблиця 2
Результати оцінки синергії та гібридності загроз

| складові безпеки | послуги безпеки | | | | |
|---|---|---|---|---|---|
| | $C$, $W_{synerg}^{C}$ | $I$, $W_{synerg}^{I}$ | $A$, $W_{synerg}^{A}$ | $Au$, $W_{synerg}^{Au}$ | Підсумок |
| $IS$, $W_{synerg}^{IB}$ | 0.011 | 0.064 | 0.018 | 0.106 | 0.0000013 |
| $CS$, $W_{synerg}^{KB}$ | 0.025 | 0.056 | 0.036 | 0.018 | 0.0000009 |
| $SI$, $W_{synerg}^{BI}$ | 0.029 | 0.019 | 0.049 | 0.034 | 0.0000009 |
| Підсумок | 0.065 | 0.139 | 0.103 | 0.158 | |
| $W_{synerg}^{IS,CS,SI} = 0.000003$ | | | $W_{synerg}^{\text{hybrid } C,I,A,Au} = 0.000147$ | | |

Наведені результати свідчать про можливість зламу КНОС в умовах застосування гібридних загроз.

В табл. 3 наведені які послуги повинні забезпечити механізми захисту, а в табл. 4 – наведений взаємозв'язок інформаційних активів з елементами узагальненої інфраструктури КНОС.

Таблиця 3
Послуги безпеки IP КНОС

| Назва, $I_{A_i}$ | $C$ | $I$ | $A$ | $Au$ |
|---|---|---|---|---|
| *SD* | 1 | 1 | 1 | 1 |
| *PID* | 1 | 1 | 1 | 1 |
| *KrD* | 1 | 1 | 1 | 1 |
| *ST* | 1 | 1 | 1 | 1 |
| *StO* | 0 | 1 | 1 | 1 |
| *Ol* | 0 | 1 | 1 | 0 |
| *YI* | 0 | 1 | 1 | 1 |
| *PD* | 1 | 1 | 1 | 1 |

Таблиця 4

Взаємозв'язок інформаційних активів з елементами узагальненої інфраструктури КНОС

| Назва, $I_{A_i}$ | Фізичний рівень | Мережевий рівень | Рівень ОС | Рівень СУБД | Рівень ПЗ |
|---|---|---|---|---|---|
| *SD* | *pt* | *pt* | *so* | *cs* | *so* |
| *PID* | *pt* | *pt* | *so* | *cs* | *so* |
| *KrD* | *pt* | *pt* | *so* | *cs* | *so* |
| *ST* | *pt* | *pt* | *so* | *cs* | *so* |
| *StO* | *pt* | *pt* | *so* | *cs* | *so* |
| *Ol* | *pt* | *pt* | *so* | *cs* | *so* |
| *YI* | *pt* | *pt* | *so* | *cs* | *so* |
| *PD* | *pt* | *pt* | *so* | *cs* | *so* |

*Примітка: 0 – зв'язок відсутній, cs – включає і зберігає, pt – обробляє або передає, so – підтримує функціонування*

Таким, чином забезпечується взаємозв'язок між ІР КНОС, елементами інфраструктури КНОС, лініями зв'язку та послугами безпеки ІР.

В табл. 5, 6 наведені результати досліджень взаємозв'язків загроз та ІР КНОС (табл. 5), та загроз і елементів інфраструктури КНОС (табл. 6). Це дозволяє визначити критичні точки (табл. 6 – ймовірність дорівнює одиниці) в системі захисту, та ймовірність несанкціонованого доступу до відповідного активу ІР КНОС.

Таблиця 5

Визначення ймовірності реалізації хоча б однієї загрози для кожного активу ІР

| ID загрози | SD | PID | KrD | ST | StO | Ol | YI | PD |
|---|---|---|---|---|---|---|---|---|
| 04.02.03.01 | 0.268 | 0.268 | 0.268 | 0.268 | 0.241 | 0.222 | 0.241 | 0.268 |
| 03.02.04.04 | 0.267 | 0.267 | 0.267 | 0.267 | 0.179 | 0.091 | 0.179 | 0.267 |
| 04.04.04.04 | 0.068 | 0.068 | 0.068 | 0.068 | 0.063 | 0.029 | 0.063 | 0.068 |
| 02.04.01.03 | 0.2 | 0.2 | 0.2 | 0.2 | 0.182 | 0.132 | 0.182 | 0.2 |
| 04.02.03.01 | 0.268 | 0.268 | 0.268 | 0.268 | 0.241 | 0.222 | 0.41 | 0.268 |
| 04.01.02.02 | 0.067 | 0.067 | 0.067 | 0.067 | 0.05 | 0.044 | 0.05 | 0.067 |
| 04.01.02.02 | 0.067 | 0.067 | 0.067 | 0.067 | 0.05 | 0.044 | 0.05 | 0.067 |
| 03.01.04.05 | 0.088 | 0.088 | 0.088 | 0.088 | 0.088 | 0 | 0.088 | 0.088 |
| 03.01.04.05 | 0.088 | 0.088 | 0.088 | 0.088 | 0.088 | 0 | 0.088 | 0.088 |
| 03.01.04.01 | 0.088 | 0.088 | 0.088 | 0.088 | 0.088 | 0 | 0.088 | 0.088 |
| 02.02.03.03 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 | 0.1 |
| 02.03.02.03 | 0.2 | 0.2 | 0.2 | 0.2 | 0.166 | 0.1 | 0.166 | 0.2 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 02.03.02.05 | 0.333 | 0.333 | 0.333 | 0.333 | 0.226 | 0.143 | 0.226 | 0.333 |
| 03.01.03.02 | 0.267 | 0.267 | 0.267 | 0.267 | 0.267 | 0 | 0.267 | 0.267 |
| 03.02.04.03 | 0.133 | 0.133 | 0.133 | 0.133 | 0.1 | 0.056 | 0.1 | 0.133 |

Таблиця 6
Визначення зв’язку між джерелами загроз і елементами АБС

| ID загрози | Фізичний рівень | Мережевий рівень | Рівень ОС | Рівень СУБД | Рівень ПЗ |
|---|---|---|---|---|---|
| 04.02.03.01 | 0.44968 | 0.44968 | 0.34748 | 1 | 0.34748 |
| 03.02.04.04 | 0.39248 | 0.39248 | 0.30328 | 0.892 | 0.30328 |
| 04.04.04.04 | 0.1089 | 0.1089 | 0.08415 | 0.2475 | 0.08415 |
| 02.04.01.03 | 0.32912 | 0.32912 | 0.25432 | 0.748 | 0.25432 |
| 04.02.03.01 | 0.44968 | 0.44968 | 0.34748 | 1 | 0.34748 |
| 04.01.02.02 | 0.231 | 0.231 | 0.1785 | 0.525 | 0.1785 |
| 04.01.02.02 | 0.231 | 0.231 | 0.1785 | 0.525 | 0.1785 |
| 03.01.04.05 | 0.06776 | 0.06776 | 0.05236 | 0.154 | 0.05236 |
| 03.01.04.05 | 0.13552 | 0.13552 | 0.10472 | 0.308 | 0.10472 |
| 03.01.04.01 | 0.13552 | 0.13552 | 0.10472 | 0.308 | 0.10472 |
| 02.02.03.03 | 0.176 | 0.176 | 0.136 | 0.4 | 0.136 |
| 02.03.02.03 | 0.31504 | 0.31504 | 0.24344 | 0.716 | 0.24344 |
| 02.03.02.05 | 0.4972 | 0.4972 | 0.3842 | 1 | 0.3842 |
| 03.01.03.02 | 0.41118 | 0.41118 | 0.31773 | 0.9345 | 0.31773 |
| 03.02.04.03 | 0.20262 | 0.20262 | 0.15657 | 0.4605 | 0.15657 |

В табл. 7 наведений результат дослідження можливості систем захисту інформації протистояти загрозам

Таблиця 7
Зв’язок між загрозами і ТЗЗІ

| ID загрози | Фізичний рівень | Мережевий рівень | Рівень ОС | Рівень СУБД | Рівень ПЗ |
|---|---|---|---|---|---|
| 04.02.03.01 | MZ | MZ | MZ | MZ | MZ |
| 03.02.04.04 | MZ | MZ | MZ | MZ | MZ |
| 04.04.04.04 | MZ | MZ | MZ | MZ | MZ |
| 02.04.01.03 | MZ | MZ | MZ | MZ | MZ |
| 04.02.03.01 | MZ | MZ | MZ | MZ | MZ |

| | | | | | |
|---|---|---|---|---|---|
| 04.01.02.02 | MZ | MZ | MZ | MZ | MZ |
| 04.01.02.02 | MZ | MZ | MZ | MZ | MZ |
| 03.01.04.05 | MZ | MZ | MZ | MZ | MZ |
| 03.01.04.05 | MZ | MZ | MZ | MZ | MZ |
| 03.01.04.01 | MZ | MZ | MZ | MZ | MZ |
| 02.02.03.03 | MZ | MZ | MZ | MZ | MZ |
| 02.03.02.03 | MZ | MZ | MZ | MZ | MZ |
| 02.03.02.05 | MZ | MZ | MZ | MZ | MZ |
| 03.01.03.02 | MZ | MZ | MZ | MZ | MZ |
| 03.02.04.03 | MZ | MZ | MZ | MZ | MZ |

У моделі використані такі типи зв'язку: MZ – є механізм захисту, що забезпечує протидію її деструктивному впливу; NMZ – немає механізму захисту для забезпечення протидії і-ї загрози.

На основі проведених досліджень та оцінки виконання вимог регуляторів, визначимо узагальнений показник рівня захищеності ІР в КНОС, який дозволяє оцінити рівень відповідності ТЗЗІ вимогам регуляторів та визначається:

$$OPZ^{ABS} = \sum_{i=1}^{k} OPZ_i,$$

де $k$ – кількість окремих показників безпеки, $OPZ_i$ –окремий показник, що набуває значення з множини: $OPZ_1$ – відсутність неприпустимих ризиків, у разі якщо в ЗВО при складанні моделі загроз/моделі зловмисника і оцінки ризиків виявлені неприпустимі за своїм рівнем ризики, то $OPZ_1$=0, в іншому випадку – $OPZ_1$=1; $OPZ_2$ – відсутність небезпечних загроз, незакритих механізмами ТЗЗІ, $OPZ_2$=0, в разі, якщо в ЗВО при складанні моделі виявлені "незакриті" загрози – $OPZ_2$=1; $OPZ_3$ – рівень відповідності безпеки ІР вимогам регуляторів визнаний рекомендованим – $OPZ_3$=1, в разі, якщо визнано нерекомендованим – $OPZ_3$=0.

Для забезпечення якості інвестування в систему ІБ пропонується використовувати удосконалений метод на основі результатів узагальненого показника рівня захищеності $OPZ^{KRES}$, узагальненої синергетичної загрози $W_{synerg}^{IS,CS,SI}$, множини активів $\{I_A\}$ – множина елементів інформаційних активів КНОС. Запропонована модель оцінки інвестицій в [3] визначається станом моделі ефективності інвестицій в ІБ ІР КНОС за наступними кроками:

*Крок 1.* Оцінювання рівня прибутковості інвестицій в ІБ:

$$ROI^{KRES} = NPV_{inv}^{KRES} - NPV_{zt}^{KRES},$$

де $NPV_{inv}^{KRES}$ – прибуток від інвестицій в ТЗЗІ (СЗІ) КНОС; $NPV_{zt}^{KRES}$ – витрати в ТЗЗІ (СЗІ) КНОС; $ROI^{KRES}$ – прибутковість інвестицій в ТЗЗІ (СЗІ) КНОС.

*Крок 2*. Оцінювання рентабельності інвестицій в ТЗСЗІ:

$$ROSI^{KRES} = NPV_{zbtszi}^{KRES} - NPV_{zvtszi}^{KRES},$$

де $NPV_{zbtszi}^{KRES}$ – витрати на усунення компрометації безпеки без впроваджених ТЗЗІ (СЗІ); $NPV_{zvtszi}^{KRES}$ – витрати на усунення компрометації безпеки з впровадженими ТЗЗІ (СЗІ).

*Крок 3*. Оцінювання чистої приведеної вартості:

$$NPV_{zbtszi}^{ABS} = \sum_{i=1}^{N} \frac{ALE_i}{(1+r)^i}, \; NPV_{zvtszi}^{ABS} = C_{sz} + \sum_{i=1}^{N} \frac{ALE_i}{(1+r)^i},$$

де $N$ – кількість інтервалів інвестування, $ALE_i$ – очікувані затрати в $i$-му періоді, $r$ – ставка дисконтування, $C_{sz}$ – вартість засобів захисту.

*Крок 4*. Оцінювання ризику ІР за методикою розрахунку *Annual loss expectancy – ALE*, тобто очікуваних втрат в кожен період оцінки –

$$ALE^{KRES} = \sum_{i=1}^{n} I\left(O_{DF}^{ABS}\right)F_i,$$

де $\left\{O_{DF}^{KRES}\right\}$ – множина загроз; $I\left(O_{DF}^{KRES}\right)$ – вартісні наслідки реалізації загрози; $ALE^{KRES}$ – очікуваний збиток від реалізації; $F_i$– частота (можливість) реалізації загрози.

*Крок 5*. Оцінювання потенційних збитків $U^{KRES}$ інформаційного активу – $U^{KRES}=p_{rj}u_j$, де $p_{rj}$ – ймовірність реалізації хоча б однієї загрози $j$-му активу; $u_j$ – цінність $j$-го активу.

*Крок 6*. Оцінювання загального очікуваного збитку:

$$OU^{KRES} = \sum_{j=1}^{n} U^{KRES}.$$

Узагальнивши параметри, які використовуються в рамках запропонованої моделі, визначимо інтегральний критерій ефективності інвестицій в безпеку ІР КНОС, використовуючи вираз: $W_{KRES}^{effinv} = \sum_{i=1}^{N} w_i M^{KRES}$.

Таким чином, модель ефективності інвестицій в безпеку ІР КНОС може знаходиться в різних станах $S^{KRES}$, які можна описати у вигляді такої множини:

$$S^{KRES} = \left\{ S_1^{KRES}, S_2^{KRES}, ..., S_m^{KRES} \right\},$$

де $S^{KRES}$ – множина можливих станів моделі; $S_1^{KRES}$ – початковий стан моделі; $S_m^{KRES}$ – кінцевий стан моделі.

При розрахунках припустимо, що на забезпечення ІБ в ЗВО університетом витрачається до 4 % від річного бюджету, витрати на розробку ТЗЗІ складають до 2 % від річного бюджету, ймовірні витрати на усунення компрометації безпеки без застосування до 5 % від річного бюджету, ймовірні витрати на усунення компрометації безпеки, що становить до 2 % від річного прибутку, Csz – вартість засобів захисту становить 30 % від загальної вартості IP. Ставка дисконтування становить 13 %. Результати загального показника ефективності наведені у табл. 8.

Таблиця 8

Результати загального очікуваного збитку, наслідків виведення з ладу ТЗЗІ, тис. у. о.

| Назва, $I_{A_i}$ | $W_{KRES}^{effinv}$ за складовими послуг безпеки | | | | Всього |
|---|---|---|---|---|---|
| | *C* | *I* | *A* | *Au* | |
| *SD* | 0,0391 | 0,0294 | 0,0196 | 0,0098 | 0,09792 |
| *PID* | 0,0098 | 0,0073 | 0,0049 | 0,0024 | 0,02448 |
| *KrD* | 0,0588 | 0,0441 | 0,0294 | 0,0147 | 0,14688 |
| *ST* | 0,0392 | 0,0294 | 0,0196 | 0,0098 | 0,09792 |
| *StO* | 0,0059 | 0,00441 | 0,0029 | 0,0015 | 0,01469 |
| *Ol* | 0,0039 | 0,0029 | 0,0020 | 0,0010 | 0,00979 |
| *YI* | 0,0196 | 0,0147 | 0,0098 | 0,0049 | 0,04896 |
| *PD* | 0,0196 | 0,01467 | 0,0098 | 0,0049 | 0,04896 |
| $W_{KRES_{заг} I_{A_i}}^{effinv}$ | 0,1958 | 0,14688 | 0,09792 | 0,04896 | |
| $W_{KRES_{заг}}^{effinv} = W_{KRES_{заг\ I_{A_i}}}^{effinv\ \ C} \bigcap W_{KRES_{заг\ I_{A_i}}}^{effinv\ \ I} \bigcap W_{KRES_{заг\ I_{A_i}}}^{effinv\ \ A} \bigcap W_{KRES_{заг\ I_{A_i}}}^{effinv\ \ Au} = 0{,}0001379$ | | | | | |

**8. Обговорення результатів використання запропонованої методології**

Запропонована концепція побудови синергетичної моделі загроз безпеки інформаційних ресурсів КНОС, базис якої становить трирівнева модель стратегічного управління безпекою інформаційних технологій КНОС. Концепція охоплює всі основні напрямки розвитку діяльності ЗВО щодо безпеки інформаційних ресурсів, ґрунтується на синергетичному підході до вибору найбільш ефективних напрямків досягнення цілей безпеки інформаційних ресурсів на кожному з рівнів моделі управління в умовах автономії закладу вищої освіти.

Запропонований класифікатор загроз безпеці інформаційних ресурсів, на відміну від існуючих, ґрунтується на синергетичній моделі загроз, що дозволяє класифікувати загрози за складовими безпеки, видами послуг та рівнями ієрархії

інфраструктури КНОС, оцінювати синергію та гібридність загроз інформаційній безпеці, кібербезпеці, безпеці інформації, ймовірність їх впливу на безпеку інформаційних ресурсів. Запропонований класифікатор є універсальним і може використовуватись при оцінці загроз будь якої ККІС. Практична реалізація класифікатора дозволить в он-лайн режимі формувати експертну оцінку рівня загроз інформаційних ресурсів, аналізувати їх синергію та гібридність, оцінювати ймовірність впливу загроз інформаційній безпеці, кібербезпеці, безпеці інформації на безпеку інформаційних ресурсів без значних витрат інвестицій та людських ресурсів.

Запропонований метод оцінювання узагальненого показника рівня захищеності інформаційних ресурсів КНОС та практична методика для оцінювання рівня захищеності інформаційних ресурсів КНОС основі синергетичної моделі загроз, удосконалених класифікатора загроз та моделі зловмисника, моделі оцінки захищеності інформаційних ресурсів та моделі інфраструктури КНОС дозволяє оптимізувати витрати коштів на побудову системи безпеки інформаційних ресурсів ЗВО. Практична значимість полягає у можливості своєчасного оцінювання взаємозв'язків між активами інформаційних ресурсів, елементами інфраструктури, технічними засобами захисту в КНОС і можливими проявами загроз інформаційній безпеці, кібербезпеці та безпеці інформації. Це дозволяє своєчасно корегувати керівні документи ЗВО з інформаційної безпеки, планувати інвестування в технічні засоби захисту інформації, формувати превентивні заходи для недопущення реалізації загроз.

Запропонований метод забезпечення конфіденційності та цілісності інформаційних ресурсів на гібридних крипто-кодових конструкціях зі збитковими кодами. Метод базується на модифікованій крипто-кодовій системі Мак-Еліса на модифікованих алгеброгеометричних кодах, що інтегровано (одним механізмом) забезпечить безпеку інформаційних ресурсів (безпечний час – $T_{\text{Б}}$>200 р., стійкість до криптоаналізу $P_{\text{К}}<10^{25}–10^{35}$ групових операцій), достовірність передачі інформаційних ресурсів в КНОС ($P_{\text{пом}}<10^{-9}$) та зменшення енергетичних витрат на їх практичну реалізацію в 10–12 разів (шифрування, розшифрування) за рахунок зменшення порядку $GF(q)$.

Для експериментального дослідження запропонованих МНККС на *MEC*, ГКККЗК були реалізовані відповідні програмні макети. Результати порівняльних досліджень НККС Мак-Еліса, МНККС Мак-Еліса на *MEC*, ГКККЗК наведені в табл. 9, 10. У табл. 9, 10 були використані умовні скорочення (префікси): *ukh*/*udh* – гібридні КККЗК з укороченими *MEC*/гібридні КККЗК з подовженими *MEC*; *uk* – МНККС з укороченими *MEC*; *ud* – МНККС з подовженими *MEC*. При розрахунках параметрів криптосистем були використані поля Галуа: для НККС Мак-Еліса – $GF(2^{10})$; для МНККС з укороченими/подовженими *MEC* – $GF(2^6)$; для гібридних КККЗК – $GF(2^4)$.

*Складність процесу декодування для НТКС на ЕС задається виразами*:

– для НТКС на *EC*: $O_{K+}=N_{покр}\times n\times r$,

де $N_{покр}\geq\dfrac{C_n^{\rho\cdot t}}{C_{n-k}^{\rho\cdot t}}=\dfrac{n(n-1)...(n-\rho\cdot t-1)}{(n-k)(n-k-1)...(n-k-\rho\cdot t-1)}$, $t=\lfloor(d-1)/2\rfloor$,

– для МНККС на укорочених кодах: $O_{K+} = N_{покр} \times \left(2\sqrt{q} + q + 1 - 1/2k\right) \times r$;

– для МНККС на подовжених кодах: $O_{K+} = N_{покр} \times \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right) \times r$.

*Складність процесу декодування для ГККК3К на укорочених МЕС має вигляд*:
– для ГККК3К на укорочених *МЕС:*

$$O_{K+} = N_{покр} \times \left(2\sqrt{q} + q + 1 - 1/2k\right) \times r + N_F \text{ або } \left(N_K\right), \qquad \text{де} \qquad N_F \approx \frac{K_C^{\,z}}{2^{1-K_C{}^{z+1}}} \times |F|;$$

$K_C$=97/128; $|F|$ – сумарна довжина вихідних прапорів (збитків) (бітів) – при відомому зловмисникові залишку (збитковому тексті) і заданих прапорах (збитках), при невідомому ключі: $N_K \approx 2^{1190 \times z}$; $z$ = 16;

– для ГККК3К на подовжених *МЕС*: $O_{K+} = N_{покр} \times \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right) \times r + N_F$ або $\left(N_K\right)$.

Таблиця 9

Результати аналізу складності злому і складності кодування для різних швидкостей *EC* (*MEC*)

| $lg(l_s)$ | Відносна швидкість кодування, *R* | | | | | |
|---|---|---|---|---|---|---|
| | 0.5 | 0.75 | 0.5(*ud*) | 0.75(*ud*) | 0.5(*uk*) | 0.75(*uk*) |
| 1 | 4.75 | 12.1 | 15.6 | 18.23 | 19.12 | 19.82 |
| 2 | 10.52 | 21.76 | 32.47 | 35.67 | 38.63 | 39.18 |
| 3 | 18.22 | 33.17 | 43.75 | 51.61 | 56.88 | 58.03 |
| 4 | 21.42 | 51.75 | 59.43 | 72.81 | 78.92 | 80.52 |
| 5 | 38.77 | 61.09 | 68.26 | 87.32 | 94.91 | 104.56 |
| 6 | 54.13 | 78.37 | **101.72** | **112.46** | **120.83** | **128.79** |
| 7 | 82.14 | 83.72 | 156.75 | 164.72 | 182.39 | 189.74 |
| 8 | 165.84 | 179.13 | 223.64 | 231.57 | 276.27 | 287.33 |
| 9 | 358.33 | 371.09 | 421.97 | 428.63 | 459.81 | 476.52 |
| 10 | **672.37** | **684.94** | 716.41 | 722.26 | 783.46 | 794.28 |

Таблиця 10

Результати аналізу складності злому і складності кодування для різних швидкостей *MEC*(*MEC*+*DC*)

| $\lg(l_s)$ | Відносна швидкість кодування, *R* | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 0.5(*ud*) | 0.75(*ud*) | 0.5(*uk*) | 0.75(*uk*) | 0.5(*udh*) | 0.75(*udh*) | 0.5(*ukh*) | 0.75(*ukh*) |
| 1 | 15.6 | 18.23 | 19.12 | 19.82 | 7.21 | 9.17 | 12.54 | 14.56 |
| 2 | 32.47 | 35.67 | 38.63 | 39.18 | 21.46 | 23.72 | 27.48 | 29.82 |
| 3 | 43.75 | 51.61 | 56.88 | 58.03 | 31.68 | 33.83 | 37.38 | 38.43 |
| 4 | 59.43 | 72.81 | 78.92 | 80.52 | **41.72** | **42.27** | **47.48** | **58.23** |
| 5 | 68.26 | 87.32 | 94.91 | 104.56 | 56.63 | 58.91 | 62.86 | 66.53 |
| 6 | **101.72** | **112.46** | **120.83** | **128.79** | 72.32 | 74.79 | 89.5 | 97.71 |

Аналіз табл. 9, 10 підтверджує, що використання збиткових кодів і подальше зменшення потужності поля Галуа призводить до значного зменшення складності формування (≈ в 12 разів) і розкодування криптограми (≈ в 20 разів).

У табл. 11, 12 наведені результати досліджень залежності ємнісної характеристики від потужності поля Галуа для програмної реалізації.

Таблиця 11
Залежність швидкості програмної реалізації від потужності поля (кількість групових операцій)

| Криптосистеми | $GF(q^m)$ | | | | | |
|---|---|---|---|---|---|---|
| | $2^5$ | $2^6$ | $2^7$ | $2^8$ | $2^9$ | $2^{10}$ |
| НККС *MacElis* на *EC* | 10018042 | 18048068 | 32847145 | 47489784 | 63215578 | **82467897** |
| МНККС *MacElis* на укорочених *MEC* | 10007947 | **17787431** | 28595014 | 44079433 | 61974253 | 79554764 |
| МНККС *MacElis* на подовжених *MEC* | 11156138 | **18561228** | 33210708 | 48297112 | 65171690 | 84051337 |

Таблиця 12
Залежність швидкості програмної реалізації від потужності поля (кількість групових операцій)

| Криптосистеми | $GF(q^m)$ | | | | | | |
|---|---|---|---|---|---|---|---|
| | $2^4$ | $2^5$ | $2^6$ | $2^7$ | $2^8$ | $2^9$ | $2^{10}$ |
| МНККС *MacElis* на укорочених *MEC* | 8293075 | 10007947 | **17787431** | 28595014 | 44079433 | 61974253 | 79554764 |
| МНККС *MacElis* на подовжених *MEC* | 8506422 | 11156138 | **18561228** | 33210708 | 48297112 | 65171690 | 84051337 |
| ГККК3К подовжених *MEC* | **5612316** | 7900315 | 14892945 | 25565274 | 42279183 | 58963778 | 76564173 |
| ГККК3К укорочених *MEC* | **5942627** | 7905257 | 14682411 | 25595014 | 42116327 | 58468143 | 75474764 |

Впровадження запропонованого методу дозволяє підвищити рівень захищеності інформаційних ресурсів та забезпечити своєчасне реагування на вимоги міжнародних і національних регуляторів безпеки інформаційних ресурсів за рахунок зміни окремих параметрів та модифікації застосування модифікованих крипто-кодових систем Мак-Еліса і Нідеррайтера з системами багатоканальної криптографії на збиткових кодах.

Запропонований метод двофакторної автентифікації на гібридних крипто-кодових конструкціях зі збитковими кодами на основі модифікованих крипто-кодових систем Мак-Еліса і Нідеррайтера з *MEC* дозволяє забезпечити рівень стійкості *OTP*-паролів при передачі відкритими каналами зв'язку та зберегти можливість подальшого використання протоколу двофакторної автентифікації на основі *SMS*-повідомлень. Незважаючи на зменшення потужності поля Галуа до $GF(2^6)$ для модифікованих крипто-кодових систем і $GF(2^4)$ для гібридних крипто-кодових конструкцій на збиткових кодах, статистичні характеристики таких крипто-кодових конструкцій виявилися, як мінімум, не гірше традиційних схем Мак-Еліса над $GF(2^{10})$.

У табл. 13 наведені результати досліджень статистичних властивостей запропонованих методів на основі пакета *NIST STS* 822.

Таблиця 13
Результати дослідження статистичної безпеки

| Криптосистеми | Кількість тестів, в яких тестування пройшли більше 99 % послідовностей | Кількість тестів, в яких тестування пройшли більше 96 % послідовностей | Кількість тестів, в яких тестування пройшли менше 96 % послідовностей |
|---|---|---|---|
| НККС *MacElis* | 149 (78,83 %) | 189 (100 %) | 0 (0 %) |
| МНККС *MacElis* на укорочених *MEC* | 151 (79,89 %) | 189 (100 %) | 0 (0 %) |
| МНККС *MacElis* на подовжених *MEC* | 152 (80,42 %) | 189 (100 %) | 0 (0 %) |
| ГККК3К на подовжених *MEC* | **153 (80,95 %)** | 189 (100 %) | 0 (0 %) |
| ГККК3К на укорочених *MEC* | **155 (82 %)** | 189 (100 %) | 0 (0 %) |

Табл. 13 продемонструвала, що незважаючи на зменшення потужності поля Галуа до $GF(2^6)$ для МНККС і $GF(2^4)$ для ГККК3К, статистичні характеристики таких крипто-кодових конструкцій виявилися, як мінімум, не гірше традиційних НККС Мак-Еліса на $GF(2^{10})$. Всі криптосистеми пройшли 100 % тестів, причому найкращий результат показала ГККК3К на укорочених *MEC*: 155 з 189 тестів пройдено на рівні 0,99, що становить 82 % від усієї кількості тестів. При цьому традиційна НККС Мак-Еліса на $GF(2^{10})$ показала 149 тестів на рівні 0,99. Таким, чином запропоновані методи забезпечують основні послуги безпеки, необхідний рівень стійкості та достовірності БІР.

Запропонований метод оцінювання безпеки інформаційних ресурсів, що на, відміну від відомих, враховує комплексний показник ефективності інвестицій, які виділяються на забезпечення безпеки інформаційних ресурсів, дозволяє оптимізувати витрати коштів на її побудову в умовах впливу гібридних загроз при одночасному забезпеченні заданого рівня їх безпеки. Практична реалізація методу дозволяє комплексно оцінювати основні показники інвестування в забезпечення

безпеки інформаційних ресурсів з урахуванням синергетичного оцінювання загроз інформаційній безпеці, кібербезпеці та безпеці інформації.

Перспективним напрямком досліджень э практичне впровадження запропонованих рішень в КНОС ЗВО.

**9. Висновки**

1. Аналіз організації автономії свідчить, що для виконання функцій інституційної автономії необхідно використовувати сучасну корпоративну мережу, яка повинна забезпечити необхідний рівень якості обслуговування. Така система відноситься до критичних кібернетичних інформаційних систем. На елементи інфраструктури КНОС діють сучасні гібридні загрози з ознаками синергізму, що потребує відповідних деструктивних заходів протидії. Разом з тим, на сьогоднішній час не має відповідних законодавчих актів, які сприяли побудові комплексної системи захисту інформаційних ресурсів КНОС. Тому виникає потреба формулювання методології побудови системи безпеки інформації в корпоративній науково-освітній системі в умовах автономності університету.

2. Запропонована концепція побудови синергетичної моделі загроз безпеки інформаційних ресурсів КНОС, базис якої становить трирівнева модель стратегічного управління безпекою інформаційних технологій. Розроблена на основі концепції модель за рахунок комплексування складових інформаційної безпеки, кібербезпеки та безпеки інформації відкриває новий напрямок у забезпеченні безпеки інформаційних ресурсів. Запропонований підхід на основі моделі управління інституційною автономією з урахуванням величини ризику на кожному рівні та дієвого контролю за виконанням функцій системи управління інформаційною безпекою закладів вищої освіти дозволяє забезпечити певний рівень безпеки ІР КНОС.

3. Запропонована методологія побудови системи безпеки інформації в КНОС на відміну від відомих підходів реалізовує принципово нову концепцію протидії гібридним загрозам сектору освіти. Її сутність та зміст полягають в раціональній організації системи забезпечення ІБ ІР в КНОС в умовах одночасної дії на систему загроз інформаційній безпеці, кібербезпеці та безпеці інформації. Такий підхід дозволяє одержувати повноцінну та адекватну оцінку рівня ІБ ІР в КНОС, що суттєво впливає на величину інвестицій в безпеку сектору освіти в умовах автономії та відкриває шляхи до прийняття обґрунтованих управлінських рішень з питань забезпечення безпеки.

Методологія ґрунтується на запропонованій трирівневої моделі стратегічного управління безпекою інформаційних технологій в ЗВО. На основі розробленої методології набув подальшого розвитку класифікатор загроз інформаційній безпеці в частині, що стосується одночасного урахування в ньому крім загроз інформаційній безпеці загроз кібербезпеці та загроз безпеці інформації ІР в КНОС. Впровадження класифікатора дозволило зробити висновок про те, що для протидії гібридним загрозам ІР в КНОС доцільно застосовувати інтегровані механізми забезпечення послуг на основі ГКККЗК.

**Литература**


1. Андрощук Г. О. Кібербезпека: тенденції в світі та Україні // Кібербезпека та інтелектуальна власність: проблеми правового забезпечення: матеріали Міжнародної науково-практичної конференції. К.: Вид-во “Політехніка”, 2017. С. 30–36.
2. Грищук Р. В., Даник Ю. Г. Основы кибербезопасности: монография / ред. Ю. Г. Даник. Житомир: ЖНАЕУ, 2016. 636 с.
3. Assessment of functional efficiency of a corporate scientific-educational network based on the comprehensive indicators of quality of service / Yevseiev S., Ponomarenko V., Ponomarenko V., Rayevnyeva O., Rayevnyeva O. // Eastern-European Journal of Enterprise Technologies. 2017. Vol. 6, Issue 2 (90). P. 4–15. doi: https://doi.org/10.15587/1729-4061.2017.118329
4. Грищук Р. В., Корченко О. Г. Методологія синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу на державні інформаційні ресурси // Науково-практичний журнал “Захист інформації”. 2012. Т. 14, № 3. С. 115–122. doi: https://doi.org/10.18372/2410-7840.14.3418
5. Баранов Г., Захарова М., Горніцька Д. Методологія синтезу систем оцінки рівня захищеності державних інформаційних ресурсів від соціотехнічних атак // Науково-практичний журнал “Захист інформації”. 2012. Т. 14, № 3. С. 98–104. doi: https://doi.org/10.18372/2410-7840.14.3396
6. Методологія синтезу та програмна реалізація системи оцінювання шкоди національній безпеці у сфері охорони державної таємниці / Корченко О., Луцький М., Захарова М., Дрейс Ю. // Науково-практичний журнал “Захист інформації”. 2013. Т. 15, № 1. С. 14–20. doi: https://doi.org/10.18372/2410-7840.15.4210
7. Rajba S., Karpinski M., Korchenko O. Generalized models, construction methodology and the application of secure wireless sensor networks with random network parameters // Ukrainian Scientific Journal of Information Security. 2014. Vol. 20, Issue 2. P. 120–125. doi: https://doi.org/10.18372/2225-5036.20.7296
8. Юдін О., Бучик С. Методологія захисту державних інформаційних ресурсів. Порівняльний аналіз основних термінів та визначень // Науково-практичний журнал “Захист інформації”. 2015. Т. 17, № 3. С. 218–225. doi: https://doi.org/10.18372/2410-7840.17.9518
9. Журиленко Б. Методология построения и анализа состояния комплекса технической защиты информации с вероятностной надежностью и учетом временных попыток взлома // Науково-практичний журнал “Захист інформації”. 2015. Т. 17, № 3. С. 196–204. doi: https://doi.org/10.18372/2410-7840.17.9515
10. Бучик С. Методологія аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів // Науково-практичний журнал “Захист інформації”. 2016. Т. 18, № 1. С. 81–89. doi: https://doi.org/10.18372/2410-7840.18.10116
11. Корченко А., Щербина В., Вишневская Н. Методология построения систем выявления аномлий порожденных кибератаками // Науково-практичний журнал “Захист інформації”. 2016. Т. 18, № 1. С. 30–38. doi: https://doi.org/10.18372/2410-7840.18.10110

12. Иванченко Е., Казмирчук С., Гололобов А. Методология синтеза систем анализа и оценки рисков потерь информационных ресурсов // Науково-практичний журнал “Захист інформації”. 2012. Т. 14, № 2. С. 5–9. doi: https://doi.org/10.18372/2410-7840.14.2178

13. Шиян А. Методологія комплексного захисту людини та соціальних груп від негативного інформаційно-психологічного впливу // Науковий журнал «Безпека інформації». 2016. Т. 22, № 1. С. 94–98. doi: https://doi.org/10.18372/2225-5036.22.10460

14. Корченко А., Казмирчук С., Иванченко Е. Методология синтеза адаптивных систем оценивания рисков безопасности ресурсов информационных систем // Науково-практичний журнал “Захист інформації”. 2017. Т. 19, № 3. С. 198–204. doi: https://doi.org/10.18372/2410-7840.19.11898

15. Бояров Е. Н. Ключевые проблемы информационной безопасности сферы образования // Педагогика высшей школы. 2016. № 3.1. С. 42–45. URL: https://moluch.ru/th/3/archive/43/1500/

16. Дорожкин А. В., Ясенев В. Н., Ясенев О. В. Методологические аспекты обеспечения информационной безопасности в ВУЗе // Инновационные методы обучения в высшей школе. 2016. С. 77–83.

17. Hryshchuk R., Yevseiev S. Shmatko A. Construction methodology of information security system of banking information in automated banking systems: monograph. Vienna: Premier Publishing s. r. o., 2018. 284 p. doi: https://doi.org/10.29013/r.hryshchuk_s.yevseiev_a.shmatko.cmissbiabs.284.2018

18. Ansari M. T. J., Pandey D., Alenezi M. STORE: Security Threat Oriented Requirements Engineering Methodology // Journal of King Saud University - Computer and Information Sciences. 2018. doi: https://doi.org/10.1016/j.jksuci.2018.12.005

19. Timpson D., Moradian E. A Methodology to Enhance Industrial Control System Security // Procedia Computer Science. 2018. Vol. 126. P. 2117–2126. doi: https://doi.org/10.1016/j.procs.2018.07.240

20. A Bayesian network methodology for optimal security management of critical infrastructures / Misuri A., Khakzad N., Reniers G., Cozzani V. // Reliability Engineering & System Safety. 2018. doi: https://doi.org/10.1016/j.ress.2018.03.028

21. Machine-Learning-Based Side-Channel Evaluation of Elliptic-Curve Cryptographic FPGA Processor / Mukhtar N., Mehrabi M., Kong Y., Anjum A. // Applied Sciences. 2018. Vol. 9, Issue 1. P. 64. doi: https://doi.org/10.3390/app9010064

22. Rehman S., Gruhn V. An Effective Security Requirements Engineering Framework for Cyber-Physical Systems // Technologies. 2018. Vol. 6, Issue 3. P. 65. doi: https://doi.org/10.3390/technologies6030065

23. Bodei C., Chessa S., Galletta L. Measuring security in IoT communications // Theoretical Computer Science. 2019. Vol. 764. P. 100–124. doi: https://doi.org/10.1016/j.tcs.2018.12.002

24. Hudic A., Smith P., Weippl E. R. Security assurance assessment methodology for hybrid clouds // Computers & Security. 2017. Vol. 70. P. 723–743. doi: https://doi.org/10.1016/j.cose.2017.03.009

25. Alguliyev R., Imamverdiyev Y., Sukhostat L. Cyber-physical systems and their security issues // Computers in Industry. 2018. Vol. 100. P. 212–223. doi: https://doi.org/10.1016/j.compind.2018.04.017

26. Rezgui Y., Marks A. Information security awareness in higher education: An exploratory study // Computers & Security. 2008. Vol. 27, Issue 7-8. P. 241–253. doi: https://doi.org/10.1016/j.cose.2008.07.008

27. Schneider F. B. Cybersecurity Education in Universities // IEEE Security & Privacy. 2013. Vol. 11, Issue 4. P. 3–4. doi: https://doi.org/10.1109/msp.2013.84

28. Conklin A. Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course // Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06). 2006. doi: https://doi.org/10.1109/hicss.2006.110

29. Method and Model of Analysis of Possible Threats in User Authentication in Electronic Information Educational Environment of the University / Lakhno V. A., Kasatkin D. Y., Blozva A. I., Gusev B. S. // Advances in Computer Science for Engineering and Education II. 2020. P. 600–609. doi: https://doi.org/10.1007/978-3-030-16621-2_56

30. Models and Algorithms of Vector Optimization in Selecting Security Measures for Higher Education Institution's Information Learning Environment / Akhmetov B., Lakhno V., Akhmetov B., Myakuhin Y., Adranova A., Kydyralina L. // Intelligent Systems in Cybernetics and Automation Control Theory. 2019. P. 135–142. doi: https://doi.org/10.1007/978-3-030-00184-1_13

31. Колгатин А. Г. Информационная безопасность в системах открытого образования // Образовательные технологии и общество. 2014. С. 417–425.

32. Аникин И. В., Емалетдинова Л. Ю., Кирпичников А. П. Методы оценки и управления рисками информационной безопасности в корпоративных информационных сетях // Вестник Казанского технологического университета. 2015. Т. 18, № 6. С. 195–197.

33. Литвинов В. А., Лыпко Е. В., Яковлева А. А. Информационная безопасность высшего учебного заведения в рамках современной глобализации. URL: http://conference.osu.ru/assets/files/conf_reports/conf13/132.doc

34. Вахонин С. Удаленный доступ и утечка данных // Информационная безопасность. 2014. № 5. URL: http://www.itsec.ru/articles2/Inf_security/udalennyy-dostup-i-utechka-dannyh/

35. Замараева О. А., Титов В. А., Кузин Д. О. Разработка политики информационной безопасности для экономического вуза: определение информации, подлежащей защите, и построение модели злоумышленника // Современные проблемы науки и образования. 2014. № 3. URL: https://www.science-education.ru/ru/article/view?id=13106

36. Степанова И. В., Мохаммед Омар А. А. Использование перспективных технологий для развития распределенных корпоративных сетей связи // T-Comm: Телекоммуникации и транспорт. 2017. Т. 11, № 6. С. 10–15.

37. Practical implementation of the Niederreiter modified crypto-code system on truncated elliptic codes / Yevseiev S., Tsyhanenko O., Ivanchenko S., Aleksiyev V.,

Verheles D., Volkov S. et. al. // Eastern-European Journal of Enterprise Technologies. 2018. Vol. 6, Issue 4 (96). P. 24–31. doi: https://doi.org/10.15587/1729-4061.2018.150903

38. Евсеев С. П. Использование ущербных кодов в крипто-кодовых системах // Системи обробки інформації. 2017. № 5 (151). С. 109–121. doi: https://doi.org/10.30748/soi.2017.151.15