DOI: https://doi.org/10.33216/1998-7927-2025-291-5-18-28

УДК 004.03: 004.67

КОНЦЕПТУАЛЬНА МОДЕЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НАВЧАЛЬНИХ КОМП'ЮТЕРНИХ ЛАБОРАТОРІЙ

Могильний Г.А., Донченко В.Ю., Швець І.М., Донченко С.М., Кузнецов В.С.

CONCEPTUAL MODEL OF INFORMATION SECURITY OF EDUCATIONAL COMPUTER LABORATORIES

Mohylnyi H.A., Donchenko V.U., Shvets I.M., Donchenko S.M., Kuznetsov V.S.

В умовах військового стану та швидкого розвитку ІКТ ефективна протидія кібератакам як елементу гібридної війни потребує спільних зусиль державних установ, об'єктів критичної інфраструктури, промислових підприємств та навчальних закладів. За таких обставин важливим стає перегляд основ інформаційної безпеки. Стаття присвячено дослідженню та класифікації моделей інформаційної безпеки, що застосовуються для побудови ефективних систем захисту інформації. У роботі розглядаються три основні типи моделей: концептуальна модель, математична модель та функціональна модель

Концептуальна модель – слугує базисом для формулювання загальних процесів створення системи безпеки, визначає ключові напрямки та структуру захисту інформації.

Окрім аналізу моделей, робота висвітлює особливості впровадження систем захисту інформації в навчальних установах. Серед основних проблем встановлено: відсутність спеціалізованих відділів та відповідальних осіб за інформаційну безпеку; недостатній рівень підготовки навчально-допоміжного персоналу; велика різниця у кваліфікації користувачів; складність забезпечення безпеки при відкритості навчального процесу та зростаючих вимогах до впровадження дистанційних освітніх технологій.

Особливості побудови системи безпеки в навчальних закладах є необхідність пошуку компромісного рішення між відкритістю навчального процесу та студентоцентрованим навчанням; забезпеченням комфортних умов доступу до всіх матеріалів навчального процесу та жорсткими положеннями до витоку конфіденційної та службової інформації

В роботі пропонується один із варіантів розробки концептуальної моделі безпеки як основи для подальшого впровадження ефективних заходів захисту, враховуючи специфіку роботи навчальних закладів та їх інформаційного середовища. Створення цієї моделі є важливим першим кроком для побудови системи безпеки. На основі проведеного аналізу пропонується переглянути основні підходи до захищеності інформації в навчальних закладах, особливо з урахуванням специфіки дистанційного навчання та відкритості освітніх процесів.

Ключові слова: *навчальна комп'ютерна лабораторія, заклад освіти, кібербезпека, загрози, модель, система захисту.*

Вступ. У сучасних умовах стрімкого розвитку інформаційно-комунікаційних технологій та систем віддаленого використання інформаційних ресурсів, ефективна протидія кібератакам, що стала важливою складовою гібридної війни, вимагає консолідації та об'єднання зусиль державних органів, об'єктів критичної інфраструктури та організацій з підготовки та перепідготовки фахівців, які активно застосовують корпоративні системи та засоби віддаленого доступу до інформації. В таких обставинах перегляд ключових принципів інформаційної безпеки набуває особливої ваги в діяльності підприємств та навчальних закладів. Важливим питанням побудови системи безпеки є розгляд та створення різних моделей інформаційної безпеки, які можуть застосовуватися під час побудови системи інформаційної безпеки.

Аналіз останніх досліджень і публікацій. Аналіз наукових джерел з питань кібербезпеки закладів вищої освіти засвідчує, що

дослідження ведуться у таких проблемних напрямах:

– проблеми забезпечення кібербезпеки в закладах вищої освіти (Ю. С. Антонов, П. В. Римар та О. Г. Антонова [2]; О. О. Ільїн, С. О. Сєрих та В. В. Вишнівський [6]; В. Ю. Кива [7]; Н. М. Кириленко [8]; О. Ю. Чубукова та І. В. Пономаренко [17]; A. Ghazvini, Z. Shukur та Z. Hood [31]; S. Hina та P. D. Dominic [32]; C. Joshi та U. K. Singh [35]);

– теоретичне обґрунтування системи управління кібербезпекою ЗВО (О. О. Ільїн [5]; А. Ю. Нашинець-Наумова, В. Л. Бурячок, Н. В. Коршун, О. Б. Жильцов, П. М. Складанний та Л. В. Кузьменко [16]; I. S. Bianchi та R. D. Sousa [25]; Y. Zeng, H. Zhang, X. Liu, Y. Fu, Q. Deng та R. Ye [34]);

– оцінювання кібербезпеки ЗВО (M. H. Suwito, S. Matsumoto, J. Kawamoto, D. Gollmann та K. Sakurai [24]; W. Yustanti, A. Qoiriah, R. Bisma та A. Prihanto [23]; Н. П. Кухарська [10]);

– проблеми кібербезпеки учасників освітньо-наукової діяльності ЗВО (В. Ю. Биков, О. Ю. Буров та Н. П. Дементієвська [3]; M. Gratian, S. Bandi, M. Cukier, J. Dykstra та A. Ginther [27]; Z. Yan, T. Robertson, R. Yan, S. Y. Park, S. Bordoff, Q. Chen та E. Sprissler [30]; W. D. Kearney та H. A. Kruger [36]; G Ogutcu, O. M. Testik та O. Chouseinoglou [39]; M. Rajab [40]);

– проблеми побудови моделей інформаційної безпеки ресурсів загалом та в закладах вищої освіти (О. Є. Ананченко [1]; А. Ю. Нашинець-Наумова, В. Л. Бурячок, Н. В. Коршун, О. Б. Жильцов, П. М. Складанний, Л. В. Кузьменко [4]; Ю. В. Кожедуб, С. В. Василенко, А. В. Максимець, В. А. Гирда [9]; О. Г. Трапезон, Т. Ф. Гумен, К. О. Трапезон, В. А. Граб, Н. С. Золотарева [14]; Я. І. Шестак, В. І. Чубаєвський [18]; О. К. Юдін, С. С. Бучик [19-20]; А. І. Ясінська [21]; J. Chang, Y. Jeon, S. Sim [26]; C. K. Wong, S. B. Maynard, A. Ahmad, and H. Naseer [33]; Y. Lee [37]).

В роботах [11-13] розглядаються особливості роботи навчальних комп'ютерних лабораторій та створення корпоративного середовища у навчальних закладах, однак практично не розглядаються питання безпеки створеного інформаційного середовища.

У результаті аналізу [22, 28, 29, 38] сучасних підходів до управління кібербезпекою та розробки інтелектуальних систем підтримки рішень встановлено, що ефективне забезпечення інформаційної безпеки в умовах зростаючих кіберзагроз потребує комплексного, адаптивного та інтелектуалізованого підходу. Морфологічні моделі дозволяють формувати раціональні стратегії захисту, враховуючи множину можливих варіантів реалізації. Особливу увагу приділено розвитку самоосвітніх систем виявлення аномалій, які здатні адаптуватися до змін у поведінці зловмисників, зокрема до варіацій інтенсивності, швидкості та тривалості атак. У свою чергу, інтелектуальні системи підтримки рішень, орієнтовані на фінансове планування та інвестування в цифрову трансформацію кібербезпеки, сприяють прийняттю обґрунтованих управлінських рішень з урахуванням специфіки предметної області. Окрему цінність становлять методи багатокритеріальної оптимізації витрат на інформаційну безпеку, зокрема з використанням генетичних алгоритмів. Таким чином, поєднання інтелектуальних технологій, адаптивних моделей та оптимізаційних підходів створює підґрунтя для побудови ефективних, гнучких і стійких систем кіберзахисту.

Існує кілька моделей, кожна з яких дозволяє відповісти на поставлені перед нею питання. Можна виділити три основні моделі інформаційної безпеки, це:

- концептуальна модель,
- математична модель,
- функціональна модель.

Концептуальна модель дозволяє сформулювати найбільш загальні процеси створення системи безпеки вона створюється на першому етапі моделювання. Ця модель інформаційної безпеки відповідає на загальні питання і схематично відбиває загальну структуру моделі інформаційної безпеки, на ній як на стрижні будуються інші моделі і концепції інформаційної безпеки.

Мета даної роботи – на засадах комплексного аналізу системи інформаційної безпеки у навчальних закладах виявити особливості її впровадження та розробити загальні основні складові концептуальної моделі безпеки, що дозволяє запровадити першочергові заходи спрямовані на підвищення інформаційної безпеки.

Математична модель – це формалізований опис сценаріїв у вигляді логічних алгоритмів представлених послідовністю дій порушників і заходів у відповідь. Розрахункові кількісні значення параметрів моделі характеризують функціональні залежності, що описують процеси взаємодії порушників із системою

захисту та можливі результати дій. Саме такий вид моделі найчастіше використовується для кількісних оцінок уразливості об'єкта, побудови алгоритму захисту оцінки ризиків та ефективності вжитих заходів.

При побудові даних моделей необхідно спиратися на такі найважливіші обставини:

- вибір критеріїв для оцінки важливості (пріоритетності) інформаційних ресурсів;
- створення кількісних показників різноманітних видів вразливостей об’єктів;
- вибір критеріїв оцінки запропонованих напрямків, методів та засобів захисту;
- створення кількісних показників різноманітних підсистем захисту;
- вибір критеріїв оптимальності системи захисту інформації для даної архітектури інформаційної системи;
- чітке математичне формулювання завдання побудови моделі засобів захисту інформації, що враховує задані вимоги до системи захисту та дозволяє побудувати засоби захисту інформації відповідно до цих критеріїв.

Безумовно з математичною моделлю напряму пов'язана функціональна модель.

У подальшому, в межах функціональної моделі, розробляються і досліджуються алгоритми щодо практичного застосування і доказовості наведених припущень. Ця модель визначає потоки інформації, дозволені в системі, та правила керування доступом до інформації.

Існує декілька основних типів функціональних моделей:

1. Модель дискреційного доступу (DAC) – контролюється доступ суб'єктів (користувачів або додатків) до об'єктів, що становлять різні інформаційні ресурси: файли, додатки, пристрої виведення тощо. Класичний варіант – закрита система, тобто спочатку об'єкт не доступний нікому, і в списку прав доступу описується набір дозволів.

2. Модель безпеки Белла-ЛаПадули – є одна з найвідоміших моделей безпеки (модель мандатного управління доступом). У ній визначено безліч понять, пов'язаних із контролем доступу. Даються визначення суб'єкта, об'єкта та операції доступу, а також математичний апарат для їх опису.

3. Рольова модель контролю доступу (RBAC) – контролює доступ користувачів до інформації на основі типів їх дій у системі. Під роллю розуміється сукупність дій та обов'язків, пов'язаних із певним видом діяльності. При цьому з кожним об'єктом зіставлено набір дозволених операцій доступу кожної ролі, а не певного користувача. Кожному користувачеві зіставлені ролі (у деяких –декілька ролей), які може виконувати.

4. Системи розмежування доступу (СРД) – це сукупність реалізованих правил розмежування доступу у засобах обчислювальної техніки чи автоматизованих системах, більшість з яких базуються на концепції диспетчера доступу – абстрактної машини (захищений, відокремлений процес), яка виступає посередником при всіх зверненнях суб'єктів до об'єктів. Диспетчер доступу використовує базу даних захисту, в якій зберігаються правила розмежування доступу і на підставі цієї інформації дозволяє або не дозволяє суб'єкту доступ до об'єкта, а також фіксує інформацію про спробу доступу в окремому журналі. Ця база будується з урахуванням матриці доступу чи однієї з її перетворень. Таким чином матриця доступу – це таблиця, в якій рядки відповідають суб'єктам, стовпці – об'єктам доступу, а на перетині рядка та стовпця містяться правила (дозвіл) доступу суб'єкта до об'єкта.]

Основними недоліками такої матриці є надмірно велика розмірність і складність адміністрування і для подолання цих складнощів матриця доступу в СРД часто замінюється деякими її перетвореннями:

- Списки керування доступом (access control lists, ACL). Для кожного об'єкта задано список суб'єктів, які мають ненульові повноваження доступу до них (із зазначенням цих повноважень).
- Списки повноважень суб'єктів. Аналогічно ACL , але для кожного суб'єкта заданий список об'єктів, доступ яких дозволено із зазначенням повноважень доступу. Таке уявлення називається профілем суб'єкта.
- Атрибутні схеми. Засновані на присвоєнні суб'єктам та/або об'єктам певних міток, що містять значення атрибутів. Елементи матриці доступу не зберігаються у явному вигляді, а динамічно обчислюються при кожній спробі доступу конкретної пари суб'єкт-об'єкт на основі їх атрибутів.

Першим важливим кроком перед створенням та запровадженням певної магматичної та функціональної моделі є проведення загального аналізу системи безпеки та створення концептуальної моделі. Основним

особливостям створення цієї моделі для навчальних установ і присвячена дана робота.

Виклад основного матеріалу дослідження. Важливим питанням у створенні інформаційної систем навчального закладу є аналіз системи безпеки та створення різних моделей інформаційної безпеки, які можуть застосовуватися під час розробки та впровадження різноманітних програмно-технічних та організаційних заходів щодо забезпечення збереження інформації. Безумовно питання стабільності роботи обладнання, організації захищеного середовища даних та програмних розробок мають цілу низьку особливостей у навчальних підрозділах та навчальних комп'ютерних лабораторіях (НКЛ). Ці питання межують між вимогами:

- відкритість навчального процесу та студентоцентроване навчання;
- забезпечити комфортні умови доступу до всіх матеріалів навчального процесу
- жорсткими положеннями до витоку конфіденційної та службової інформації.

Попередній аналіз діяльності навчальних установ свідчить, що важною особливістю впровадження системи захисту є відсутність окремих відділів по захисту інформації .

В більшості випадків завдання по забезпеченню кібербезпеки покладено навчально допоміжний персонал. Крім того, слід враховувати дуже складну ситуацію у закладах середньої освіти де всіма питаннями по налаштуванню роботи обчислювальної техніки, забезпеченню захисту інформації та організацію інформаційного освітнього середовища у більшості випадків покладено на викладачів інформатики. У системі вищої школи та закладах середньої освіти не передбачено окремі посади, які відповідають за питання кіберзлочинності.

Значною особливістю вишів є велика різниця та великий розкид у кваліфікації викладачів та студентів різноманітних спеціальностей. Навчальний процес більшості спеціальностей та освітніх програм містить освітні компоненти спрямовані на використання обчислювальної техніки та програмного забезпечення якоїсь певної (дуже різноманітної) галузі знань. Обладнання у НКЛ використовують студенти різноманітним спеціальностей як з великим обсягом комп'ютерних дисциплін, так спеціальностей у яких знання засобів обчислювальної техніки та методів програмування не включено до основних професійних компетентностей.

В результаті такого становища, процеси створення моделей захисту, впровадження певних заходів по їх удосконаленню, аналізу спроб несанкціонованого використання інформаційних ресурсів практично не виконуються або підтримуються на дуже слабкому рівні.

Таким чином, особливостями впровадження системи захисту інформації у навчальних установах та окремих НКЛ є:

- Відсутність відділів та осіб відповідальних за систему інформаційної безпеки;
- Недостатній рівень підготовки навчально-допоміжного персоналу в напрямку інформаційної безпеки;
- Значна різниця у кваліфікації користувачів: здобувачів освіти та викладачів;
- Відсутність системи моніторингу питань інформаційної безпеки;
- Недостатнє фінансування;
- Необхідність підтримки дистанційної освіти та організації віддаленого доступу до інформації;
- Швидкий перехід на інформаційно-комунікаційні технології;
- Необхідність підтримки «відкритості» навчального процесу, всіх його складових та впровадження нових засобів розповсюдження інформації;
- Необхідність створення умов для використання різноманітних обчислювальних пристроїв (особистих комп'ютерів, мобільних пристроїв, планшетів та інше) викладачів та здобувачів освіти;
- Використання спеціалізованого програмного забезпечення для налаштування, моніторингу, обслуговування різноманітних обчислювальних приладів у навчальному процесі;
- Відсутність необхідного матеріально-технічного забезпечення в умовах швидкого впровадження рішень спрямованих на впровадження дистанційної освіти.

Для побудови концептуальної моделі інформаційної безпеки незалежно від того, наскільки проста чи складна інформаційна система, необхідно як мінімум відповісти на три питання:

- що захищати;
- від кого захищати;
- як захищати.

Рис. 1. Загальна концептуальна модель інформаційної безпеки

Це обов'язковий мінімум, якого може бути достатньо для невеликих інформаційних систем. Однак, беручи до уваги можливі наслідки, то краще виконати побудову повної концептуальної моделі інформаційної безпеки, в якій необхідно визначити (Рис. 1):

- джерела інформації,
- пріоритет чи ступінь важливості інформації,
- джерела загроз,
- цілі загроз,
- загрози,
- способи доступу,
- напрями захисту,
- засоби захисту,
- методи захисту.

При побудові моделі слід враховувати особливості діяльності навчального закладу або окремого структурного підрозділу. В межах цієї роботи розглянемо концептуальну модель за умови, що інші структурні підрозділи навчального закладу знаходяться у відокремленому, окремому та захищеному інформаційному середовищі. Тому до моделі включено тільки інформацію, яка може бути розташована або використана у НКЛ.

З врахуванням особливостей діяльності НКЛ та особливостей сучасного стану системи захисту інформації у навчальних закладах при побудові концептуальної моделі системи захисту інформації необхідно врахувати та планувати наступні дії:

1. Провести попередній моніторинг існуючої (або відсутньої) системи захисту інформації. За необхідністю, створити тимчасову комісію з питань інформаційної безпеки.

2. Призначити відповідальних осіб за систему захисту інформації.

3. Провести попередній аналіз доцільності впровадження системи з віддаленим доступом до НКЛ в умовах наявності/відсутності системи захисту інформації.

4. Відокремити першочергові заходи.

5. Провести попередній аналіз необхідних коштів для впровадження систем з віддаленим доступом та забезпечення певних мінімальних вимог до захисту інформації.

Безумовна концептуальна модель інформаційної безпеки НКЛ (рис.2) включає основні положення загальної моделі. В процесі її розробки необхідно проаналізувати та провести уточнення основних положень.

Джерела інформації НКЛ це:

- Навчально-методичні матеріали, які використовуються у навчальному процесі. Особливу увагу необхідно надати їх цілісності та створити умови для цілодобового використання. Слід зауважити, що матеріали комп'ютерних дисциплін можуть мати спеціальну навчально-технічну інформацію.
- Кабельна мережа, мережа Wi-Fi, її структура та адресування, імена користувачів та паролі. Дуже велике значення можуть мати «відкриті» імена користувачів та паролі, які використовуються у навчальних цілях.
- Співробітники, викладачі та студенти, які мають можливість випадково (або навмисно) повідомляти о наявних інформаційних ресурсах та шляхах їх використання.
- Серверні, локальні та особисті накопичувачі. Слід враховувати, що особисті накопичувачі слабо контролюються та можуть бути джерелами вірусів або використовуватись для несанкціонованого доступу до інформації.

• Спеціалізоване програмне забезпечення, яке використовується у навчальному процесі. Особливу увагу слід приділити ПЗ, яке орієнтовано на налаштування, моніторинг та обслуговування обчислювальної техніки і використовується у навчальному процесі комп'ютерних спеціальностей.

• Мобільні пристрої та ноутбуки викладачів та студентів – це пристрої які можуть бути використані для створення різноманітних атак на інформаційну систему.

• Особисті документи викладачів, які зберігаються на інформаційних ресурсах

Пріоритетність інформаціє НКЛ має значні особливості в залежності від спрямованості самої НКЛ та її структури. Попередній аналіз показав необхідність врахування інформації яка може створити умови для порушення системи безпеки, наприклад:

• Структура та адресування мережі, розташування серверних машин та мережевих приладів – це одна з найважливіших складових, використання якої може надати зловмиснику вагомі переваги у створенні загрози. Слід враховувати, що більшість НКЛ розповсюджує цю інформації в процесі виконання певних лабораторних робот.

• Пріоритетні користувачі, їх імена, паролі та права доступу.

• Навчально-методичні матеріали можуть бути використані з метою особистої вигоди, впливу на оцінювання.

• Спеціалізоване програмне забезпечення може бути використано для організації атаки. Особливу загрози створюють спеціалізовані програми спрямовані на вивчення та моніторинг комп'ютерного та мережевого обладнання.

• Загальне програмне забезпечення може бути непрацездатним та перешкодити проведенню навчальних занять.

• Особисті документи викладачів – ця інформація найменшого пріоритету для НКЛ.

Джерела загроз у НКЛ мають незначні особливості

• Інтернет – загроза, вплив якої значно зростає зі створенням системи віддаленого доступу і дає вплив на НКЛ постійно. Крім того, ця загроза надає можливість впливати на діяльність НКЛ багатьом користувачам, які підключені до Інтернет.

• Внутрішня мережа, яка в багатьох випадках «відкрита» для використання викладачами, гостями та здобувачами освіти та створює умови для проведення різноманітних кібератак .

• Прилади студентів та викладачів, які використовуються в межах «відкритого навчального середовища»

• Спеціалізовані прилади та ПЗ навчального процесу, яке може бути використано для несанкціонованого доступу.

• Інші відвідувачі, які відвідують навчальний заклад.

Цілі загроз у НКЛ в цілому співпадають з багатьма іншими підрозділами: ознайомлення, дублювання, модифікація, знищення, порушення працездатності. Слід відзначити, що треба додатково врахувати специфічні для НКЛ: цікавість, випадковість, порушення авторського права, використання в особистих цілях.

Загрози у НКЛ не відрізняються від інших установ та складаються з: доступність інформації, непрацездатність приладів та ПЗ, цілісність ПЗ та інформації, конфіденційність

До засобів доступу у НКЛ відносяться: розголошення, витік, особисті прилади, несанкціонований доступ.

Напрями захисту це: програмно – апаратний, організаційний, інженерно-технічний. Однак практично не можливо використати правовий (юридичний) напрям захисту, тому що більшість учасників освітнього процесу не пов'язано трудовими відносинами.

До методів захисту слід віднести: попередження, роз`яснення, запобігання. Більш слабкі методи у НКЛ: аналіз та вивчення випадків, припинення, протидія тому що вони потребують створення спеціалізованого підрозділу з безпеки інформації.

Таким чином, концептуальну модель інформаційної безпеки можна представити у вигляді схеми, що зображена на рис. 2.

Висновки. В результате проведеного дослідження літературних джерел наведено огляд та класифікацію різноманітних моделей, які використовуються в процесах створення системи інформаційної безпеки. Встановлено, що першим важливим кроком є створення концептуальної моделі безпеки інформації.

Аналіз системи інформаційної безпеки у НКЛ показав, що більшості навчальних закладів необхідно більше уваги приділити процесам підвищення захищеності інформації. Важливу складову додає необхідність швидкого впровадження дистанційних методів навчання. Встановлено та наведено особливості процесу впровадження цієї системи. До основних, з яких, відносяться:відкритість навчального процесу

Рис. 2. Концептуальна модель безпеки НКЛ

- та необхідність забезпечення доступу до всіх матеріалів навчального процесу;
- відсутність відділів та осіб відповідальних за систему інформаційної безпеки;
- значна різниця у кваліфікації користувачів: здобувачів освіти та викладачів;
- недостатнє фінансування;
- використання спеціалізованого програмно-технічного забезпечення у навчальному процесі та дозвіл на використання особистої техніки учасників навчального процесу.

З урахуванням цих особливостей розроблено концептуальну модель безпеки, на засадах якої можна розробити першочергові заходи спрямовані на підвищення інформаційної безпеки у навчальних закладах.

Література

1. Ананченко О. Розробка корпоративної освітньої інформаційної системи за допомогою методів машинного навчання та методик забезпечення інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2023. № 2(22). С. 264–273. URL: https://doi.org/10.28925/2663-4023.2023.22.264273
2. Антонов Ю., Римар П., Антонова О. Проблема DoS/DDoS атак навчальних ресурсів студентами. Сучасний захист інформації. 2019. № 4(40). С. 52–62.
3. Биков В., Буров О., Дементієвська Н. Кібербезпека в цифровому навчальному середовищі. Інформаційні технології і засоби навчання. 2019. № 2(70). С. 313–331.
4. Дослідження розвитку та інновації кіберзахисту на об’єктах критичної інфраструктури / Я. Машталяр та ін. Кібербезпека: освіта, наука, техніка. 2023. № 2. С. 156–167. URL: https://doi.org/10.28925/2663-4023.2023.22.156167.
5. Ільїн О. О. Когнітивна модель управління інформаційною безпекою вищого навчального закладу. Сучасний захист інформації: науково технічний журнал. 2017. № 2(30). С. 24–30.
6. Ільїн О., Сєрих С., Вишнівський В. Аналіз уразливості інформаційного ресурсу вищого навчального закладу та класифікація загроз інформаційної безпеки. Сучасний захист інформації. 2017. № 1. С. 66–72.
7. Кива В. Аналіз чинників, які впливають на кібербезпеку вищого військового навчального закладу. Кібербезпека: освіта, наука, техніка. 2022. № 3(15). С. 53–70. URL: https://doi.org/10.28925/2663-4023.2022.15.5370.
8. Кириленко Н. Проблеми інформаційної безпеки освітнього середовища вищого навчального закладу. Інформаційно-телекомунікаційні технології в сучасній освіті: досвід, проблеми, перспективи : Третя міжнар. наук.- практ. конф. : у 2 ч.. Львів, 2012. С. 149–151.
9. Концептуальна модель захисту інформації об’єктів критичної інформаційної інфраструктури України / Ю. Кожедуб та ін. Information Technology and Security. 2021. Т. 9, № 2(17). С. 151–164.
10. Кухарська Н. П. Оцінка інформаційного середовища вищих навчальних закладів та аналіз загроз його безпеці. Інформаційнокомунікаційні технології в сучасній освіті: досвід, проблеми, перспективи. 2015. Вип. 4. Ч. 2. С. 31–35.
11. Могильний Г. Аналіз програмно-апаратних засобів створення системи з віддаленим доступом до навчальних комп’ютерних лабораторій закладів середньої освіти. Вісник Східноукраїнського національного університету імені Володимира Даля. 2023. № 1(277). С. 5–19.

URL: https://doi.org/10.33216/1998-7927-2019-256-8-5-19
12. Могильний Г., Донченко В., Донченко С. Огляд та аналіз інструментів створення корпоративного середовища. Інформаційні технології та суспільство. 2024. № 4 (15). С. 99–107. URL: https://doi.org/10.32689/maup.it.2024.4.16
13. Могильний Г., Семенов М., Кірєєв І. Впровадження системи віддаленого доступу до інформаційних ресурсів комп'ютерних лабораторій. Вісник Східноукраїнського національного університету імені Володимира Даля. 2022. № 2 (272). С. 7–14. URL: https://doi.org/10.33216/1998-7927-2022-272-2-7-14.
14. Моделі безпеки в інформаційних системах / О. Трапезон та ін. Київ: WORLD SCIENCE. Page 2. ISSN 2413-1032. № 12(16), Vol.1, December 2016.
15. Моделювання мінімальної кількості вузлів кластера віртуалізації приватних університетської хмари / В. Лахно та ін. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2023. № 1(21). С. 177–192. URL: https://doi.org/10.28925/2663-4023.2023.21.177192.
16. Технологія забезпечення інформаційної і кібербезпеки в закладах вищої освіти україни / А. Ю. Нашинець-Наумова та ін. Information Technologies and Learning Tools. 2020. № 3(77). С. 337–354. URL: https://doi.org/10.33407/itlt.v77i3.3424
17. Чубукова О., Пономаренко І. Інформаційна безпека у навчальних закладах України. Вісник Київського національного університету технологій та дизайну. 2018. Спец.випуск. С. 388–395.
18. Шестак Я., Чубаєвський В. Моделювання інформаційної інфраструктури ЗВО. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2023. № 1(21). С. 121–135. URL: https://doi.org/10.28925/2663-4023.2023.21.121135
19. Юдін О. К., Бучик С. С. Державні інформаційні ресурси. Методологія побудови класифікатора загроз. – 2015.
20. Юдін О., Бучик С. Концептуальна модель інформаційної безпеки державних інформаційних ресурсів. Наукоємні технології. 2014. вип. 4. С. 462–466. URL: http://nbuv.gov.ua/UJRN/Nt_2014_4_15.
21. Ясінська А. Інформаційна безпека підприємства: концептуальні засади ефективного захисту інформації . Економіка та суспільство. 2023. № 56. URL: https://doi.org/10.32782/2524-0072/2023-56-118
22. A model developed for teaching an adaptive system of recognising cyberattacks among non-uniform queries in information systems / V Lakhno et al. Eastern-European Journal of Enterprise Technologies. 2016. № 4(9(82). P.27–36. URL: https://doi.org/10.15587/1729-4061.2016.73315
23. An analysis of Indonesia's information security index: a case study in a public university. / W. Yustanti et al. IOP Conference Series: Materials Science and Engineering. 2018. T.296. URL: https://doi.org/10.1088/1757-899x/296/1/012038.
24. An Analysis of IT Assessment Security Maturity in Higher Education Institution / M. Suwito et al. Information Science and Applications. 2016. P. 701–713.
25. Bianchi I., Sousa R. IT Governance Mechanisms in Higher Education. Procedia Computer Science.2016. № 100. P. 941–946. URL: https://doi.org/10.1016/j.procs.2016.09.253.
26. Chang J., Jeon Y., Sim S. Information Security Modeling for the Operation of a Novel Highly Trusted Network in a Virtualization Environment. International Journal of Distributed Sensor Networks. 2021. URL: https://doi.org/10.1155/2015/359170.
27. Correlating human traits and cyber security behavior intentions. / M. Gratian et al. Computers & Security. 2018. №73. P.345–358. URL: https://doi.org/10.1016/j.cose.2017.11.015.
28. Decision Support Model for Assessing Projects by a Group of Investors with Regards of Multi-factors / V Lakhno et al. In: Silhavy, R. (eds) Artificial Intelligence and Bioinspired Computational Methods. CSOC. Advances in Intelligent Systems and Computing, 2020. vol 1225. Springer, Cham. URL: https://doi.org/10.1007/978-3-030-51971-1_1
29. Development of a support system for managing the cyber protection of an information object / V Lakhno et al. Journal of Theoretical and Applied Information Technology. 2017. № 95(6). P. 1263–1272
30. Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? / Z. Yan et al. Computers in Human Behavior. 2018. № 84. P. 375–382. URL: https://doi.org/10.1016/j.chb.2018.02.019
31. Ghazvini A., Shukur Z., Hood Z. Review of Information Security Policy based on Content Coverage and Online Presentation in Higher Education. International Journal of Advanced Computer Science and Applications. 2018. №9(8). P. 410–423. URL: https://doi.org/10.14569/ijacsa.2018.090853.
32. Hina S., Dominic P. Information security policies' compliance: A perspective for higher education institutions. Journal of Computer Information Systems. 2020. № 60(3). P. 201–211.

33. Information Security Governance: A Process Model and Pilot Case Study / C. Wong та ін. ICIS 2020. ISSN 978-1-7336325-5-3. URL: https://aisel.aisnet.org/icis2020.
34. Information system and management for campus safety. У SIGSPATIAL '19: 27th ACM SIGSPATIAL / Y. Zeng et al. International Conference on Advances in Geographic Information Systems. ACM. 2019. URL: https://doi.org/10.1145/3356998.3365760.
35. Joshi C., Singh U. Information security risks management framework – A step towards mitigating security risks in university network. Journal of Information Security and Applications. 2017. №35. P. 128–137.
36. Kearney W., Kruger H. Can perceptual differences account for enigmatic information security behaviour in an organisation? Computers & Security. 2016. № 61. P. 46–58.
37. Lee Y. Information Security Investment Model and Level in Incomplete Information. Journal of the Korea Institute of Information Security & Cryptology. 2017. T. 27, is.4. P. 855–861. URL: https://doi.org/10.13089/JKIISC.2017.27.4.855
38. Multi-criterial optimization composition of cyber security circuits based on genetic algorithm / V Lakhno et al. Journal of Theoretical and Applied Information Technology 15th April 2022. Vol. 100. № 07. P. 1996–2006. URL: http://www.jatit.org/volumes/Vol100No7/3Vol100No7.pdf
39. Ogutcu G., Testik O., Chouseinoglou O. Analysis of personal information security behavior and awareness. Computers & Security. 2016. № 56. P. 83–93.
40. Rajab M. The relevance of social and behavioral models in determining intention to comply with information security policy in higher education environments. Eastern Michigan University. Computers & Security. 2019. T.80. P. 211-223.

References

1. Ananchenko O. Rozrobka korporatyvnoi osvitnoi informatsiinoi systemy za dopomohoiu metodiv mashynnoho navchannia ta metodyk zabezpechennia informatsiinoi bezpeky. Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika». 2023. № 2(22). S. 264–273. URL: https://doi.org/10.28925/2663-4023.2023.22.264273
2. Antonov Yu., Rymar P., Antonova O. Problema DoS/DDoS atak navchalnykh resursiv studentamy. Suchasnyi zakhyst informatsii. 2019. № 4(40). S. 52–62.
3. Bykov V., Burov O., Dementiievska N. Kiberbezpeka v tsyfrovomu navchalnomu seredovyshchi. Informatsiini tekhnolohii i zasoby navchannia. 2019. № 2(70). S. 313–331.
4. Doslidzhennia rozvytku ta innovatsii kiberzakhystu na obiektakh krytychnoi infrastruktury / Ya. Mashtaliar ta in. Kiberbezpeka: osvita, nauka, tekhnika. 2023. № 2. S. 156–167. URL: https://doi.org/10.28925/2663-4023.2023.22.156167.
5. Ilin O. O. Kohnityvna model upravlinnia informatsiinoiu bezpekoiu vyshchoho navchalnoho zakladu. Suchasnyi zakhyst informatsii: naukovo tekhnichnyi zhurnal. 2017. № 2(30). S. 24–30.
6. Ilin O., Sierykh S., Vyshnivskyi V. Analiz urazlyvosti informatsiinoho resursu vyshchoho navchalnoho zakladu ta klasyfikatsiia zahroz informatsiinoi bezpeky. Suchasnyi zakhyst informatsii. 2017. № 1. S. 66–72.
7. Kyva V. Analiz chynnykiv, yaki vplyvaiut na kiberbezpeku vyshchoho viiskovoho navchalnoho zakladu. Kiberbezpeka: osvita, nauka, tekhnika. 2022. № 3(15). S. 53–70. URL: https://doi.org/10.28925/2663-4023.2022.15.5370.
8. Kyrylenko N. Problemy informatsiinoi bezpeky osvitnoho seredovyshcha vyshchoho navchalnoho zakladu. Informatsiino-telekomunikatsiini tekhnolohii v suchasnii osviti: dosvid, problemy, perspektyvy : Tretia mizhnar. nauk.- prakt. konf. : u 2 ch.. Lviv, 2012. S. 149–151.
9. Kontseptualna model zakhystu informatsii obiektiv krytychnoi informatsiinoi infrastruktury Ukrainy / Yu. Kozhedub ta in. Information Technology and Security. 2021. T. 9, № 2(17). S. 151–164.
10. Kukharska N. P. Otsinka informatsiinoho seredovyshcha vyshchykh navchalnykh zakladiv ta analiz zahroz yoho bezpetsi. Informatsiinokomunikatsiini tekhnolohii v suchasnii osviti: dosvid, problemy, perspektyvy. 2015. Vyp. 4. Ch. 2. S. 31–35.
11. Mohylnyi H. Analiz prohramno-aparatnykh zasobiv stvorennia systemy z viddalenym dostupom do navchalnykh kompiuternykh laboratorii zakladiv serednoi osvity. Visnyk Skhidnoukrainskoho natsionalnoho universytetu imeni Volodymyra Dalia. 2023. № 1(277). S. 5–19. URL: https://doi.org/10.33216/1998-7927-2019-256-8-5-19
12. Mohylnyi H., Donchenko V., Donchenko S. Ohliad ta analiz instrumentiv stvorennia korporatyvnoho seredovyshcha. Informatsiini tekhnolohii ta suspilstvo. 2024. № 4 (15). S. 99–107. URL: https://doi.org/10.32689/maup.it.2024.4.16
13. Mohylnyi H., Semenov M., Kirieiev I. Vprovadzhennia systemy viddalenoho dostupu do informatsiinykh resursiv kompiuternykh laboratorii. Visnyk Skhidnoukrainskoho natsionalnoho universytetu imeni Volodymyra Dalia. 2022. № 2 (272). S. 7–14. URL: https://doi.org/10.33216/1998-7927-2022-272-2-7-14.
14. Modeli bezpeky v informatsiinykh systemakh / O. Trapezon ta in. Kyiv: WORLD SCIENCE. Page 2. ISSN 2413-1032. № 12(16), Vol.1, December 2016.
15. Modeliuvannia minimalnoi kilkosti vuzliv klastera virtualizatsii pryvatnykh universytetskoi khmary /

V. Lakhno ta in. Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika». 2023. № 1(21). S. 177–192. URL: https://doi.org/10.28925/2663-4023.2023.21.177192.
16. Tekhnolohiia zabezpechennia informatsiinoi i kiberbezpeky v zakladakh vyshchoi osvity ukrainy / A. Yu. Nashynets-Naumova ta in. Information Technologies and Learning Tools. 2020. № 3(77). S. 337–354. URL: https://doi.org/10.33407/itlt.v77i3.3424
17. Chubukova O., Ponomarenko I. Informatsiina bezpeka u navchalnykh zakladakh Ukrainy. Visnyk Kyivskoho natsionalnoho universytetu tekhnolohii ta dyzainu. 2018. Spets.vypusk. S. 388–395.
18. Shestak Ya., Chubaievskyi V. Modeliuvannia informatsiinoi infrastruktury ZVO. Elektronne fakhove naukove vydannia «Kiberbezpeka: osvita, nauka, tekhnika». 2023. № 1(21). S. 121–135. URL: https://doi.org/10.28925/2663-4023.2023.21.121135
19. Iudin O. K., Buchyk S. S. Derzhavni informatsiini resursy. Metodolohiia pobudovy klasyfikatora zahroz. – 2015.
20. Iudin O., Buchyk S. Kontseptualna model informatsiinoi bezpeky derzhavnykh informatsiinykh resursiv. Naukoiemni tekhnolohii. 2014. vyp. 4. S. 462–466. URL: http://nbuv.gov.ua/UJRN/Nt_2014_4_15.
21. Iasinska A. Informatsiina bezpeka pidpryiemstva: kontseptualni zasady efektyvnoho zakhystu informatsii . Ekonomika ta suspilstvo. 2023. № 56. URL: https://doi.org/10.32782/2524-0072/2023-56-118
22. A model developed for teaching an adaptive system of recognising cyberattacks among non-uniform queries in information systems / V Lakhno et al. Eastern-European Journal of Enterprise Technologies. 2016. № 4(9(82). P.27–36. URL: https://doi.org/10.15587/1729-4061.2016.73315
23. An analysis of Indonesia's information security index: a case study in a public university. / W. Yustanti et al. IOP Conference Series: Materials Science and Engineering. 2018. T.296. URL: https://doi.org/10.1088/1757-899x/296/1/012038.
24. An Analysis of IT Assessment Security Maturity in Higher Education Institution / M. Suwito et al. Information Science and Applications. 2016. P. 701–713.
25. Bianchi I., Sousa R. IT Governance Mechanisms in Higher Education. Procedia Computer Science.2016. № 100. P. 941–946. URL: https://doi.org/10.1016/j.procs.2016.09.253.
26. Chang J., Jeon Y., Sim S. Information Security Modeling for the Operation of a Novel Highly Trusted Network in a Virtualization Environment. International Journal of Distributed Sensor Networks. 2021. URL: https://doi.org/10.1155/2015/359170.
27. Correlating human traits and cyber security behavior intentions. / M. Gratian et al. Computers & Security. 2018. №73. P.345–358. URL: https://doi.org/10.1016/j.cose.2017.11.015.
28. Decision Support Model for Assessing Projects by a Group of Investors with Regards of Multi-factors / V Lakhno et al. In: Silhavy, R. (eds) Artificial Intelligence and Bioinspired Computational Methods. CSOC. Advances in Intelligent Systems and Computing, 2020. vol 1225. Springer, Cham. URL: https://doi.org/10.1007/978-3-030-51971-1_1
29. Development of a support system for managing the cyber protection of an information object / V Lakhno et al. Journal of Theoretical and Applied Information Technology. 2017. № 95(6). P. 1263–1272
30. Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? / Z. Yan et al. Computers in Human Behavior. 2018. № 84. P. 375–382. URL: https://doi.org/10.1016/j.chb.2018.02.019
31. Ghazvini A., Shukur Z., Hood Z. Review of Information Security Policy based on Content Coverage and Online Presentation in Higher Education. International Journal of Advanced Computer Science and Applications. 2018. №9(8). P. 410–423. URL: https://doi.org/10.14569/ijacsa.2018.090853.
32. Hina S., Dominic P. Information security policies' compliance: A perspective for higher education institutions. Journal of Computer Information Systems. 2020. № 60(3). P. 201–211.
33. Information Security Governance: A Process Model and Pilot Case Study / C. Wong та ін. ICIS 2020. ISSN 978-1-7336325-5-3. URL: https://aisel.aisnet.org/icis2020.
34. Information system and management for campus safety. У SIGSPATIAL '19: 27th ACM SIGSPATIAL / Y. Zeng et al. International Conference on Advances in Geographic Information Systems. ACM. 2019. URL: https://doi.org/10.1145/3356998.3365760.
35. Joshi C., Singh U. Information security risks management framework – A step towards mitigating security risks in university network. Journal of Information Security and Applications. 2017. №35. P. 128–137.
36. Kearney W., Kruger H. Can perceptual differences account for enigmatic information security behaviour in an organisation? Computers & Security. 2016. № 61. P. 46–58.
37. Lee Y. Information Security Investment Model and Level in Incomplete Information. Journal of the Korea Institute of Information Security & Cryptology. 2017. T. 27, is.4. P. 855–861. URL: https://doi.org/10.13089/JKIISC.2017.27.4.855
37. Multi-criterial optimization composition of cyber security circuits based on genetic algorithm / V Lakhno et al. Journal of Theoretical and Applied

Information Technology 15th April 2022. Vol. 100. № 07. P. 1996–2006. URL: http://www.jatit.org/volumes/Vol100No7/3Vol100No7.pdf
39. Ogutcu G., Testik O., Chouseinoglou O. Analysis of personal information security behavior and awareness. Computers & Security. 2016. № 56. P. 83–93.
40. Rajab M. The relevance of social and behavioral models in determining intention to comply with information security policy in higher education environments. Eastern Michigan University. Computers & Security. 2019. T.80. P. 211-223.

Mohylnyi H.A., Donchenko V.U., Shvets I. M., Donchenko S.M., Kuznetsov V.S. Conceptual model of information security of educational computer laboratories

In conditions of martial law and rapid development of ICT, effective counteraction to cyberattacks as an element of hybrid warfare requires joint efforts of state institutions, critical infrastructure facilities, industrial enterprises and educational institutions. Under such circumstances, it becomes important to review the foundations of information security. The article is devoted to the study and classification of information security models used to build effective information protection systems. The paper considers three main types of models: conceptual model, mathematical model and functional model.

Conceptual model – serves as a basis for formulating general processes for creating a security system, determines key areas and structure of information protection.

In addition to analyzing models, the work highlights the features of implementing information protection systems in educational institutions. Among the main problems identified are: lack of specialized departments and persons responsible for information security; insufficient level of training of teaching and support staff; large differences in user qualifications; difficulty in ensuring security with the openness of the educational process and increasing requirements for the implementation of distance education technologies.

The peculiarities of building a security system in educational institutions are the need to find a compromise solution between the openness of the educational process and student-centered learning; ensuring comfortable conditions for access to all materials of the educational process and strict provisions for the leakage of confidential and official information. The paper proposes one of the options for developing a conceptual security model as a basis for the further implementation of effective protection measures, taking into account the specifics of the work of educational institutions and their information environment. The creation of this model is an important first step in building a security system. Based on the analysis, it is proposed to review the main approaches to information security in educational institutions, especially taking into account the specifics of distance learning and the openness of educational processes.

Keywords: educational computer laboratory, educational institution, cybersecurity, threats, model, protection system.

Могильний Геннадій Анатолійович – к. т. н., доцент, директор Навчально-наукового інституту математики та інформаційних технологій Луганського національного університету імені Тараса Шевченка, g.mogilniy@gmail.com
Донченко Володимир Юрійович – старший викладач кафедри інформаційних технологій та систем Навчально-наукового інституту математики та інформаційних технологій Луганського національного університету імені Тараса Шевченка, ifmit.s.2014@gmail.com
Швець Ірина Михайлівна – асистент кафедри математики та інформатики Навчально-наукового інституту математики та інформаційних технологій Луганського національного університету імені Тараса Шевченка, irinachipenkooo@gmail.com
Донченко Світлана Миколаївна – асистент кафедри інформаційних технологій та систем Навчально-наукового інституту математики та інформаційних технологій Луганського національного університету імені Тараса Шевченка, donchenko.lana77@gmail.com
Кузнецов Віталій Сергійович – асистент кафедри інформаційних технологій та систем Навчально-наукового інституту математики та інформаційних технологій Луганського національного університету імені Тараса Шевченка, vitaliilkuznetsov.mm@gmail.com

Стаття подана 25.05.2025.