ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»
МІНІСТЕРСТВА ОСВІТИ І НАУКИ УКРАЇНИ
Кафедра комп'ютерних інтелектуальних систем та мереж

ГЕРШУН Вікторія Сергіївна

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ДАНИХ ЛАБОРАТОРІЇ З ВІДДАЛЕНИМ ДОСТУПОМ. ЦІЛІСНІСТЬ

Спеціальність 123 – Комп’ютерна інженерія
Спеціалізація – Комп'ютерні системи та мережі

Керівник: Тішин Петро Металінович,
кандидат фізико-математичних наук, доцент

Одеса – 2021

АНОТАЦІЯ

Гершун В. С. Дослідження методів захисту даних лабораторії з віддаленим доступом. Цілісність – Кваліфікаційна робота магістра. Одеса, 2021: 68 с., 27 рис., 11 джерел.

Об’єктом дослідження є загрози для інформаційного середовища лабораторії віддаленого доступу та механізми забезпечення захищеності цілісності даних.

Предметом дослідження є методи забезпечення цілісності даних лабораторії з віддаленим доступом.

Метою роботи є дослідження існуючих рішень для контролю цілісності даних та обґрунтування вибору оптимального методу захисту цілісності даних лабораторії віддаленого доступу.

Методи дослідження базуються на використанні теорії захисту інформації та моделей інформаційної безпеки, що мають за основу фундаментальні результати теорії множин, математичної логіки та теорії графів. Побудовані моделі загроз ґрунтуються на використанні методології об'єктно-орієнтованого проектування.

Робота присвячена дослідженню методів захисту даних лабораторії з віддаленим доступом, і зокрема параметра цілісності. Розглянуто основні методи захисту інформаційної безпеки та типові для лабораторії віддаленого доступу загрози. На основі результатів дослідження сформовані моделі інформаційних загроз та сценарії протидії. Обрано оптимальні рекомендації захисту цілісності даних лабораторії віддаленого доступу та запропонована модель оцінки захищеності даних для подальшого покращення рівня безпеки та проведення коригувальних дій у разі потреби.

ІНФОРМАЦІЙНА БЕЗПЕКА, ЗАХИСТ ДАНИХ, ІНФОРМАЦІЙНІ ЗАГРОЗИ, ЦІЛІСНІСТЬ ДАНИХ

ABSTRACT

Hershun V. S. Research methods of data protection of the laboratory with remote access. Integrity - The master qualifying work. Odessa, 2021: 68 pages., 27 pic.,11 sources.

The object of the study are threats to the information environment of the remote access laboratory and mechanisms to ensure the protection of data integrity.

The subject of the research is the methods of ensuring the integrity of laboratory data with remote access.

The aim of the work is to study the existing solutions for data integrity control and justify the choice of the optimal method of data integrity protection of the remote access laboratory.

Research methods are based on the use of information security theory and information security models, which are based on the fundamental results of set theory, mathematical logic and graph theory. The built models of threats are based on the use of object-oriented design methodology.

The work is devoted to the study of methods of data protection of the laboratory with remote access, and in particular the integrity parameter. The main methods of information security protection and typical for the laboratory of remote access to the threat are considered. Based on the results of the research, models of information threats and counteraction scenarios are formed. The best recommendations for data integrity protection of the remote access laboratory have been selected and a data security assessment model has been proposed to further improve the level of security and take corrective action if necessary.

INFORMATION SECURITY, DATA PROTECTION, INFORMATION THREATS, DATA INTEGRITY

ЗМІСТ

ВСТУП

Одним із основних факторів конкурентоспроможності сучасного вищого навчального закладу стають знання, інновації та способи їхнього практичного застосування. Управління знаннями, яке забезпечує інтегрований підхід до створення, збирання, доступу та використанню інформаційних ресурсів, у сучасних умовах стає напрямком діяльності будь-якої організації. Складовою процесу підготовки фахівців у галузі інформаційних технологій є лабораторний практикум.

Поняття «лабораторія з віддаленим доступом» пов'язане з розвитком мережевих комп'ютерних технологій, що дозволяють реалізувати лабораторний практикум у режимі віддаленого доступу до реального обладнання чи програмного забезпечення.

Така лабораторія віддаленого доступу є програмно-апаратним комплексом, що дозволяє проводити експерименти, не маючи безпосереднього доступу до об'єкта дослідження. При цьому експерименти проводяться з використанням віддаленого доступу до реального об'єкта. До складу комплексу входить реальна лабораторія, програмно-апаратне забезпечення для управління встановленням та оцифрування отриманих даних, а також засоби комунікації.

Проектування лабораторії з віддаленім доступом вимагає забезпечення високого рівня надійності, ефективності та технологічності. Це стає можливим лише за умови захищеності інформації, що зберігається чи передається між складовими частинами програмно-апаратного комплексу. Для цього необхідно використовувати спеціальні засоби захисту, що забезпечать оптимальні властивості захищеності інформації: конфіденційність, цілісність та доступність.

При безперечній важливості аспектів забезпечення конфіденційності та доступності інформації, питання захисту інформації від несанкціонованої зміни мають одне з пріоритетних значень. При цьому необхідно зазначити, що умовою

забезпечення інформаційної безпеки автоматизованої інформаційної системи в цілому є впевненість у відсутності несанкціонованих змін алгоритмів, що обробляють інформацію, а також гарантована цілісність технологій, що забезпечують інформаційну безпеку системи. Під цілісністю розуміється властивість інформації бути захищеною від несанкціонованого спотворення, руйнування чи знищення. Прикладами порушення цілісності даних можуть бути такі дії, як підробка документа, випадкова зміна інформації при передачі, зміна інформації при несправній роботі жорсткого диска чи іншого обладнання, спотворення інформації.

Таким чином, дослідження методів та засобів програмного та апаратного забезпечення цілісності лабораторії віддаленого доступу є актуальним завданням, що потребує наукової розробки. Її рішення дозволить підвищити інформаційну безпеку програмно-апаратного комплексу в цілому.

У зв'язку з цим необхідно провести аналіз загроз цілісності інформації, визначити на якому етапі та від чого необхідно забезпечувати інформаційну безпеку. Існує необхідність розробки моделі загроз і розгляду пов'язаних з нею питань оцінки поточного стану інформаційної системи та рекомендацій щодо вдосконалення захисту інформації. У дипломній роботі розглянуто підхід до побудови моделі загроз, що ґрунтується на використанні методології об'єктно-орієнтованого проектування. Такий підхід передбачає активне використання UML-діаграм при описі концептуальної моделі загроз інформаційної безпеки, способів реалізації загроз, сценаріїв реалізації загрози та сценаріїв захисту. У свою чергу, слід зазначити, що в даний час існує кілька підходів забезпечення цілісності в інформаційних системах. Їх необхідно також проаналізувати, виявити переваги та недоліки та визначити, який підхід забезпечить найкращу захищеність інформації у випадку лабораторії з віддаленим доступом.

Мета кваліфікаційної роботи полягає в дослідженні існуючих рішень для контролю цілісності даних та обґрунтування вибору оптимального методу захисту цілісності даних лабораторії віддаленого доступу.

Для досягнення мети вирішені наступні задачі:

- сформовані типові інформаційні загрози та модель порушення цілісності даних лабораторії віддаленого доступу;
- проведено дослідження існуючих методів захисту цілісності даних;
- досліджені оптимальні методи захисту цілісності даних на етапі зберігання, обробки та передачі даних;
- визначено перелік рекомендацій та алгоритм забезпечення необхідного рівня захищеності цілісності даних для лабораторії віддаленого доступу.

Об’єктом дослідження є загрози для інформаційного середовища лабораторії віддаленого доступу та механізми забезпечення захищеності цілісності даних.

Предметом дослідження є методи забезпечення цілісності даних лабораторії з віддаленим доступом.

Методи дослідження базуються на використанні теорії захисту інформації та моделей інформаційної безпеки, що мають за основу фундаментальні результати теорії множин, математичної логіки та теорії графів. Побудовані моделі загроз ґрунтуються на використанні методології об'єктно-орієнтованого проектування.

Наукова новизна роботи полягає в дослідженні і обґрунтуванні оптимальних методів захисту для типової лабораторії віддаленого доступу, враховуючи особливості її реалізації на базі навчального закладу. Запропоновані методи захисту є адаптованими до типової архітектури лабораторії віддаленого доступу. Представлені інформаційні загрози, що можуть виникнути на різних етапах роботи з інформацією, яка циркулює в системі навчального закладу. Передбачено модель оцінки захищеності інформації, що дозволяє проводити коригувальні заходи з метою покращення рівня захищеності.

Робота складається з чотирьох розділів, кожний з яких досліджує особливості реалізації захисту лабораторії віддаленого доступу. Перший розділ представляє собою аналітичне дослідження сутності лабораторії віддаленого доступу та розглядає основні переваги використання такої технології на базі реальних навчальних лабораторій. Проаналізовано можливі інформаційні загрози та існуючі методи захисту інформації і цілісності даних зокрема. За результатами дослідження були сформовані основні методи захисту, що застосовуються на кожному етапі

життя інформації.

Другий розділ присвячено формуванню дослідницького завдання та визначенню основних параметрів, що допоможуть обрати оптимальний захист для лабораторії віддаленого доступу. Інформація, що циркулює в інформаційній системі класифікована за типом регламентації поширення та використання. Досліджені державні нормативні вимоги і вимоги, що є обов’язковими для інформаційної безпеки даних, що обробляються в системах навчального закладу. На основі цих вимог описані очікувані результати від захисту інформації загалом і безпосередньо параметру цілісності.

Третій розділ моделює загрози інформаційної безпеки лабораторії віддаленого доступу. Це необхідно для розуміння принципів порушення інформаційної безпеки та є основою для вибору методів захисту лабораторії. За допомогою поетапного порядку моделювання загроз можна досягнути охоплення всіх основних ризиків та отримати розуміння принципів на яких потрібно будувати захист системи. На основі об’єктно орієнтованого моделювання описані структури загроз та сценарій реалізації, на основі якого розроблено сценарій протидії. Функціональні моделі допомогли змоделювати порушення цілісності сегмента лабораторії віддаленого доступу та сформувати аналогічну модель для недопущення таких дій.

Четвертий розділ передбачає визначені напрямки захисту інформації та оптимальні засоби для забезпечення цілісності даних. А також модель оцінювання захищеності інформації, для розуміння рівня поточного захисту даних. На основі оцінки є можливість сформувати коригувальні дії та перевірити доречність обраних методів захисту.

1 ІНФОРМАЦІЙНІ ЗАГРОЗИ ТА МЕТОДИ ЗАХИСТУ ЦІЛІСНОСТІ ДАНИХ ЛАБОРАТОРІЇ ВІДДАЛЕНОГО ДОСТУПУ

1.1 Поняття лабораторії віддаленого доступу

Викладання основної кількості інженерних дисциплін передбачає демонстрацію роботи реального промислового обладнання, що стає можливим завдяки використанню лабораторних приборів та установок різноманітної складності та вартості. Віддалений доступ до обладнання дозволяє студентам мати доступ до проведення експериментів в режимі реального часу, що передбачає отримання практичних навичок роботи, незважаючи на неможливість фізичного доступу в навчальну лабораторію.

Лабораторія віддаленого доступу є різновидом віртуальної лабораторії і відрізняється наявністю підключення до реального лабораторного обладнання та програмного забезпечення, за допомогою яких і проводиться експеримент. Передбачається програмно-апаратний комплекс, завдяки якому користувачу надається можливість роботи з лабораторним обладнанням чи програмним забезпеченням, без взаємодії з реальною фізичною установкою [1].

Реалізація та використання лабораторії віддаленого доступ в навчальному процесі має ряд переваг:

- можливість виконувати лабораторні досліди в онлайн режимі, з використанням унікального сучасного обладнання;
- доступ до технічного забезпечення, незважаючи на обставини, що заважають фізичній присутності в лабораторії;
- у порівнянні з програмами емуляторами, отримання точних результатів, що максимально наближені до реальних умов.
- безпечний і захищений доступ до інформації, що мінімізує можливість несанкціонованого доступу і зміни даних.

Одним з можливих напрямів використання наведених технологій є організація віддаленого доступу для учбових стендів оснащених програмованими логічними контролерами та додатковими модулями, що розташовані в лабораторії Державного університету «Одеська політехніка». Забезпечити взаємодію з лабораторним обладнанням, за умови відсутності реального фізичного доступу, можна різними способами. Незмінною лишається необхідність забезпечення оптимального рівня інформаційної безпеки за усіма основними принципами захисту інформації.

Для виявлення ключових проблем інформаційної безпеки, причин та джерел їх виникнення, а також оцінки їх наслідків, необхідно попередньо розглянути загальну архітектуру лабораторії віддаленого доступу, яка зображена на рисунку 1.1

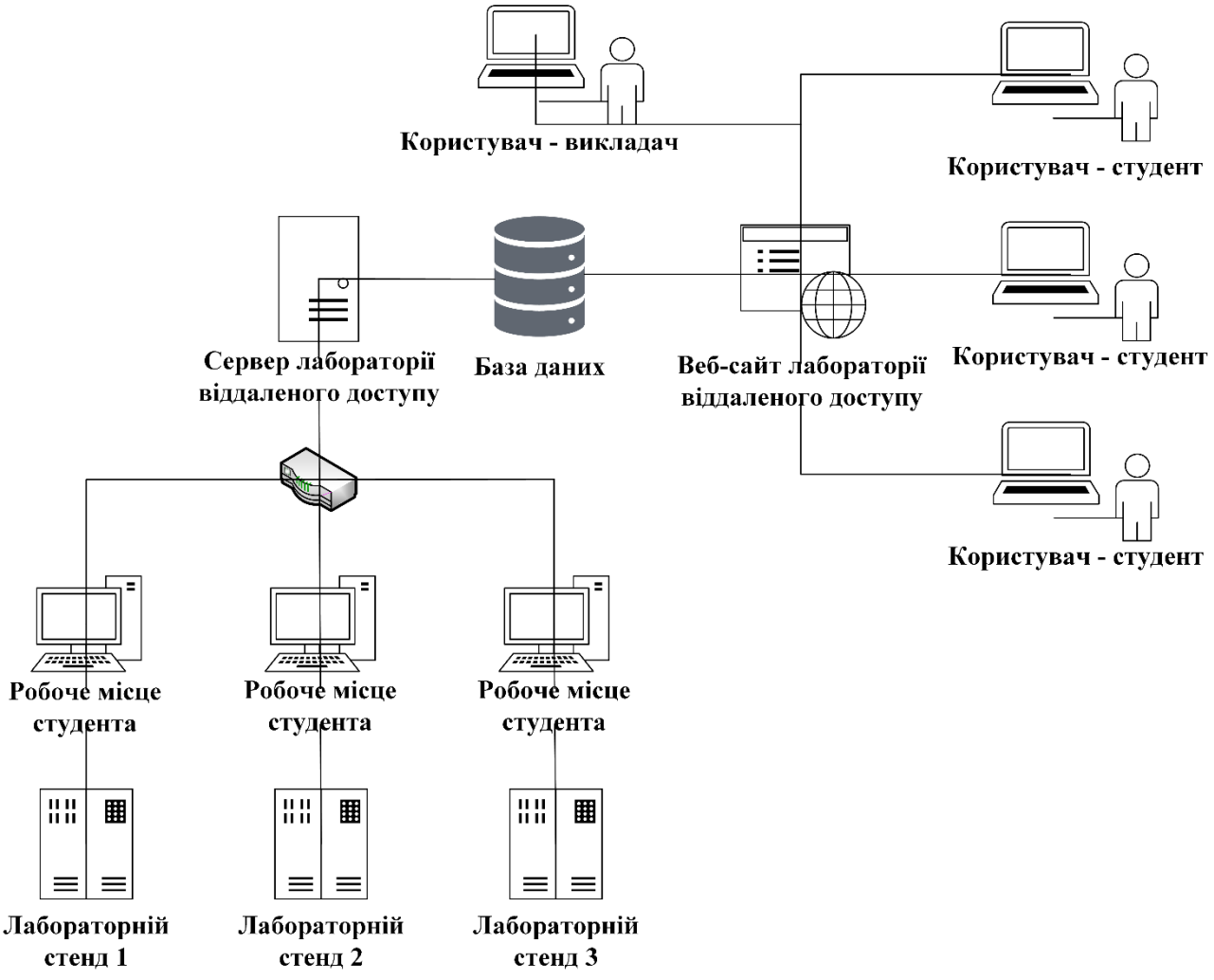

Рисунок 1.1 – Загальна архітектура лабораторії віддаленого доступу

В якості основних функціональних компонентів лабораторії віддаленого доступу можна виділити:

- веб-додаток, тобто зовнішній інтерфейс, призначений для організації віддаленого доступу студентів до змісту навчальних курсів;
- база даних, у якій може зберігатися наповнення навчальних курсів, оціночні матеріали, електронні підручники, дані про успішність;
- сервер лабораторії віддаленого доступу, що є ядром системи та забезпечує основні функціональні можливості;
- безпосередньо апаратне та програмне забезпечення лабораторії.

Розуміння базової комплектації та загального принципу роботи лабораторії віддаленого доступу дозволяє проаналізувати вразливі місця інформаційної безпеки та дослідити загрози і моделі можливих порушень цілісності даних.

1.2 Загрози інформаційної безпеки лабораторії віддаленого доступу

Визначення переліку загроз та побудова моделі порушника є обов'язковим етапом проектування системи захисту. Під загрозою безпеки інформації (інформаційною загрозою) розуміється дія або подія, яка може призвести до руйнування, спотворення або несанкціонованого використання інформаційних ресурсів, включаючи збережену, передану та оброблювану інформацію, а також програмні та апаратні засоби [2].

За наявності в системі вразливості потенційна загроза може реалізуватися у вигляді атаки. Атаки прийнято класифікувати залежно від цілей, мотивів, використовуваного механізму, місця в архітектурі системи та місцезнаходження порушника. Для попередження успішних атак необхідний пошук та аналіз вразливостей системи.

Загроза - це фактор, що прагне порушити роботу системи. На основі основних властивостей інформації, що захищається, можна виділити 3 основних види загроз [3]:

- загрози порушення конфіденційності;

- загрози порушення цілісності;
- загрози порушення доступності.

Дані види загроз можна вважати первинними, або безпосередніми, тому що якщо розглядати поняття загрози як деякої потенційної небезпеки, реалізація якої завдає шкоду інформаційній системі, то реалізація перелічених вище загроз призведе до безпосереднього впливу на інформацію, що захищається [3].

В даний час розглядається досить великий перелік загроз інформаційній безпеці, що налічує сотні пунктів. Крім зазначених видів можливих загроз, їх можна класифікувати за низкою різноманітних ознак. Кожна з ознак класифікації відображає одну із вимог до системи захисту. При цьому загрози, відповідні кожній ознаці класифікації, дозволяють уточнити вимоги. На рисунку 1.2 представлено приклад класифікації основних видів загроз інформаційної безпеки.

Рисунок 1.2 – Класифікації загроз інформаційної безпеки

Для кожної системи перелік найбільш ймовірних загроз безпеки, а також характеристика найбільш ймовірного порушення індивідуальні. Захищеність інформації забезпечується лише за відповідності передбачуваних загроз реальній

обстановці. Зважаючи на принцип роботи та складові компоненти лабораторії віддаленого доступу, можна припустити, що найбільш уразливими з погляду інформаційної безпеки будуть процеси:

- передачі ідентифікаційних та автентифікаційних даних користувача лабораторії віддаленого доступу;
- обмін даними між браузером віддаленого користувача та веб-сайтом лабораторії віддаленого доступу.
- авторизації користувача в системі;
- вилучення та запис даних у базу даних;
- обмін даними між сервером лабораторії віддаленого доступу та інформаційною мережею навчального закладу.

Подібний висновок в першу чергу пов'язаний з тим, що саме в процесі виконання даних дій, найімовірніша спроба зловмисника реалізувати атаку на систему лабораторії та отримати доступ до її ресурсів, сервісів та даних.

Статистика також підтверджує, що основним джерелом порушень є мережа, включаючи браузер, мережеві ресурси та сервіси, на частку яких припадає 39,6% всіх порушень [3].

Зловмисник може бути як зовнішнім, так і внутрішнім і при реалізації атаки переслідувати такі цілі:

- отримання несанкціонованого доступу до ресурсів та сервісів лабораторії віддаленого доступу;
- одержання через зламану систему лабораторії несанкціонованого доступу до внутрішньої інформаційної мережі навчального закладу;
- крадіжка матеріалів та інтелектуальної власності: навчальних матеріалів, оціночних матеріалів та матеріалів, створюваних колективно учасниками навчального процесу;
- отримання доступу до персональних даних студентів та співробітників навчального закладу;
- крадіжка та розголошення персональних даних студентів та співробітників навчального закладу;

- отримання несанкціонованого доступу та внесення змін до баз даних навчальних відомостей;
- отримання несанкціонованого доступу до внутрішньої службової та іншої конфіденційної інформації, що зберігається та обробляється в інформаційній мережі навчального закладу;
- отримання несанкціонованого доступу та крадіжка результатів науково-дослідницької та інноваційної діяльності вузу;
- порушення цілісності та/або знищення навчальних матеріалів та даних про навчальний процес;
- порушення доступності веб-сайту і сервера лабораторії віддаленого доступу;
- порушення доступності інформації та матеріалів навчальних курсів для користувачів.

При реалізації атак на засоби дистанційної освіти, зловмисники можуть використовувати:

- уразливості у веб-додатку та сервісах лабораторії віддаленого доступу;
- слабкі паролі та недоліки процесу аутентифікації користувачів на сервері лабораторії віддаленого доступу;
- помилки у конфігуруванні та адмініструванні;
- шкідливе програмне забезпечення (віруси, троянські програми, руткіти, програмні бомби та закладки);
- інші слабкості системи захисту інформації.

1.3 Загрози безпеки цілісності даних

Одним із ключових аспектів забезпечення захищеності інформації є її цілісність. Перш ніж перейти до самих підходів забезпечення цілісності інформації, слід визначити, що є порушенням цілісності інформації та провести аналіз загроз. Це необхідно для того, щоб чітко визначити, від чого необхідно захищатись.

В одному з найпоширеніших трактувань під цілісністю даних мається на увазі відсутність неналежних змін: цілісність - це властивість інформації бути

захищеною від несанкціонованого спотворення, руйнування чи знищення [3]. Порушення цілісності інформації – ушкодження, що веде до неможливості використовувати інформацію без відновлення. Крім ймовірності втратити важливі дані, загроза небезпечна для працездатності всієї інформаційної системи.

Слід зазначити, що доступності, а тим більше конфіденційності, без забезпечення цілісності інформації досягти неможливо. Наприклад, виходячи із сучасних вимог до криптосистем, незначна зміна вихідного тексту має призводити до значної зміни шифрованої послідовності. Якщо в процесі передачі спотвориться один біт шифрограми, що передається, то після розшифровки отриманий текст сильно відрізнятиметься від вихідного. Таким чином, можна говорити про проблему забезпечення цілісності інформації, яка не вирішена повною мірою на сьогоднішній день.

Виходячи з визначення цілісності інформації, можна виділити такі види впливу на інформацію:

- модифікацію інформації;
- підміну інформації;
- знищення інформації.

Модифікація передбачає зміни будь-якої частини інформації. Ці зміни можуть бути як випадковим, так і навмисним. У другому випадку вони можуть бути санкціонованими або несанкціонованими.

Підміна передбачає нав'язування хибної інформації шляхом заміни істинної (початкової) інформації.

Знищення найчастіше пов'язується зі знищенням фізичного носія інформації та/або розмагнічуванням (форматуванням) електронних носіїв.

Загроза цілісності існує на всіх етапах життєвого циклу інформації:

- на етапі зберігання;
- на етапі обробки;
- на етапі транспортування.

У процесі зберігання інформації основними загрозами є несанкціонований доступ для модифікації (можливо до знищення) інформації, шкідливі програми

(віруси, трояни, черв'яки, логічні бомби) і технічні несправності.

При обробці інформації порушення цілісності інформації може виникнути внаслідок технічних несправностей, алгоритмічних та програмних помилок, помилок та деструктивних дій обслуговуючого персоналу, зовнішнього втручання, дії руйнівних та шкідливих програм (вірусів, експлойтів, черв'яків, логічних бомб).

У процесі передачі інформації можуть впливати різноманітних перешкоди як природного, так і штучного походження. При цьому можливе її спотворення чи стирання (знищення). Крім цього, можливе перехоплення інформації з метою її модифікації та подальшого спотворення.

Для визначення загроз цілісності інформації розглянемо моделі порушників інформаційної безпеки.

За сферою впливу на інформаційну систему потенційних порушників поділяють на внутрішніх та зовнішніх. Внутрішніми порушниками є працівники, які мають фізичний та/або логічний доступ до ресурсів інформаційної системи [4].

За характером можна виділити такі загрози внутрішнього порушення цілісності інформації:

Саботаж - пошкодження, що настало внаслідок цілеспрямованих зловмисних дій. Сюди належить діяльність співробітників, які вирішили з різних причин завадити функціонуванню системи. Зустрічаються й інші ситуації, зумовлені корисливими мотивами, помстою та іншими [4];

Збій програм. Він пов'язаний з некоректним налаштуванням програми, яка може модифікувати чи видалити дані.

Під зовнішніми порушниками маються на увазі фізичні особи, які не є співробітниками закладу, але мають фізичний та/або логічний доступ до ресурсів інформаційної системи, у тому числі особи, які отримали доступ у незаконний спосіб.

За характером загроз зовнішнього порушення цілісності інформації слід враховувати хакерські атаки. Під хакерською атакою мається на увазі можливість, у межах мережного доступу до інформаційної системи закладу, здійснити модифікацію чи видалення даних [4].

1.4 Забезпечення цілісності інформації на етапі зберігання даних

В інформаційній системі основне місце зберігання інформації – електронні носії, тож необхідно розглянути заходи захисту стосовно цього класу носіїв.

Визначаючи порядок зберігання інформації на електронних носіях, слід мати на увазі, що від стану носіїв залежить якість програм і даних, що захищаються. Електронні носії є пристроями, що піддаються інтенсивному зносу.

Заходи захисту цілісності інформації на електронних носіях можна поділити на дві основні групи [5]:

- організаційні заходи щодо підтримки цілісності інформації;
- технологічні заходи контролю цілісності бітових послідовностей.

Організаційні заходи захисту спрямовані на запобігання розкраданню чи втраті носіїв, а разом з ними інформації. Організаційні заходи викладаються у документах, що описують режим зберігання конфіденційної інформації.

Організаційні заходи поділяються на дві групи:

- створення резервних копій інформації;
- забезпечення правильних умов зберігання та експлуатації носіїв.

Найпоширенішим і найскладнішим підходом до забезпечення цілісності інформації є її резервування. За допомогою резервних копій можна відновити інформаційну систему до вихідного стану, якщо вона була піддана програмному збою або успішній атаці, результати яких призвели до модифікації або видалення інформації [5]. Проте, щоб метод резервування даних забезпечив найбільшу захищеність цілісності інформації, необхідно дотримуватися таких рекомендацій:

- для забезпечення надійності зберігання резервних копій необхідно використовувати відмовостійке обладнання систем зберігання даних (використання надлишкового масиву незалежних дисків), дублювати інформацію та замінювати віддалену або модифіковану останньою зарезервованою копією;
- для того, щоб наслідки, через які довелося відновлювати інформаційну систему на стан останньої зробленої резервної копії, завдали мінімальної шкоди, необхідно проводити регулярно і часто резервування даних;

- основні дані та їх резервні копії мають бути фізично поділені на різних носіях інформації.

Перевагою даного методу є можливість відновити знищену чи спотворену інформацію. Недоліком слід вважати те, що відновлення даних із резервної копії займає досить багато часу, що призводить до суттєвого уповільнення роботи інформаційної системи. Ще одним недоліком є необхідність зберігати основні та зарезервовані дані на фізично розділених відмовостійких носіях інформації, що робить цей підхід дорогим.

Забезпечення правильних умов зберігання та експлуатації визначається конкретним типом носія.

Необхідно розглянути і технологічні заходи контролю за цілісністю бітових послідовностей, що зберігаються на електронних носіях. Цілісність інформації у галузях даних перевіряється за допомогою контрольного коду, контрольні числа якого записуються після відповідних областей, причому у контрольовану область включаються відповідні маркери [6].

Для забезпечення контролю цілісності інформації частіше застосовують циклічний контрольний код. Цей метод, дає хороші результати при захисті від впливу випадкових факторів (перешкод, збоїв та відмов), але не забезпечує захист від цілеспрямованих впливів порушника, що призводять до нав'язування помилкових даних.

Для контролю цілісності можна використовувати методи імітозахисту, засновані на криптографічних перетвореннях. Вони забезпечують надійний контроль даних, що зберігаються в системі, але водночас реалізуються у вигляді об'ємних програм і потребують значних обчислювальних ресурсів [7].

1.5 Контроль цілісності даних, що зберігаються на віддалених серверах

Для перевірки цілісності даних, що зберігаються на віддалених серверах, пропонуються різні протоколи доказу володіння даними (Proof of Data Possession, PDP)[7].

Оригінальна PDP-модель передбачає наявність на стороні клієнта метаданих, які мають бути сформовані перед завантаженням інформації на віддалений сервер. Для перевірки цілісності файлу клієнту необхідно надіслати запит на сервер, який, у свою чергу, має відповісти повідомленням, заснованим на файлі, що цікавить клієнта. Порівнюючи відповідь сервера з метаданими, що є у клієнта, можна судити про доступність файлу у його початковому вигляді. Описана модель дозволяє досягти високої ймовірності визначення некоректної роботи сервера при незначних обчислювальних витратах та витратах на зберігання інформації, проте вона застосовна лише для файлів, які не змінюються після завантаження на сервер. На рисунку 1.3 зображено загальний вигляд протоколу доказу володіння даними.

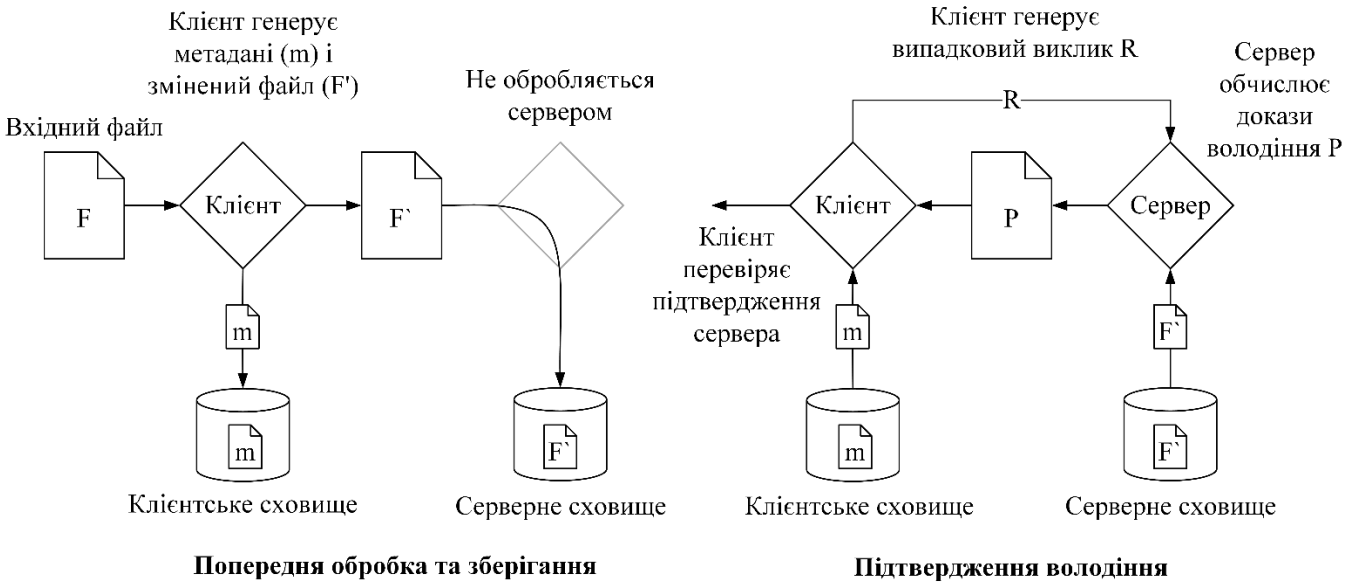

Рисунок 1.3 – Протокол доказу володіння даними

Інший механізм перевірки цілісності даних - доказ вилучення (Proof of retrievability, POR), тобто того, що файл - у наявності і може бути витягнутий [7]. Ця модель призначена для мінімізації як обсягів зберігання даних (як на стороні клієнта, так і на сервері), так і складності виконання перевірки та числа блоків даних, до яких необхідно звертатися під час перевірки. Користувач зберігає лише ключ, використовується для шифрування вихідного файлу F в F', причому в F' впроваджується набір контрольних значень. Сервер зберігає зашифрований файл

F', не знаючи, де саме розташовані контрольні значення, оскільки вони не відрізняються від звичайних блоків даних. Для перевірки цілісності файлу серверу необхідно повернути деяке підмножина контрольних значень F'. Якщо F' змінено або видалено, велика ймовірність того, що необхідні контрольні значення також зіпсовані чи втрачені. Через обмежену кількість контрольних значень, при незначних пошкодженнях файлу пропонований протокол може повертати помилкове підтвердження цілісності даних. Як оригінальну PDP-модель, так і POR-модель можна використовувати тільки для статичних файлів.

Динамічна PDP-модель має повну підтримку операцій додавання, зміни, вставки та видалення [8]. Результати експериментів показують, що, незважаючи на зростання обчислювальних витрат, модель виявляється ефективною. Наприклад, для перевірки цілісності файлу розміром 1 Гб, динамічній моделі необхідно згенерувати всього 415 Кб даних та витратити 30 мс на обчислювальні витрати. Протокол аналізованої PDP-моделі має три нові операції: "підготувати зміну", "застосувати зміну", "перевірити зміну". Перша запускається клієнтом для підготовки запиту на оновлення даних. Друга запускається сервером для фактичного оновлення файлу, після чого повертає доказ зміни клієнту, який, у свою чергу, перевіряє поведінку сервера під час зміни даних.

Модель шару високої доступності та цілісності для хмарного зберігання (High-Availability and Integrity Layer, HAIL) відрізняється від згаданих вище, оскільки пропонує розподілене оточення, при якому клієнт повинен завантажувати файл відразу на кілька серверів з резервуванням і зберігати тільки невеликий незмінний стан на локальному пристрої.

Перевірка коректності віддалених хмарних обчислень – завдання більш трудомістке та актуальне. Традиційні стратегії перевірки діляться на 4 категорії: повторне обчислення, реплікація, аудит, довірені обчислення.

Повторне обчислення полягає в тому, що необхідно ще раз зробити обчислення локально та порівняти з отриманими раніше результатами. Стратегія гарантує 100% точність визначення помилки, не вимагає довіри до хмарного постачальника. Проте вартість виявляється значною, оскільки кожна перевірка

вимагає, як мінімум, стільки часу, скільки витрачено на віддалене обчислення. Тому клієнти не використовують стратегію, що розглядається, в чистому вигляді. Різновид повторного обчислення - вибіркове обчислення, яке надає ймовірні гарантії виявлення помилок, що залежать від вибірки. Вибіркове повторне обчислення жертвує точністю заради ефективності.

Реплікація призначає одне завдання кільком пристроям, потім порівнює результати. Якщо відносна більшість результатів збігаються, можна судити про правильність обчислень. Реплікація передбачає наявність певної довіри до постачальника хмари, оскільки обчислення та перевірка правильності виконуються віддалено. Зловмисник, що контролює певну частину машин, може обійти перевірку коректності результату за допомогою реплікації, повертаючи з підконтрольних йому пристроїв некоректний результат, аналогічний отриманому раніше.

Аудит зазвичай застосовують разом із журналюванням. Під час виконання обчислень окремий компонент записує всі критичні події до журналу, який надсилається одному або декільком аудиторам для перевірки. Аудит – типовий підхід до криміналістичної перевірки. Один з недоліків аудиту полягає в тому, що зловмисник краще, ніж перевіряючий, розуміється на обчисленнях, що дозволяє йому залишатися непоміченим, змінюючи деякі дані.

Ключовим методом перевірки цілісності є віддалена атестація: обладнання генерує сертифікат, що містить докладні відомості у тому, яке програмне забезпечення запущено. Цей сертифікат надсилається перевіряльнику, щоб підтвердити, що програмне забезпечення не було змінено. Припущення, на якому ґрунтується метод довірчих обчислень, полягає в тому, що деякі компоненти, наприклад, апаратна частина та гіпервізор не змінені зловмисником.

Отже, щодо цілісності даних у хмарних системах виділяють дві основні проблеми: значні обсяги даних виключають використання звичайних алгоритмів хешування; перевірка цілісності може бути застосована лише після реалізації додаткових вимог, які збільшують складність.

1.6 Забезпечення цілісності інформації на етапі передачі даних

Засоби контролю цілісності повинні забезпечувати захист від несанкціонованої зміни інформації порушником під час її передачі каналами зв'язку.

Схема контролю цілісності даних передбачає виконання двома сторонами - джерелом і приймачем - деяких (можливо, різних) криптографічних перетворень даних. Джерело перетворює вихідні дані та передає їх приймачеві разом із деяким додатком, що забезпечує надмірність шифрограми. Приймач обробляє отримане повідомлення, відокремлює додаток від основного тексту та перевіряє їхню взаємну відповідність, здійснюючи таким чином контроль цілісності. Контроль цілісності може виконуватися з відновленням чи без відновлення вихідних даних [9].

Цілісність окремого повідомлення забезпечується імітовставкою, електронним цифровим підписом або шифруванням, цілісність потоку повідомлень - відповідним механізмом цілісності.

Імітовставка передбачає, що для забезпечення цілісності в текст повідомлення часто вводиться деяка додаткова інформація, яка легко обчислюється, якщо секретний ключ відомий, і є важкообчислюваною в іншому випадку. Якщо така інформація виробляється та перевіряється за допомогою одного і того ж секретного ключа, то її називають імітовставкою (у закордонних джерелах використовується термін код аутентифікації повідомлень - Message Authentication Code (MAC) - оскільки крім цілісності може забезпечуватись ще й аутентифікація об'єкта) [9]. Імітовставкою може бути значення хеш-функції, що залежить від секретного ключа, або вихідні дані алгоритму шифрування як зчеплення блоків шифру. На рисунку 1.4 зображено схему обчислення імітовставки.

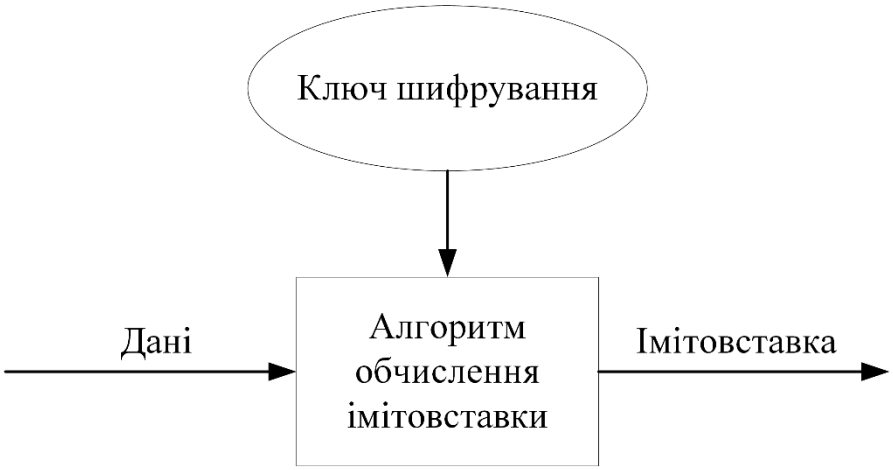

Рисунок 1.4 – Схема обчислення імітовставки

Цілісність даних можна забезпечити і за допомогою їх шифрування симетричним криптографічним алгоритмом за умови, що текст, що підлягає захисту, має деяку надмірність. Це необхідно для того, щоб порушник, не знаючи ключа шифрування, не зміг створити шифрограму, яка після розшифрування успішно пройшла б перевірку цілісності [10].

Надмірності можна досягти багатьма способами. В одних випадках текст може мати достатню природну надмірність (наприклад, у тексті, написаному будь-якою мовою, різні літери та буквосполучення зустрічаються з різною частотою). В інших можна приєднати до тексту шифрування деяке контрольне значення, яке, на відміну від імітівставки та цифрового підпису, не обов'язково має оброблятися криптографічними алгоритмами, може представляти собою просто послідовність заздалегідь визначених символів.

1.7 Забезпечення цілісності інформації на етапі обробки даних

Під час розгляду питання цілісності даних під час обробки використовується інтегрований підхід, заснований на ряді робіт Д. Кларка і Д. Вілсона, а також їх послідовників і опонентів і включає дев'ять теоретичних принципів [10]:

- коректність транзакцій;
- аутентифікація користувачів;

- мінімізація привілеїв;
- розмежування функціональних обов'язків;
- аудит подій, що відбулися;
- об'єктивний контроль;
- управління передачею привілеїв;
- забезпечення безперервної працездатності;
- простота використання захисних механізмів.

Поняття коректності транзакцій передбачає, що користувач не повинен модифікувати дані довільно, а лише певними способами, тобто так, щоб зберігалася цілісність даних.

Другий принцип свідчить, що зміна даних може здійснюватися тільки спеціально автентифікованими для цієї мети користувачами. Цей принцип працює разом із наступними чотирма, із якими тісно пов'язана його участь у загальній схемі забезпечення цілісності.

Мінімізації привілеїв передбачає те, що процеси повинні бути наділені тими і лише тими привілеями, які природно та мінімально необхідні для виконання процесів. Принцип мінімізації привілеїв поширюється і на програми, і на користувачів.

Розмежування функціональних обов'язків має на увазі організацію роботи з даними таким чином, що у кожній з ключових стадій, що становлять єдиний критично важливий, з погляду цілісності, процес, необхідна участь різних користувачів [10]. Це гарантує неможливість виконання одним користувачем всього процесу повністю (або навіть двох його стадій) з тим, щоб порушити цілісність даних.

Аудит подій, включаючи можливість відновлення повної картини того, що сталося, є превентивним заходом щодо потенційних порушників.

Принцип об'єктивного контролю полягає у тому, що контроль цілісності даних має сенс лише тоді, коли ці дані відбивають реальний стан речей. У зв'язку з цим Кларк та Вілсон вказують на необхідність регулярних перевірок, що мають за мету виявлення можливих невідповідностей між даними, що захищаються, і

об'єктивною реальністю, яку вони відображають [10].

Управління передачею привілеїв необхідне для ефективної роботи всієї політики безпеки. Якщо схема призначення привілеїв неадекватно відображає організаційну структуру та не дозволяє легко керувати нею, захист стає обтяжливим та провокує спроби обійти його.

Принцип забезпечення безперервної роботи включає захист від збоїв, стихійних лих та інших форс-мажорних обставин.

Простота використання захисних механізмів необхідна, у тому числі для того, щоб користувачі не прагнули обійти їх через незручності. Простота використання захисних механізмів передбачає, що найбезпечніший шлях експлуатації системи буде також найпростішим, і навпаки, найпростіший — найзахищенішим [8].

1.8 Криптографічні методи забезпечення цілісності інформації

При побудові систем захисту від загроз порушення цілісності інформації використовуються такі криптографічні примітиви:

- цифрові підписи;
- криптографічні хеш-функції;
- коди автентифікації.

Цифровий підпис є механізмом підтвердження справжності та цілісності цифрових документів. Багато в чому вона є аналогом рукописного підпису – зокрема до неї пред'являються практично аналогічні вимоги.

Цифровий підпис повинен дозволяти довести, що саме законний автор і ніхто інший свідомо підписав документ.

Цифровий підпис повинен бути невід'ємною частиною документа. Повинно бути неможливо відокремити підпис від документа та використовувати його для підписування інших документів.

Цифровий підпис повинен забезпечувати неможливість зміни підписаного документа, зокрема і самим автором.

Факт підписування документа має бути юридично доведеним. Має бути неможливим відмова від авторства підписаного документа.

У найпростішому випадку для реалізації цифрового підпису може бути використаний механізм, аналогічний до асиметричної криптосистеми. Різниця полягатиме в тому, що для зашифрування (що є в даному випадку підписуванням) буде використаний секретний ключ, а для розшифрування, що відіграє роль перевірки підпису, загальновідомий відкритий ключ.

На рисунку 1.5 зображено принцип роботи підписування документа та перевірки підпису. Алгоритм підписання документа, поданий на малюнку наступній:

- підписуючий зашифровує документ закритим (секретним) ключем, далі зашифрована копія поширюється разом із оригіналом документа у вигляді цифрового підпису;
- одержувач використовує загальнодоступний відкритий ключ підписувача та розшифровує підпис, порівнює його з оригіналом та переконується у справжності підпису.

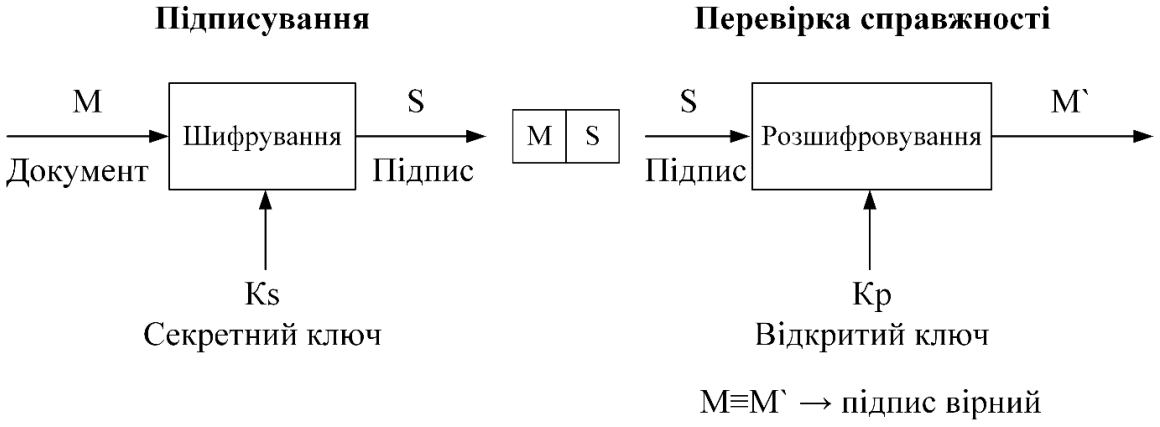

Рисунок 1.5 – Принцип роботи підписування документа та перевірки підпису

Криптографічні хеш-функції. Функція виду y=f(x) називається криптографічної хеш-функцією, якщо вона задовольняє наступні властивості [7]:

- на вхід хеш-функції може надходити послідовність даних довільної довжини, результат (хеш, що називається, або дайджест) має фіксовану довжину;
- значення y за наявним значенням x обчислюється за поліноміальний час, а значення x за наявним значенням y майже у всіх випадках обчислити неможливо;
- обчислювально неможливо знайти два вхідних значення хеш-функції, що дають ідентичні хеш;
- при обчисленні хешу використовується вся інформація вхідної послідовності;
- опис функції є відкритим та загальнодоступним;

Можна підписувати не весь документ, як у першому випадку, а лише його хеш. Тоді збережеться обсяг даних, що пересилаються. Принцип такої реалізації наведено на рисунку 1.6.

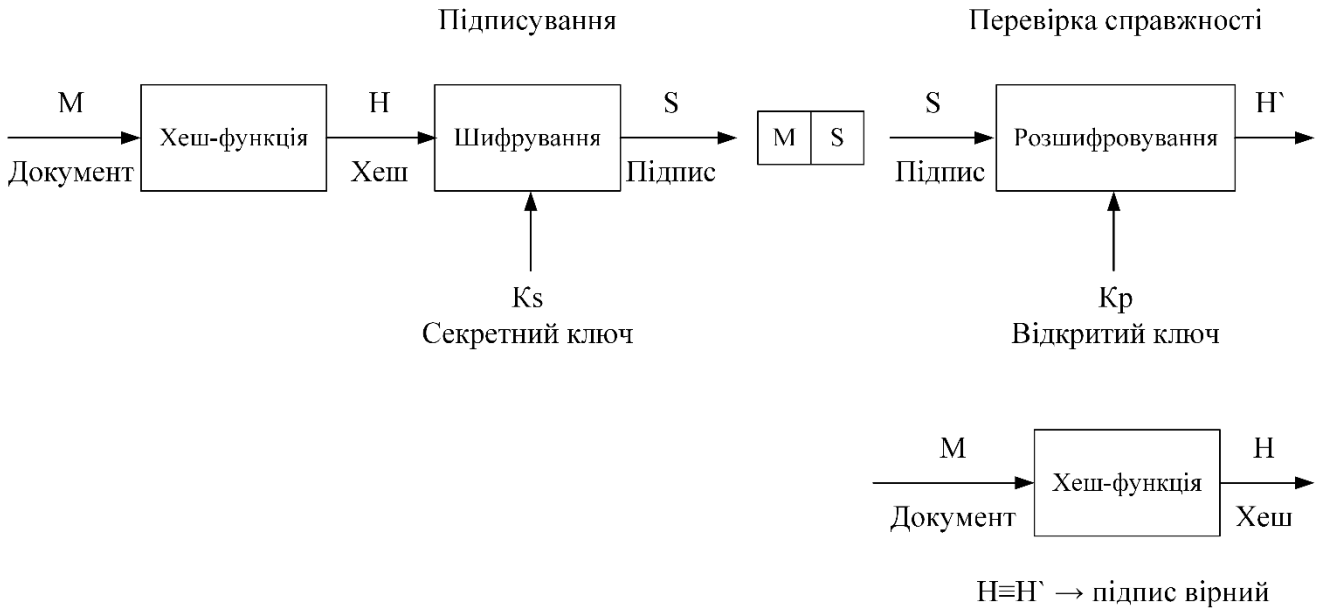

Рисунок 1.6 - Принцип роботи підписування хешу документа та перевірки підпису

Якщо підписати хеш замість вихідного повідомлення, результат буде передаватися разом з вихідним повідомленням. Одержувач розшифрує підпис і порівняє отриманий результат з хешем повідомлення. Якщо результат збігається, то можна впевнено вважати, що підпис є дійсним.

Коди автентифікації. Часто криптографічні хеш-функції використовуються як засоби контрольного підсумовування: наприклад, для деякого файлу, розміщеного в публічному доступі на ftp-сервері, може бути наведений його хеш, підрахований з використанням деякого алгоритму [10]. У цьому випадку користувач, який завантажив файл, може переконатися в його автентичності,

Однак у цьому випадку зловмисник може підмінити файл і привести хеш, який відповідає новому файлу – виявити подібні маніпуляції, використовуючи звичайні хеш-функції, неможливо. Захист від таких атак забезпечується шляхом застосування кодів перевірки автентичності.

Коди автентифікації, або MAC-коди, є криптографічні хеш-функції, для обчислення яких необхідно знати секретний ключ. Використання ключа дозволяє гарантувати неможливість підміни об'єктів, що захищаються, аналогічною наведеній вище: зловмисник, який не знає секретного ключа, не зможе перерахувати хеш для нового файлу [10].

Як коди автентифікації часто використовуються модифікації симетричних криптографічних систем.

Отже, криптографічні методи не забезпечують цілісність інформації, вони забезпечують лише контроль цілісності. Якщо буде розкрито спотворення інформації, то джерелу необхідно повторно передавати повідомлення і повторювати цей процес доти, доки цілісність інформації не буде підтверджено. У цьому випадку між користувачами доведеться організувати канали зв'язку для зворотної та повторної передачі повідомлень. Їм потрібно буде виконувати багаторазове повторення передачі та прийому інформації, що значно збільшує час затримки обміну даними між користувачами. Таким чином, цей підхід забезпечення цілісності інформації обмежений для інформаційних систем, у яких необхідно здійснювати оперативний обмін даними.

1.9 Висновки до розділу

В першому розділі порушено проблему інформаційної безпеки лабораторії

віддаленого доступу, що є актуальним дослідження у зв'язку з поширенням використання таких технологій у сучасному освітньому процесі. Проаналізовано архітектуру типової системи віддаленого доступу до лабораторії та виявлено найбільш вразливі та критичні місця. Проведено аналіз причин порушення інформаційної безпеки системи лабораторії віддаленого доступу і виділено три основні напрямки захисту:

- порушення конфіденційності;
- порушення цілісності;
- порушення доступності.

Цілісність інформації – це базовий параметр захисту інформації, без якого неможливо досягнути захищеності системи в цілому. Можна зробити висновок, що порушення цілісності інформації є одним з найбільш небезпечних впливів на всі системи, включаючи критичні. Проаналізувавши загрози цілісності інформації, було виявлено, що є внутрішні та зовнішні порушники, які становлять загрозу цілісності даних на етапах зберігання, передачі та обробки інформації.

В загальному вигляді методи забезпечення цілісності інформації можна представити на рисунку 1.7.

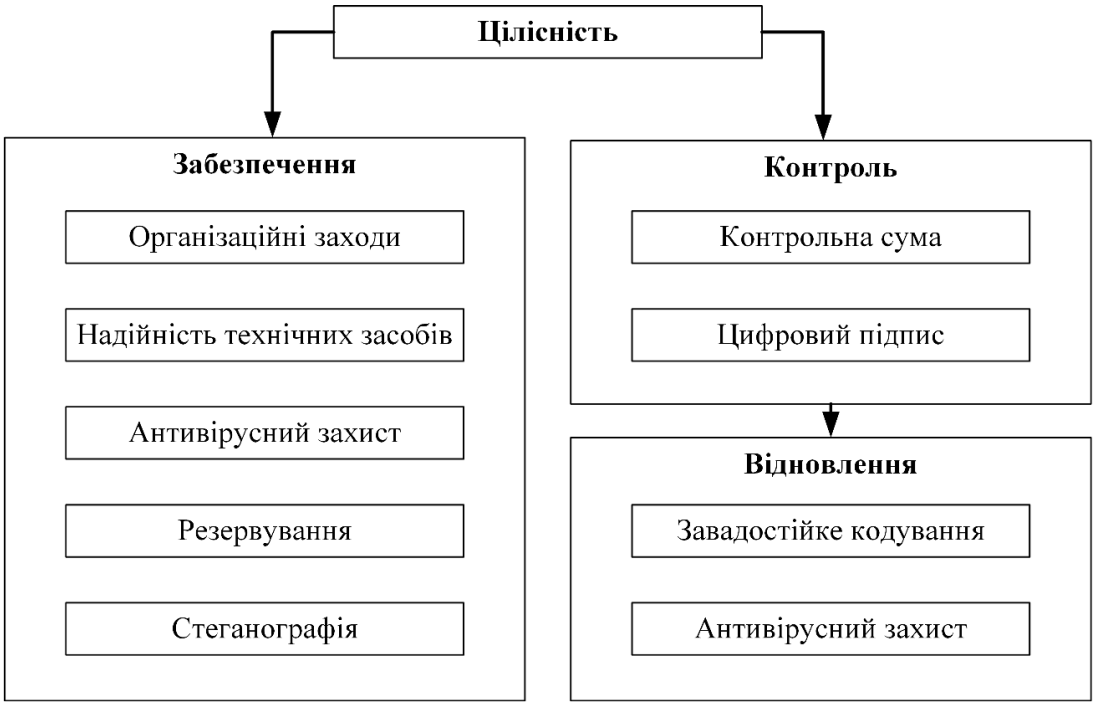

Рисунок 1.7 – Методи забезпечення цілісності інформації

Проведений аналіз базових методів забезпечення цілісності інформації, виявив, що цілісність інформації передбачає комплекс заходів з забезпечення, контролю та відновлення інформації у разі потреби.

Для перевірки цілісності даних, що зберігаються на віддалених серверах, пропонуються різні протоколи доказу володіння даними. В них виділяють дві основні проблеми: значні обсяги даних виключають використання звичайних алгоритмів хешування; перевірка цілісності може бути застосована лише після реалізації додаткових вимог, які збільшують складність. Правильно спроектовані методи перевірки повинні задовольняти такі умови: навантаження локальних обчислень для перевірки цілісності має бути менше, ніж для вихідного віддаленого обчислення; повинна бути можливість проводити перевірку на будь-якій із складових частин для забезпечення відмовостійкості.

Розглянуті підходи криптографічного контролю інформації, що забезпечують контроль цілісності даних. Використання цифрових підписів дозволяє переконатися, що інформація змінювалася лише уповноваженими особами. Але у цьому випадку необхідно ввести додатковий контроль за зберіганням носія цифрового підпису.

Всі зазначені методи мають свої переваги та недоліки і щоб досягти стану максимальної захищеності цілісності інформації лабораторії віддаленого доступу, необхідно розробити комплексну методику захисту. Застосування декількох підходів одразу значно підвищить надійність цілісності інформації у системі лабораторії віддаленого доступу.

2 ПОСТАНОВКА ДОСЛІДНИЦЬКОГО ЗАВДАННЯ ТА ВИЗНАЧЕННЯ ПАРАМЕТРІВ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ДАНИХ ЛАБОРАТОРІЇ ВІДДАЛЕНОГО ДОСТУПУ

Необхідною умовою високої якості навчання з технічних дисциплін є проведення лабораторних робіт та експериментів, що максимально відповідають реальним умовам. Використання програм-емуляторів дозволяє значно розширити кількість та складність досліджуваних пристроїв. Однак такі програми не можуть повністю замінити експерименти із реальним обладнанням, оскільки не враховують всіх особливостей модельованих елементів та їх взаємодії. Внаслідок цього більш суттєвою стає ймовірність отримання недостовірних результатів роботи обладнання і, як наслідок, формування невірного уявлення про предмет вивчення. Через це доречним буде використання віддаленого доступу до реальних навчальних лабораторій, де вже встановлене необхідне промислове обладнання та програмне забезпечення.

У процесі свого функціонування такий вид організації роботи може піддаватись ряду негативних впливів випадкового та навмисного характеру, що в результаті може призвести до порушення інформаційної безпеки не лише системи лабораторії віддаленого доступу, а й усієї інформаційної мережі навчального закладу. Такі порушення несуть загрозу для всіх учасників навчального процесу. Відповідно, для зниження шкоди від подібних впливів та запобігання ризикам інформаційної безпеки необхідно застосовувати спеціалізовані засоби та механізми захисту і особливу увагу приділити забезпеченню цілісності даних, адже захист інформації від несанкціонованої зміни має одне з пріоритетних значень. Цим обумовлена актуальність дослідження моделей захисту даних та вибору тих, які можна вдало адаптувати для обраного виду системи.

Метою кваліфікаційної роботи магістра є дослідження методів і моделей

захисту цілісності даних лабораторії віддаленого доступу і в подальшому формування списку рекомендацій для протидії можливим інформаційним загрозам цілісності даних.

Завданням роботи є дослідження загальноприйнятих принципів забезпечення захищеності цілісності даних і можливості їх безпосереднього застосування для захисту лабораторії віддаленого доступу. Ще одним важливим аспектом дослідження є формування основних видів загроз та моделей порушників цілісності даних, а також аналіз вразливих частин системи лабораторії віддаленого доступу. Це дозволить зробити висновки про доцільні засоби захисту даних для досягнення оптимального рівня захищеності лабораторії. За результатами проведених досліджень можна визначити перелік оптимальних рекомендацій та алгоритм захисту цілісності даних лабораторії віддаленого доступу.

Для проведення дослідження були обрані методи, в основі яких лежить теорія захисту інформації та принципи побудови моделей інформаційної безпеки. Для їх реалізації використано структурно-функціональне моделювання, теорія множин, математична логіка та теорія графів. Для побудови моделі загроз була використана методологія об'єктно-орієнтованого проектування.

2.1 Вимоги до захищеності даних лабораторії віддаленого доступу

Інформаційні ресурси будь-якого навчального закладу включають документальні та інформаційні потоки для забезпечення навчального та наукового процесів. До них належать робочі плани спеціальностей, робочі програми дисциплін, навчальні графіки. відомості про контингент вузу, накази та розпорядження ректора університету та деканів факультетів, електронний каталог бібліотеки, електронні журнали та інші повнотекстові бази даних, як створювані на місці, так і придбані. Сукупність інформаційних ресурсів, поряд із висококваліфікованим персоналом є однією із складових успішного функціонування вищого навчального закладу. Усі матеріали, підготовлені навчальним закладом, пов'язані із забезпеченням навчального процесу, є

службовими, і вимагають особливого звернення. Частина не підлягає розголошенню, інші матеріали вимагають спеціального режиму використання. Це підтверджує, що у ВНЗ, циркулює інформація різного рівня доступу та функціонального наповнення. Цю інформацію можна розділити на два основних типи з точки зору регламентації поширення та використання: загальнодоступна інформація та інформація обмеженого поширення. На рисунку 2.1 представлена класифікація інформації за типом регламентації поширення та використання.

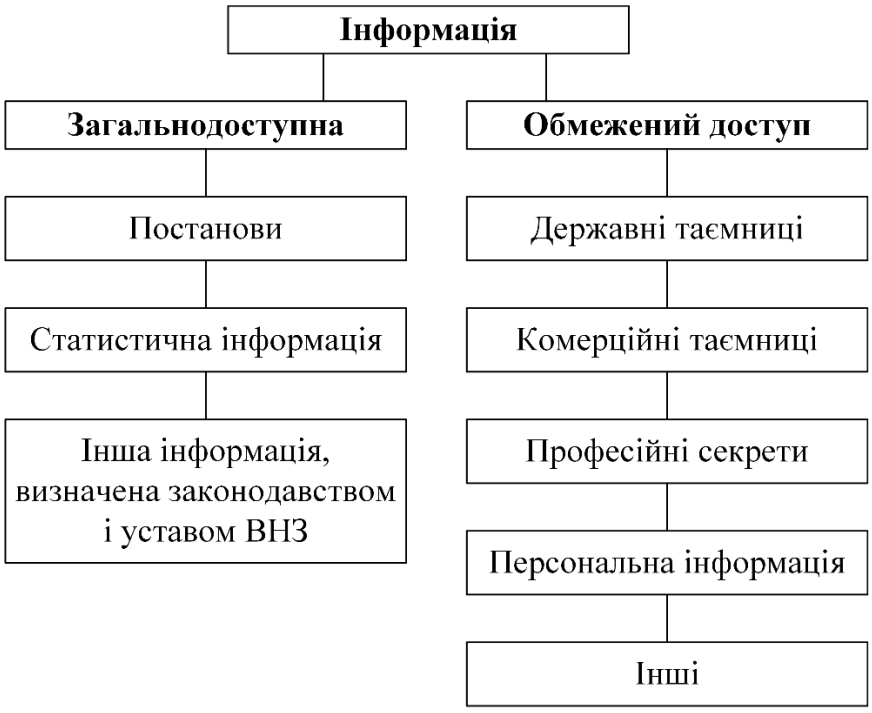

Рисунок 2.1 – Класифікація інформації за типом регламентації поширення та використання

Під загальнодоступною інформацією розуміється інформація, що збиралась, створювалась та зберігається навчальним закладом і, яка не становить державної або іншого виду таємницю, визначену законодавством, або статутом ВНЗ. До неї можна віднести: навчальні розклади, методичні рекомендації та ін.

До інформації обмеженого доступу належить інформація, визначена законодавством чи статутом навчального закладу, як інформація обмеженого доступу. До цього типу можна віднести наступні види інформації.

Державна таємниця. ВНЗ, володіють значним обсягом інформації, що відноситься до передових напрямів науки і техніки, що використовується як під час підготовки фахівців, так і при виконанні науково-дослідних робіт, значна частина яких фінансувалася, і фінансується нині державою. Серед цього потоку інформації існує значна кількість відомостей, що становлять державну таємницю, розголошення яких може завдати шкоди державним інтересам. Поводження з цими даними вимагає особливого режиму, що виключає допуск сторонніх осіб. Права та обов'язки учасників інформаційних процесів при роботі зі відомостями, що становлять державну таємницю, регламентуються законом «Про державну таємницю».

Комерційна таємниця - існує ціла низка відомостей, що не є державними секретами, пов'язаними з виробництвом, технологією, управлінням, фінансами, іншою діяльністю господарюючого суб'єкта, розголошення яких (передача, витік) може завдати шкоди його інтересам. Такі відомості прийнято називати службовою та/або комерційною таємницею.

Професійні секрети - секрети, пов'язані з організацією навчальних процесів.

Персональні дані – під персональними даними розуміється будь-яка документована та/або занесена на машинні носії інформація, що відноситься до конкретної людини або яка може бути ототожнена з конкретною людиною. Це інформація про студентів, про викладачів, партнерів та інших.

Доступ до загальнодоступної інформації є відкритим та її використання не може завдати шкоди інформаційній системі. Що ж до інформації обмеженого доступу, то доступ до неї має бути суворо регламентований. Тобто має бути чітко встановлено, де, ким, у якому обсязі та яких умовах може бути здійснено використання цієї інформації. Дане розмежування має обумовлюватися тим, що користувачі інформаційної мережі навчального закладу і зокрема лабораторії мають різні професійні інтереси та рівень підготовки під час роботи з різною інформацією. Це викладачі, зайняті постановкою нових лекційних курсів, лабораторних та дослідницьких практикумів; наукові співробітники, які ведуть дослідницькі та проектні розробки; співробітники офісних служб ВНЗ, навчального

та науково-дослідного відділів, деканатів, бібліотеки тощо, а також студенти.

З цього випливає, що інформація обмеженого доступу повинна піддаватися захисту від впливу різних подій, явищ як внутрішніх так і зовнішніх, здатних в тій чи іншій мірі завдати шкоди цій інформації.

Для протидії актуальним для лабораторії віддаленого доступу загрозам та утримання ризиків в межах допустимого, використовуються різні механізми та засоби захисту інформації, організаційно-правового, технічного та програмного характеру, які повинні необхідно враховувати низку особливостей пов'язаних із процесом їх функціонування системи лабораторії віддаленого доступу:

- міжмережні екрани та застосування SSL не завжди забезпечують захист від злому системи лабораторії віддаленого доступу оскільки, доступ до веб-сайту із зовнішніх мереж має бути завжди відкритий;
- система лабораторії віддаленого доступу часто має прямий доступ до даних, що обробляються в інформаційній мережі навчального закладу: бази даних, інформація про інноваційні розробки та наукової діяльності ВНЗ, навчальні відомості, персональні дані та ін;
- оскільки, лабораторії віддаленого доступу є вузькоспрямованими, та передбачають власну розробку навчальним закладом, вони більше сприйнятливі до атак, оскільки не піддаються такому тривалому тестуванню та експлуатації, як загальнодоступні відомі комерційні системи дистанційної освіти;
- традиційні засоби захисту не призначені для відображення спеціалізованих атак на веб-додатки системи віртуальної лабораторії, тому зловмисники за допомогою браузерів легко проходять через периметр інформаційної мережі навчального закладу та отримують доступ до внутрішніх систем та серверів;
- ручне виявлення та усунення вразливостей у системі лабораторії віддаленого доступу часто не дає позитивних результатів - розробники можуть знаходити та виправляти сотні вразливостей у коді, але зловмиснику для проведення результативної атаки достатньо виявити лише одну.

З цього можна зробити висновок, що забезпечення захисту лабораторії віддаленого доступу має здійснюватися як на етапі проектування та розробки самої

системи, шляхом створення безпечного коду, так і в процесі його експлуатації із внесенням у разі потреби своєчасних коригувань. Бо навіть якщо у програмному коді вразливостей немає, необхідний комплексний захист, що враховує наявність бази даних, веб - додатку лабораторії віддаленого доступу, сервера та інших елементів IT-платформи навчального закладу.

2.2 Вхідні дані та очікувані результати захисту лабораторії віддаленого доступу

Основна інформація для захисту даних лабораторії віддаленого доступу:

- Відомості про архітектуру системи лабораторії віддаленого доступу;
- Відомості про мережеві підключення лабораторії віддаленого доступу;
- Відомості про інформаційні ресурси і компоненти системи лабораторії віддаленого доступу;
- Відомості про вразливості систем та мереж лабораторії віддаленого доступу;
- Відомості про типи внутрішніх і зовнішніх користувачів;
- Категорії та види можливих порушників інформаційної безпеки;
- Моделі загроз та атак на лабораторію віддаленого доступу;
- Відомості про рівень значущості інформаційних ресурсів і компонентів.

Завдяки переліку вимог до функціонування системи захисту даних лабораторії віддаленого доступу і необхідних вхідних даних, можна зробити висновки про очікувані результати від дослідження.

На рисунку 2.2 представлена структура дослідницького завдання з захищеності даних лабораторії віддаленого доступу.

Рисунок 2.2 – Структура дослідницького завдання

В результаті виконання дослідницького завдання можна очікувати сформовану модель оцінки захищеності даних лабораторії віддаленого доступу, що дозволить говорити про те, чи є функціональною існуюча система захисту даних і яким чином сформована за результатами дослідження модель може покращити рівень захисту. Перелік сформованих рекомендацій зможе забезпечити оптимальний рівень захисту і адаптованість конкретно під особливості загроз інформації лабораторії віддаленого доступу.

2.3 Висновки до розділу

Другий розділ присвячений постановці дослідницького завдання. Нині сформувалося стійке ставлення до інформації всіх видів, як цінного ресурсу. Тому

особлива увага має приділятися проблемам формування, використання та захисту інформаційних ресурсів на основі застосування інформаційних та комунікаційних технологій. У кваліфікаційній роботі досліджується захист даних в інформаційній системі навчального закладу та лабораторії віддаленого доступу. Особливу увагу необхідно приділити аспекту цілісності інформації і дослідити засоби його захисту у комплексній системі забезпечення інформаційної безпеки. Надійний захист забезпечується лише за умови аналізу джерел загроз, зіставляння їм вразливостей системи та визначати потенційних загроз, реалізація яких прямо чи опосередковано може завдати шкоди інформаційній системі навчального закладу і лабораторії віддаленого доступу. Можна зробити висновок, що при формуванні політики інформаційної безпеки лабораторії віддаленого доступу, повинний здійснюватися комплексний підхід до захисту усієї інформаційної системи лабораторії, а також інформаційної мережі навчального закладу. Комплексний підхід передбачає використання єдиної сукупності законодавчих, організаційних та технічних заходів, спрямованих на виявлення, відображення та ліквідацію різних видів загроз інформаційній безпеці.

Сформована структура дослідницького завдання дозволяє чітко виділити необхідні вхідні дані, що є основою інформаційного захисту лабораторії віддаленого доступу, а три основні напрямки захисту допомагають сформулювати вимоги до захисту даних та зрозуміти, на які результати можна очікувати за результатами виконання кваліфікаційної роботи.

3 МОДЕЛІ ІНФОРМАЦІЙНИХ ЗАГРОЗ ЛАБОРАТОРІЇ ВІДДАЛЕНОГО ДОСТУПУ

На основі "Методики визначення загроз безпеці інформації в інформаційних системах"[11], що описує порядок моделювання та визначення актуальності загроз безпеці інформації, можна описати поетапно порядок моделювання загроз інформаційної безпеки лабораторії віддаленого доступу, що представлено на рисунку 3.1.

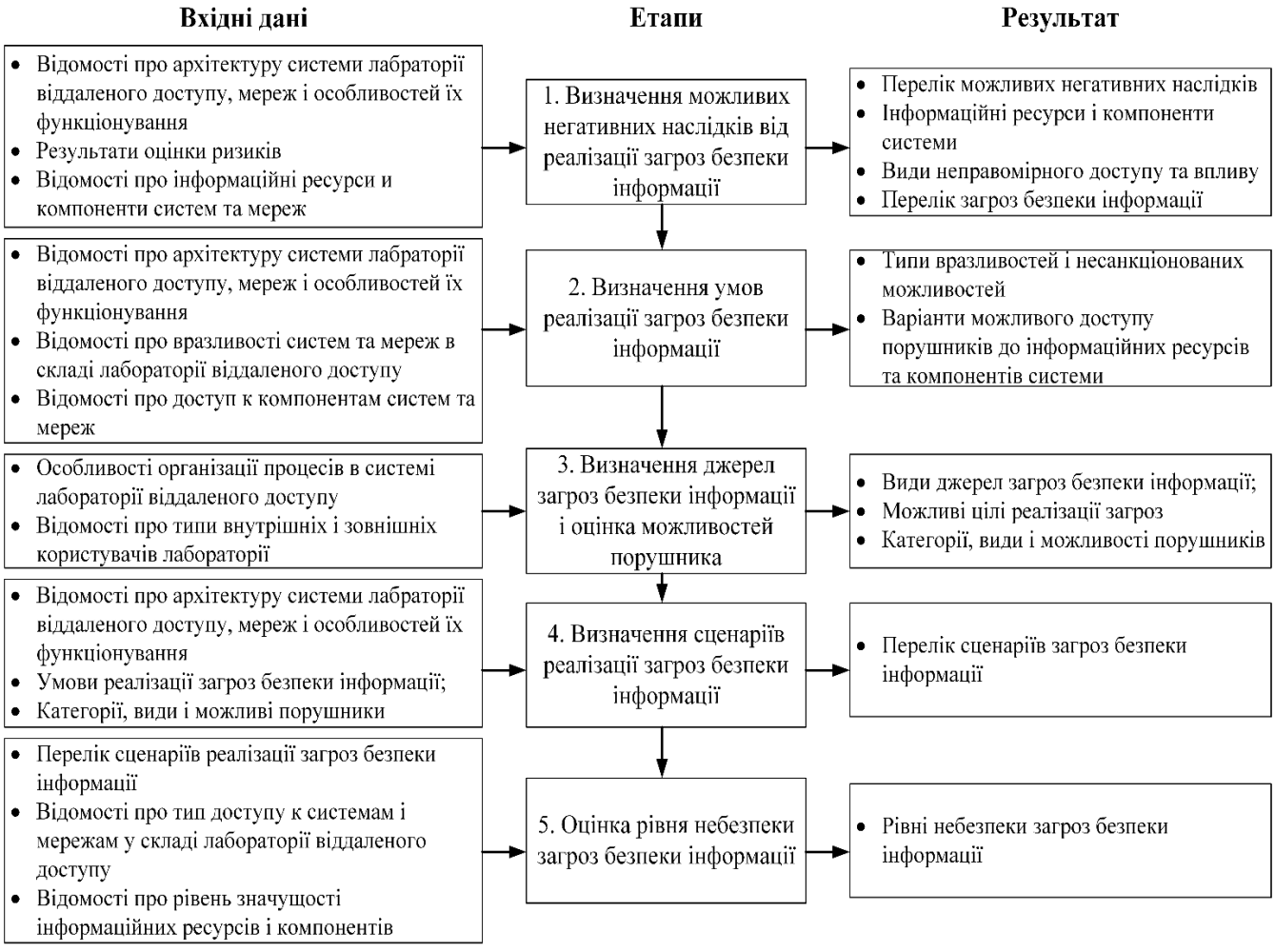

Рисунок 3.1 – Порядок моделювання загроз інформаційної безпеки лабораторії віддаленого доступу

На першому етапі пропонується визначити всі можливі негативні наслідки від реалізації загроз безпеці. Допомагати в цьому повинна або проведена раніше оцінка шкоди (ризиків) від порушення основних критичних процесів, або експертна оцінка, або інформація, що отримується від підрозділів, що експлуатують інформаційну систему.

За будь-якого обраного підходу необхідно визначити інформаційні ресурси, що забезпечують виконання критичних процесів (безпосередньо інформація, програмно-апаратні засоби, засоби захисту інформації та інші) та основні види неправомірного доступу по відношенню до кожного з ресурсів.

На другому етапі необхідно визначити наявність потенційних вразливостей та їх типи, наявність несанкціонованих можливостей в інформаційних системах, а також необхідність доступу до системи для реалізації кожної загрози безпеці.

Як основний метод виявлення потенційних вразливостей в інформаційній системі на етапі її експлуатації є тестування на проникнення, яке проводиться у тому числі з урахуванням функціональних можливостей та налаштувань засобів захисту.

Наступним, третім етапом є визначення порушників безпеки та оцінка їх можливостей. Як джерела загроз пропонується розглядати як антропогенні, так і техногенні: перші розглядаються абсолютно для всіх інформаційних систем, тоді як другі – тільки для тих систем, для яких пред'являються вимоги до стійкості та надійності функціонування.

Підхід до визначення можливих антропогенних джерел загроз – порушників – є стандартним і полягає у виявленні конкретних видів порушників, їх потенціалу та можливостей при реалізації загроз щодо інформаційної системи, що захищається. Варто зазначити, що за наявності зв'язку інформаційної системи з Інтернетом зовнішній порушник як мінімум з низьким потенціалом завжди розглядається як актуальне джерело загроз.

На заключному етапі здійснюється аналіз можливих тактик та технік реалізації загроз.

За визначення актуальності загрози безпеці інформації відповідають етапи з

першого до четвертого. Загроза безпеці буде актуальною за наявності хоча б одного сценарію її реалізації і якщо її реалізація призведе до якихось негативних наслідків для власника інформації.

Мета п'ятого етапу – визначити небезпеку кожної із актуальних загроз. Дана характеристика має виключно інформаційний характер і не має прямого впливу ні на підсумковий документ, який формується за результатами моделювання, ні на можливі варіанти нейтралізації загрози. Цей параметр повинен використовуватися для визначення черговості закриття загрози.

3.1 Моделі загроз інформаційній безпеці на основі методології об'єктно-орієнтованого проектування

Враховуючи складну об'єктну структуру інформаційної системи лабораторії віддалено доступу, а також багатогранність понять інформаційної безпеки для опису моделей загроз інформаційної безпеки доцільно залучати методологію об'єктно-орієнтованого проектування, реалізовану мовою моделювання UML, яка часто використовується при розробці проекту інформаційних систем. Моделі, що реалізуються у вигляді діаграм мови UML, дозволяють візуально уявити структуру складних об'єктів та процесів з необхідного ракурсу та ступенем деталізації. Оскільки модель загроз інформаційної безпеки вимагає розгляду питання у кількох розрізах (наприклад, порушники, активи, що захищаються), то використання такої методології є найбільш успішною.

У рамках цього дослідження створювалася об'єктно-орієнтована модель загроз для інформаційної системи лабораторії віддаленого доступу, що має такі характеристики:

- система розподілена, функціонує на базі сервера додатків, клієнтська частина системи реалізована у вигляді веб-додатка;
- доступ до системи мають лише працівники навчального закладу;
- система має безперебійно функціонувати протягом усього робочого дня;
- вкрай небажаний витік інформації, що обробляється в інформаційній системі.

У процесі проектування системи інформаційної безпеки лабораторії віддаленого доступу було сформульовано нефункціональні та функціональні вимоги. Функціональні вимоги представлені сценаріями захисту інформаційної системи у межах кожної з актуальних загроз. Нефункціональні вимоги описують організаційні та технічні характеристики системи інформаційної безпеки, які належать до якісних її характеристик та не описуються сценаріями.

Для опису розглядаються два типи джерел загроз: внутрішній користувач системи лабораторії віддаленого доступу, зовнішній користувач (зловмисник, який не має санкціонованого доступу до системи). За наявності розгорнутої класифікації джерел загроз доцільно сформувати діаграму класів, де можна буде простежити типи зв'язків відповідних об'єктів.

Критично важливі активи були зазначені в вимогах до системи. Це цілісність системи, доступність системи та конфіденційність даних. Для кожного з активів було визначено актуальні загрози безпеці інформаційної системи, які разом з джерелами загроз представлені на діаграмі варіантів використання (Use Case Diagram).

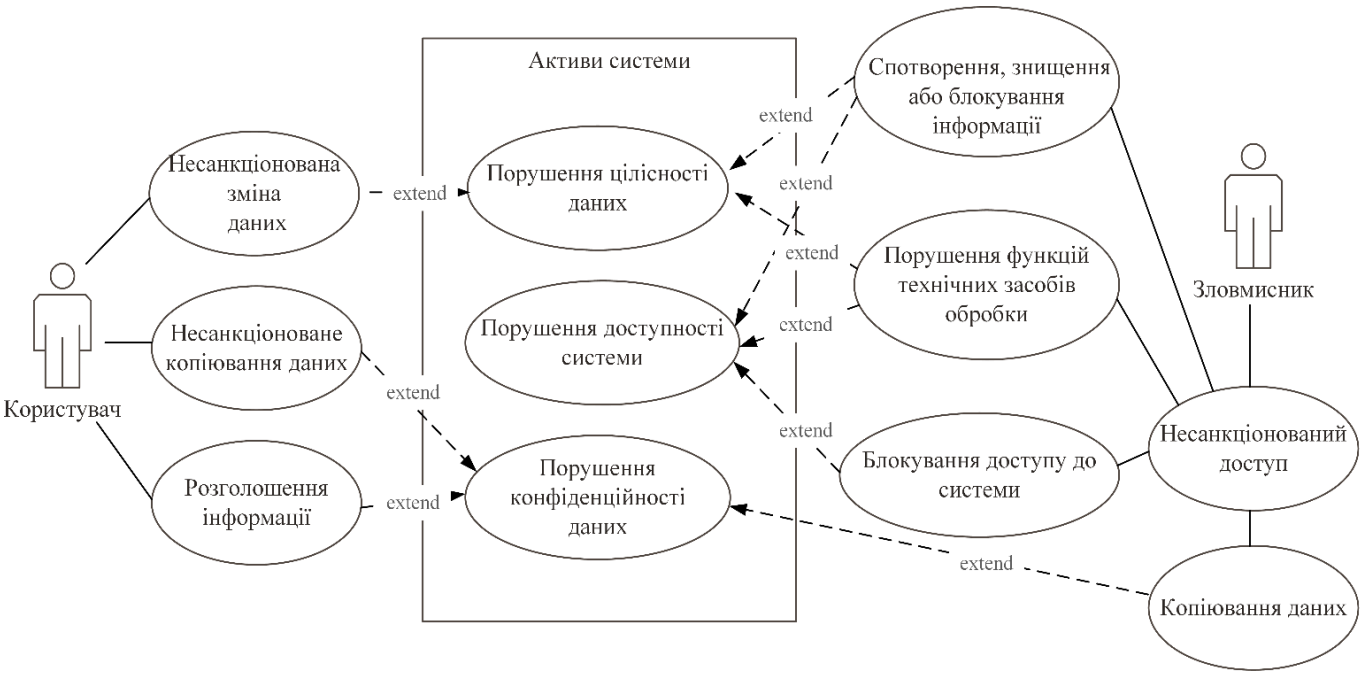

Рисунок 3.2 - Діаграма варіантів використання. Концептуальні моделі загроз

Подана на малюнку 3.2 діаграма визначає варіанти реалізації загроз за всіма активами інформаційної системи та за всіма джерелами загроз. У цьому сенсі ця модель є концептуальною моделлю загроз. Способи реалізації описаних за допомогою прецедентів загроз – це погляд на окрему загрозу. Об'єктна методологія UML дає змогу проводити декомпозицію об'єктів, представлених на діаграмах. В цьому випадку способи реалізації – це також загрози, що розширюють вихідні. Відповідно, вони мають бути пов'язані відношенням успадкування у діаграмах декомпозиції (Use Case Composite Diagram). Приклад опису способу реалізації загрози «несанкціонований доступ» наведено на рисунку 3.3.

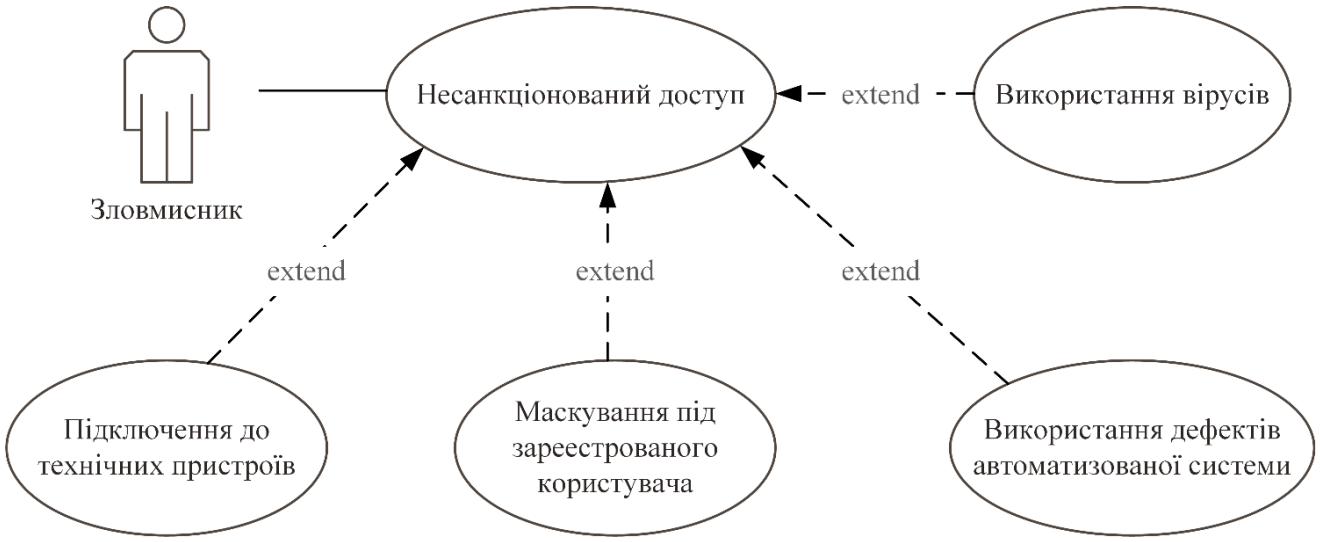

Рисунок 3.3 - Способи реалізації загрози "Несанкціонований доступ"

Для перегляду загроз, спрямованих на кожен окремий актив, доцільно використати діаграму взаємодії (Communication Diagram). Отримана діаграма визначає зв'язок між об'єктами системи. На рисунку 3.4 такими об'єктами є користувач, порушник та цілісність інформації, що пов'язані прецедентами.

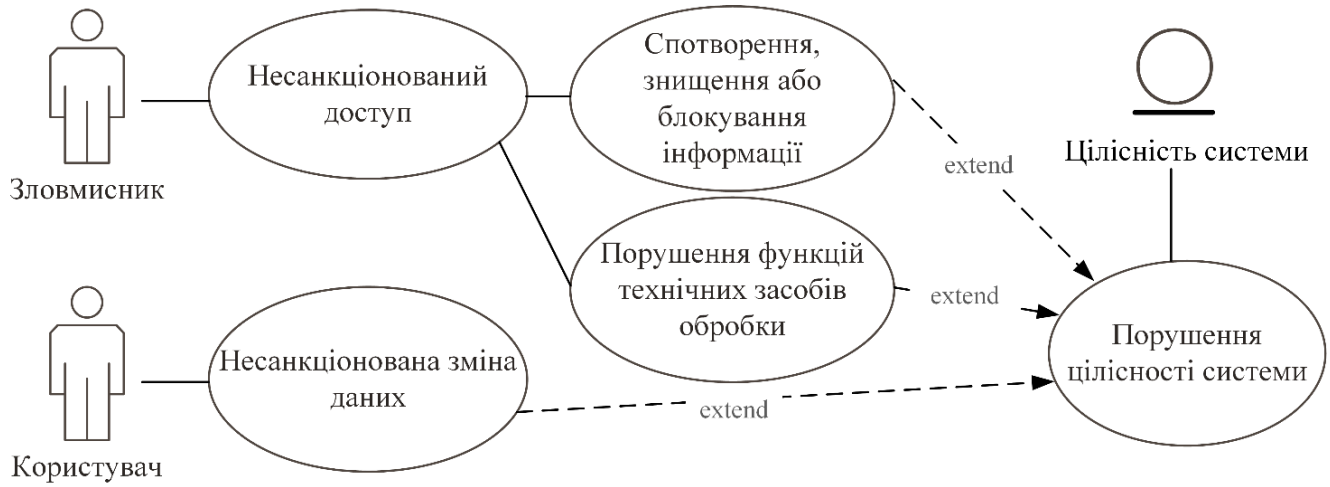

Рисунок 3.4 – Діаграма взаємодії. Загрози цілісності системи

Таким чином, візуалізація моделі загроз використовує діаграму варіантів використання (концептуальну модель), яка деталізується: – за межами інформаційної безпеки (активами системи – цілісність, доступність, конфіденційність) – за допомогою діаграми взаємодії; - За способами реалізації загроз - за допомогою дочірньої діаграми варіантів використання. Остання може використовуватися при розподілі загроз за заходами на них (програмні, технічні та організаційні).

3.2 Моделювання загрози «Несанкціонована зміна даних»

Для кожної загрози можлива побудова двох сценаріїв:

- сценарій реалізації загроз;
- сценарій захисту від загрози.

Сценарій реалізації загрози можна розглядати як поточний стан інформаційної безпеки. У термінах моделювання бізнес-процесів така ситуація описується терміном As – Is (як є). Приклад реалізації загрози «Несанкціонована зміна даних» наведено на малюнку 3.5. Такий сценарій описує ситуацію, коли користувач системи, що здійснив вхід до системи, може виконати будь-які дії щодо зміни даних, надані йому інтерфейсом системи. Таким чином, з боку системи відсутній контроль доступності операції для користувача, можливість її виконання

відповідно до посадових обов'язків, рівня доступу і т.д. Наслідком такої відсутності контроля та повноважень користувача може бути загроза інформаційній безпеці.

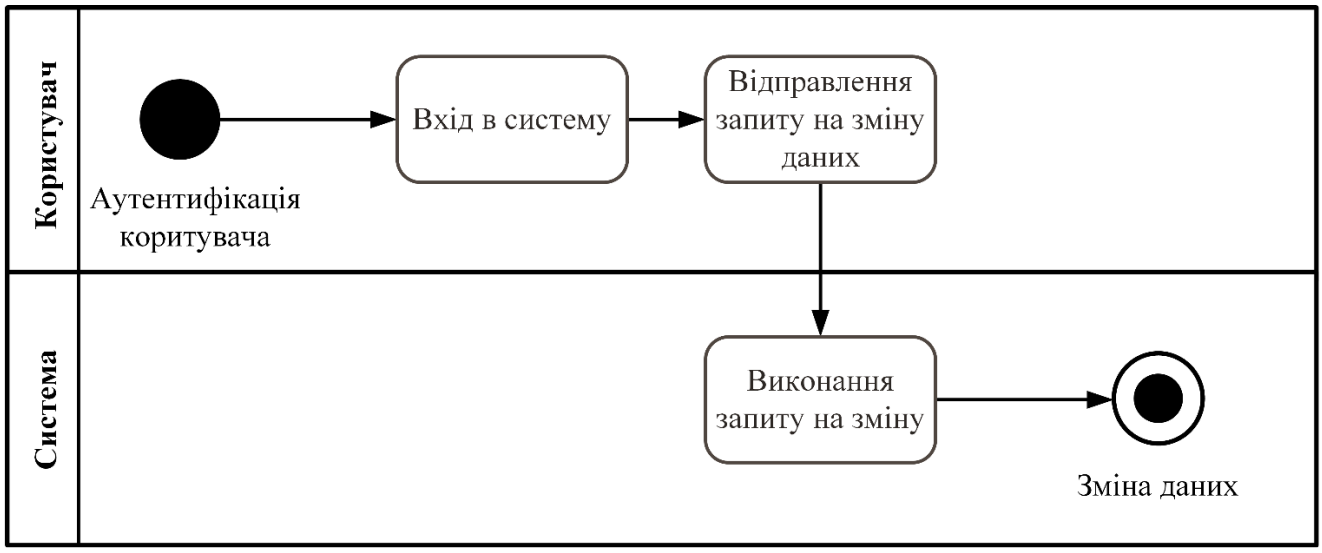

Рисунок 3.5 – Сценарій реалізації загрози «Несанкціонована зміна даних»

Для вдосконалення системи забезпечення інформаційної безпеки у випадку небезпеки «Несанкціонована зміна даних» необхідно розробити і описати модель сценарію To - Be (як має бути), що представлена у четвертому розділі. Така модель протидії дозволить підвищити рівень інформаційного захисту і не допустити несанкціонованої зміни даних.

3.3 Функціональна модель процесів порушення цілісності інформації лабораторії віддаленого доступу

Перший рівень функціональної моделі процесів порушення цілісності інформації лабораторії віддаленого доступу відповідає першому рівню декомпозиції цільової функції $F^{(0)}$ - «Порушення цілісності інформації сегмента лабораторії віддалено доступу». Перший рівень функціональної моделі процесів порушення цілісності інформації сегмента лабораторії віддаленого доступу зображено на рисунку 3.6.

На даному рівні виділяються наступні підфункції.

$F_1^{(1)}$ – «Умисне спотворення інформації сегменту лабораторії віддаленого доступу» та $F_2^{(1)}$ – «Ненавмисне спотворення інформації сегменту лабораторії віддаленого доступу».

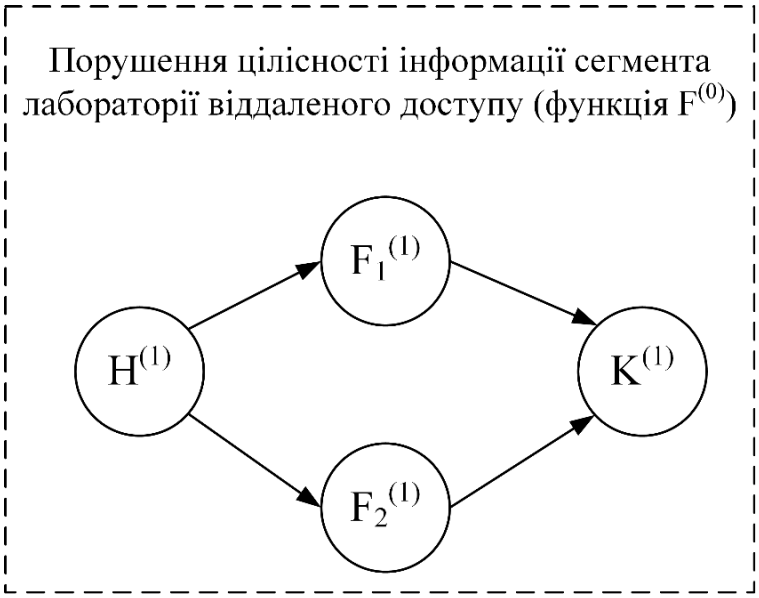

Рисунок 3.6 – Перший рівень функціональної моделі процесів порушення цілісності інформації сегмента лабораторії віддаленого доступу

Умисне спотворення інформації сегмента лабораторії віддаленого доступу зображено на рисунку 3.7.

Функція $F_1^{(1)}$ реалізується за допомогою наступних підфункцій.

$F_{11}(2)$ – аналіз захищеності сегмента лабораторії віддаленого доступу. $F_{12}^{(2)}$ – підбір паролів до компонентів обмеження доступу механізмів захисту від несанкціонованого доступу сегмента лабораторії віддаленого доступу. $F_{13}^{(2)}$ – використання хибного довіреного суб'єкта доступу сегмента лабораторії віддаленого доступу; $F_{14}^{(2)}$ – аналіз інформації, що проходить через впроваджений довірений суб'єкт сегмента лабораторії віддаленого доступу; $F_{15}^{(2)}$ – несанкціоноване маніпулювання інформацією сегмента лабораторії віддаленого доступу.

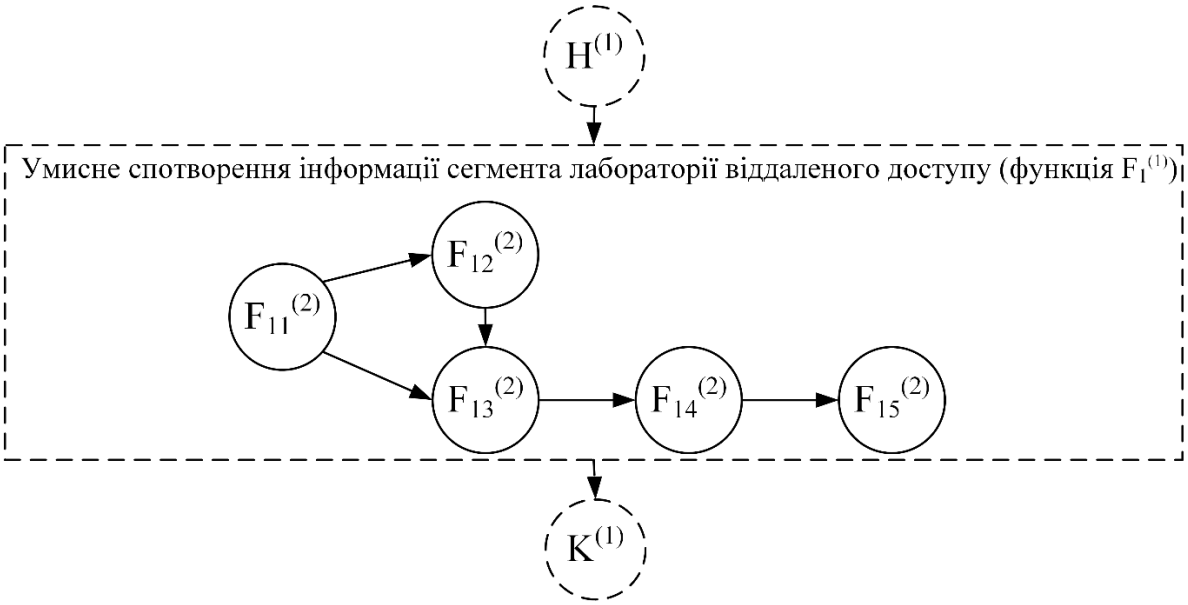

Рисунок 3.7 – Умисне спотворення інформації сегмента лабораторії віддаленого доступу

На рисунку 3.8 зображено неумисне спотворення інформації сегмента лабораторії віддаленого доступу. Функція $F_2^{(1)}$ реалізується такими підфункціями: $F_{21}^{(2)}$ – збій у сегменті лабораторії віддаленого доступу; $F_{22}^{(2)}$ – відмова у сегменті лабораторії віддаленого доступу. Деталізація функцій $F_1^{(1)}$ та $F_2^{(1)}$ формує другий рівень декомпозиції цільової функції.

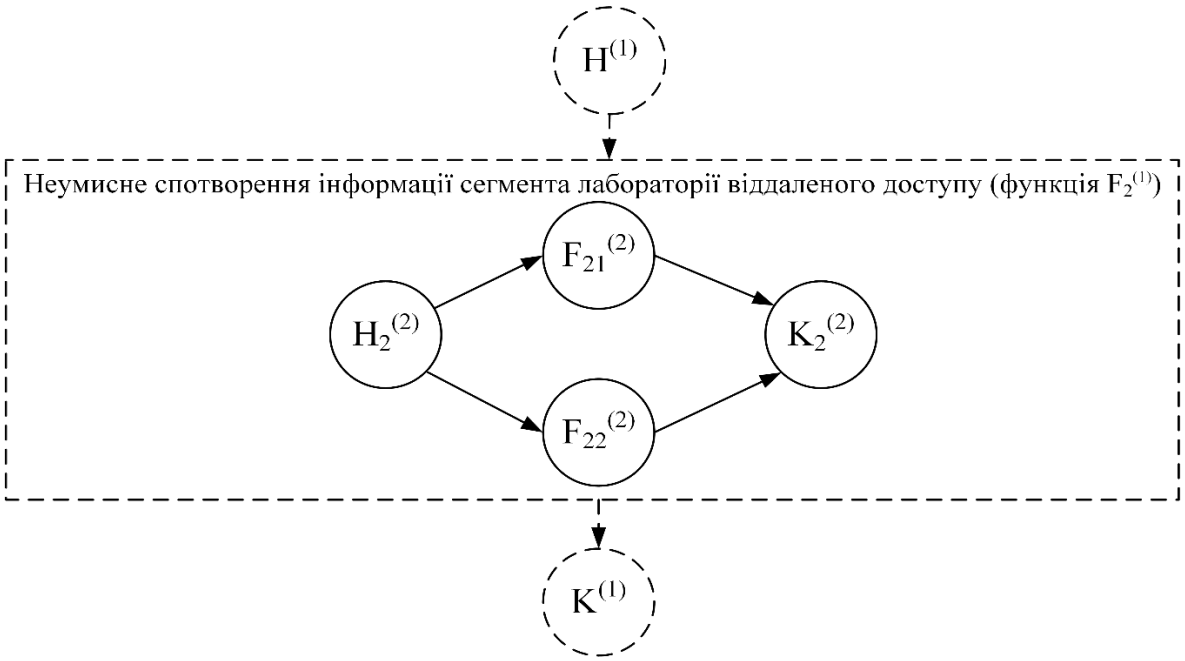

Рисунок 3.8 – Неумисне спотворення інформації сегмента лабораторії віддаленого доступу

Модель аналізу захищеності сегмента лабораторії віддаленого доступу представлено на рисунку 3.9.

Функція $F_{11}^{(2)}$ реалізується наступними підфункціями.

$F_{111}^{(3)}$ – збирання інформації про об'єкт протиправних дій. $F_{112}^{(3)}$ – створення зловмисником умов фізичного доступу до сегменту лабораторії віддаленого доступу. $F_{113}^{(3)}$ – ідентифікація активних служб, які виконуються на серверах сегмента лабораторії віддаленого доступу.

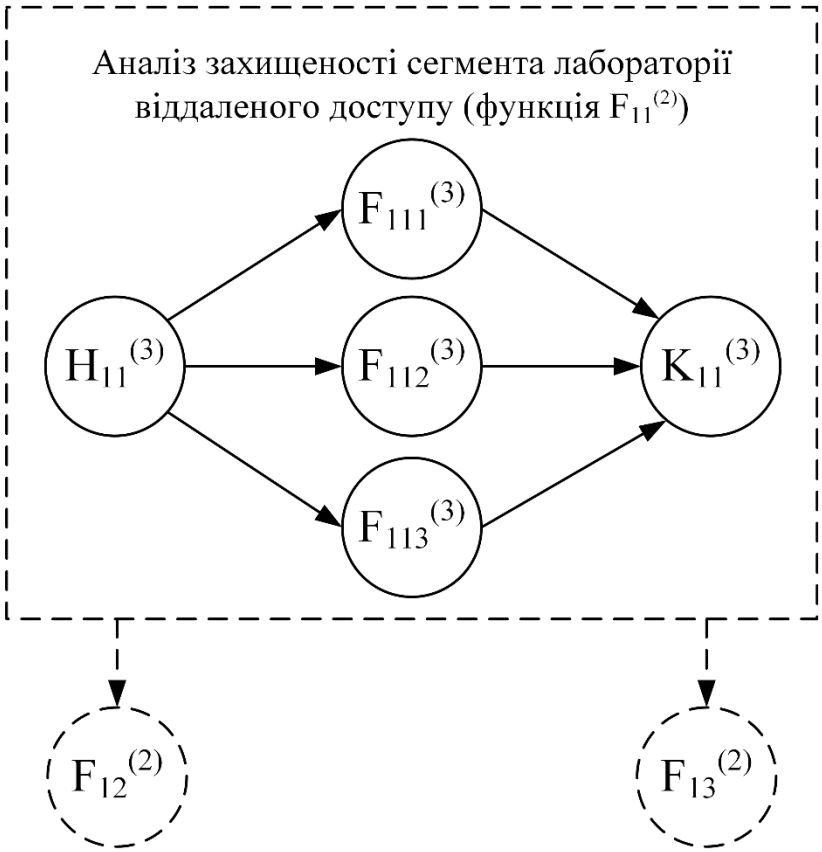

Рисунок 3.9 – Аналіз захищеності сегмента лабораторії віддаленого доступу

Модель підбору паролів до компонентів обмеження доступу механізмів захисту інформації від несанкціонованого доступу зображено на рисунку 3.10.

Функція $F_{12}^{(2)}$ реалізується наступними підфункціями.

$F_{121}^{(3)}$ – підбір пароля безпосередньо у сегменті лабораторії віддаленого доступу. $F_{122}^{(3)}$ – підбір пароля засобами зловмисника з використанням наявного файлу з даними про паролі.

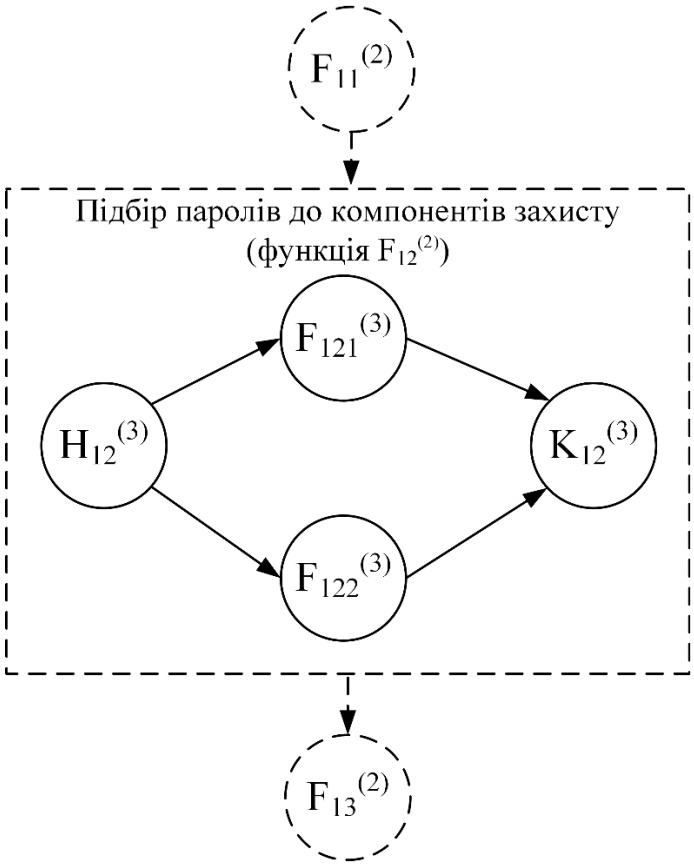

Рисунок 3.10 – Підбір паролів до компонентів обмеження доступу механізмів захисту інформації від несанкціонованого доступу

Модель впровадження помилкового довіреного суб’єкта доступу сегмента лабораторії віддаленого доступу зображено на рисунку 3.11.

Функція $F_{13}^{(2)}$ реалізується наступними підфункціями.

$F_{131}^{(3)}$ – зміна статусу довіреного суб'єкта на «хибний» на основі використання недоліків алгоритмів віддаленого пошуку. $F_{132}^{(3)}$ – зміна статусу довіреного суб'єкта на «хибний» за допомогою шкідливих програм. $F_{133}^{(3)}$ – зміна статусу довіреного суб'єкта на «хибний» шляхом протиправних дій щодо легального персоналу (підкуп, шантаж, дезінформація тощо). $F_{134}^{(3)}$ – зміна статусу довіреного суб'єкта на «хибний» шляхом зарахування зловмисника в обслуговуючий персонал лабораторії віддаленого доступу.

Аналіз інформації, що проходить через впроваджений довірений суб’єкт сегмента лабораторії віддаленого доступу зображено на рисунку 3.12.

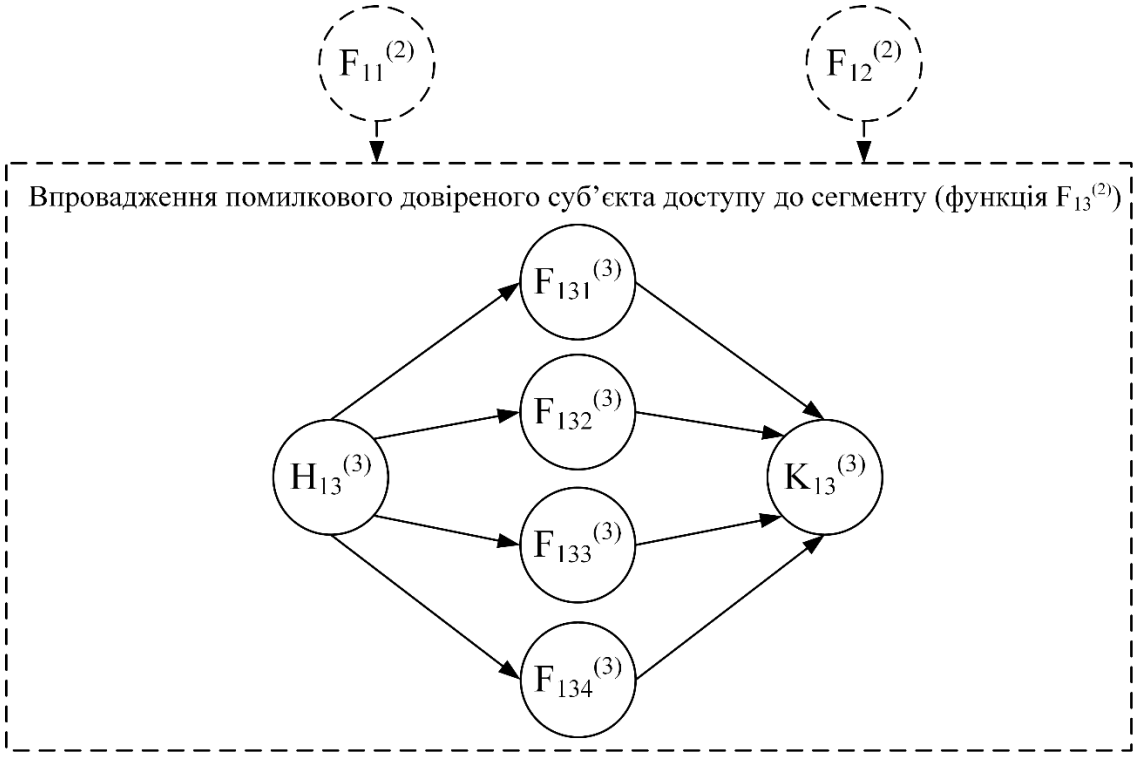

Рисунок 3.11 – Впровадження помилкового довіреного суб'єкта доступу сегмента лабораторії віддаленого доступу

Функція $F_{14}^{(2)}$ реалізується наступними підфункціями (рисунок 3.12): $F_{141}^{(3)}$ – аналіз повноважень доступу до ресурсам; $F_{142}^{(3)}$ – аналіз коментарів до облікових записів; $F_{143}^{(3)}$ – виявлення налаштувань маршрутизатора.

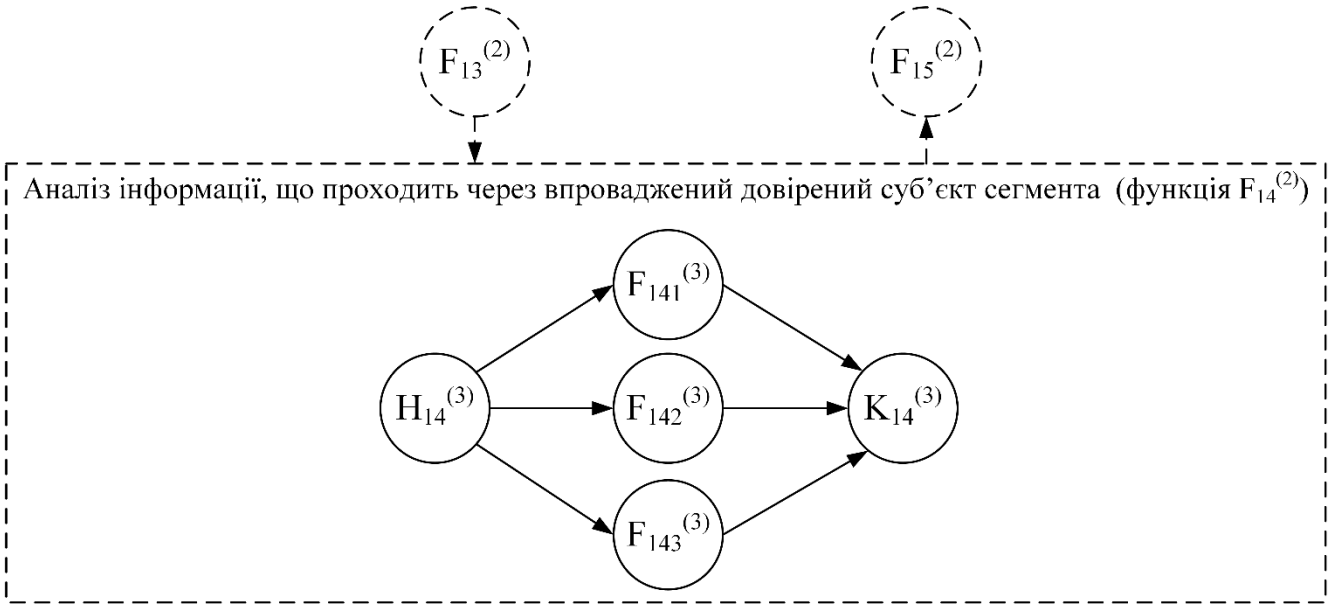

Рисунок 3.12 – Аналіз інформації, що проходить через впроваджений довірений суб'єкт сегмента лабораторії віддаленого доступу

Модель несанкціонованого маніпулювання інформацією лабораторії віддаленого доступу зображена на рисунку 3.13.

Функція $F_{15}^{(2)}$ реалізується наступними підфункціями.

$F_{151}^{(3)}$ – пошук інформації, що цікавить; $F_{152}^{(3)}$ – модифікація інформації; $F_{153}^{(3)}$ – знищення інформації; $F_{154}^{(3)}$ – створення умов подальшого легального доступу.

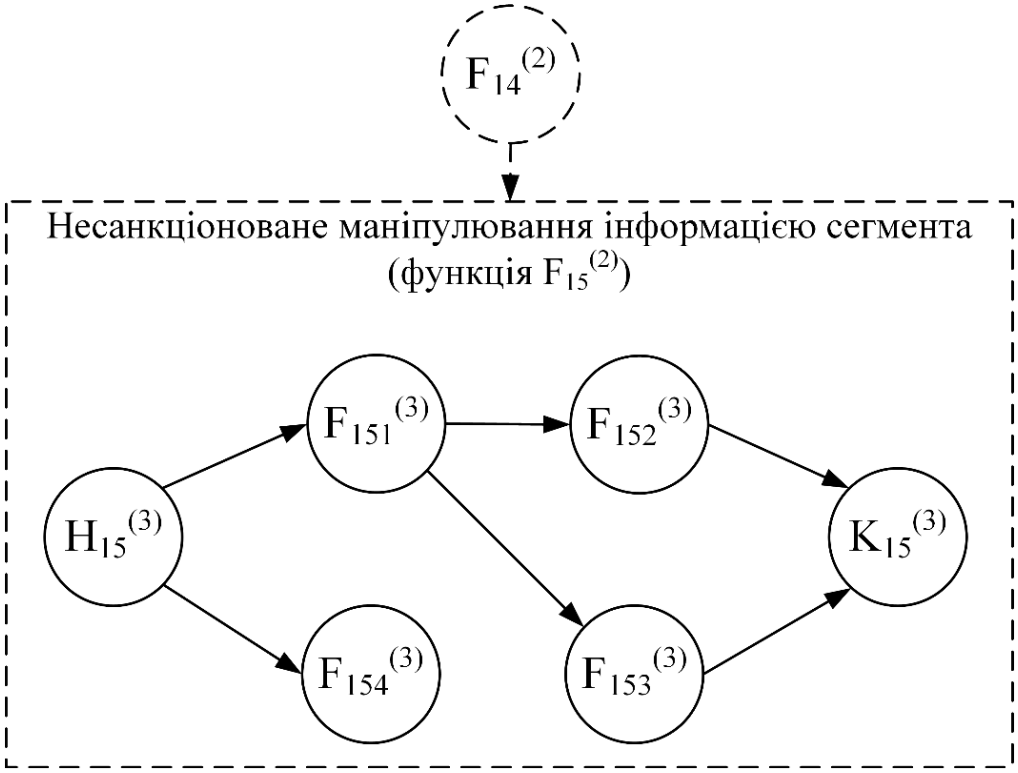

Рисунок 3.13 – Несанкціоноване маніпулювання інформацією лабораторії віддаленого доступу

Модель збою в сегменті лабораторії віддаленого доступу зображено на рисунку 3.14.

Функція $F_{21}^{(2)}$ реалізується такими підфункціями третього рівня:

$F_{211}^{(2)}$ -збій програмного забезпечення в сегменті лабораторії віддаленого доступу; $F_{212}^{(2)}$ – збій апаратного забезпечення у сегменті лабораторії віддаленого доступу.

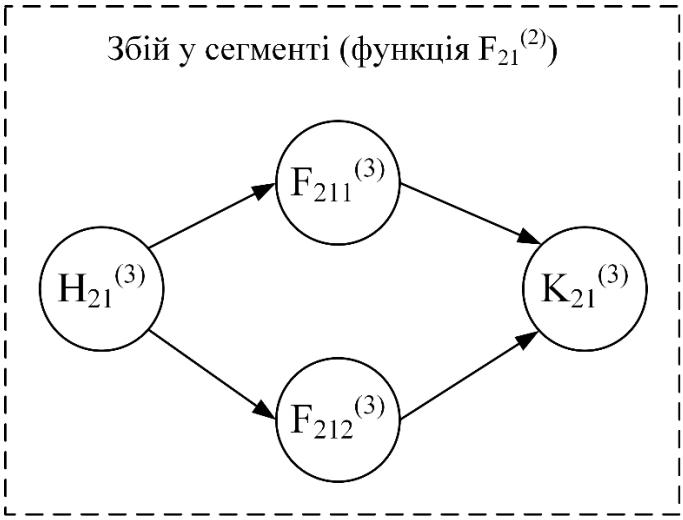

Рисунок 3.14 – Збій в сегменті лабораторії віддаленого доступу

Функція $F_{22}^{(2)}$ «Відмова в сегменті лабораторії віддаленого доступу» (рисунок 3.15) реалізується такими підфункціями третього рівня: $F_{221}^{(2)}$ -відмова програмного забезпечення в сегменті лабораторії віддаленого доступу; $F_{222}^{(2)}$ – відмова апаратного забезпечення у сегменті лабораторії віддаленого доступу.

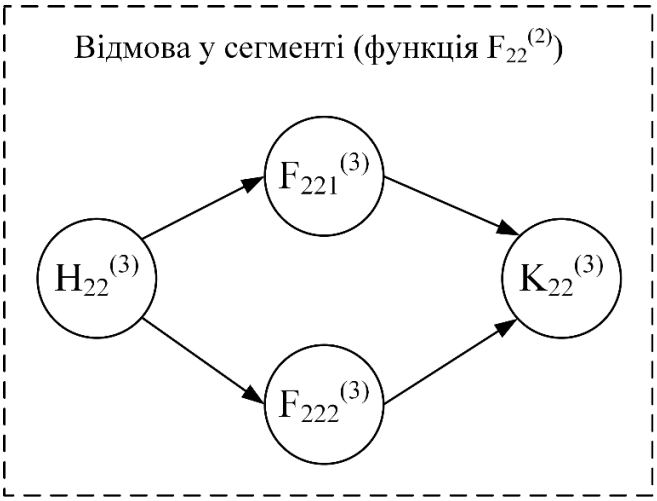

Рисунок 3.15 – Відмова в сегменті лабораторії віддаленого доступу

На основі розглянутої функціональної моделі процесів порушення цілісності інформації сегменту лабораторії віддаленого доступу нескладно отримати функціональну модель процесів протидії такого роду загроз інформаційної безпеки. Така модель матиме аналогічну структуру, а зміст функцій при цьому формуватиметься з принципу «дія - протидія».

3.4 Висновки до розділу

В третьому розділі сформовано поетапний порядок моделювання загроз інформаційної безпеки лабораторії віддаленого доступу. Таким чином, заходи щодо визначення актуальності загроз безпеки є цілісним та структурованим процесом, здатним враховувати особливості функціонування різних типів інформаційних систем.

Відповідно до «Методики визначення загроз безпеки інформації в інформаційних системах», на основі якої було сформовано порядок моделювання, модель загроз безпеки інформації має містити такі основні розділи:

- опис інформаційної системи та особливостей її функціонування.
- можливості порушників (модель порушника).
- актуальні загрози безпеці інформації.

Добре опрацьовані моделі загроз безпеки інформації дозволяють сформулювати план захисту, який зосереджений на актуальних загрозах та передбачає ефективні контрзаходи, що підвищують рівень інформаційної безпеки. Враховуючи це, наведені приклади наочно демонструють, що об'єктно-орієнтована методологія проектування є корисним інструментом у розробці проекту системи інформаційної безпеки загалом та моделі загроз безпеки інформаційної системи, зокрема. Оскільки модель загроз інформаційної безпеки вимагає розгляду питання у кількох розрізах, то використання такої методології є однією з найбільш успішних.

Сформована функціональна модель загроз сегмента лабораторії віддаленого доступу дозволяє отримати абсолютно аналогічну модель протидії визначеним загрозам і за рахунок цього покращити показник інформаційної безпеки і не допустити несанкціонованого втручання в систему лабораторії і навчального закладу в цілому.

4 ЗАХИСТ ЦІЛІСНОСТІ ДАНИХ ЛАБОРАТОРІЇ ВІДДАЛЕНОГО ДОСТУПУ

4.1 Рекомендації по захисту даних лабораторії віддаленого доступу

Для забезпечення захищеності інформації в системі лабораторії віддаленого доступу доречно будувати захист за трьома основним напрямам:

1) контроль за безпекою коду та наявністю вразливостей у системі лабораторії віддаленого доступу;
2) використання спеціалізованих засобів захисту інформації:

- прямі та зворотні проксі-сервера;
- класичні міжмережеві екрани та міжмережеві екрани рівня додатків;
- багатофакторні системи аутентифікації (сертифікати, тимчасові додаткові паролі та ключові слова на додаток до пари логіна та пароля користувача, методи статичної та динамічної біометричної автентифікації та ін.);
- системи виявлення атак та запобігання вторгненням;
- антивірусне програмне забезпечення;
- системи реєстрації та аналізу подій;
- VPN та захищені протоколи передачі даних;
- шифрування даних;
- засоби резервування та відновлення даних.

3) проведення періодичного контролю захищеності системи лабораторії віддаленого доступу та вироблення коригувальних дій у разі потреби.

Розглянемо детальніше методи забезпечення безпосередньо цілісності інформації лабораторії віддаленого доступу. Резервування інформації є поширеним способом підвищення надійності технічних засобів, і як наслідок, забезпечення цілісності інформації. Якщо розглядати технічні засоби з точки зору інформаційної складової, то підвищення надійності досягається за рахунок послідовного

з’єднання елементів системи, що відповідають за дану складову. Для забезпечення гарантоздатності такого інформаційно-технічного комплексу необхідно застосовувати послідовно-паралельну архітектуру побудови системи технічних засобів.

Ще одним доречним засобом є резервування у контексті можливості програмних засобів створювати свої копії в процесі виконання програм. Це досягається створенням точки відкату, до яких програма працювала належним чином. У ситуації, коли за якоїсь причини сталося порушення працездатності програми, вона повертається до заздалегідь зазначеної точки та продовжує роботу.

Дієвим способом забезпечення цілісності інформації є добре продуманий і надійний захист від вірусів. Пропонованим способом захисту від вірусів є використання антивірусних програм, яких на даний момент існує достатня кількість. Однак, варто зазначити, що не одна антивірусна програма не зможе гарантувати забезпечення виявлення та захисту від невідомого або нового виду вірусу.

Для контролю цілісності інформації можна використовувати два основних методи. Перший передбачає використання контрольної суми, в якій виділяють безпосередньо контрольну суму і хеш суму. Другий зазначений метод є використання цифрового підпису.

На сьогоднішній день одним з найбільш популярних є спосіб застосування хеш-функції, при якій від кожного із блоків даних обчислюється хеш-значення. Недоліком даного способу є висока надмірність при контролі цілісності блоків даних. Тому, обраним за результатами дослідження способом контролю цілісності даних, є спосіб, що ґрунтується на застосуванні хеш-функції за принципом поєднань хеш-значень. Цей спосіб контролю цілісності полягає в тому, що застосовуючи хеш-функцію до певної кількості підблоків пам'яті M_i за допомогою поєднань отриманих хеш-значень H_j можливо здійснювати контроль цілісності даних для пошуку одноразової помилки.

Основна ідея способу контролю цілісності даних на основі застосування хеш-функції за принципом поєднань хеш-значень полягає у використанні формули

комбінаторики C_n^m для обчислення поєднань хеш-значень таким чином, що кожному з підблоків пам'яті M_i ставиться у відповідність комбінація з H_j. При цьому кількість використовуваних хеш-значень завжди менше кількості підблоків пам'яті M_i , які необхідно захистити. Однією з переваг такого способу є зниження введеної надмірності при контролі цілісності даних.

Блок даних M, який необхідно захистити, представляється у вигляді кінцевої лічильної множини підблоків пам'яті v. Кількість поєднань обчислюється за формулою:

$$C_n^m = \frac{n!}{n!\,(n-m)!}$$

де n – кількість хеш-значень, що використовуються для захисту всіх підблоків блоку даних M, а m – кількість хеш-значень, що використовуються для захисту одного підблоку даних M_i.

Кількість підблоків пам'яті k менше або дорівнює кількості поєднань хеш-значень H_j, необхідних для захисту блоку даних. Це означає, що потрібно використовувати менше ресурсів системи зберігання даних для зберігання хеш-значень, отже зменшиться надмірність збереженої інформації.

Схема, що пояснює метод контролю за цілісністю даних на основі застосування хеш-функції за принципом поєднань хеш-значень представлена малюнку 4.1 .

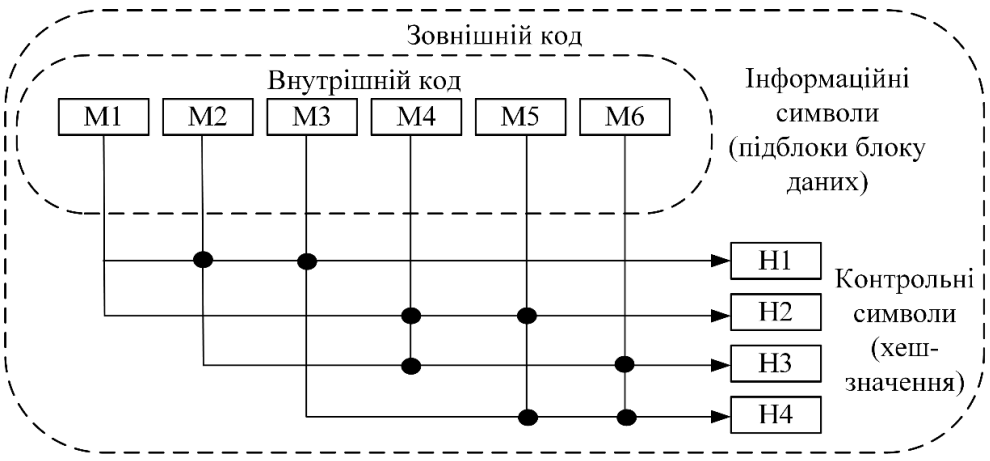

Рисунок 4.1 - Спосіб контролю цілісності на основі використання хеш-функції за принципом хеш-значень

4.2 Протидія загрозі «Несанкціонована зміна даних»

В третьому розділі було розглянуто сценарій реалізації загрози «Несанкціонована зміна даних», де користувач системи міг виконати будь-які дії щодо зміни даних, надані йому інтерфейсом системи. Таким чином, з боку системи відсутній контроль доступності операції для користувача, можливість її виконання відповідно до посадових обов'язків, рівня доступу, що може спричинити ряд негативних наслідків для безпеки системи.

Для вдосконалення системи забезпечення інформаційної безпеки необхідно розробити чітку структуру протидії визначеній загрозі. Для цього необхідно описати модель сценарію To - Be (як має бути) для загрози «Несанкціонована зміна даних» за допомогою діаграми діяльності. Така модель представлена на малюнку 4.1. Вона фактично є сценарієм захисту і використовує три контури захисту:

- перевірка прав на виконання операції , заснована на політиці привілеїв;
- перевірка критичності змін, що використовує класифікатор операцій;
- логування (реєстрація у таблицях логів) операцій.

У сукупності вони утворюють модуль безпеки за загрозою "Несанкціонована зміна даних", який передбачає внесення функціональних змін у конструкцію інформаційної системи. З погляду інформаційної безпеки така модель дозволяє сформулювати функціональні вимоги до інформаційної системи:

- використання політики привілейованого доступу;
- наявність класифікатора критичності операцій;
- наявність таблиць логів по операціях, що здійснюються;
- реалізація програмно-апаратного комплексу підтвердження операцій третьою особою;
- реалізація програмно-апаратного комплексу оповіщення служби безпеки.

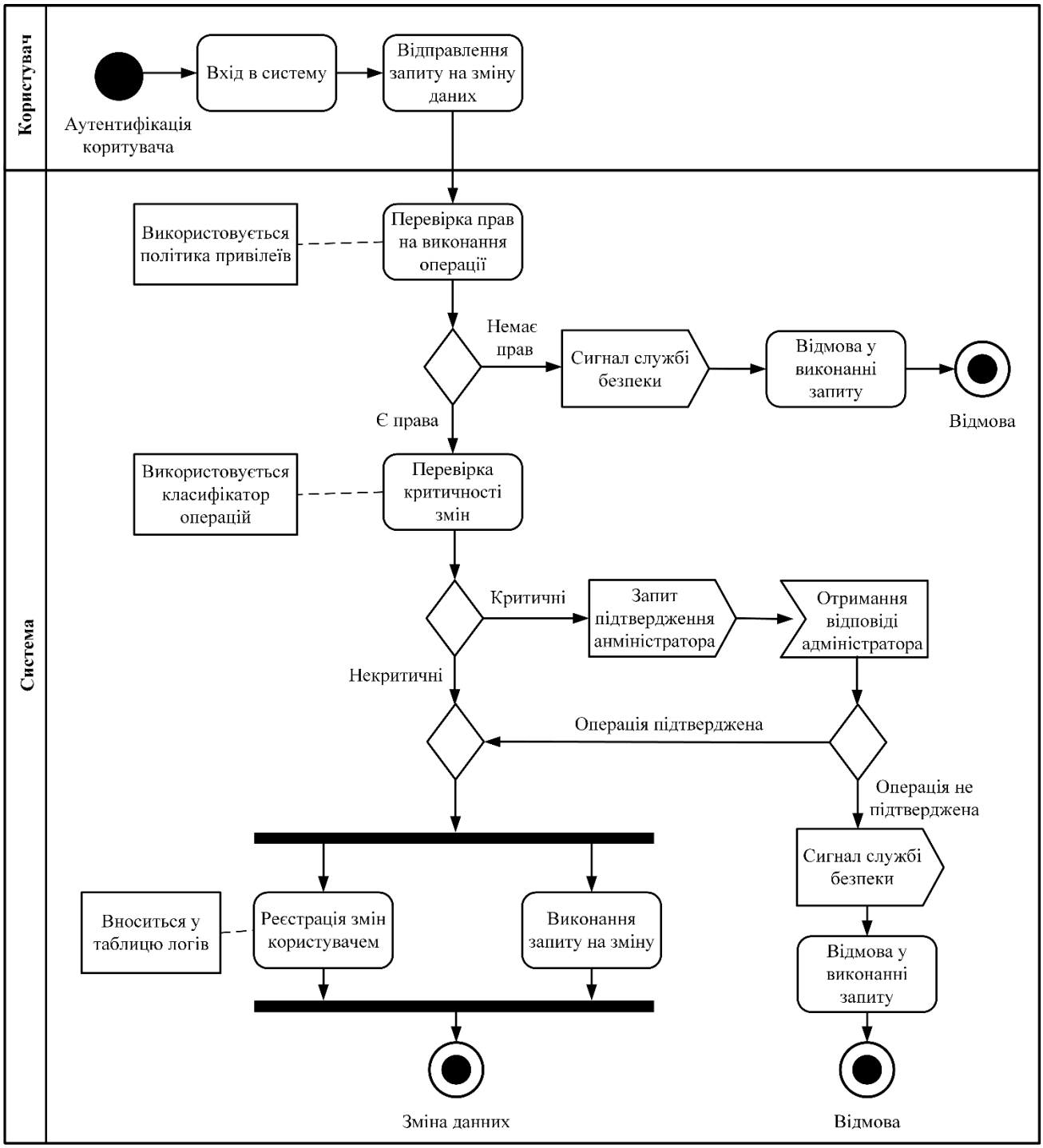

Рисунок 4.2 – Діаграма діяльності. Сценарій захисту

Заходи захисту, що реалізують озвучені вимоги, можуть використовувати як типові, так і приватні рішення. Зазначені заходи в подальшому включаються до плану захисту інформаційної системи, який є сукупністю функціональних і нефункціональних вимог до системи безпеки.

4.3 Модель оцінки захищеності даних лабораторії віддаленого доступу

Для контролю за ефективністю системи захисту та заходів щодо усунення наслідків можливих порушень захищеності інформації, а також ступенем виконання нормативних вимог до рівня забезпечення інформаційної безпеки слід проводити регулярну оцінку рівня захищеності системи лабораторії віддаленого доступу.

В даний час існує багато підходів до оцінки захищеності інформації в різних системах, однак, більшість з них вимагають адаптації до конкретного виду систем та специфіки їх використання. У зв'язку з цим, необхідно дослідити існуючі підходи та модернізувати їх до оцінки захищеності, які враховуватимуть саме особливості організації та функціонування лабораторії віддаленого доступу.

Для вирішення завдань оцінки захищеності системи лабораторії віддаленого доступу, необхідно, щоб у моделі оцінки були передбачені такі функції:

- збір даних про систему лабораторії віддаленого доступу, її функції, архітектуру та технікоексплуатаційні характеристики, категорію оброблюваної інформації, видах та вартості інформаційних ресурсів, кількості видах засобів захисту, обмежень на вартість коштів захисту та рівень допустимого ризику;
- складання моделі актуальних для лабораторії віддаленого доступу загроз;
- розрахунок ризиків від реалізації кожної загрози з моделі актуальних загроз,
- розрахунок загального ризику;
- ранжування загроз за рівнем допустимості ризику;
- оцінка поточного рівня захищеності лабораторії віддаленого доступу;
- порівняння поточного рівня захищеності з необхідним навчальному закладу рівнем захищеності;
- ухвалення рішення про необхідність зміни складу або реконфігурації засобів захисту лабораторії віддаленого доступу;
- складання списку рекомендацій захисту інформації лабораторії віддаленого доступу;
- формування звіту про результати оцінки захищеності та видача рекомендацій

щодо повішення захищеності.

Таким чином, концептуальну модель оцінки захищеності лабораторії віддаленого доступу можна побачити на рисунку 4.3.

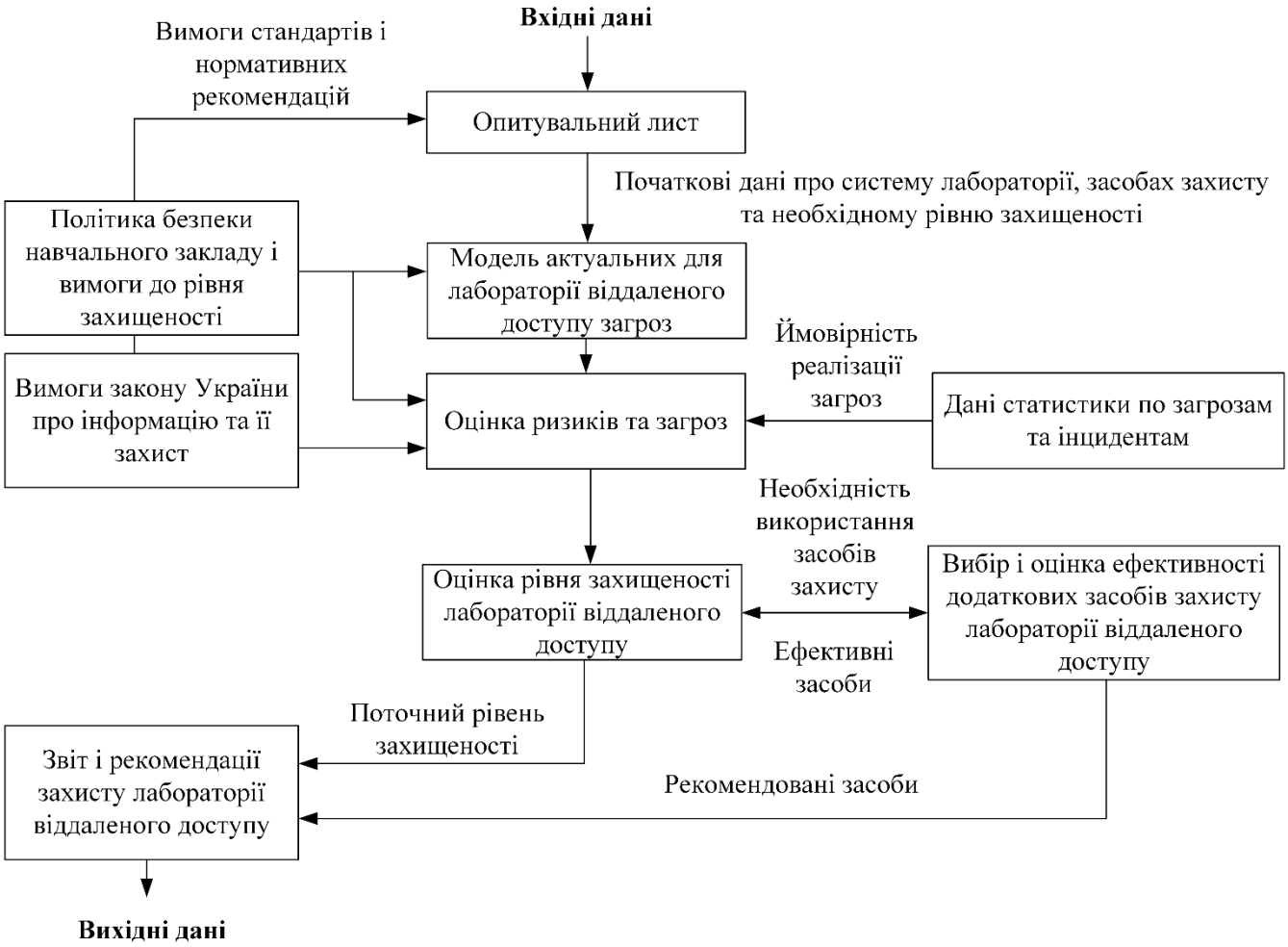

Рисунок 4.3 – Концептуальна модель оцінки захищеності лабораторії віддаленого доступу

Вхідними даними моделі є:

- інформація про лабораторію віддаленого доступу: архітектура та тип;
- інформація про дані та послуги, що підлягають захисту в лабораторії віддаленого доступу (тип та найвищі категорії оброблюваної інформації);
- список інформаційних ресурсів та сервісів із зазначенням їх вартості, можна встановити загальну вартість всіх ресурсів або інвентаризувати всі файли та дані в системі та оцінити вартість кожного;

- вимоги до рівня захисту лабораторії віддаленого доступу;
- списки можливих для системи лабораторії віддаленого доступу загроз;
- списки засобів захисту, що використовуються в лабораторії віддаленого доступу.

Вихідними даними оцінки захищеності лабораторії віддаленого доступу є:

- розрахований рівень захищеності лабораторії віддаленого доступу;
- ступінь відповідності рівня захищеності лабораторії віддаленого доступу вимогам безпеки навчального закладу;
- рішення щодо необхідності підвищення рівня захищеності;
- рекомендації щодо неприпустимих ризиків та список потенційних засобів захисту, застосування яких дозволить підвищити захищеність лабораторії віддаленого доступу.

Оцінка захищеності є регулярною заходом, що проводиться відповідальною за інформаційну безпеку особою або особами з метою контролю за станом безпеки системи і дозволяє не лише оцінити рівень захищеності, а й у разі невідповідності підібрати найбільш раціональні засоби захисту для системи, застосування яких дозволить усунути виявлені на етапі аналізу показників захищеності невідповідності вимогам та підвищити рівень захищеності.

4.4 Висновки до розділу

Розділ розглядає забезпечення інформаційної безпеки і безпосередньо цілісності інформації для лабораторії віддаленого доступу. Пропонується спрямовувати захист за трьома основними напрямками: контроль за безпекою коду та наявністю вразливостей у системі лабораторії віддаленого доступу; використання спеціалізованих засобів захисту інформації; проведення періодичного контролю захищеності системи лабораторії віддаленого доступу та вироблення коригувальних дій у разі потреби. Такий підхід дозволить забезпечити оптимальний рівень захищеності інформації і наддасть можливість корегувати методи захисту в залежності від актуальної ситуації і даних моніторингу загроз.

Для контролю цілісності інформації обраний метод, що ґрунтується на застосуванні хеш-функції за принципом поєднань хеш-значень. Такий спосіб, у порівнянні з класичними методами, дозволяє знизити надмірність при контролі цілісності даних, за рахунок скорочення кількості еталонних хеш-значень,

Описаний сценарій захисту від загрози «Несанкціонована зміна даних» передбачає ефективну протидію відсутності контролю доступності операції для користувача, можливості їх виконання відповідно до посадових обов'язків, рівня доступу. В основі сценарію лежать три основні пункти: необхідність перевірки прав на виконання операції , заснована на політиці привілеїв; перевірка критичності змін, що використовує класифікатор операцій; логування (реєстрація у таблицях логів) операцій.

Розроблена модель оцінки захищеності лабораторії віддаленого доступу використовує комбінований підхід, побудований на застосуванні кількісно-якісної оцінки захищеності, за якого захищеність є функцією від значень рекомендацій щодо усунення ризику від реалізації кожної актуальної загрози для системи. Така модель дозволяє не лише оцінити рівень захищеності, а й у разі невідповідності підібрати найбільш раціональні засоби захисту. Застосування оптимальних методів захисту є передумовою для відповідності законодавчим вимогам щодо захищеності інформації, а також основним положенням навчального закладу.

ВИСНОВКИ

Дипломний проект досліджує методи захисту даних лабораторії з віддаленим доступом, особливу увагу приділяючи параметру цілісності. В наш час використання віддаленого доступу до реальних навчальних лабораторій є невід'ємною складовою покращення якості навчального процесу для студентів інженерних дисциплін. В процесі функціонування така система може піддаватись ряду негативних впливів та інформаційних загроз, що в результаті може мати наслідки для безпеки всієї інформаційної системи навчального закладу. Тому для коректного використання таких технологій необхідно забезпечувати оптимальний рівень захищеності даних, що циркулюють в інформаційній системі навчального закладу та лабораторії віддаленого доступу.

Одним із базових параметрів захисту інформації є цілісність. Порушення цілісності інформації може призвести не лише до втрати важливих даних, а й до загрози працездатності всій інформаційній системі. Тому аналіз загроз є одним із ключових моментів політики безпеки. Розробляючи систему для захисту інформації доцільно використовувати комплексний підхід, з урахуванням особливостей реалізації віддаленого доступу до обладнання лабораторії. Належний рівень захисту інформації досягається не лише створенням і вибором відповідних механізмів захисту, а й регулярним процесом оцінки захищеності інформації, що здійснюється на всіх етапах життєвого циклу інформаційної системи.

В роботі було розглянуто типову архітектуру лабораторії віддаленого доступу, на основі якої були визначені можливі напрямки реалізації загроз інформаційній безпеці і цілісності даних. Для недопущення таких дій розглядаються загальноприйняті методи по контролю, забезпеченню та відновленню інформаційної цілісності на етапі зберігання, обробки та передачі.

Розглянуті нормативні державні вимоги та вимоги навчального закладу до

рівня забезпечення інформаційної безпеки, були сформовані очікувані результати від системи захисту лабораторії віддаленого доступу. До них належить: модель оцінки захищеності даних; оптимальний метод захисту лабораторії віддаленого доступу та перелік рекомендацій для покращення захищеності.

Поетапно формалізовано порядок моделювання загроз інформаційної безпеки лабораторії віддаленого доступу. Всього передбачається п’ять етапів моделювання:

- визначення можливих негативних наслідків реалізації загроз;
- визначення умов реалізації загроз;
- визначення джерел загроз і оцінка можливостей порушника;
- визначення сценаріїв реалізації загроз;
- оцінка рівня небезпеки загроз.

Для кожного етапу визначені необхідні вхідні дані та очікувані результати. Такий підхід має декілька вагомих переваг: універсальність та можливість використання для системи лабораторії віддаленого доступу; структурований та зрозумілий підхід до визначення актуальності загроз безпеці; залежність актуальності загроз від важливих факторів; наявність потенційних негативних наслідків від реалізації загрози та сценаріїв її реалізації.

На основі дослідження і аналізу інформаційних небезпек та принципів об’єктно-орієнтованого проектування було змоделювано концептуальні моделі загроз, способи реалізації загроз, загрози цілісності системи та сценарії протидії. На основі функціональних моделей досліджено порушення цілісності даних сегмента лабораторії віддаленого доступу та визначено, що цьому можна запобігти аналогічними моделями протидії.

Обрані рекомендації захисту даних лабораторії віддаленого доступу спрямовані на три основних напрямки: контроль за безпекою коду та наявністю вразливостей у системі лабораторії віддаленого доступу; використання спеціалізованих засобів захисту інформації; проведення періодичного контролю захищеності системи лабораторії віддаленого доступу та вироблення коригувальних дій у разі потреби. Рекомендований спосіб контролю цілісності

даних на основі застосування хеш-функції, головною перевагою якого є одночасне здійснення контролю цілісності даних для заданого рівня захищеності з мінімальною надмірністю.

Концептуальна модель оцінки захищеності дозволяє проводити контроль за рівнем захисту і передбачає наступні функції:

- збір основних даних про систему лабораторії віддаленого доступу;
- складання моделі актуальних для лабораторії віддаленого доступу загроз;
- розрахунок ризиків від реалізації кожної загрози з моделі актуальних загроз;
- ранжування загроз за рівнем допустимості ризику;
- оцінка поточного рівня захищеності лабораторії віддаленого доступу;
- порівняння поточного рівня захищеності з необхідним навчальному закладу рівнем захищеності;
- ухвалення рішення про необхідність зміни складу або реконфігурації засобів захисту лабораторії віддаленого доступу;

Це дозволяє проводити моніторинг поточної ситуації щодо безпеки інформації та модернізувати існуючі моделі захисту, на основі результатів оцінки. Всі описані методи покликані забезпечувати оптимальний рівень захищеності цілісності даних лабораторії віддаленого доступу.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Умрик М.А. Дистанційне навчання і професійна освіта / М.А. Умрик // Матер. докл. Междунар. конф. памяти проф. И.И. Мархеля «Новые информационные технологии в учебных заведениях Украины», Одесса, 21 – 26 июня 2005 г. — Одесса: Астропринт, 2005. — С. 170–173.

2. Жукова М. Н. Коромыслов Н.А. Модель оценки защищенности автоматизированной системы с применением аппарата нечеткой логики // Известия ЮФУ. Технические науки. – 2013. - №12 (149). - С. 63-69.

3. Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал. ун-та, 2019.— 204 с.

4. Певнев В. Я. Методы обеспечения целостности информации в инфокоммуникационных системах/ В. Я. Певнев // Вісник національного технічного університету «ХПІ». Серія: Техніка та електрофізика високих напруг. – 2015. - № 51. С. 74-77.

5. Диченко, С. А. Концептуальная модель обеспечения целостности информации в современных системах хранения данных / С. А. Диченко // Информатика: проблемы, методология, технологии. Сборник материалов XIX международной научно-методической конференции. Под ред. Д. Н. Борисова. – Воронеж, 2019. – С. 697-701.

6. Пєвнєв В.Я. Спосіб відновлення інформації при обміні даними у телекомунікаційних системах / В.Я.Пєвнєв и др. // Д.п. № 26778. Бюл., 2007. – № 16.

7. Li J., Wang Q., Wang C., Cao N., Ren K., Lou W. Fuzzy keyword search over encrypted data in cloud computing. [Електронне джерело] Режим доступу: https://www.researchgate.net/publication/220336297_Enabling_Efficient_Fuzzy_Keyword_Search_over_Encrypted_Data_in_Cloud_Computing

8. Bingwei Liu and Yu Chen Auditing for Data Integrity and Reliability

in Cloud Storage [Електронне джерело] Режим доступу: https://www.researchgate.net/publication/283524440_Auditing_for_Data_Integrity_and_Reliability_in_Cloud_Storage.

9. Mahbub M. Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics // Journal of Network and Computer Applications. 2020. vol. 168. no. 102761. pp. 1–26.

10. Захист інформації. Технічний захист інформації. Терміни і визначення: ДСТУ 3396.2-97. – [Чинний від 1998.01.01]. – К. : Держстандарт України, 1998. – 20 с.

11. Korzun D. et al. Ambient Intelligence Services in IoT Environments: Emerging Re-search and Opportunities // IGI Global. 2019.