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

ЗУЄВА Єлизавета Олександрівна

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ДАНИХ ЛАБОРАТОРІЇ З ВІДДАЛЕНИМ ДОСТУПОМ. КОНФІДЕНЦІАЛЬНІСТЬ

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

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

Одеса – 2021

АНОТАЦІЯ

Зуєва Є. О. Дослідження методів захисту даних лабораторії з віддаленим доступом. Конфіденційність – Кваліфікаційна робота магістра. Одеса, 2021: 65 с., 22 рис., 18 джерел.

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

Предметом дослідження є методи забезпечення конфіденційності даних у лабораторії з віддаленим доступом

Метою роботи є всебічне дослідження аспектів інформаційної безпеки, загроз, атак та вразливостей збоку кібербезпеки, актуальних структур організації лабораторій з дистанційним доступом та запропонування власного комплексного підходу до забезпечення конфіденційності, яка здатна класифікувати загрози, конкретизувати механізми атак, перевіряти механізми захисту та оцінювати наслідки.

Методи дослідження базуються на використанні теорії захисту інформації та моделей інформаційної безпеки, що мають за основу фундаментальні результати теорії множин, математичної логіки, теорії графів. Побудована модель атаки ґрунтуються на використанні теорії графів.

Робота присвячена дослідженню методів захисту інформаційної безпеки у лабораторії з віддаленим доступом, акцентуючись на питаннях конфіденційності. Досліджено існуючі архітектури організації лабораторій з віддаленим доступом та на основі цього дослідження побудовано власну архітектуру лабораторії. Побудовано модель потоку даних та атак на конфіденційність Запропоновано власну комплексну систему захисту конфіденційності, яка компонує актуальні методи попередження, реагування або класифікації ризику.

ІНФОРМАЦІЙНА БЕЗПЕКА, МОДЕЛІ ЗАХИСТУ, ВІДДАЛЕНИЙ ДОСТУП, КОНФІДЕНЦІЙНІСТЬ

ABSTRACT

Zuieva E.A. Research of methods of data protection of the laboratory with remote access. Confidentiality - The master qualifying work r. Odessa, 2021: 65 pages, 22 pic., 18 sources.

The object of the study is threats and vulnerabilities for the remote access laboratory and mechanisms to ensure the protection of data integrity.

The subject of the study is the methods of ensuring the confidentiality of data in the laboratory with remote access

The aim of the work is to comprehensively study aspects of information security, threats, attacks and vulnerabilities on the part of cybersecurity, current structures of remote access laboratories and to propose its own comprehensive approach to privacy, which can classify threats, specify attack mechanisms, test protection mechanisms and assess consequences.

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, graph theory. The constructed model of attack is based on the use of graph theory.

The work is devoted to the study of methods of information security protection in the laboratory with remote access, focusing on issues of confidentiality. The existing architectures of the organization of laboratories with remote access are studied and on the basis of this research the own architecture of the laboratory is built. The model of data flow and privacy attacks is built. Own complex system of privacy protection is offered, which composes actual methods of risk prevention, response or classification.

INFORMATION SECURITY, MODELS OF PROTECTION, REMOTE ACCESS, CONFIDENTIALITY

ЗМІСТ

ВСТУП

З розвитком та формуванням інформаційного суспільства проблема забезпечення інформаційної безпеки стає все більш актуальною. Усі сучасні організації, у тому числі заклади освіти, прагнуть збільшити інтеграцію інформаційних технологій у свої сфери діяльності, оскільки це дозволяє перейти на якісно новий рівень зберігання, обробки та передачі інформації.

Основним способом реалізації набутих навичок у ході навчання на інженерних спеціальностях є робота з апаратно-технічними засобами лабораторії. Устаткування допомагає підготовити майбутніх спеціалістів до роботи зі справнім організаційним інженерним обладнанням.

При реалізації дистанційного навчання найчастіше використовуються емулятори існуючого устаткування для демонстрації можливого відклику системи. Але віддаючи перевагу цьому методу знижується ефективність навчання. Програми-емулятори можуть лише спробувати передбачити та відтворити реальну поведінку системи. Насправді ж, головна ціль використання реального обладнання полягає у тому, щоб показати, які бувають раптові та непередбачувані проблеми та мати можливість самостійно подумати, як вони вирішуються.

Тому останнім часом все більше зарубіжних освітніх закладів впроваджують системи віддаленого доступу до лабораторії замість віртуальної лабораторії з емуляторами. На вітчизняному просторі майже відсутні приклади реалізації подібних систем.

Вибір лабораторії з дистанційним доступом також вирішує питання доступності не лише для студентів, які мали можливість до цього перебувати у реальній лабораторії, а і для маломобільних студентів, для яких взагалі доступ до обладнання практично не можливий в існуючих умовах.

Метою дистанційного експериментального рішення є максимально наближення взаємодії студента з віддаленою системою до роботи на реальному обладнанні. Іншими словами, необхідно забезпечити найкращий зворотний зв'язок для дій користувача, щоб звести до мінімуму недоліки, властиві відстані між користувачем і фізичним обладнанням. Перший недолік –це затримка передачі інформації від клієнта до сервера і назад. Другий небажаний ефект – це складність відтворення на стороні клієнта стану віддаленого обладнання, його динаміки та умов його роботи.

Разом з тим, для успішного розвитку дистанційної форми навчання в освітніх закладах, зазвичай необхідні значні зусилля не лише програмістів та фахівців у галузі комп'ютерних комунікацій, а й спеціалістів у предметних галузях, методистів, які добре знайомі із сучасними тенденціями та концепціями у системі освіти, теоріями, педагогічними технологіями, психологічними особливостями взаємодії в мережі та ін. Навчальний процес у дистанційній формі більш трудомісткий та містить більше аспектів, ніж у очній формі, але ці труднощі обумовлені тим, що він відкриває доступ для всіх студентів у будь-яких умовах.

Впровадження лабораторій з віддаленим доступом поступово реалізується різними університетами вже більше 10 років [1]. Проте стабільність таких послуг не забезпечується належним чином у багатьох навчальних закладах. Основна проблема полягає в переході від однієї дослідницької установки, доступної час від часу, до професійної інфраструктури віддаленої лабораторії з багатьма установками, доступними в усьому світі та 24/7. Необхідно враховувати не тільки технічні аспекти, але й зручність використання рішень та підтримку клієнтів. З технічної сторони рішення має бути надійним для студентів та зовнішніх шкідливих атак. Лабораторія повинно бути повністю автономною і здатною до самодіагностики. У разі виникнення проблем вона повинна мати можливість повернутися до відомого стабільного стану та повідомити про проблему адміністратору. З освітньої сторони навчальне середовище має бути перероблено, щоб врахувати недоліки, властиві дистанції, щоб зробити взаємодію студента з

дистанційною системою якомога ближче до фактичної роботи на реальному обладнанні та уможливити спільну роботу.

В сучасних умовах при проектуванні будь-яких систем, а не лише організації віддаленого доступу, гостро стоїть питання захисту. Постійно зростає кількість атак на безпеку, а разом з цим збільшується величина шкоди, яку вони причиняють.

Актуальність роботи також полягає в тому, що у літературі мало уваги приділяється безпеці, за винятком хімічних та біологічних лабораторії [2]. Хоча Scopus перелічує понад 2000 робіт, присвячених віддаленим і мережевим лабораторіям, лише деякі з них детально обговорюють питання безпеки та надійності. Спостерігається відсутність структурованого підхіду до безпеки та захист доступу для державних віддалених лабораторій. Більше того, більшість дослідників зосереджуються лише на загальній безпеці, і їм не вистачає роботи, яка б детально розглядала такий важливий аспект безпеки, як конфіденційності.

Через те, що реалізація систем віддаленого доступу з’явилися не так давно, з часу їх запровадження та використання існувало лише кілька дійсних загроз захисту інформації. Насамперед це було пов’язано з тим, що комп’ютери були дорогими, рідкісними та ретельно охоронюваними. Комп’ютерні системи, які містили інформацію, були відкриті лише для обмеженої кількості людей із навичками програмування на комп’ютерах, які мали доступ до інформації, і це потенційно могло бути дійсною загрозою. Таким чином, початкова увага для захисту інформації була спрямована на забезпечення надійності самої системи, щоб гарантувати, що вона буде постійно працювати, коли це необхідно. В результаті захист інформації досягався в основному за рахунок контролю фізичного доступу до комп’ютерів. Зі зменшенням вартості комп’ютерної техніки та збільшенням її використання відбулося зміщення уваги із захисту комп’ютерів до захисту інформації. Якщо раніше надійність комп’ютерів була домінантною, то поняття конфіденційності, цілісності та доступності почало набувати значення.

Існуючі моделі захисту безпеки загалом стосуються великих організацій та корпорацій, для яких конфіденційність даних являється важливим активом. Тому

у науковій літературі більшість підходів до цього аспекту безпеки описано з позиції прибутку.

У зв’язку з цим з’являється інша проблема – обмежене фінансування збоку університету та системи освіти загалом. Поширеним рішенням для забезпечення безпеки на всіх рівнях функціонування систем є комплексні програмно-технічні засоби, які доказали свою високу ефективність. Але в обмежених умовах фінансування використання подібних систем не є можливим.

Особливістю лабораторного середовища є використання телекомунікаційних засобів та каналів зв’язку для побудови захищеного обміну інформацією, що обумовлює критичність спотворення та втрати інформаційних ресурсів, що зберігаються та оброблюються обчислювальними засобами середовища.

Порушення конфіденційності інформаційних ресурсів, в першу чергу середовища лабораторії, призводять до істотних економічних витрат, оскільки саме несанкціонований доступ до інформаційного ресурсу лабораторії, може бути каналом зв’язку, який дозволить порушнику здійснити несанкціоновані впливи по відношенню до будь-яких ресурсів університетської мережі зв’язку.

Проблеми зі складністю та багатоплановістю інформації в корпоративних мережах зв’язку, зокрема у захисті обґрунтованого вибору рівня конфіденційності, обумовлює актуальність розробки методів захисту побудови комплексної системи захисту інформаційних ресурсів. Тому порушення цих умов обумовлює доцільність реалізації методів об’єктивної та обґрунтованої оцінки приватної інформації в корпоративній мережі, з іншої сторони ставити перед розробкою додаткових завдань захисту інформаційних ресурсів корпоративної мережі від несанкціонованого доступу.

Розробка науково-обґрунтованої моделі та методів оцінки конфіденційності інформаційних ресурсів мережі зв'язку дозволить скоротити економічні витрати на побудову системи захисту мережі та економічний потенціал від порушеної інформації в мережі.

Виходячи з цього актуальною є розробка віртуальної лабораторії на базі веб-порталу з дистанційним доступом до обладнання, призначеної для проведення

наукових експериментів, які легко здійснюються в режимі реального часу, є актуальним науковим завданням, що має важливе практичне значення. У зв’язку з цим існує гостра потреба аналізу існуючих методів загроз безпеки інформаційних систем у контексті конфіденційності, а також моделювання вразливостей та проектуванні системи рекомендацій дотримання безпеки. У дипломній роботі розглянуто метод побудови моделі загроз, що ґрунтується на теорії графів. На основі аналізу запропоновано власну систему забезпечення безпеки інформаційної системи лабораторії, яка базується на синтезі актуальних методів захисту кожного з елементів системи. При проектуванні та реалізації лабораторії у майбутньому їх потрібно проаналізувати та адаптувати.

Метою кваліфікаційної роботи є всебічне дослідження аспектів інформаційної безпеки, загроз, атак та вразливостей збоку кіберпезпеки, актуальних структур організації лабораторій з дистанційним доступом та запропонування власного комплексного підходу до забезпечення конфіденційності, яка здатна класифікувати загрози, конкретизувати механізми атак, перевіряти механізми захисту та оцінювати наслідки.

Для досягнення поставленої мети вирішено наступні задачі:

– Досліджено існуючі архітектури організації лабораторій з віддаленим доступом та на основі цього дослідження побудовано власну архітектуру лабораторії;

– Побудовано модель потоку даних та атак на конфіденційність

– Запропоновано власну комплексну систему захисту конфіденційності, яка компонує актуальні методи попередження та реагування на атаки або класифікації ризику.

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

Предметом дослідження є методи забезпечення конфіденційності даних у лабораторії з віддаленим доступом.

Методи дослідження базуються на використанні теорії захисту інформації та моделей інформаційної безпеки, що беруть за основу фундаментальні результати теорії множин, математичної логіки, теорії графів. Побудована модель атаки ґрунтується на використанні теорії графів.

Наукова новизна полягає у створенні системи, яка всесторонньо захищає кожен з аспектів конфіденційності у існуючій лабораторії з віддаленим доступом на базі навчального закладу. Ці методи адаптовані до запропонованої моделі архітектури дистанційного доступу.

Робота складається з трьох розділів. У першому розділі досліджуються загальні виклики в інформаційній безпеці як предметній області. Розбираються терміни, через плутанину в яких погіршується розуміння та пошук методів захисту. Аналізується, яке саме місце методи дистанційного доступу займають у онлайн-навчанні. Проводяться висновки щодо того, яке саме місце конфіденційність відіграє у інформаційній безпеці та чому важливо у першу чергу захистити саме її.

У другому розділі проводиться аналіз методик, які потрібно врахувати при побудуванні моделі захисту. Розглядається такий аспект як архітектура лабораторії з віддаленим доступом та важливість правильного вибору його методу реалізації. Для того, щоб створити модель захисту та глибше дослідити тему загроз приводиться модель інформаційного потоку, та атаки на конфіденційність на її базі.

У третьому розділі пропонується методика побудови системи захисту з урахуванням існуючих інструментів інформаційної безпеки. Приводиться комплексна модель захисту інформаційної безпеки у лабораторії з віддаленим доступом на базі дослідження різним методів профілактики, контролю доступу, виявленню та відповіді на загрози з можливістю покращення системи.

1 ОГЛЯД КОНЦЕПЦІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У КОНТЕКСТІ ДИСТАНЦІЙНОГО ДОСТУПУ

1.1 Фундаментальні основи інформаційної безпеки

У дослідженні інформаційної безпеки є багато аспектів. Нам потрібно зрозуміти основні цілі безпеки, які полягають у забезпеченні доступності, цілісності та конфіденційності (тріада AIC) для критичних активів. Кожен актив вимагатиме різних рівнів цих типів захисту. Усі засоби контролю, механізми та запобіжні заходи реалізовані для забезпечення одного або кількох із цих типів захисту, а всі ризики, загрози та вразливості вимірюються на предмет їх потенційної здатності скомпрометувати один або всі принципи AIC на рисунку 1.

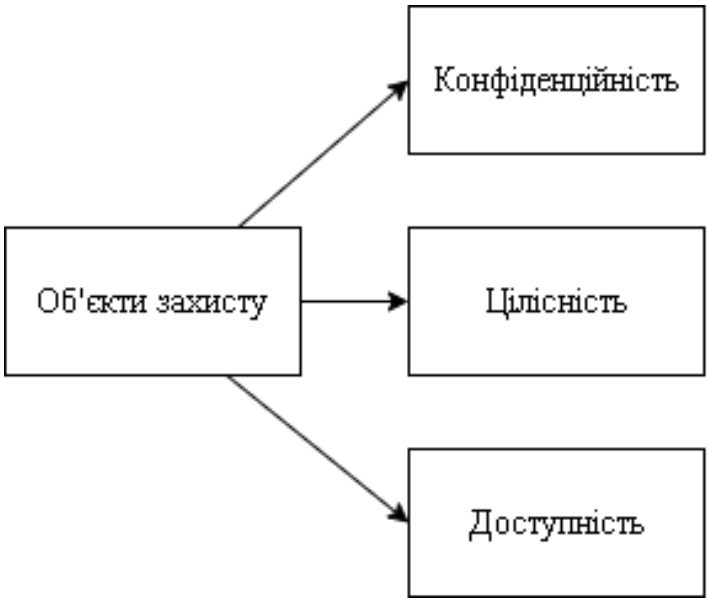

Рисунок 1. Тріада інформаційної безпеки

Згідно з [3] дуже важливим являється розуміння різниці між цими трьома концепціями.

Цілісність даних відноситься до вимоги захисту інформації від неналежної модифікації. Цілісність втрачається, якщо в дані або IT-систему вносяться несанкціоновані зміни в результаті навмисних або випадкових дій. Крім того, порушення цілісності може бути першим кроком в успішній атаці на доступність або конфіденційність системи.

Доступність – це властивість системи або системного ресурсу, доступність і використання за запитом уповноваженого системного об’єкта відповідно до специфікацій продуктивності системи. Забезпечення доступності передбачає запобігання атак відмови в обслуговуванні.

Конфіденційність відноситься до захисту інформації від несанкціонованого розкриття. Для підтримки конфіденційності даних необхідні криптографічні методи, такі як шифрування, заповнення мережевого трафіку та контроль доступу.

Тріаду CIA неодноразово критикували за її вузьку технічну орієнтацію та цілеспрямованість, а отже, її обмежену корисність, коли необхідно враховувати ширші організаційні та соціальні аспекти безпек. Тому, якщо дослідити тему глибше, то взаємодія між цими аспектими насправді виглядає так як на рисунку 2:

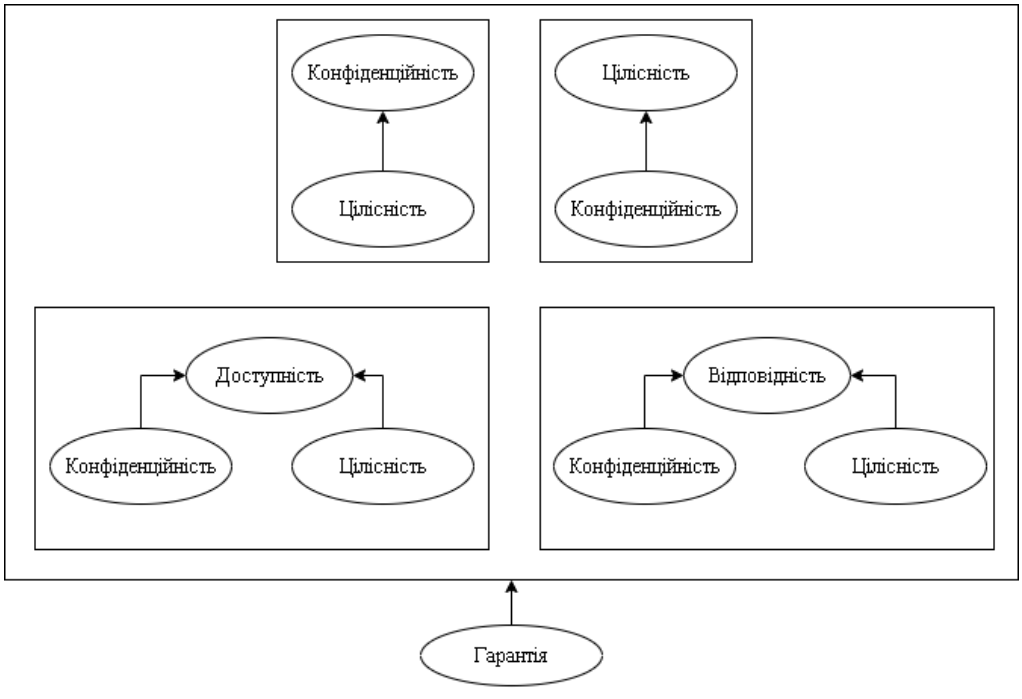

Рисунок 2 — Розширена модель взаємодії компонентів інформаційної безпеки

Тому відношення, які відбуваються між цими елементами, являються взаємозалежними.

Конфіденційність залежить від цілісності, оскільки якщо цілісність системи буде втрачено, то більше немає розумних очікувань, що механізми конфіденційності все ще дійсні.

Цілісність залежить від конфіденційності, оскільки, якщо конфіденційність певної інформації буде втрачено (наприклад, пароль суперкористувача), то механізми цілісності, швидше за все, будуть обійти.

Доступність та підзвітність залежать від конфіденційності та доброчесності, оскільки:

– у разі втрати конфіденційності певної інформації (наприклад, пароля суперкористувача), механізми, що реалізують ці цілі, легко обійти; і

– якщо втрачена цілісність системи, то втрачається і впевненість у дійсності механізмів, що реалізують ці цілі.

Усі ці цілі взаємозалежні від гарантії безпеки системи. При проектуванні системи інженер встановлює рівень впевненості у системі як цільовий рівень. Ця ціль досягається шляхом визначення та виконання вимог до функціональності в кожній із чотирьох інших цілей і виконання цього з достатньою «якістю». Упевненість підкреслює той факт, що для того, щоб система була безпечною, вона повинна не тільки забезпечувати передбачувану функціональність, але й гарантувати, що небажані дії не відбуваються.

Окрім цього, інформаційна безпека охоплює низку термінів, одним із найважливіших з яких являється контроль доступу. Це широкий термін, який охоплює кілька різних типів механізмів, які забезпечують контроль доступу до комп’ютерних систем, мереж та інформації. Він надзвичайно важливий, оскільки він є однією з перших ліній захисту в боротьбі з несанкціонованим доступом до систем і мережевих ресурсів. Коли користувачеві пропонується ввести ім’я користувача та пароль для використання комп’ютера, це контроль доступу. Щойно користувач увійде в систему та пізніше спробує отримати доступ до файлу, цей

файл може мати список користувачів і груп, які мають право доступу до нього. Якщо користувача немає в цьому списку, користувачу відмовлено. Це ще одна форма контролю доступу. Дозволи та права користувачів можуть ґрунтуватися на їх особі, дозволі та/або членстві в групі. Контроль доступу дає організаціям можливість контролювати, обмежувати, контролювати та захищати доступність ресурсів, цілісність і конфіденційність.

Основою, найсуттєвішою ідеєю в інформаційній безпеки є контроль доступу до ресурсів, щоб вони могли бути захищені Засоби контролю, які забезпечують контроль доступу, можуть бути технічними, фізичними або адміністративними. Ці типи контролю мають бути інтегровані в документацію на основі політики, програмне забезпечення та технології, проектування мережі та компоненти фізичної безпеки. Контроль доступу є одним із найбільш експлуатованих аспектів безпеки, ще через те, що являється шлюзом який веде до критичних активів. Елементи контролю доступу мають застосовуватися за допомогою багатошарового методу поглибленого захисту, і розуміння того, як ці елементи керування використовуються, надзвичайно важливо. Цей аспект представляє собою функції безпеки, які контролюють, як користувачі та системи спілкуються та взаємодіють з іншими системами та ресурсами. Вони захищають системи та ресурси від несанкціонованого доступу і можуть бути компонентами, які беруть участь у визначенні рівня авторизації після успішного завершення процедури аутентифікації.

Досягнення контролю стосується потоку інформації між суб’єктом і об’єктом. Суб’єкт – це активна сутність, яка запитує доступ до об’єкта або даних всередині об’єкта. Суб'єктом може бути користувач, програма або процес, який звертається до об'єкта для виконання завдання. Коли програма звертається до файлу, програма є суб’єктом, а файл – об’єктом. Об'єкт - це пасивна сутність, яка містить інформацію або необхідні функції. Об’єктом може бути комп’ютер, база даних, файл, комп’ютерна програма, каталог або поле, що міститься в таблиці в базі даних. Коли ви шукаєте інформацію в базі даних, ви є активним суб’єктом, а база даних — пасивним об’єктом.

Хоча ми зазвичай сприймаємо користувача як користувача, який потребує доступу до мережевого ресурсу або інформації, існує багато інших типів сутностей, які потребують доступу до інших мережевих об’єктів і ресурсів, які підлягають контролю доступу.

Для успішного проектування системи безпеки, потрібно не лише продумати статистичні елементи, а також передбачити методи управління та регулювання комплексу дій.

Управління безпекою охоплює всі дії, необхідні для підтримки програми безпеки в працездатності та розвитку. Вона включає в себе управління ризиками, документацію, впровадження та управління безпекою, процеси та процедури, безпеку персоналу, аудит та постійне навчання з питань безпеки. Аналіз ризиків визначає критичні активи, виявляє загрози, які ставлять їх під загрозу, і використовується для оцінки можливої шкоди та потенційних збитків, які організація може зазнати, якщо будь-яка з цих загроз стане реальною. Аналіз ризиків допомагає керівництву скласти бюджет із необхідними коштами для захисту визнаних активів від їх ідентифікованих загроз і розробити застосовні політики безпеки, які забезпечують напрямок діяльності з безпеки. Засоби захисту визначаються, впроваджуються та підтримуються, щоб підтримувати ризики безпеки організації на прийнятному рівні. Навчання та інформованість щодо безпеки доносять цю інформацію до кожного співробітника компанії, щоб кожен був належним чином проінформований і міг легше працювати для досягнення тих самих цілей безпеки.

Теж стосується і управління ризиками. Ризик у контексті безпеки — це можливість нанесення шкоди та наслідки такої шкоди, якщо вона станеться. Управління інформаційними ризиками (IRM) — це процес виявлення та оцінки ризику, зниження його до прийнятного рівня та впровадження правильних механізмів для підтримки цього рівня. Не існує такого поняття, як 100-відсоткове безпечне середовище. Кожне середовище має вразливості та загрози. Навичка полягає в тому, щоб визначити ці загрози, оцінити ймовірність їх дійсного виникнення та шкоду, яку вони можуть завдати, а потім зробити правильні кроки

для зниження загального рівня ризику в навколишньому середовищі до того, що організація визначає як прийнятного.

1.2 Різниця між кібер- та інформаційною безпекою

У наукових журналах, порталах та форумах тема кіберпезпеки посідає далеко не останнє місце. Але під час аналізу робіт, присвячених кібербезпеці та методам кібербезпеки, було виявлено неточність, яка може вплинути на якість цієї та поточних робіт, присвячених цій темі. У більшості літератури кібербезпека використовується як термін «все разом».

В залежності від джерел, мета та визначення інформаційної безпеки відрізняються. Але найточніше та правильно визначення цьому терміну надає міжнародний стандарт ISO/IEC 27002 (2005), який визначає інформаційну безпеку як збереження конфіденційності, цілісності та доступності інформації (ISO/IEC 27002, 2005, стор. 1). У контексті ISO/IEC 27002 (2005) інформація може приймати різні форми. Інформацію можна роздрукувати або написати на папері, зберігати в електронному вигляді, передавати поштою чи електронними засобами, показувати у фільмах, передавати в розмові тощо (ISO/IEC 27002, 2005, стор. 1).

По-перше, має бути зрозуміло, що інформаційна безпека — це не продукт чи технологія, а процес. За словами [4] інформаційна безпека раніше була суто технічною проблемою. Однак, по мірі розвитку використання комп’ютерів і мереж, процес захисту цих комп’ютерів і мереж також мав розвиватися, щоб вийти за рамки лише технічних. Процес інформаційної безпеки може вимагати використання певних продуктів, але це не те, що можна купити з полиці.

Другим важливим фактором, на який слід звернути увагу на наведені вище визначення, є те, що інформаційна безпека зазвичай визначається з точки зору властивостей або характеристик, які повинна мати захищена інформація. Вони зазвичай включають конфіденційність, цілісність і доступність інформації, але можуть включати додаткові характеристики.

Важливо зазначити, що існує різниця між інформаційною безпекою та безпекою інформаційних технологій (або інформаційно-комунікаційних технологій).

Безпека інформаційно-комунікаційних технологій (ІКТ) має справу із захистом фактичних систем, заснованих на технології, на яких зазвичай зберігається та/або передається інформація. Той самий стандарт, який зазначався раніше, визначає безпеку ІКТ як усі аспекти, що стосуються визначення, досягнення та підтримки всіх складових інформаційної безпеки, невідмовності, підзвітності, автентичності та надійності інформаційних ресурсів. Оскільки інформаційна безпека включає захист основних інформаційних ресурсів, можна стверджувати, що безпека ІКТ є підкомпонентом інформаційної безпеки.

Як згадувалося раніше, багато сучасних публікацій, що стосуються кібербезпеки, використовують термін кібербезпека як взаємозамінний термін інформаційна безпека. Якщо кібербезпека є синонімом інформаційної безпеки, було б розумно припустити, що інциденти нападу на безпеку також можна описати з точки зору характеристик, які використовуються для визначення інформаційної безпеки. Таким чином, ці інциденти наприклад, також призведять до порушення конфіденційності, цілісності або доступності інформації.

Це справедливо для більшості загроз, пов’язаних із кібербезпекою, яким можуть піддаватися користувач та/або організація. Однак існують загрози кібербезпеки, які не є частинною інформаційної безпеки. Але у цій роботі вони опускаються.

Будь-яка безпека — це захист активів від різних загроз, що виникають через певні притаманні вразливості, які досліджуються нижче. Процеси безпеки зазвичай стосуються вибору та впровадження засобів контролю безпеки (також званих контрзаходами), які допомагають зменшити ризик, пов’язаний із цими вразливими місцями. У випадку безпеки ІКТ, активи, які необхідно захистити, — це базова інфраструктура інформаційних технологій. Інформаційна безпека, з іншого боку, розширює це визначення активів, які підлягають захисту, щоб охопити всі аспекти самої інформації. Таким чином, він включає захист базових активів ІКТ, а потім

виходить за рамки просто технології, щоб включати інформацію, яка не зберігається або не передається безпосередньо за допомогою ІКТ.

Тому можна підсумувати термінологію. Інформаційна безпека – це захист інформації, яка є активом, від можливої шкоди, що виникає внаслідок різноманітних загроз і вразливостей. З іншого боку, кібербезпека — це не тільки захист самого кіберпростору, а й захист тих, хто функціонує в кіберпросторі, і будь-яких їхніх активів, до яких можна отримати доступ через кіберпростір.

1.3 Місце дистанційного доступу у е-навчанні

Електронні експерименти поширені в школах та університетах по всьому світу. Сьогодні декілька дистанційних лабораторій для таких експериментів доповнюють практичні в науково-технічній освіті [5]. Деякі з віддалених лабораторій, де студенти онлайн можуть виконувати фізичні експерименти та отримувати ті самі результати, що й у практичній лабораторії, є більш-менш копіями практичних. Таким чином, онлайн-учні складають схеми, використовуючи реальні компоненти, і роблять реальні вимірювання на створених схемах.

Останнім часом віртуальні лабораторії та лабораторії з віддаленим доступом стали надійною альтернативою традиційним лабораторіям. Відповідні лабораторні мережі дозволяють розподіляти витрати, забезпечують ефективний контроль доступу користувачів до експериментального середовища та можуть покращити доступність лабораторної інфраструктури. Безпека та захист в реальних лабораторіях є важливими питаннями, щоб уникнути як неправильної поведінки, так і навмисної шкоди. Це особливо актуально для віддалених лабораторій, оскільки це системи з високим рівнем зв'язку. Віддалені лабораторії в державних установах, таких як університети та школи, надзвичайно вразливі до проблем безпеки. Те, що віддалена лабораторія являється державною, навіть включаючи незалежні та мережеві структури, являється фактором, який збільшує ризики безпеки.

Більшість реалізацій веб-лабораторій зосереджені на можливостях взаємодії для маніпулювання ресурсами лабораторії через мережу. Такі засоби намагаються відтворити на комп'ютері користувача ті самі механізми взаємодії, які використовуються під час роботи ресурсів на сайті. Наприклад, експеримент у лабораторії, в якому використовується аналізатор спектру, може запропонувати інтерфейс, який досконало відображає консоль обладнання з його екранами, кнопками, ручками, перемикачами та світлом. За допомогою цього інтерфейсу віддалений студент може керувати обладнанням приблизно так само, як якщо б він фізично перебував у лабораторії.

Хоча взаємодія є ключовою проблемою в дизайні дистанційної лабораторії, вона не єдина. Оскільки швидкість інтернет-з'єднання постійно зростає, а високошвидкісні академічні мережі охоплюють все більше студентів і дослідників, очікується, що такі лабораторії стануть цінними інструментами для практичних експериментів у навчальній та дослідницькій діяльності. У цьому сценарії установи також можуть виявити інтерес до спільного використання веб-лабораторій, щоб розширити спектр лабораторних можливостей, що пропонуються своїм студентам і дослідникам. Такі питання, як безпека, якість обслуговування та функціонування поза межами організації, стають вирішальними для успіху майбутніх проектів.

Лабораторії віддаленого доступу використовуються по всьому світу, щоб дати можливість студентам-інженерам практикувати практичні навички та покращувати свої знання шляхом практичних експериментів [6]. Ці засоби також розширюють доступ, дозволяючи користувачам проводити експерименти в будь-якому місці в будь-який час, забезпечуючи більшу гнучкість і мобільність. Кілька систем дистанційних лаборіторій успішно досягли цих цілей. Однак роль дизайнерів експериментів рідко досліджувалася або розширювалася з моменту задуми лаборіторій. Експерименти розроблені та розміщені в Інтернеті невеликою групою експертів у відповідних областях. Хоча ці системи були успішними для університетів, де є експерти та відповідне середовище, вони рідко використовувалися в школах; та наукова, технологічна, інженерно-математична (STEM) освіта. Оскільки педагогічний дизайн зараз розглядається як критична

розробка в спонуканні до нових експериментів, будь-яка ініціатива лабораторії з дистанційним доступом для інженерної освіти повинна враховувати педагогічні міркування з самого початку.

Технології лабораторій з дистанційним доступом поки що обмежувалися копіюванням досвіду лабораторій на місці з великою точністю в онлайн-середовищі renote для підтримки еквівалентних результатів навчання. Ці лабораторії постійно зосереджуються на сферах вищої освіти, але не мають можливості інфраструктурної підтримки для скорочення STEM та пов’язаних з ними фізичних навантажень. Отримані інструменти онлайн-навчання в основному спрямовані на вирішення обмежених ресурсів університетів, освіта STEM має інші потреби. Ключовими вимогами є співпраця та практичний досвід створення та проведення експериментів. Сучасні функції лаборіторій є складними і є перешкодою для осіб з невеликим досвідом роботи в мережах, комп’ютерних системах та приладах. Використовуючи новітні веб-технології та парадигму однорангового доступу, такі системи можуть забезпечити набагато більш багаті умови та досвід для студентів, які дистанційно взаємодіють із експериментами та співпрацюють у спільній діяльності в контексті інженерної освіти.

Останнім часом існує занепокоєння щодо повільної адаптації віддалених лабораторій з викладачами для своїх студентів. Основною причиною недостатнього використання технологій дистанційної лабораторії назвали опір викладачів впроваджувати нові технології в питання викладання та технічної підтримки. Ці причини стають більш помітними, якщо установки, які мають використовувати вчителі, насправді розроблені кимось іншим, а не ними. Інше дослідження в Європі робить висновок, що школи та вчителі дуже зацікавлені у віддалених лабораторіях, але не знають, як інтегрувати їх у програму навчання. Здебільшого це пов'язано з тим, що вони не в змозі виконати обчислювальні вимоги в реалізаціях лабораторій і відповідних педагогічних і технічних концепціях.

Оскільки дистанційні лабораторії вважаються розширеними лабораторіями на місці, їх навчальний план і структура дуже нагадують місцеву лабораторію. Це ідеально підходить для вищої освіти, де експерименти мають фіксований характер

і проводяться за допомогою спеціального обладнання, і є менше місця для «гравання» з налаштуванням. З іншого боку, у STEM-освіті, хоча список цілей може бути статичним, фізична система, як правило, дуже гнучка. Такий самий вид діяльності можна виконувати з різними налаштуваннями, щоб зрозуміти концепції STEM, що стоять за цим. Ці установки мають бути створені та використані учнями для ефективного навчання.

Існує кілька засобів контролю безпеки для усунення вразливостей у віддаленому доступі. Засоби керування безпекою, наприклад, антивірус заснований на сигнатурах, де для ефективного виявлення необхідно знати варіант шкідливого програмного забезпечення. Коли справа доходить до евристичних підходів, вони схильні до високого рівня помилкових спрацьовувань і довго аналізують трафік на предмет зловмисного програмного забезпечення та інших компромісів. Протягом багатьох років було розроблено та впроваджено кілька підходів для забезпечення безпеки в мережах, багато з яких зосереджені на безпеці віддаленого доступу.

З точки зору дистанційних лабораторій, однорангова система може вирішити проблеми традиційних віддалених комплексів. Користувачі можуть бути як творцями експериментів, так і ділитися ними з іншими та бути користувачами інших експериментів. Після того, як люди отримають можливість розробляти та проводити експеримент, це може створити більшу гнучкість на стороні постачальників лабораторій. Студенти, які користуються цими лабораторіями, можуть співпрацювати один з одним у запуску установки, таким чином даючи користувачам новий погляд на ту саму проблему, яка може відрізнятися від їхньої. Таким чином можуть бути реалізовані нові та цікаві ідеї щодо практичного навчання та методології навчання на основі запитів.

1.4 Роль конфіденційності у інформаційній безпеці

Цей розділ призначений аналізу конфіденційності, а саме: визначенню терміна конфіденційність, місце конфіденційності в інформаційній безпеці, а також

Конфіденційність забезпечує дотримання необхідного рівня секретності на кожному етапі обробки даних і запобігає несанкціонованому розголошенню. Цей рівень конфіденційності має переважати, поки дані знаходяться в системах і пристроях у мережі, під час їх передачі та після досягнення місця призначення.

Зловмисники можуть перешкодити механізмам конфіденційності за допомогою моніторингу мережі, перегляду даних, крадіжки файлів паролів, зламу схем шифрування та соціальної інженерії. Ці теми будуть більш детально розглянуті в наступних розділах.

Користувачі можуть навмисно або випадково розкрити конфіденційну інформацію, не шифруючи її перед відправкою іншій особі, ставши жертвою атаки соціальної інженерії, ділячись конфіденціальною інформацією лабораторії, або не дотримуючись особливої обережності для захисту конфіденційної інформації під час її обробки.

Після втрати конфіденційність неможливо відновити[7]. Тому служби виявлення та відновлення, які можуть відігравати важливу роль у підтримці доступності та цілісності, не поширюються на конфіденційність. Захист повідомлень від розголошення, забезпечення авторизованих доступів на читання та можливість збереження конфіденційності забезпечують конфіденційність.

На рисунку 3 зображено метод первинного забезпечення конфіденційності.

Конфіденційність може бути забезпечена шляхом шифрування даних під час їх зберігання та передачі, забезпечення суворого контролю доступу та класифікації даних, а також навчанням студентів належним процедурам захисту даних.

Захист конфіденційності стосується даних, які зберігаються, під час обробки та передачі. Для багатьох організацій конфіденційність часто стоїть за доступністю та цілісністю з точки зору важливості. Проте для деяких систем і для конкретних типів даних у більшості систем (наприклад, аутентифікатори) конфіденційність надзвичайно важлива.

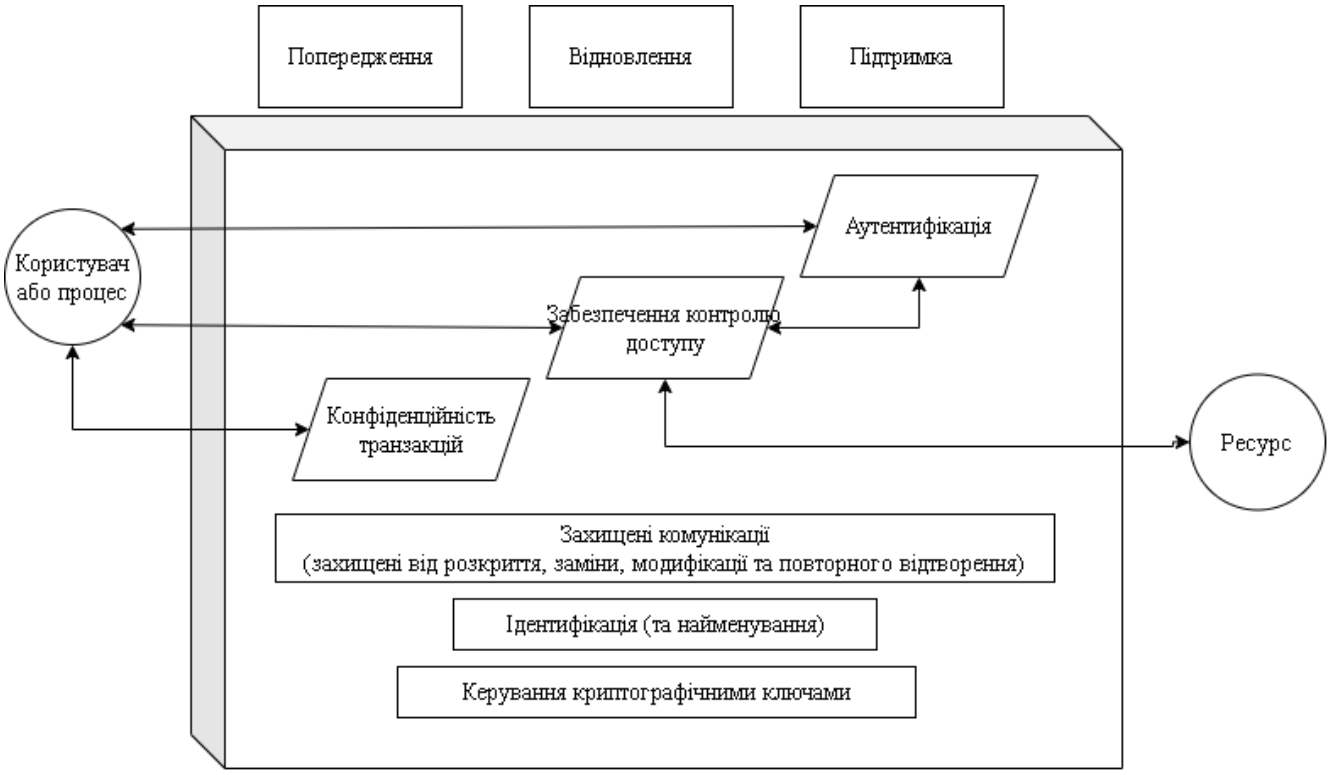

Рисунок 3 — Метод первинного забезпечення конфіденційності

1.5 Атаки, вразливості та загрози

Передача інформації через інтернет це швидко, легко та дешево. Однак цей спосіб зв’язку та доступу через загальнодоступні мережі схильний до різного роду загроз безпеці, які експлуатують вразливі місця в мережах зв’язку. У віддаленому доступі вразливості є очевидними від точки ініціалізації зв’язку, що йде за каналом зв’язку, до ресурсів, до яких здійснюється доступ. Загрози відрізняються залежно від типу пристрою, який використовується для отримання віддаленого доступу. Але попри це, існують розбіжності у тому, що саме вважати загрозою.

Слова «вразливість», «загроза», «ризик» і «експозиція» часто міняються місцями, хоча вони мають різні значення. Важливо розуміти визначення кожного слова та зв’язку між поняттями, які вони уявляють.

Уразливість — це відсутність контрзаходу або слабкість у контрзаході, який діє. Це може бути програмна, апаратна, процедурна або людська слабкість, яку можна використати. Уразливістю може бути служба, що працює на сервері, невиправлені програми чи операційні системи, необмежена точка бездротового

доступу, відкритий порт на брандмауері, слабка фізична безпека, що дозволяє будь-кому ввійти до серверної кімнати, або невимушене керування паролями на серверах і робочих станціях.

Загроза – це будь-яка потенційна небезпека, пов’язана з використанням уразливості. Загроза полягає в тому, що хтось чи щось визначить конкретну вразливість і використає її проти компанії чи особи. Суб'єкт, який використовує переваги вразливості, називається агентом загрози. Агентом загрози може бути зловмисник, який отримує доступ до мережі через порт брандмауера, процес, який отримує доступ до даних таким чином, що порушує політику безпеки, торнадо, що знищує об’єкт, або працівник, який робить ненавмисну помилку, яка може розкрити конфіденційну інформацію.

Ризик — це ймовірність використання агентом загрози уразливості та відповідного впливу на бізнес. Якщо брандмауер має кілька відкритих портів, є більша ймовірність того, що зловмисник використає один для доступу до мережі несанкціонованим способом. Якщо користувачі не ознайомлені з процесами та процедурами, існує більша ймовірність того, що працівник зробить ненавмисну помилку, яка може знищити дані. Якщо система виявлення вторгнень (IDS) не реалізована в мережі, є більша ймовірність, що атака залишиться непоміченою, поки не стане занадто пізно. Ризик пов’язує вразливість, загрозу та ймовірність експлуатації з результуючим впливом на бізнес.

Експозиція – це випадок ризику зазнати збитків. Уразливість наражає організацію на можливі збитки. Якщо керування паролями є слабким і правила паролів не дотримуються, компанія наражається на можливість захоплення та використання паролів користувачів у несанкціонований спосіб. Якщо компанія не перевіряє електропроводку та не вживає заходів щодо запобігання пожежам, вона піддається потенційно руйнівним пожежам.

Для пом’якшення (зменшення) потенційного ризику вводиться контроль або контрзахід. Контрзаходом може бути конфігурація програмного забезпечення, апаратний пристрій або процедура, яка усуває вразливість або зменшує ймовірність того, що агент загрози зможе використати вразливість. Приклади контрзаходів

включають надійне керування паролями, брандмауери, охорону, механізми контролю доступу, шифрування та навчання з питань безпеки.

Якщо компанія має антивірусне програмне забезпечення, але не оновлює підписи, це є вразливістю. Компанія вразлива до атак зловмисного програмного забезпечення. Загроза полягає в тому, що вірус з'явиться в навколишньому середовищі та порушить продуктивність. Ймовірність появи вірусу в навколишньому середовищі і заподіяння шкоди, а також потенційної шкоди, що випливає з цього, є ризиком. Якщо вірус проникає в середовище компанії, це означає, що вразливість використано, і компанія зазнає збитків. Контрзаходами в цій ситуації є оновлення сигнатур і встановлення антишкідливого програмного забезпечення на всіх комп'ютерах.

Застосування правильного контрзаходу може усунути вразливість та ризик, а отже, зменшити ризик. Компанія не може усунути агента загрози, але вона може захистити себе та запобігти використанню цього агента загроз уразливими місцями в середовищі.

Багато робіт опускає ці основні терміни, думаючи, що вони не настільки важливі, як інші речі інформаційній безпеці. Але якщо команда безпеки не має узгодженої мови, може душе швидко прийти плутанина. Ці терміни охоплюють основні поняття безпеки, і якщо їх будь-яким чином плутають, то зазвичай плутають дії, які впроваджуються для забезпечення безпеки.

Дані та інформація, що передаються через Інтернет, швидко, легко та дешево. Однак цей спосіб зв'язку та доступу через загальнодоступні мережі схильний до різного роду загроз безпеці, які експлуатують вразливі місця в мережах зв'язку. У віддаленому доступі вразливості є очевидними від точки ініціалізації зв'язку, що йде за каналом зв'язку, до ресурсів, до яких здійснюється доступ. Загрози відрізняються залежно від типу пристрою, який використовується для отримання віддаленого доступу. Один із видів пристроїв віддаленого доступу можна вважати настільки безпечним, оскільки організація, що надає послуги, ймовірно, видає його для віддаленого доступу. Таким чином, організація забезпечує встановлення оновлень і виправлень, які захищають пристрій, а також інше програмне

забезпечення безпеки та інші засоби контролю, які вважаються необхідними відповідно до політики безпеки організації-видавця. Пристрої віддаленого доступу називаються керованими пристроями віддаленого доступу. Інший тип пристроїв вважається ризикованим і небезпечним, оскільки вони знаходяться поза контролем і моніторингом організації. Пристрої є ризикованими, оскільки в них відсутні заходи для забезпечення або підтримки базових планів безпеки, як зазначено в політиці безпеки організації.

1.6 Висновки

У першому розділі оглянуто основні концепції, з якими доводиться стискатися при проектуванні систем безпеки. Без дослідження аспектів термінології важко заплутатися у дослідженнях і методах.

Протягом майже 40 років, починаючи з часів моделей Белла-Ла Падули та Біби, які стосувалися конфіденційності та цілісності даних відповідно терміни «конфіденційність», «цілісність» і «доступність» були широко використовується в практиці інформаційної безпеки та в науковій літературі. «Тріада CIA», як відомо, спочатку відноситься до фундаментальних елементів контролю безпеки в інформаційних системах. Ці три ключові терміни не тільки сформували та поінформували наше теоретичне розуміння інформаційної безпеки, але й самі практики, за допомогою яких безпека розробляється та впроваджується в організаціях.

Можна зробити наступні висновки по лабораторіям з дистанційним доступом. Хоча кілька розробників вдосконалювали й працювали над різними аспектами лабораторії з віддаленим доступом, такими як інтерфейс користувача та педагогіка експерименту, основна архітектура залишилася незмінною. Деякі подібності можна підсумувати таким чином:

1. Сучасні тенденції розробки дозволяють створювати експеримент лише досвідченим і розробникам-експертам. Тому різноманітність експериментів обмежена і зосереджена на окремих галузях вищої освіти.

2. Інструменти та пристрої, що використовуються, переважно дорогі та складні у будівництві та експлуатації. Вони використовують промислові стандарти, для підключення обладнання до комп'ютерних серверів. Високопродуктивне програмне забезпечення для інженерії, таке як Lab VIEW, VEE та MATLAB, також широко використовується для реалізації цих налаштувань експерименту. Таким чином, робота над устаткуванням залишається проблемою високої складності в усіх подібних лабораторіях.

3. Системи управління лабораторією мають переважно клієнт-серверний характер. Усі користувачі мають увійти в облікові дані, щоб авторизувати доступ, вибрати експеримент перед його використанням. Будь-яка реалізована мережева технологія по суті обмежена серверною стороною архітектури. Конфігурація експерименту являються також централізованими лабораторними умовами. Усі лабораторії розраховані на тривалу експлуатацію та постійно доступні для студентів.

4. Є дуже обмежені можливості для співпраці між студентами в різних географічних місцях і зазвичай недоступні в таких лабораторіях, , хоча цьому питанню надається важливе значення в деяких системах. Також існує тенденція до включати 3D-інтерфейси користувача для цілей спільного навчання.

5. Експерименти, що передбачають інженерні курси в бакалавраті та магістратурі. Здається, мало уваги приділяється інженерній науковій освіті, яка швидко стає важливою сферою розвитку з використанням методів навчання на основі запитів.

Методологія навчання на основі дистанційної інженерної освіті вимагає від студентів аналізувати проблеми та знаходити рішення за допомогою практичних знань та впровадження для розуміння концепцій. Таким чином, може існувати нескінченна кількість різноманітних установок і пристроїв, які можна використовувати для розробки різних концепцій. Більше того, у шкільних системах саме вчителі та учні ближче до розробки експериментальної установки, ніж експерти, які вже надають обладнання для попереднього налаштування. Але, з вищезазначеними особливостями створення нових лабораторій для них складно.

Хоча безпека та захист необхідні, в першу чергу слід враховувати конкретні вимоги до університетських лабораторій:

1. Необхідність простого підходу до вирішення питань безпеки та захисту, оскільки університетам доводиться мати справу з обмеженою кількістю людських ресурсів для виконання оперативних завдань.

2. Необхідність спільно дивитися на безпеку та захист, зменшувати зусилля та розглядати взаємодію обох тем, що впливають одна на одну.

3. Необхідність гнучкого та ітеративного підходу, оскільки університетські лабораторії постійно змінюються, особливо в навчальних темах, пов’язаних з новими технологіями.

Державні віддалені інфраструктури покладаються на фізичне обладнання (фізичний світ), пов’язане з IT, яке є дуже вразливими для кібершпигунства. Отже, віддалений доступ входить до десятки загроз для промислових систем керування. Існує підвищений ризик через цифрове збільшення поверхонь атаки. Хоча автономні лабораторії вимагають фізичної присутності для атаки на систему, віддалені лабораторії можуть бути атаковані по всьому світу. Тому проблеми безпеки у «віртуальному світі» можуть завдати шкоди у «фізичному світі». Важливо, що безпеку та захист для дистанційних лабораторій потрібно вирішувати спільно.

Важливо розуміти, що поява нових технологій не тільки породжує нові способи атак, але й розширює існуючий список загроз, і, як відомо, кожна загроза може бути здійснена великою кількістю різноманітних атак. Поява нових технологій нелінійно знижує рівень безпеки існуючих систем. У зв’язку з цим на перший план виходить необхідність формування повного переліку інформаційних загроз, але ця проблема не має простого вирішення. Що вже говорити про звичайних користувачів, навіть якщо фахівці з інформаційної безпеки не завжди можуть правильно скласти повний список усіх можливих загроз. Для вирішення цієї проблеми створюються різноманітні моделі загроз, які базуються на всіляких математичних інструментах та інформаційних моделях.

З усього вищесказаного випливають наступні тези:

– при визначенні переліку загроз конфіденційності, цілісності та доступності інформації слід використовувати різні моделі загроз;

– необхідно здійснювати суворий контроль за каналами передачі інформації;

– процес формування моделі загрози повинен враховувати не тільки вузли системи, а й канали, інакше така модель ніколи не досягне завершеності.

2 АНАЛІЗ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ У КОНТЕКСТІ ДИСТАНЦІЙНОГО ДОСТУПУ

2.1 Постановка завдання

Конфіденційність — це гарантія того, що інформація не буде розголошена неавторизованим особам, програмам або процесам. Деякі відомості є більш конфіденційними, ніж інші, і вимагають більш високого рівня конфіденційності. Повинні бути встановлені механізми контролю, щоб диктувати, хто може отримати доступ до даних і що суб’єкт може робити з ними після того, як вони отримали до них доступ. Цю діяльність необхідно контролювати, перевіряти та контролювати. Деякі механізми безпеки, які забезпечують конфіденційність, — це шифрування, контроль логічного та фізичного доступу, протоколи передачі, представлення бази даних та контрольований потік трафіку.

Конфіденційність пов’язана з приватністю інформації, включаючи дозвіл на її перегляд, обмін та використання. Інформація з низьким рівнем конфіденційності може вважатися «публічною» або іншим чином не загрозливою, якщо вона розкривається за межами цільової аудиторії. Інформація з високим рівнем конфіденційності вважається таємною та має бути конфіденційною, щоб запобігти крадіжці особистих даних, компрометації облікових записів і систем, правовій чи репутаційній шкоді та іншим серйозним наслідкам.

Для співробітників лабораторного комплексу важливо визначити дані, які мають бути засекречені, щоб розробники могли гарантувати, що найвищий пріоритет безпеки захищає цю інформацію та зберігає її конфіденційність. Якщо цю інформацію не виділити окремо, можна витратити занадто багато часу та грошей на впровадження однакового рівня безпеки для критичної та повсякденної інформації. Може знадобитися налаштувати віртуальні приватні мережі (VPN) між організаціями та використовувати протокол шифрування IPSec для шифрування

всіх повідомлень, що передаються під час передачі конфіденційних даних або обміну інформацією про студентів. Це вимагає певної кількості обладнання, праці, коштів та накладних витрат. Отже, першим кроком у захисті конфіденційності даних є визначення того, яка інформація є конфіденційною і в якій мірі, а потім запровадити механізми безпеки для її належного захисту.

Для початку, потрібно з’ясувати, яка інформація захищається.

– Персональна інформація студентів

– Комерційні таємниці

– Паролі, які повинні залишатися конфіденційними для захисту систем і облікових записів.

У разі порушення конфіденційності це може призвести до несанкціонованого доступу до особистої інформації або навіть до повної втрати конфіденційності!

Керуючи конфіденційністю даних, також потрібно враховувати наступне:

– Кому можуть бути розкриті дані

– Незалежно від того, чи вимагають закони, постанови чи контракти, щоб дані залишалися конфіденційними

– Чи можна використовувати або оприлюднювати дані лише за певних умов

– Чи є дані конфіденційними за своєю природою і чи будуть вони мати негативний вплив, якщо їх розкрити

– Чи будуть дані цінними для тих, кому не дозволено їх володіти (наприклад, хакерам)

Різні механізми безпеки можуть забезпечити різний ступінь конфіденційності. Навколишнє середовище, класифікація даних, які підлягають захисту, і цілі безпеки повинні бути оцінені, щоб забезпечити придбання та впровадження належних механізмів безпеки.

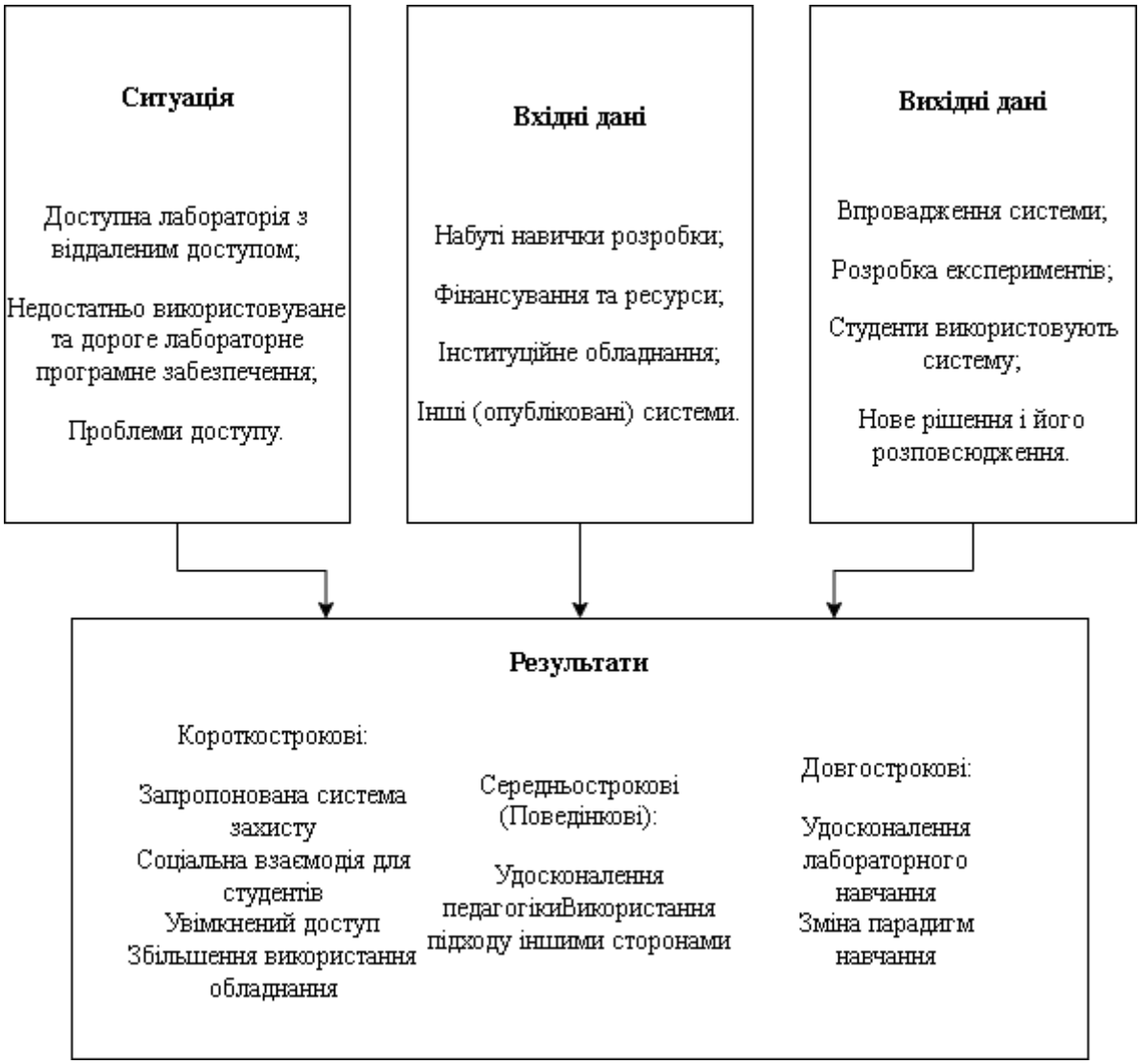

Рисунок 4 – Постановка завдання

2.2 Дослідження методів організації дистанційного доступу

Спостерігається тенденція заміни традиційних місцевих лабораторій відкритими та дистанційними. PLC широко використовується у виробництві для координації різноманітних складних завдань, таких як моніторинг безпеки, управління споживанням енергії та керування автоматичними виробничими лініями. Як наслідок, існує велика потреба в інженерах із сильними навичками та знаннями в цій галузі.

Хоча багато навчальних закладів охоплюють PLC на курсах бакалавра, але студентам бракує ресурсів, щоб стати кваліфікованим програмістом на PLC.

Обмежений доступ до лабораторій та обмежена наявність обладнання ускладнюють студентам достатні можливості для практики. Особливо гострою стала проблема з початком пандемії COVID-19, коли реалізувати доступ до існуючого обладнання просто неможливо. У результаті, знижується продуктивність навчання, а також простоює лабораторне обладнання. Створення умов для віддаленого доступу також може відкрити можливості для людей з підвищеними потребами та літнім людям (через знаходження лабораторії на 10-му поверсі та нестабільності роботи ліфта).

Перед організацією системи безпеки віддаленої лабораторії, потрібно проаналізувати існуючі успіхи та невдачі, зроблені при виборі того чи іншого методу. У цьому розділі досліджуються існуючі моделі організації дистанційного доступу, а також їх основні проблеми та недоліки. На основі аналізу пропонується оптимальний варіант архітектури.

2.2.1 Згрупування видів організації дистанційного доступу

Для інженерних програм лабораторія є основним елементом викладання та навчання. Лабораторії дозволяють студентам застосовувати абстрактні або теоретичні знання, отримані на лекціях, і розвивати своє розуміння за допомогою цього застосування. Останні досягнення в Інтернеті та технології створили нові можливості, і, як наслідок, імітовані та віддалені лабораторії досягли широкого проникнення в інженерну освіту. Дослідження, що вивчали різні режими доступу (практичний, змодельований, віддалений), показали, що режим доступу може впливати на результати навчання студентів різними та складними способами. Тому, де це можливо, рекомендується доповнити практичну лабораторію моделюванням або дистанційною лабораторією.

Хоча приклади віддалених інженерних лабораторій можна знайти майже для кожної інженерної дисципліни, існує дуже мало повідомлень про віддалені лабораторії, які спеціально націлені на програмування програмованого логічного контролера (ПЛК).

Курс програмування на ПЛК являється частиною програми третього та четвертого курсу бакалаврів комп'ютерної інженерії з дисциплін «Системи реального часу», «Захист інформації» та «Проектування корпоративних мереж» і торкається великого об'єму теоретичних та практичних знань. Метою цих курсів є познайомити студентів з апаратним і програмним забезпеченням, пов'язаним з комерційними ПЛК, і розвинути компетенцію для проектування програмованих логічних програм. Для досягнення цієї мети курс проводиться в середовищі студійного типу, обладнаному як для лекцій, так і для практичних експериментів. Більша частина занять має практичну спрямованість. Студенти взаємодіють з апаратним забезпеченням ПЛК, пов'язаним програмним забезпеченням, розробляють рішення для певних проблем процесу або впроваджують і тестують свої розроблені рішення.

Проаналізувавши загальні тенденції в організації та проектуванні лабораторій з віддаленим доступом можна зробити декілька висновків. По-перше, серед досліджень дистанційних лабораторій виділяють дві основні класифікації. Перша категорія це лабораторії, де дистанційний доступ заснований на моделюванні програмного забезпечення друга — на апаратному інтерфейсі.

На основі робіт [13, 14, 15] можна проілюструвати узагальнений підхід до організації дистанційної лабораторії на базі програмного забезпечення (рисунок 5):

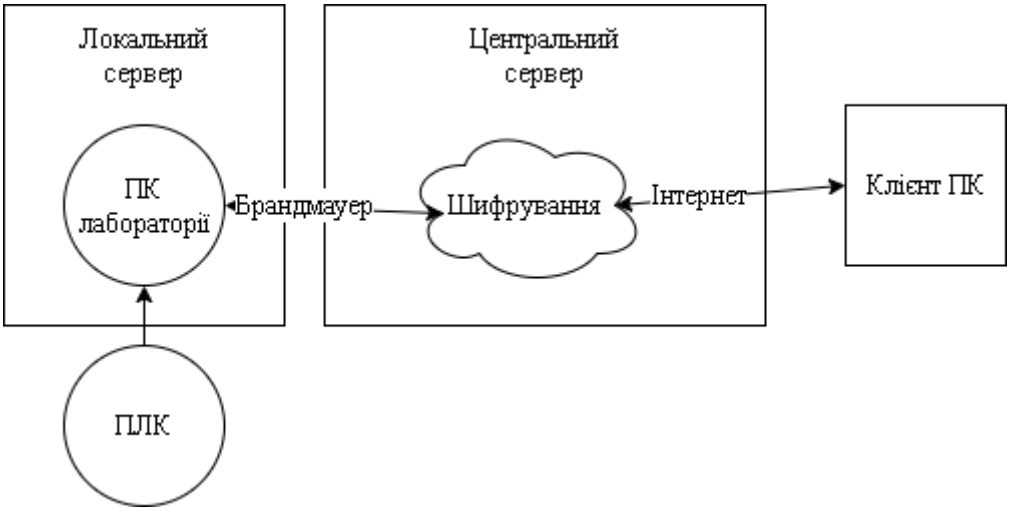

Рисунок 5 – Модель лабораторії на програмній базі

З іншого боку, роботи [10, 11, 12] дозволяють зрозуміти, до якої організації архітектури приходять розробники, у ході розробки лабораторій з дистанційним доступом (рисунок 6):

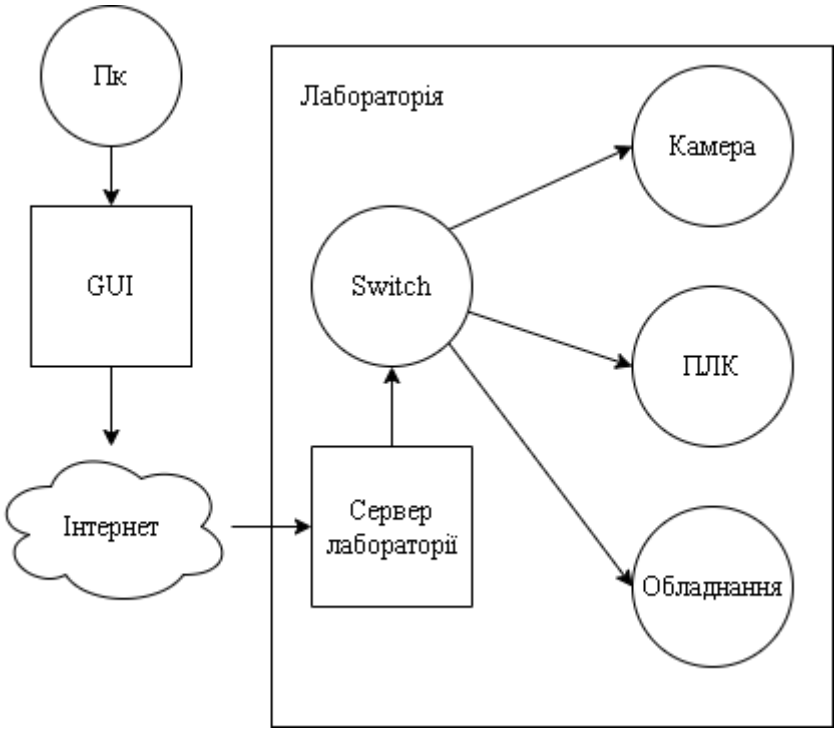

Рисунок 6 – Модель лабораторії на апаратній базі

Але незалежно від того, який метод буде прийнятий, для нього потрібні певні специфічні знання. Не завжди викладач, або, наприклад, лаборант, у лабораторії з ПЛК має можливість мати стільки знань для застосування. Для подолання недоліків непорозуміння потрібно прийняти рішення використовувати відоме програмне забезпечення дистанційного керування для реалізації дистанційного керування ПЛК, яке забезпечить студентам реальне експериментальне середовище.

Віртуальні лабораторії (VL) можуть бути реалізовані як настільні програми (запущені в операційній системі користувача) або веб-додатки (запущені у веб-браузері користувача). У порівнянні з веб-додатками, настільні програми мають такі недоліки:

– Вони менш портативні: настільні програми прив’язані до певної платформи, напр. операційну систему, віртуальну машину Java, середовище виконання загальної мови .NET тощо.

– Вони менш безпечні: настільні програми зазвичай вимагають повного доступу для встановлення, вони мають повний доступ до жорсткого диска користувача, вони можуть відкривати необмежені з’єднання із зовнішнім світом тощо.

2.2.2 Визначання оптимальної моделі архітектури

На основі існуючих моделей архітектури побудовано модель архітектури, яка найбільш відповідає вимогам безпеки та організації віддаленого доступу. Архітектура віддаленого доступу створена на базі мережі лабораторії. Структура топології показана на рисунку (7). Різні навчальні моделі ПЛК в різних місцях можуть бути підключені до локальної мережі через локальний комп'ютер як веб-сервер.

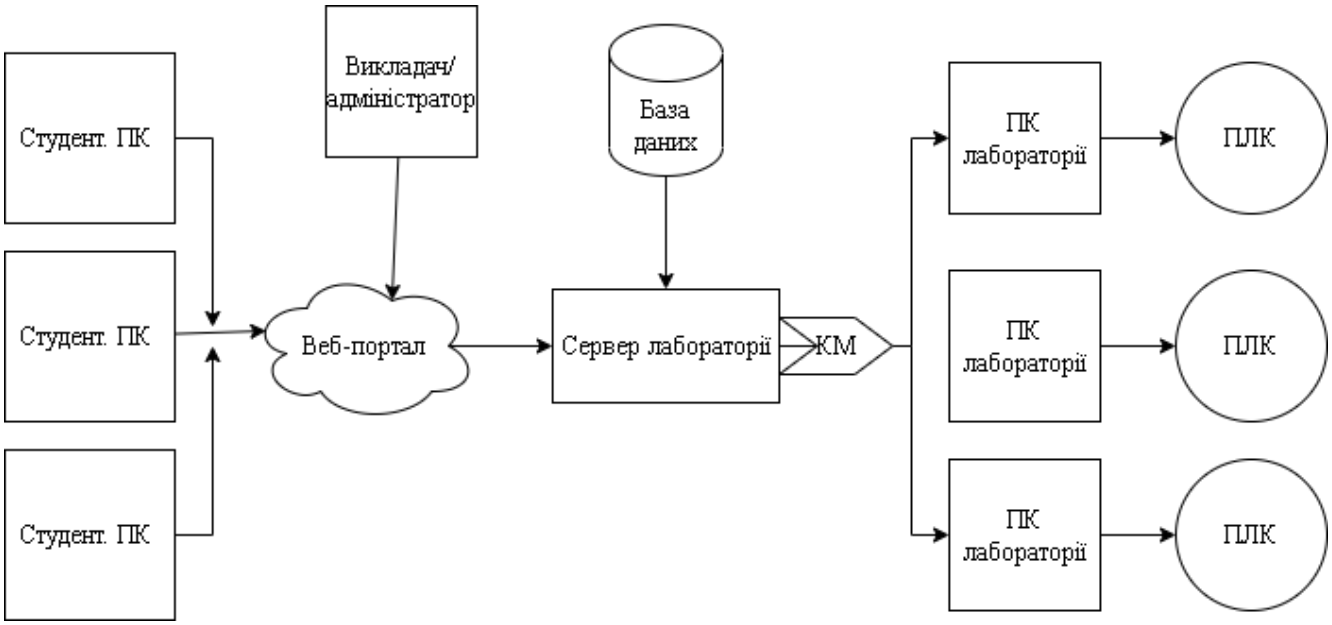

Рисунок 7 – Оптимальна модель архітектури

Для дистанційного навчання з використанням віддалених лабораторій потрібен пристрій візуалізації, який дозволить перевіряти та контролювати правильне функціонування програм під час завантаження програм у ПЛК. Ця

візуалізація посилює сприйняття «реального світу» для студентів і дійсно демонструє їм, що вони не виконують моделювання, а виконують реальну лабораторну роботу.

Після того, як студент встановив шлях зв'язку з локальним сервером, йому негайно з'являється екран для початку сеансу, використовуючи свій ідентифікаційний номер студента. Студенти вибирають ПЛК, який вони мають намір використовувати, а потім можуть вибирати з різноманітних експериментів. Ці експерименти будуть розроблені з дотриманням принципів розробки навчального змісту для віддалених лабораторій.

З огляду на те, у більшості це вступний курс, експерименти мають починатися з дискретних вхідних і вихідних сигналів, аналогових вхідних і вихідних сигналів та керування. Вступні експерименти повинні обов'язково передбачатись системою, тому що вони служать для розвитку компетенції з програмним середовищем програмування.

2.3 Обґрунтування моделі захисту конфіденційності

(ISC)² відрізняє політику безпеки від моделі безпеки наступним чином. Політика безпеки визначає, як здійснюється доступ до даних, який рівень безпеки необхідний і які дії слід вжити, якщо ці вимоги не виконуються. Політика окреслює очікування комп'ютерної системи чи пристрою. Модель безпеки — це твердження, що викладає вимоги, необхідні для належної підтримки та реалізації певної політики безпеки. Якщо політика безпеки диктує, що всі користувачі мають бути ідентифіковані, автентифіковані та авторизовані перед доступом до мережевих ресурсів, модель безпеки може викласти матрицю контролю доступу, яку слід побудувати так, щоб вона відповідала вимогам політики безпеки. Якщо політика безпеки стверджує, що ніхто з нижчого рівня безпеки не повинен мати можливість переглядати або змінювати інформацію на вищому рівні безпеки, допоміжна модель безпеки окреслить необхідну логіку та правила, які необхідно запровадити, щоб гарантувати, що ні за яких обставин не може суб'єкт нижчого рівня отримує

доступ до об’єкта вищого рівня несанкціонованим способом. Модель безпеки надає більш глибоке пояснення того, як повинна бути розроблена операційна система комп'ютера, щоб належним чином підтримувати конкретну політику безпеки.

Термін комп’ютерна безпека може визивати певні непорозуміння, оскільки навіть у науковому суспільстві для різних ситуацій може означати різні речі. Існує багато аспектів системи, які можна захистити, і безпека може відбуватися на різних рівнях і в різному ступені. Інформаційна безпека складається з таких основних атрибутів:

– Доступність. Запобігання втрати доступу до ресурсів і даних

– Цілісність. Запобігання несанкціонованої модифікації даних

– Конфіденційність. Запобігання несанкціонованому розголошенню даних/

Звідси ці основні атрибути розгалужуються до більш детальних атрибутів безпеки, таких як автентичність, підзвітність, невідмовність і надійність. Для того, щоб дізнатися, які саме атрибути потрібні для конкретного випадку, в якій мірі вони потрібні, і чи операційні системи та програми, які вони використовують, насправді забезпечують ці функції та захист, потрібно прикласти певні зусилля. Ці питання стають набагато складнішими, якщо глибше заглянути в самі питання та системи. Університет повинен бути стурбованим не лише тим, щоб шифрувалися повідомлення електронної пошти, коли вони проходять через Інтернет. А також конфіденційними даними, що зберігаються в їхніх базах даних та конкретно в базах даних лабораторії, безпекою їхніх веб-ферм, які підключені безпосередньо до Інтернету, цілісністю значень введення даних, що надходять у програми, внутрішніми користувачами, які передають інформації, зовнішніми зловмисники, які виводять з ладу сервери та впливають на продуктивність, розповсюджують віруси, внутрішню узгодженість сховищ даних та багато іншого. Ці проблеми не тільки впливають на продуктивність, але також викликають юридичні проблеми та питання відповідальності щодо захисту даних. Університет та керівництво, яке керує ними, можуть бути притягнуті до відповідальності, якщо багато з

вищезгаданих проблем підуть не так. Тому для лабораторії дуже важливо знати, яка безпека їм потрібна і як бути належним чином впевненим, що захист насправді забезпечується в системі, до якої вони надають доступ.

Багато з цих питань безпеки необхідно продумати до та під час фази проектування та визначення архітектури системи. Найкращих покажчиків безпеки можливо досягти лише у тому випадку, якщо вона розроблена та вбудована в основу операційних систем і програм, а не додана як позаду. Після того, як безпека інтегрована як важлива частина системи, її необхідно розробити, впровадити, протестувати, перевірити, оцінити, сертифікувати та акредитувати. Безпека, яку забезпечує той чи інший елемент, має оцінюватися на основі доступності, цілісності та конфіденційності, на яку він претендує. Потім розробники використовують повинні визначити, чи забезпечують певні аспекти необхідний рівень безпеки. Це довгий шлях, до якого пов’язано багато суб’єктів із різними обов’язками. У цій роботі, поступово, крок за кроком освячуються аспекти, необхідні перед фактичною розробкою, до того, як ці системи оцінюються та оцінюються, а також що ці рейтинги насправді означають.

2.4 Побудова моделі атаки на конфіденційність

Важливим етапом перед проектуванням моделі захисту є дослідження можливих атак та сценаріїв посягання на конфіденційність. Для розуміння того, як побудувати сценарій захисту, потрібно дослідити методи здійснення атак, а також загроз приватності, з якими найчастіше зіштовхуються, коли мають на увазі конфіденційність.

Сприйняття та розуміння кібератак може бути складним завданням, і для сприйняття кібератак потрібні більш ефективні методи. Методи моделювання атак – такі як графіки атак, дерева атак і дерева відмов є популярним методом математичного та візуального представлення послідовності подій, які призводять до успішної кібератаки. Не існує стандартизованої візуальної конфігурації

графічного синтаксису атак, так само, як і не існує стандартного методу представлення графіків атак або дерев атак і що для стандартизації представлення.

На основі роботи [16] можна зробити висновки про ефективність теорії графів для моделювання моделі загроз. Саме опираючись на теорію графів, можна ефективно та доступно побудувати модель атаки.

Першим етапом, для підготовки перед моделюванням самих атак, являється візуалізація потоку інформації у системі. Фактично будь-який інцидент порушення інформаційної безпеки можна описати так: будь-яка несанкціонована дія в інформаційній системі є появою неперевіреного інформаційного потоку.

Якщо представити V — як множину носіїв інформації (набір вершин графа), E — набір каналів передачі інформації (набір ребер графа). Порівнюючи будь-які два елементи з V і один з E, отримуємо елементарний інформаційний потік у вигляді неорієнтованого графа з двома вершинами. То елементарний потік даних можна представити на рисунку 8:

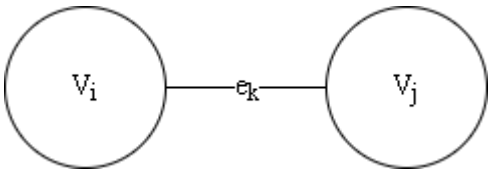

Рисунок 8 – Елементарний потік даних

Використовуючи позначення теорії графів, описання наведеного вищу потому інформаціє буде таким:

$$g = (v_i , e_k , v_j),$$

де v_i, v_j – можливі носії інформації; e_k можливий каналом зв’язку.

Доцільно поділити сукупність носіїв інформації на три підмножини:

$$V = \{V_1, V_2, V_3\},$$

де V_1 — набір користувачів; V_2 — набір програмних засобів; V_3 — набір електронних ресурсів.

Якщо вважати, що користувач взаємодіє з програмним забезпеченням за допомогою операційної системи, та розділивши інформацію за рівнями OSI, то на

виході отримуємо дві класифікації: канали зв’язку можна розділити на локальні та віддалені; канали можна розділити на діючі у віртуальному та електромагнітному середовищі.

Якщо об’єднати ці дві класифікації, то набір каналів передачі інформації буде мати такий вигляд:

$$E = \{e_1, e_2, e_3, e_4\},$$

де e_1 – канал передачі в електромагнітному середовищі; e_2 – канал передачі у віртуальному середовищі; e_3 – дистанційний канал передачі в електромагнітному середовищі; e_4 – це віддалений канал передачі у віртуальному середовищі.

Множина всіх елементарних потоків матиме такий вигляд:

$$G = \{g1, g2, g3, g4, g5, g6, g7, g8\},$$

де $g_1 = \{V_1, e_1, V_2\}$; $g_2 = \{V_1, e_2, V_2\}$; $g_3 = \{V_2, e_1, V_2\}$; $g_4 = \{V_2, e_2, V_2\}$; $g_5 = \{V_2, e_3, V_2\}$; $g_6 = \{V_2, e_4, V_2\}$; $g_7 = \{V_2, e_1, V_3\}$; $g_8 = \{V_2, e_2, V_3\}$.

Результатом об’єднання всіх наведених вище графів буде неорієнтований мультиплікативний граф (рисунок 9), який представлятиме модель інформаційних потоків при зверненні до електронних інформаційних ресурсів.

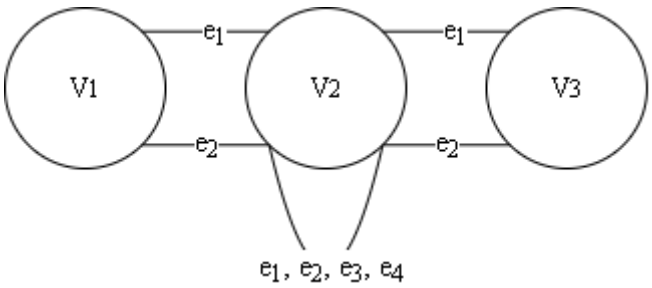

Рисунок 9 – Модель інформаційних потоків

На основі цього можна побудувати модель порушення доступу.

Якщо класифікувати види доступу, то їх можна поділити на декілька категорій. Перше, це несанкціонований доступ до інформації – це доступ до захищеної інформації з порушенням встановлених прав та/або правил доступу, що призводить до витоку, спотворення, підроблення, знищення, блокування доступу до інформації, а також втрати, знищення чи несправності носія інформації.

Саме визначення несанкціонованого доступу має на увазі появу в системі нового елемента, який забезпечить цей доступ, зобразимо його на рисунку 10:

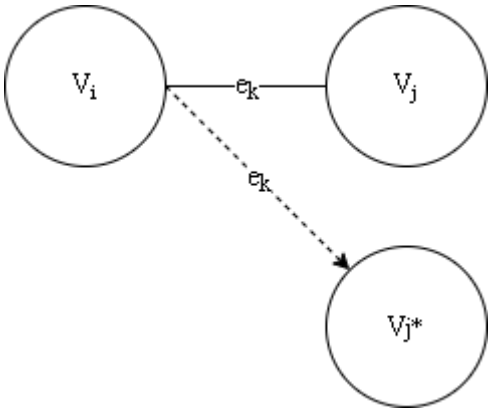

Рисунок 10 – Несанкціонований доступ

Поява несанкціонованого елемента V_{j*}, який отримує інформацію від елемента V_i.

Подібна ситуація можлива для будь-якого елемента інформаційного потоку. За аналогією з описаною вище ситуацією, доступ може здійснюватися як до елемента V_j, так і до e_k (рисунок 11).

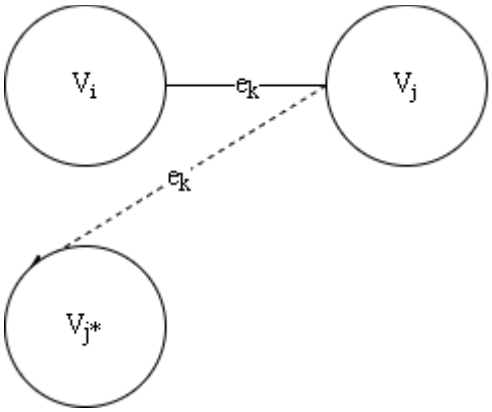

Рисунок 11 – Несанкціонований доступ альтернативний

Поява несанкціонованого елемента V_{i*}, який отримує інформацію від елемента V_j (рисунок 12):

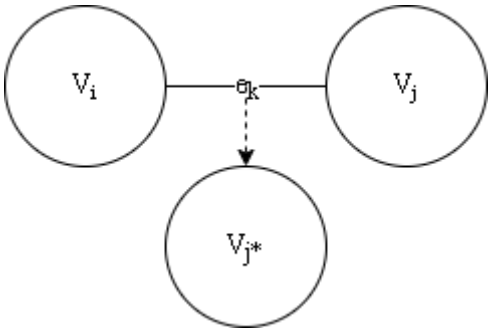

Рисунок 12 – Несанкціонований доступ друга альтернатива

Поява несанкціонованого елемента Vj *, який отримує інформацію від елемента e_k.

Модель інформаційного потоку дає можливість звести опис будь-якої інформаційної системи до обмеженого набору елементарних інформаційних потоків. Ця модель має високий рівень абстракції, через те, що у подальшому можливі зміни у конструкції лабораторії. Також це дозволяє застосувати подібну методику при проектуванні моделі загроз для інших аспектів інформаційної безпеки: цілісності та доступності.

2.5 Висновки

Віддалені лабораторії можуть бути різноманітними; ми зосереджуємось на віддалених лабораторіях, де користувачі в основному мають доступ до фізичного обладнання для дистанційного експериментування. Дистанційне експериментування зазвичай вводиться як доповнення до практичних лабораторних занять у традиційних вищих навчальних закладах, щоб уникнути поїздок до навчальних центрів дистанційного навчання або запропонувати живі демонстрації на заняттях у класі. Віддалені лабораторії часто використовуються в управлінні, робототехніці та мехатронному навчанні для ілюстрації теоретичних принципів і методологій розгортання. Як приклад, різні етапи проектування та

впровадження контролю, які навчаються студентам на курсах керування (ідентифікація системи, проектування контролера, керування в реальному часі, перевірка продуктивності тощо), можуть ефективно виконуватися дистанційно на мехатронних системах, оскільки вони демонструють візуально спостережувану динамічну поведінка. Крім того, важливим елементом освітньої методики є порівняння результатів моделювання та фактичного впровадження.

Віртуальні лабораторії можуть бути реалізовані як настільні програми (запущені в операційній системі користувача) або веб-додатки (запущені у веб-браузері користувача). У порівнянні з веб-додатками, настільні програми мають такі недоліки:

– Вони менш портативні: настільні програми прив’язані до певної платформи, напр. операційну систему, віртуальну машину Java, середовище виконання загальної мови .NET тощо.

– Вони менш безпечні: настільні програми зазвичай вимагають повного доступу для встановлення, вони мають повний доступ до жорсткого диска користувача, вони можуть відкривати необмежені з’єднання із зовнішнім світом тощо.

Програмування дистанційних з нуля вимагає значних зусиль і включає повторювану роботу. Наприклад, основною вимогою до віртуальних лаборіторійє інтерактивність і динамічність: будь-яка зміна параметрів моделювання має бути негайно відображена в графічному інтерфейсі користувача. Таким чином, студенти можуть дуже швидко, як поведінка моделі розвивається відповідно до значень інтерактивних параметрів. Програмування такої інтерактивності не є тривіальним, і це потрібно робити для кожної лабораторії.

Оскільки віддалені лабораторії (RL) дистанційно керують реальним обладнанням, вони, як правило, складніші та дорожчі, ніж VL. Щоб подолати таку складність, RL дотримуються архітектури клієнт-сервер.

На стороні клієнта RL зазвичай є веб-додаток, який взаємодіє з сервером, щоб дистанційно керувати фактичним налаштуванням і візуалізувати інформацію з лабораторії (потокове відео, дані датчиків тощо).

Лабораторія і її клієнтська сторона мають багато спільних функцій (зрештою, вони є багатими Інтернет-додатками для лабораторних експериментів), і, отже, обидва зазвичай реалізуються за допомогою однієї технології (тобто Java в минулому та JavaScript на даний момент). . Крім того, деякі підходи використовують переваги цієї подібності до віртуальних і віддалених лабораторій блендера, накладаючи графічне представлення поведінки VL на зображення, надане веб-камерою.

У ході дослідження було також розроблено дві моделі, які мають практичне застосування в процесах інформаційної безпеки:

— модель інформаційних потоків;

— модель загроз конфіденційності інформації.

3 МЕТОДИЧНІ ІНСТРУКЦІЇ ТА МОДЕЛЬ ДОСЯГНЕННЯ КОНФІДЕНЦІЙНОСТІ ДАНИХ

У цьому розділі пропонується комплексна система захисту конфіденційності у лабораторії з віддаленим доступом. Теоретичний аналіз літератури та існуючих методів рішення проблем безпеки дозволив створив фундамент для побудування схеми вибору інструментів інформаційної безпеки, з урахуванням всіх досліджених елементів, а саме: побудованої моделі архітектури, типу організації віддаленого доступу. Дотримуючись положень моделі атаки на конфіденційність представлена багаторівнева модель, а також список рекомендацій, які неможливо оминути при побудові лабораторії з віддаленим доступом.

В результаті дослідо було отримано матеріал, аналіз якого дозволив зробити комплексне рішення з урахуванням того, що на нього будуть посилатися безпосередньо до моменту організації функціонуючої лабораторії. Іншими словами, якщо замислитися про питання безпеки ще на етапі проектування перед самою реалізацією та дослідити існуючі експерименти, їх недоліки та зробити висновки опираючись на помилки інших — можна уникнути дуже багатьох проблем з безпекою у майбутньому.

3.1 Впровадження методів інформаційних систем

Розроблюючи архітектуру системи інформаційної безпеки, потрібно враховувати, що вона базується на наступних принципах:

– Система розглядається як комплекс засобів безпеки, призначених для забезпечення захисту інформаційної системи та даних, що в ній обробляються;

– Кожен засіб інформаційної безпеки являє собою комплекс реалізованих механізмів безпеки;

– До кожного можливого потоку інформації об’єкт-суб’єкт і суб’єкт-суб’єкт необхідно застосовувати механізми безпеки;

– Кожен механізм безпеки призначений для нейтралізації конкретної загрози конкретному інформаційному потоку.

При розробці системи, рішення приймалися покладаючись на досвід дослідження стану предметної області, щоб вирішити які механізми безпеки будуть використані. На сьогодні не існує такого остаточного переліку методів захисту, реалізованих у будь-якому конкретному інструменті безпеки, який би пов’язував їх із конкретними загрозами. Описана методика дає можливість представити засоби захисту у вигляді переліку механізмів інформаційної безпеки.

На рисунку 13 представлено процес формування списку рекомендованих інструментів інформаційної безпеки. За діаграму потоку даних приймається модель інформаційних потоків, яка представлена в 2.4 цієї роботи.

Рисунок 13 – Формування списку рекомендованих інструментів

Технологія формування рекомендованого переліку засобів захисту інформації на рисунку:

– Визначити перелік загроз для кожного інформаційного потоку в лабораторії;

– Для кожного інформаційного потоку визначити механізми безпеки, які використовуються в лабораторії, і визначити, чи вони достатні для безпеки;

– Для кожного інформаційного потоку визначте рекомендовані інструменти, які дають змогу нейтралізувати загрози, які наразі не охоплені.

За цими пунктами можливо розширення методики до наступного зображення:

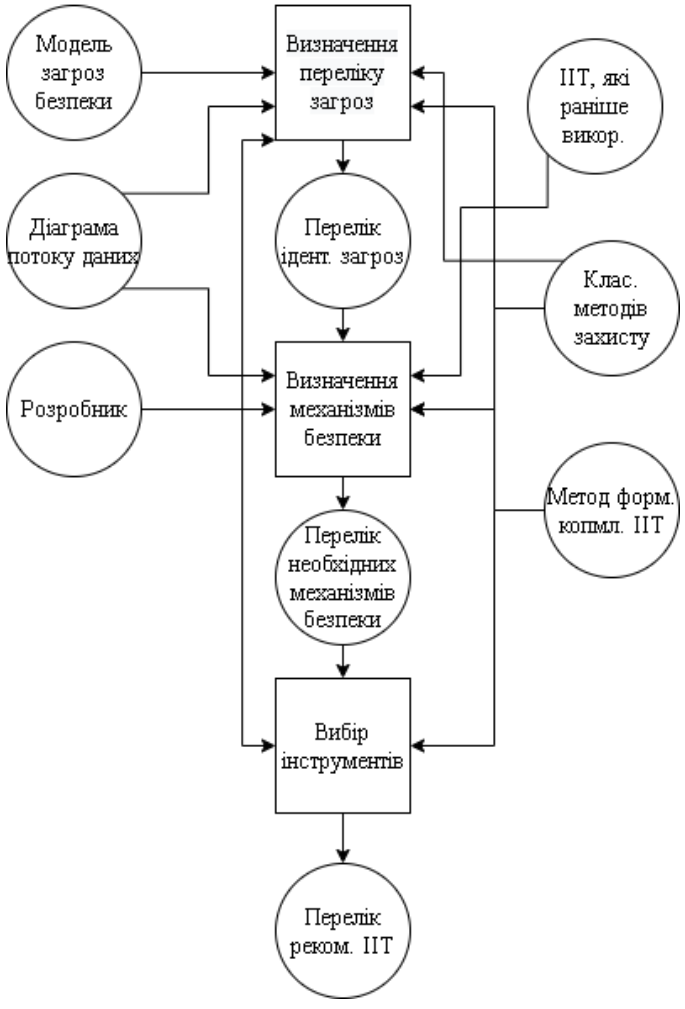

Рисунок 14 – Алгоритм формування інструментів безпеки

3.2 Створення системи захисту конфіденційності

Як було розглянуто у першому та другому розділі роботи, на даний момент існує багато методів захисту інформації, у тому числі такого важливого аспекту, як конфіденційності. Але єдиного універсального систематичного підходу до безпеки не існує, кожен має свої переваги та недоліки. Тому найкращим варіантом являється розглядання кожного випадку окремо, встановлення пріоритетів та створення комбінованої методики в залежності від потреб та можливостей програмного забезпечення та обладнання.

Конфіденційність – поширений термін. Це означає захист інформації від усіх, крім тих, хто має на неї права. Зазвичай це стосується бізнесу та корпоративних технологій, так як ця сфера напряму впливає на кошти та дохід організацій. Конфіденційна інформація включає наступне:

- Приватні дані фізичних осіб
- Інтелектуальна власність бізнесу (у даному випадку може враховуватися університет)
- Національна безпека країн і урядів

І тому зазвичай контроль безпеки — це те, що організація робить, щоб зменшити ризик. На прикладі описання подібних підходів можна визначити ті ключові елементи, які розповсюджуються на не-комерційні установи, а точніше, університети та заклади освіти, та адаптувати їх під вимоги та потреби конкретної задачі. Наступні пункти — це рекомендації, якими користуються та на які опираються спеціалісти з безпеки при побудуванні комплексних моделей захисту конфіденційності CISSP [3].

- Проведення тренінгу з питань безпеки для працівників та студентів, або хоча б розроблення техніки безпеки. Це допомагає нагадати як викладачам, так і людям, що навчаються, про належне поводження з приватними даними. Це також сприяє поінформованості про систему політики безпеки, стандарти, процедури та особисті рекомендації від університету.

– Запровадження політики безпеки ІТ. Структура політики схожа на схему, яка визначає, де слід використовувати засоби контролю безпеки.

– Розробка багатошарового рішення безпеки для ІТ-інфраструктури. Чим більше шарів або відсіків блокують або захищають приватні дані та інтелектуальну власність, тим складніше їх знайти та вкрасти. Цей принцип взятий за основу роботи, тому що вона намагається торкнутися теми безпеки, та вчасності, конфіденційності, на всіх можливих рівнях.

– Виконання періодичних оцінок ризиків безпеки, аудитів та тестів на проникнення на веб-сайтах та ІТ-інфраструктурі. Завдяки цьому фахівці з безпеки перевіряють, чи правильно вони встановили елементи керування. Для оцінки ефективності та покращенню роботи системи потрібно хоча б на елементарному рівні (та з певною періодичністю) перевіряти результати роботи, у даному випадку це лог-файли. Без аналізу ефективність системи безпеки може стрімко впасти через виявлення вразливостей студентами. Саме тому у запропонованих рішення представлена модель оцінки ризиків.

– Увімкнення моніторингу інцидентів безпеки та подій у точках входу та виходу в Інтернет. Цей пункт припускає використання організаціями методів SIEM, які найчастіше представляють собою програмні продукти, які у реальному часі аналізують та управляють подіями безпеки. Незважаючи на продуктивність цієї методики, подібне рішення дуже затратне, а також потребує фахівця з безпеки для нагляду. Замість цього пропонується менш затратна, хоча і менш ефективна модель, що поєднує детектування на відповідь на інциденти безпеки.

– Використання антивірусного та шкідливого програмного захисту автоматизованих робочих станцій і серверів. Це спосіб захистити ваш комп’ютер від вірусів і шкідливого програмного забезпечення.

– Використання суворішого контролю доступу, крім ідентифікатора входу та пароля для конфіденційних систем, програм і даних. Ідентифікатори входу з паролями – це лише одна перевірка користувача. Доступ до більш чутливих систем повинен мати другий тест, щоб підтвердити особу користувача. Найбільш

ефективним методом, який у тому числі пропонується у запропонованій системі є чотирьохступінчата модель доступу до веб-ресурсу.

– Мінімізація недоліків програмного забезпечення на ваших комп'ютерах і серверах шляхом оновлення їх за допомогою виправлень та виправлення безпеки. Це спосіб підтримувати свою операційну систему та програмне забезпечення в актуальному стані.

Інформаційна безпека та побудова систем для захисту як її аспект — це спеціалазація, яка вимагає наявності великої кількості знань та розумінню багатьох аспектів безпеки на всіх рівнях функціонування системи. Не існує системи захисту створеної конкретно для запропонованої лабораторії.

Кожен випадок вимагає створення свої особистої системи безпеки, першочергово опираючись на аналіз існуючих рішень кожного елементу окремо. У роботі представлено модель безпеки, яка повністю покриває собою загрози, атаки та вразливості конфіденційності, а також не оминає питання захисту SCADA-систем, дистанційного доступу та кібербезпеку взагалі. Це пов’язано з тим, що є рішення, які впливають на декілька факторів одночасно, але без них не можливо уявити повноцінну модель захисту.

Робота торкається багатьох аспектів організації ефективної роботи лабораторії і з іншої причини. Нерозуміння різних областей і рівнів безпеки мережевих пристроїв, операційних систем, апаратного забезпечення, протоколів і програм може спричинити вразливості безпеки, які можуть вплинути на середовище в цілому.

У ході аналізу вимог існуючих авторитетних стандартів та рекомендацій було визначено, що найкраще рішення – це запровадження комплексної систему, яка складається з наступних ступенів:

– Попередження / профілактика software/hardware
– Методи запобігання несанкціонованого доступу та оцінки ризиків
– Модель детектування / виявлення атак та модель відповіді / відклику
– Оцінка ефективності роботи системи

При цьому кожен з цих ступенів потребує становлення системи на певному етапі розробки. Результат роботи представлено на рисунку 15.

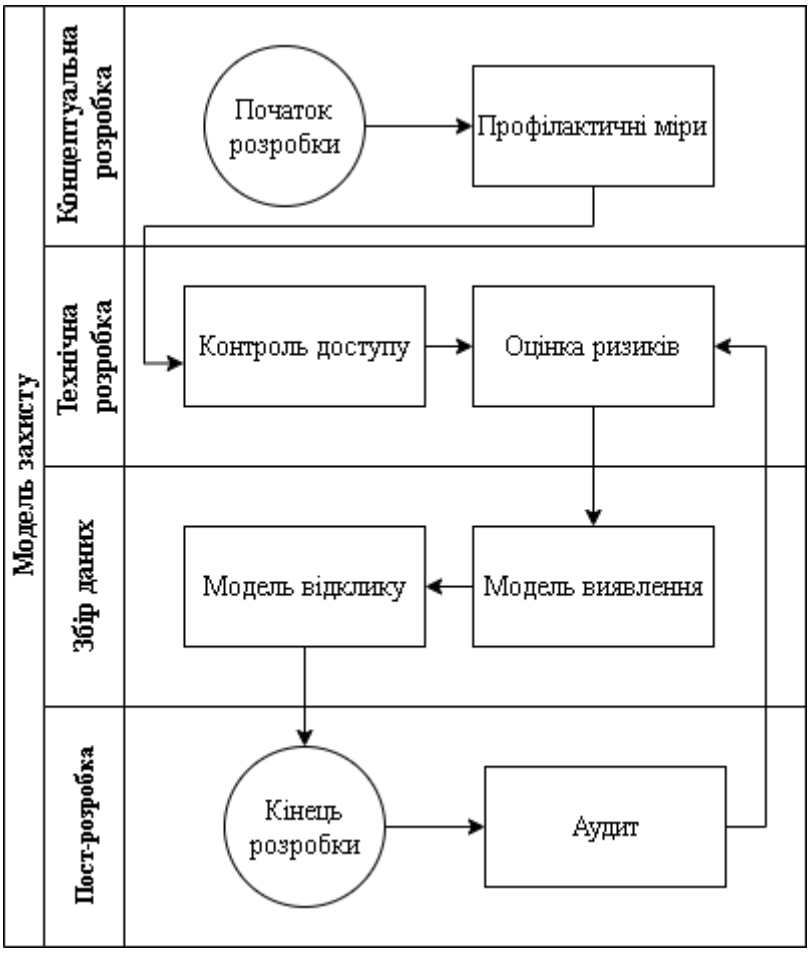

Рисунок 15 – Система, що пропонується

Для того, щоб краще розуміти, які самі стадії вимагають певних дій, потрібно звернутися до теми проектування комп’ютерних систем. У примирливому підході можна синтезувати інженерію інформаційних систем, ілюструючи її життєвий цикл на основі наступних етапів: аналіз, проектування, розробка, експлуатація, як це зроблено у роботі [17]. Тому, на основі цього, а також знань в області проектування інформаційних систем можна представити наступну таблицю 1.

Таблиця 1 – Стадії та заходи при проектуванні інформаційної системи

Стадії інженерії інформаційних систем	Заходи безпеки
Аналіз та дизайн	Encrypt sensitive files
Розробка та реалізація	Manage data access
Інтеграція та тестування	Managing devices
Оцінка ризиків та документація	Managing data acquisition
Планування	Managing data utilization

Також у таблиці показано конкретні дії забезпечення безпеки конфіденційності на кожному з цих етапів. Цей емпіричний досвід підкріплюється стандартами, рекомендаціями, методами та посібниками.

Для кожного елементу системи запропонована модель, а також список рекомендацій щодо впровадження та реалізації. Ці елементи описуються нижче.

3.2.1 Формулювання профілактичних мір

У цьому пункті представлені рекомендації щодо захисту рішень віддаленого доступу. З технічного боку він фокусується на безпеці сервера віддаленого доступу та розміщенні сервера. Також представлені рекомендації щодо захисту клієнтського програмного забезпечення віддаленого доступу. Але перш ніж розглядати апаратно-технічні рекомендації, потрібно врахувати існуючі вимоги до запровадження віддалених лабораторій з боку організаційних навичок.

Стабільність роботи лабораторії залежить від якісної її організації. Державні віддалені лабораторні середовища відповідають різноманітним регіональним, національним та організаційним вимогам. Щоб знайти спільну настанову, необхідні простота і гнучкість. Виходячи з потреби в простоті, визначається необхідність спільного розгляду питань безпеки та захисту. Ці потреби більш детально описані нижче.

– Потреба в простоті: експлуатація університетських лабораторій трудомістка і дорога. Будь-який додатковий тягар, у тому числі додаткові заходи

щодо безпеки та захисту, які мають на увазі віддалений доступ до лабораторій, негативно вплине на згоду інтегрувати лабораторії в мережу лабораторій.

– Потреба в гнучкому та ітеративному підході: оскільки університетські лабораторії постійно оновлюються та вдосконалюються за допомогою поточних досліджень, викладачам, дослідникам та лаборантам потрібна певна гнучкість. Сучасні дослідницькі підходи «...відсутня оцінка їхньої підтримки для ефективної обробки системних оновлень». Ітераційні заходи безпеки та безпеки повинні стосуватися всього життєвого циклу віддалених лабораторій, включаючи розробку, тестування, технічне обслуговування та експлуатацію.

– Оскільки сервери віддаленого доступу, такі як шлюзи VPN і сервери порталів, надають можливість зовнішнім хостам (таким як пристрої дистанційної роботи) отримати доступ до внутрішніх ресурсів, їх безпека особливо важлива. Крім дозволу несанкціонованого доступу до ресурсів, скомпрометований сервер може використовуватися для «підслуховування» комунікацій віддаленого доступу та маніпулювання ними, а також як слугувати відправною точкою для атаки на інші хости в організації. Сервери віддаленого доступу мають бути повністю справними, керуватися з використанням базової конфігурації безпеки, визначеної університетом, керуватися лише з надійних хостів авторизованими адміністраторами.

Також важливим буде дотримуватися загальних правових рекомендацій щодо безпеки продукції, у тому числі технічної. Європейська Директива 89/391 заснована на переліку загальних принципів:

– Уникнення ризиків;
– Оцінка ризиків;
– Пристосування роботи до особистості;
– Адаптація технічного прогресу;
– Заміна небезпечного на не- або менш небезпечне;
– Розробка цілісної загальної політики профілактики ризиків;

– Пріоритетність колективних заходів (над індивідуальними захисними заходами);

– Надання відповідних інструкції працівникам.

Але найважливішим моментом у проектуванні лабораторії з веб-порталом, який вимагає постійного стабільного інтернет-підключення, а також віддаленого підключення, стабільність результатів якого залежить від швидкості та продуманості мережевого обладнання — це серверна організація.

Шлюзи та портали VPN можуть запускати безліч служб і програм, таких як брандмауери, програмне забезпечення для захисту від шкідливих програм і програмне забезпечення для виявлення вторгнень. Існує потреба ретельно продумати безпеку будь-яких рішень, які передбачають запуск сервера віддаленого доступу на тому самому хості, що й інші служби та програми. Такі рішення можуть дати переваги, наприклад, заощадити на обладнання, але компроміс будь-якої із служб або програм може дозволити зловмиснику скомпрометувати весь сервер віддаленого доступу. Розміщення сервера віддаленого доступу на окремому виділеному хості зменшує ймовірність компрометації сервера віддаленого доступу та обмежує його потенційний вплив. Використання окремого хоста також може бути доцільним, якщо сервер віддаленого доступу може піддавати значно підвищеному ризику інші служби та програми. За можливості слід розглянути використання кількох рішень віддаленого доступу, якщо її користувачі віддаленого доступу мають дуже різні потреби в безпеці, наприклад, одна група отримує доступ до типових ресурсів з низьким рівнем ризику, а інша група отримує доступ до критично важливих конфіденційних даних.

Безпека збережених даних є ще одним важливим фактором безпеки сервера віддаленого доступу. Для серверів порталів, які можуть тимчасово зберігати конфіденційні дані користувача, видалення таких даних із сервера, як тільки вони більше не потрібні, може зменшити потенційний вплив компрометації сервера. Необхідність стирання конфіденційних даних із серверів віддаленого доступу має визначатися на основі оцінки ризику.

Для лабораторії з віддаленим доступом сервер являється важливою технічною структурною одиницею. Основні фактори, які слід враховувати при визначенні місця розміщення сервера віддаленого доступу, включають наступне:

– Продуктивність пристрою. Служби віддаленого доступу можуть бути інтенсивними обчисленнями, насамперед через шифрування та дешифрування. Надання послуг віддаленого доступу з пристрою, який також надає інші послуги, може призвести до занадто високого навантаження на сервер під час пікового використання під час проведення лабораторних занять, що спричинить перебої в роботі служби. Вплив на продуктивність, викликаний шифруванням та обміном ключами, можна зменшити, виконуючи їх на апаратних чіпах криптографічного прискорювача. Ці мікросхеми можуть розташовуватися на материнській платі комп’ютера або на платі додаткових компонентів.

– Дорожньо-технічна експертиза. Оскільки вміст зашифрованих комунікацій віддаленого доступу не може бути перевірений мережевими брандмауерами, системами виявлення вторгнень та іншими пристроями безпеки мережі, зазвичай рекомендується, щоб архітектура віддаленого доступу була розроблена таким чином, щоб незашифрована форма зв’язку могла бути перевірена відповідним контроль безпеки мережі та/або хоста.

– Трафік не захищений рішенням віддаленого доступу. Розробники лабораторії повинні уважно розглядати загрози мережевому трафіку, який не захищений рішенням віддаленого доступу, наприклад трафік, що передається між сервером віддаленого доступу та внутрішніми ресурсами.

– Перетворення мережевих адрес або NAT. Використання NAT може викликати проблеми з роботою деяких рішень віддаленого доступу. Наприклад, будь-яка система віддаленого доступу, яка вимагає від віддаленого працівника безпосереднього підключення до хоста всередині мережі, наприклад системи віддаленого робочого столу або VPN з загальнодоступною кінцевою точкою всередині мережі, не може працювати з NAT без спеціальної конфігурації, яка може або може не працює. NAT також запобігають використання програм, які

вимагають, щоб адреси не змінювалися (наприклад, вбудовування адрес у вміст програми). Протоколи та механізми, які проривають NAT для вирішення конкретних проблем доступу, часто створюють власні проблеми безпеки, наприклад, можливість доступу до різних хостів всередині NAT в різний час. Деякі новітні технології NAT, зокрема ті, що стосуються IPv6, ще недостатньо вивчені, а їхні властивості безпеки ще не повністю проаналізовані.

Загалом:

– Інженерам, які займаються розробкою лабораторії слід ретельно продумати безпеку будь-яких рішень віддаленого доступу, які передбачають запуск сервера віддаленого доступу на тому самому хості, що й інші служби та програми.

– При розробці слід враховувати кілька основних факторів, визначаючи місце розташування сервера віддаленого доступу, зокрема продуктивність пристрою, перевірку трафіку, незахищений трафік і перетворення мережевих адрес. Університет повинен розміщувати сервери віддаленого доступу на периметрі мережі, якщо немає вагомих причин робити інакше.

– Будь-яка конфіденційна інформація від комунікацій віддаленого доступу, що проходить через Інтернет, бездротові мережі та інші ненадійні мережі, повинна забеспечувати конфіденційність та цілісність за допомогою використання криптографії.

– Слід ретельно спланувати, як буде підтримуватися та керуватися безпека клієнтського програмного забезпечення віддаленого доступу, перш ніж вибрати та розгорнути рішення для віддаленого доступу. Розробники також повинні планувати, як клієнтські пристрої дистанційної роботи, які вони надають студентам, будуть керуватися та підтримуватися. Вони повинні забезпечити належний захист віддаленого керування, зокрема шифрувати мережеві комунікації та виконувати взаємну аутентифікацію кінцевих точок.

Існують також проблеми програмного забезпечення. Програмне забезпечення, яке керує фізичним обладнанням, а також програмне забезпечення

клієнтського інтерфейсу має бути надійним і написаним із застосуванням захисного підходу до непередбачуваного використання. Розробник програмного забезпечення для віддаленого експериментування повинен гарантувати, що зловмисно створена інформація, надіслана на сервер, не заважатиме контролю над фізичним обладнанням і не спричиняє пошкоджень. Отримана інформація повинна бути ретельно перевірена перед використанням. Ці вимоги зазвичай вимагають серйозного перегляду програмного забезпечення при розробці рішень професійної якості, які очікують студенти.

Розроблене програмне забезпечення також має бути адаптивним для легкої інтеграції та/або адаптації до нових компонентів. Програмне забезпечення, написане для керування фізичним обладнанням, як правило, старіє так само, як і контрольоване обладнання. Програмне забезпечення для віддаленого експериментування спирається на архітектуру клієнт-сервер. Хоча програмне забезпечення на стороні сервера працює у відомому середовищі, це не стосується програмного забезпечення, яке використовується клієнтом для керування віддаленим налаштуванням. Особливу увагу потрібно приділяти клієнтській програмі, щоб правильно працювати з невідомим середовищем. Це особливо актуально для програмного забезпечення, яке використовує веб-браузер для запуску клієнтського інтерфейсу (GUI).

Стійкість до апаратних збоїв або недоступності також є ключовим питанням для прийнятності парадигми віддаленого експериментування студентами. Якщо під час підключення вони не зможуть отримати доступ до вибраного експерименту, вони можуть втратити мотивацію та інтерес.

3.2.2 Систематизація методів контроль доступу

За допомогою контролю доступу до ресурсів лабораторії, вони захищаються від несанкціонованої зміни або розкриття і являє собою шлюз до критичних активів.

Контроль доступу представляє собою функції безпеки, які контролюють, як саме користувачі та системи спілкуються та взаємодіють з іншими системами та ресурсами у лабораторії.

Впровадження зумовлене тим, що його функції захищають системи та ресурси від несанкціонованого доступу і можуть бути компонентами, які беруть участь у визначенні рівня авторизації після успішного завершення процедури аутентифікації.

У роботі контроль доступу розглядається концептуально, також розглядаються технології, які галузь запроваджує для забезпечення виконання цих концепцій. Важливою частино дослідження є представленні методи, які використовують для атаки на ці технології.

Рисунок 18 ілюструє чотири кроки, які необхідно виконати, щоб суб'єкт отримав доступ до об'єкта. Детальніше питання суб'єктів та об'єктів розглядається у огляді фундаментальних основ інформаційної безпеки розділу 1.

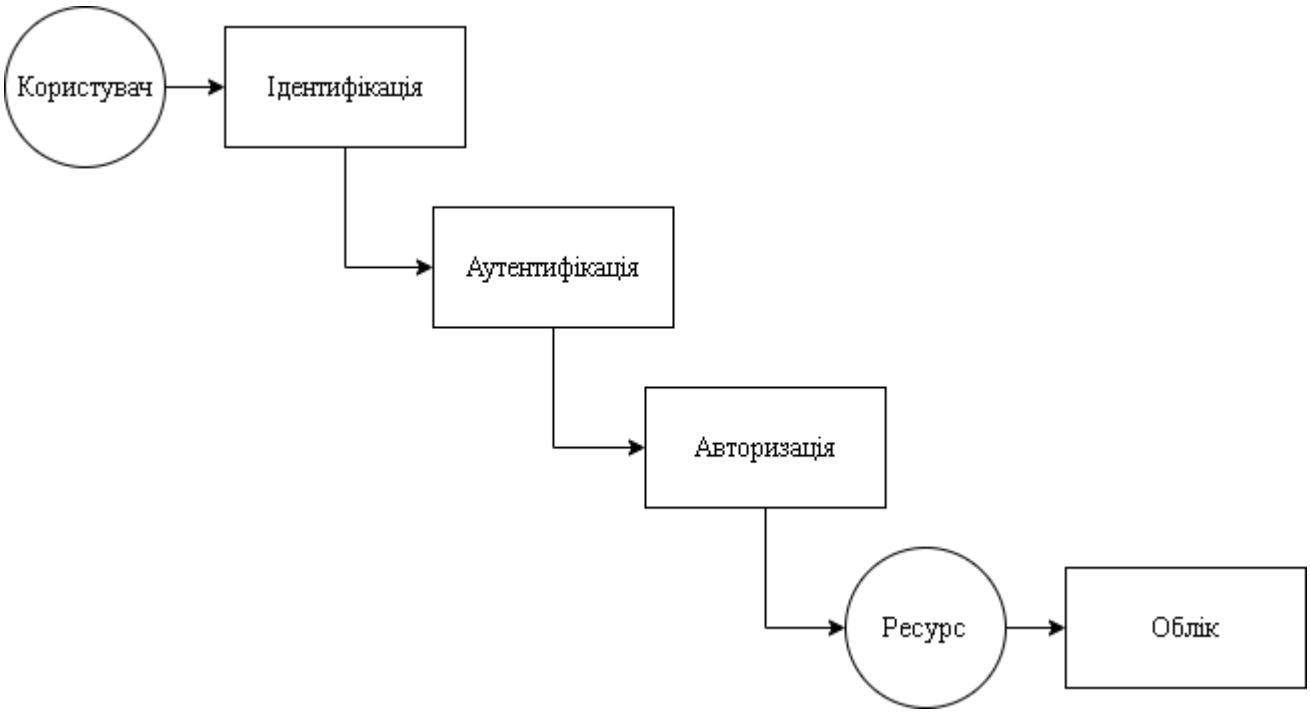

Рисунок 18 – Ідентифікація, аутентифікація, авторизація та облік

Щоб користувач, тобто студент, міг отримати доступ до ресурсу, він спочатку повинен довести, що він є тим, за кого себе видає, має необхідні облікові дані та йому надано необхідні права чи привілеї для виконання дій, які він запитує. Після успішного виконання цих кроків студент зможе отримати доступ до

мережевих ресурсів лабораторії і використовувати їх; однак необхідно відстежувати діяльність користувача та забезпечити відповідальність за його дії. Ідентифікація описує метод забезпечення того, що суб’єкт (користувач, програма чи процес) є сутністю, за яку він видається. Ідентифікація може здійснюватися за допомогою імені користувача або номеру студентського квитка. Для належної автентифікації суб’єкт, як правило, повинен надати другий елемент до набору облікових даних. Це може бути пароль, парольна фраза, криптографічний ключ або номер залікової книжки. Ці два елементи облікових даних порівнюються з інформацією, яка раніше була збережена для цього предмета. Якщо ці облікові дані збігаються із збереженою інформацією, суб’єкт аутентифікується.

Після того, як суб’єкт надає свої облікові дані та правильно ідентифікований, система, до якої він намагається отримати доступ, повинна визначити, чи надано цьому суб’єкту необхідні права та привілеї для виконання запитуваних дій. Система розгляне певний тип матриці контролю доступу або порівняє мітки безпеки, щоб переконатися, що цей суб’єкт дійсно може отримати доступ до запитуваного ресурсу та виконати дії, які він намагається. Якщо система визначає, що суб’єкт може отримати доступ до ресурсу, вона авторизує суб’єкта.

Хоча ідентифікація, аутентифікація, авторизація та облік мають близькі та взаємодоповнювальні визначення, кожне з них має різні функції, які відповідають певним вимогам у процесі контролю доступу до лабораторії. Студент може бути належним чином ідентифікований та автентифікований у мережі, але він може не мати авторизації на доступ до файлів на файловому сервері. З іншого боку, користувач може отримати дозвіл на доступ до файлів на файловому сервері, але поки він не буде належним чином ідентифікований та аутентифікований, веб-лабораторія буде недоступна для нього.

Студент повинен нести відповідальність за дії, вчинені в системі. Єдиний спосіб забезпечити відповідальність – це однозначно ідентифікувати суб’єкта та зафіксувати його дії.

3.2.3 Складня постулатів з оцінки ризику

Частота атак на безпеку, у тому дистанційного доступу, зростає дуже швидко. Проте виявити та запобігти всім загрозам та вразливостям безпеки в інформаційних системах важко. Тому існує нагальна потреба проаналізувати ризики, які несуть загрози безпеці, та ефективно попередити їх. Аналіз ризиків безпеки – це підхід, який дозволяє виявити та оцінити ризики нещасних випадків до того, як вони завдадуть серйозних збитків лабораторії. Це дозволе у майбутньому розробити безпечне управління інформацією та встановлювати практичні політики безпеки для лабораторії. Крім того, цей підхід надає цінні дані аналізу для майбутньої оцінки ризику. Щоб керувати ризиком безпеки, аналіз ризиків включає визначення найбільш ймовірних загроз для систем та аналіз пов’язаної вразливості їх до цих загроз.

Успішний аналіз ризиків безпеки дозволяє нам розробити захищену систему управління інформацією всередині лабораторії та надає цінні дані аналізу для майбутньої оцінки ризиків.

Ця методика, яка використовується для виявлення та оцінки факторів ризику, які можуть загрожувати системі лабораторії. Якщо узагальнити, то вона складається з трьох етапів, які показано на рисунку 19.

Етап 1 (вимоги безпеки) — це крок, який визначає обсяг зусиль, межі системи, ресурси та інформацію, а також методологію університету чи інституту. Етап 2 (аналіз ризику) — це крок, який визначає активи, загрози та вразливості та вимірює ризик безпеки. Важливим завданням на цьому етапі є класифікація та категоризація активів, загроз і вразливостей, які представлені у розділі другому. Крім того, він включає типи загроз і вразливостей, які існують для конкретного активу, а також ймовірність того, що загрози можуть виникнути. Нарешті, ризик безпеки лабораторії оцінюється шляхом підсумовування всіх ризиків компонентів системи з урахуванням наявних загроз в основних активах інституту та ступеня вразливості кожної загрози.

Класифікація важливої інформації представлена у 2.1.

Після проведення аналізу ризику адміністратори системи можуть використовувати різні методи зниження ризику для завершення процесу на етапі 3 (зменшення ризику та оцінка). Тобто, фаза 3 — це процес, який показує список поточних протидій безпеки в інституті, вибирає відповідні методи пом'якшення загроз, а потім показує їх ефективність.

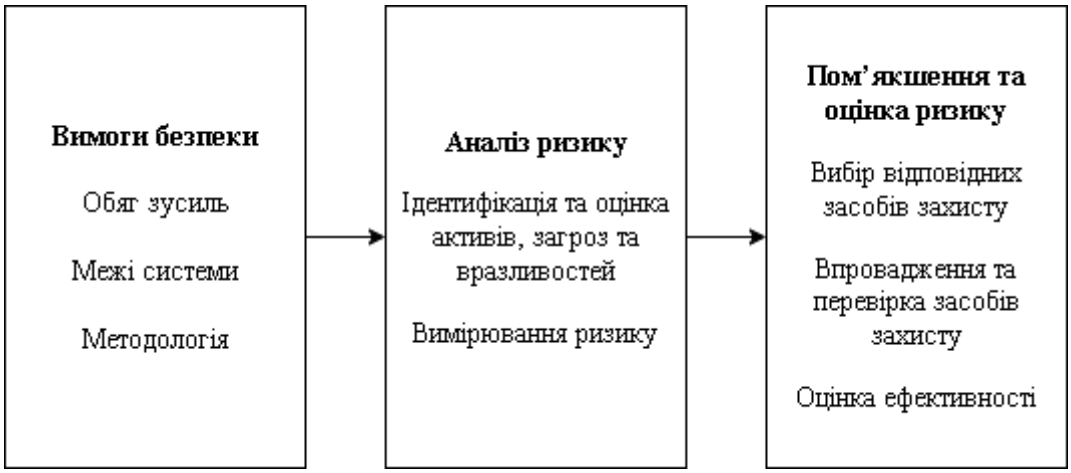

Рисунок 19 – Оцінка ризику

Це рішення доказало свою ефективність у захисті конфіденційності та цілісності.

3.2.4 Реалізація методу виявлення

Основний процес виявлення показано на рисунку 20. Система збирає системні log-файли або журнали, тобто журнал трафіку, журнал маніпуляцій тощо. Усі зібрані журнали статично аналізуються та вивчаються як звичайні або нормальні дані. У цей період, передбачається, що система не зазнає атаки. Після цього періоду навчання система може виявити нові атаки.

Після певного періоду функціонування, тобто життєвого циклу, система починає аналізувати зібрані дані. Коли система виявляє відхилення, вона аналізує дані більш детально. Виявлення не обов'язково є вторгненням. Коли в системі користувача вводяться нові інструменти або нові послуги, це може створювати новий трафік або моделі використання. Тому необхідно перевірити, чи є вони результатом нормального використання або атак. Припускається, що цим буде займатися адміністратор. Коли нетипова поведінка є вторгненнями ззовні, ці дії

блокуються. З іншого боку, коли нетипових трафік є результатами належних, але нових процедур, вони дозволені й засвоюються як звичайні дані. Після вивчення певної кількості цих даних вони не класифікуються як дані, що виявляються.

Цей крок зворотного зв’язку для реєстрації належної, але нової процедури як звичайних даних необхідний, оскільки лабораторія постійно розвивається, та впроваджуються нові програми та служби згідно з методами навчання.

Конкретні цілі цієї системи полягають у наступному.

– Система може виявити нові невідомі вторгнення.

– Система може виявляти вторгнення в режимі реального часу.

– Можна виявити не тільки зв'язок з/назовні, а й нерегулярні комунікації/операції в локальній мережі.

– Виявлені інциденти можуть бути досліджені системними адміністраторами та вирішити, чи є вони фактичними вторгненнями чи звичайним використанням.

Рисунок 20 – Метод виявлення

3.2.5 Підготовка методів відповіді

Беручи до уваги досвід експертів з реагування на інциденти з кіберпезпеки, можна зробити певні висновки. Зазвичай виконуються певні кроки, щоб допомогти ефективно впоратися з інцидентом, що має бути частиною більш широкого підходу з акцентом на розслідування (звідки та чому з'явилася загроза).

Щоб процес виявлення мав будь-яку цінність, має бути своєчасна відповідь. Реакцію на інцидент слід спланувати заздалегідь. Прийняття важливих рішень або вироблення політики під час нападу є дуже невірним рішенням.

На рисунку 21 представлено покрокове рішення щодо відповіді на детекцію загроз.

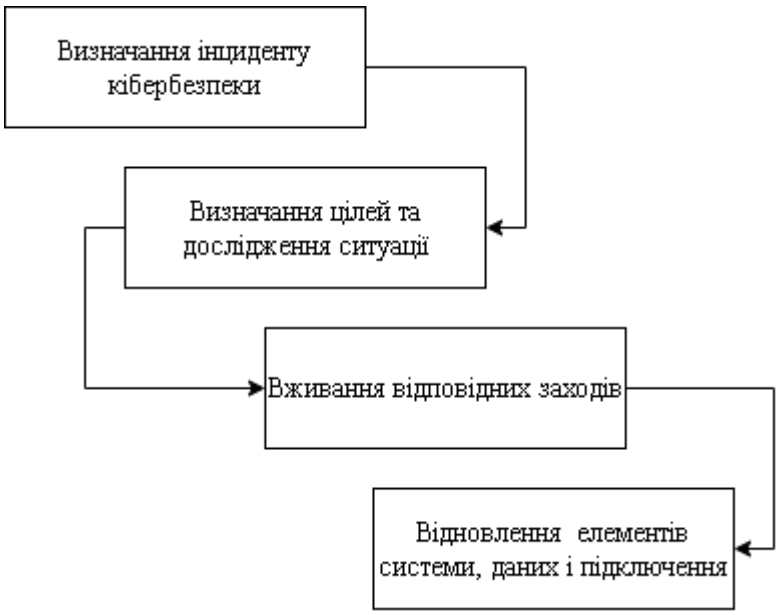

Рисунок 21 – Метод відповіді

Існує потреба розібрати кожен крок окремо.

Перший крок це ідентифікація або визначення інциденту. Здебільшого найскладнішою частиною процесу реагування на інцидент є точне виявлення та оцінка можливих інцидентів кібербезпеки – визначення того, чи стався інцидент, і, якщо так, тип, масштаб і масштаб проблеми.

У ході досліджень можна прийти до висновків, що чотири основні проблеми, з якими стикаються організації, намагаючись швидко, ефективно та послідовно визначити інцидент кібербезпеки, є:

– Виявлення підозрюваного інциденту кібербезпеки (наприклад, моніторинг доказів незвичайних подій та оцінка одного або кількох тригерних моментів)

– Аналіз всієї доступної інформації, пов'язаної з потенційним інцидентом кібербезпеки

– Визначення того, що сталося насправді (наприклад, DDOS, атака зловмисного програмного забезпечення, злом системи, викрадення сеансу або пошкодження даних)

– Підтвердження того, що вони дійсно зазнали атаки кібербезпеки або мали кібер-злом (невідомий елемент)

Після виявлення інциденту кібербезпеки наступним етапом є визначення цілей заходів реагування та відповідне дослідження ситуації. Слідчі мають шукати відповіді на багато запитань, наприклад: Хто скоїв напад? Які масштаби атаки? Коли стався напад? і т.д.

Як і у попередньому кроці, існують три основні проблеми, з якими стикаються, при реагуванні на інциденти кібербезпеки швидким, ефективним і послідовним чином:

– Визначення того, яка інформація була розкрита неуповноваженим сторонам, вкрадена, видалена або пошкоджена

– З’ясування того, хто це зробив (тобто який агент або агенти загрози) і чому (наприклад, фінансова вигода, хактивізм, шпигунство, помста, виклик або просто для розваги)

– Визначення того, які системи, мережі та інформація (активи) були скомпрометовані.

Однією з перших ключових дій, які необхідно вжити після первинного розслідування (і часто в рамках цього розслідування), є обмеження шкоди, завданої

інцидентом кібербезпеки, наприклад, зупинивши його поширення на інші мережі та пристрої та не тільки.

Стримання зазвичай включає ряд одночасних дій, спрямованих на зменшення безпосереднього впливу інциденту кібербезпеки, насамперед шляхом видалення зловмисника доступу до системи. Мета стримування не завжди полягає в тому, щоб повернутися (безпосередньо) до звичайного режиму роботи, а в тому, щоб докласти всіх зусиль, щоб повернутися до нормальної функціональності, продовжуючи аналізувати інцидент та планувати довгострокове усунення.

Серед безлічі способів локалізації інцидентів, для нашого конкретного випадку можна застосувати наступні:

– Блокування (і реєстрація) несанкціонованого доступу
– Блокування джерел шкідливого програмного забезпечення (наприклад, адрес електронної пошти та веб-сайтів)
– Закриття окремих портів і поштових серверів
– Зміна паролів системного адміністратора, якщо є підозра на саботаж
– Фільтрація брандмауера
– Переміщення домашніх сторінок веб-сайту

Останнім кроком у реагуванні на інцидент кібербезпеки є відновлення нормальної роботи систем, підтвердження того, що системи функціонують нормально, і усунення вразливостей, щоб запобігти подібним інцидентам.

Основні проблеми, з якими доводиться стикатися, коли відновлюються після інциденту кібербезпеки швидким, ефективним і послідовним способом, є:

– Підтвердження того, що виправлення пройшло успішно
– Повторне підключення мереж; відновлення систем; і відновлення, відтворення або виправлення інформації.

Тому важливо мати відповідний план відновлення, зміст якого повинен бути запроваджений після того, як систему буде реалізовано.

Попри все, схема реагування має зазнати змін у процесі створення системи. План реагування має бути написаний та затверджений відповідними рівнями

керівництва. Вона повинна чітко розставляти пріоритети різних типів подій і вимагати рівня сповіщення та/або відповіді, відповідного рівню події/загрози. Так як в умовах обмеження ресурсів та персоналу лабораторії, неможливе створення групи реагування на інциденти з комп'ютерною безпекою. Але є гостра необхідність у вдосконаленні системи, тому відповідні ролі та обов'язки повинні бути призначені викладачам та/або адміністраторам лабораторії. На цю людину слід покласти на нього відповідальність за оголошення інциденту, координацію діяльності та передачу звітів для подальшого покращення.

3.5.6 Характеризування методів аудиту/ оцінки ефективності

Під оцінкою ефективності мається на увазі оцінювання того, наскільки допустимими являються отримані ризики, основуючись на вже отриманих та оброблених даних. Ціллю цієї моделі також являється одночасно як облегшення ресурсів лабораторії, «відкидаючи» ризики, які не представляють цінність.

Рисунок 22 показує, де відбувається зниження ризику в умовах навмисних «атак». Термін «атака» береться в лапки, оскільки проблема є «навмисною», а не зловмисною. Відносно поширеним є випадки, коли безпеку інколи навмисно «атакують» у нешкідливих цілях, наприклад, «просто виконати роботу».

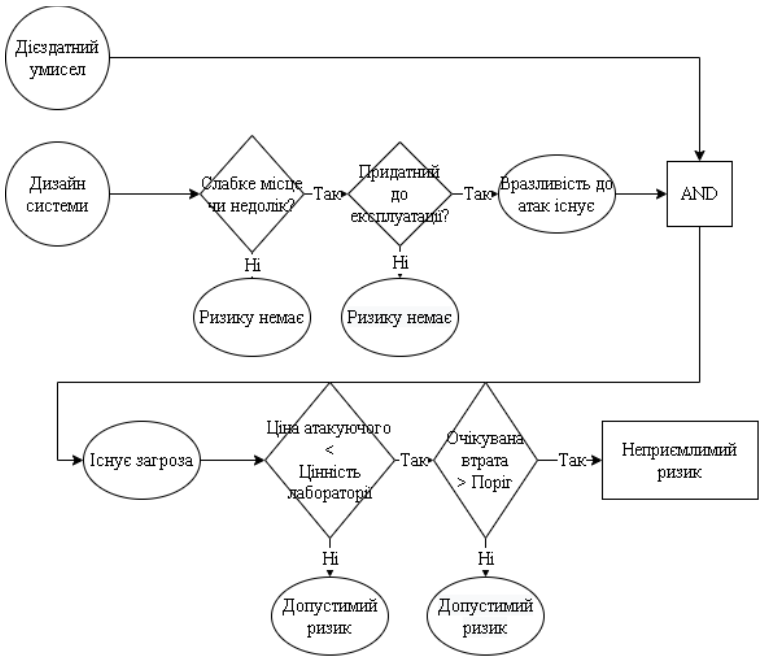

Рисунок 22 – Аудит та оцінка

Незважаючи на те, що в університетських лабораторіях необхідно гарантувати безпеку та безпеку обладнання в лабораторіях, зовнішні аудити корисні для підтвердження відповідності нормам і виявлення потенційних загроз на основі досвіду аудиторів. Початкові перевірки після встановлення можуть запропонувати виробники відповідних систем безпеки.

Для захисту середовища роботи в лабораторії первинний аудит охоплює:

– Запис технічних даних щодо пристрою та програми;
– Визначення безпеки праці у відповідній небезпечній зоні машини;
– Перевірка функціональності використовуваного обладнання;
– Перевірка охорони небезпечної зони;
– Перевірка інтеграції в систему управління відповідно до специфікацій виробника;
– Підготовка протоколу випробувань;
– Наклейка з огляду яка показує, якщо тест пройдено;
– Встановлення онлайн-з'єднання з пристроєм;
– Читання конфігурації пристрою;
– Створення PDF-файлу як вкладення до звіту про перевірку.

Регулярні перевірки мотивують весь залучений персонал контролювати та покращувати безпеку в лабораторіях. У деяких університетах зовнішній аудит лабораторій проходить один раз на рік, а у інших – кожні два роки. Результати аудиту документуються. Однак у перервах між аудиторськими перевірками є вірогідність того, що відбулися зміни в налаштуваннях або середовищі. Може знадобитися етап авторизації вручну відповідальним керівником лабораторії. Подальші засоби для перевірки поточного стану безпеки та безпеки та автоматичної авторизації безпосередньо перед початком лабораторного експерименту потребують подальшого дослідження.

Однак ці перевірки показують два недоліки, що стосуються об'єднаних мереж лабораторій. По-перше, загрози, пов'язані з безпекою та безпекою мережі, не знаходяться в центрі уваги цих аудитів. По-друге, відсутній аудит академічної

цінності. Академічний аудит необхідний, оскільки він показує, де ми знаходимося і що ми шукаємо.

Однак у об’єднаній мережі лабораторій якість лабораторії можна забезпечити за допомогою процесу експертної перевірки.

3.3 Висновки

Третій розділ присвячений розробці комплексної системи захисту інформації, роблячи уклін в конфіденційність даних.

Методологія вибору інструментів інформаційної безпеки, яка преведена на початку, створена з метою систематизувати великий обсяг знань та методів захисту.

Наведено спочатку загальний вигляд системи, а також аспекти, якими слід займатися на різних етапах проектування системи, враховуючи як базові рекомендації для побудування інформаційної системи, так і специфічні методи досягнення конфіденційності, які адаптовано до лабораторних умов.

Кожен з елементів завдяки яким досягається безпека, таких як детектування загроз, оцінка ризику, відповідь на атаку розглядається, окремим підпунктом, де детально описується принцип його роботи.

ЗАГАЛЬНІ ВИСНОВКИ

Дипломна робота досліджує методи захисту даних у лабораторії з віддаленим доступом на конкретних існуючих умовах. Головний акцент ставиться на досягнені конфіденційності. Доводиться, що незважаючи на думки багатьох викладачів про те, що в системі освіти доцільно скрізь, де це можливо, переходити в лабораторних практикумах від використання реального фізичного обладнання до математичного моделювання, тобто використання віртуальних лабораторій, оснащених відповідним прикладним програмним забезпеченням.

Дистанційне підключення, на відміну від реальної лабораторії створює простір для злочинців, які користуються ситуацією, оскільки рівень захисту домашнього комп'ютера студента з великою ймовірністю нижче, ніж у корпоративної техніки: причиною може бути старе програмне забезпеченням, відсутність антивірусу. Десятки, а то й сотні віддалених пристроїв, складніше контролювати за межами університету. У гіршому випадку зловмисник зможе повністю паралізувати діяльність лабораторії, атакувавши VPN-сервіс.

Розглянуто умови, які створюють загрозу порушення конфіденційності. Атаки, загрози, та ризики на базі яких побудовано модель інформаційних потоків та розповсюдженої атаки на конфіденційність. Тому що є дані, підтверджені статистикою та звітами різних компаній, що й активність зловмисників зросла у період «віддалення», що актуально і для лабораторій, які ставлять ціллю запровадження дистанційного доступу. Під особливим прицілом зловмисників знаходяться чутлива інформація, що перекочувала на особисті пристрої користувачів, та онлайн-сервіси.

Питання інформаційної безпеки передбачає комплексний підхід. Необхідно торкнутися максимально можливої кількості аспектів у сфері захисту інформації,

зокрема визначити повний перелік загроз і в подальшому використовувати цей перелік загроз щодо конкретної системи. Важливою є повнота переліку загроз, оскільки за відсутності будь-якого елемента ймовірність компрометації інформації та/або системи різко зростає. За визначенням, моделювання загроз — це стратегія управління ризиками для активного захисту. Таким чином, формування моделі загроз, здатної забезпечити повний перелік загроз, є першочерговим завданням інформаційної безпеки. Моделі загроз мають стати відправною точкою для оцінки ризиків та розробки майбутніх систем безпеки для комп'ютерних та інформаційних систем.

В роботі розглянуто архітекти існуючих лабораторій з віддаленим доступом, які базуються на різних моделях організації. В результаті подібних досліджень стає можливим побудувати власну архітектуру організації дистанційного доступу для лабораторії на базі веб-порталу.

Головним етапом перед запровадженням системи є встановлення низки вимог, які повинні враховуватися на кожному етапі проектування інформаційної системи. Представлені рекомендації щодо захисту рішень віддаленого доступу. Він фокусується на безпеці сервера віддаленого доступу та розміщенні сервера. У цьому розділі представлені рекомендації щодо захисту клієнтського програмного забезпечення віддаленого доступу.

Окремо розглядається кожний елемент, який формує повну картину забезпечення конфіденційності. Наведено алгоритм роботи та принципи їх функціонування.

Незважаючи на те, що запропоновано повноцінну модель, багато аспектів мають високий рівень абстрактності, який рекомендується подолати безпосередньо у процесі створення лабораторного комплексу.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Challenges in Remote Laboratory Sustainability - Salzmann, Christophe; Gillet, Denis

2. Uckelmann, D., Mezzogori, D., Esposito, G., Neroni, M., Reverberi, D., Ustenko, M., & Baalsrud-Hauge, J. (2021). Guideline to Safety and Security in Federated Remote Labs. International Journal of Online and Biomedical Engineering (iJOE), 17(04), pp. 39–62

3. CISSP All-in-One Exam Guide, Eighth Edition, 8th Edition by Shon Harris

4. Von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102.

5. Javier García Zubía and Gustavo R. Alves (eds.) Using Remote Labs in Education

6. Ananda Maiti, Andrew D. Maxwell, Alexander A. Kist: Features, Trends and Characteristics of Remote Access Laboratory Management Systems.

7. Gary Stoneburner, Computer security - Recommendations of the National Institute of Standards and Technology 2001

8. A Remote PLC Laboratory Design and Realization – Xiaomei Chen. Procedia Engineering Volume 31, 2012, Pages 1168-1172

9. Geaney, G.; OMahony, T. (2015). Design and evaluation of a remote PLC laboratory. International Journal of Electrical Engineering Education

10. Ferrater-Simon, C.; Molas-Balada, L.; Gomis-Bellmunt, O.; Lorenzo-Martinez, N.; Bayo-Puxan, O.; Villafafila-Robles, R. (2009). A Remote Laboratory Platform for Electrical Drive Control Using Programmable Logic Controllers. , 52(3), 425–435.

11. Bellmunt, O.G.; Miracle, D.M.; Arellano, S.G.; Sumper, A.; Andreu, A.S. (2006). A distance PLC programming course employing a remote laboratory based on a flexible manufacturing cell. , 49(2), 278–284.

12. Wei-Fu Chang, ; Yu-Chi Wu, ; Chui-Wen Chiu, ; Wen-Ching Yu, (2003). - Design and implementation of a Web-based distance PLC laboratory. , (), 326–329.

13. Sheng-Jen Hsieh, ; Patricia Yee Hsieh, ; Dongmin Zhang, (2003). [IEEE 33rd Annual Frontiers in Education, 2003. FIE 2003. - Westminster, Colorado, USA (Nov. 5-8, 2003)]

14. Munoz, J. A.; Guzman, J. L.; Rodriguez, F.; Berenguel, M.; Pawlowski, A. (2009). [IEEE Factory Automation (ETFA 2009) - Palma de Mallorca, Spain (2009.09.22-2009.09.25)]

15. Lallie, Harjinder Singh; Debattista, Kurt; Bal, Jay (2020). A review of attack graph and attack tree visual syntax in cyber security.

16. Lallie, Harjinder Singh; Debattista, Kurt; Bal, Jay (2020). A review of attack graph and attack tree visual syntax in cyber security.

17. Threat scenario-based security risk analysis using usecase modeling in information systemsYoung-Gab Kim and Sungdeok Cha

18. Anomaly Detection System for Video Data Using Machine Learning Tadashi Ogino