Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА
Дипломної роботи

магістра
(назва освітньо-кваліфікаційного рівня)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній рівень ***магістр***
(назва освітнього рівня)

кваліфікація
(код і назва кваліфікації)

на тему: *Розробка моделі захищеної інформаційної технології підтримки та забезпечення функціонування сучасної системи підготовки та підвищення кваліфікації фахівців в галузі інформаційної безпеки*

Виконавець: студентка ***2*** **курсу, групи** ***КБм-21***

(підпис) ***Хижняк Анна Олександрівна*** (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Оцінка**	**Підпис**
Науковий керівник	*Толюпа С.В.*		
Рецензент	**Степанов М. М.**		
Нормоконтроль	**Даков С. Ю.**		

Київ
2021

Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри
кібербезпеки та захисту інформації
_____ Лукова-Чуйко Н.В.
«_____»_____20___року

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студенту *КБм-21* *Хижняк Анна Олександрівна*
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи *Розробка моделі захищеної інформаційної технології підтримки та забезпечення функціонування сучасної системи підготовки та підвищення кваліфікації фахівців в галузі інформаційної безпеки*

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол №_____ від _____

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень *Процес розробки захищених інформаційних систем дистанційного навчання*

Предмет досліджень *Методи та засоби оцінки захищеності систем дистанційного навчання*

Мета *Розробити математичну модель експертної оцінки захищеної системи дистанційного навчання*

Вихідні дані для проведення роботи *Сучасне законодавство України в сфері кібербезпеки, Технічні вимоги до системи дистанційного навчання,*

Технічне завдання на інформаційно-телекомунікаційну систему.

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна *Розробка математичної моделі розрахунку рейтингу експертів та математичної моделі оцінювання захищеності складної системи з урахування рейтингу експертів*

Практична цінність *Використання математичної моделі для експертної оцінки захищеності інформаційних систем*

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	**Строки виконання робіт (початок-кінець)**
1. Уточнення постановки задачі	20.09.2020 – 19.10.2020
2. Збір даних	22.10.2020 – 14.01.2021
3. Розробка 1 розділу	15.01.2021 – 25.03.2021
4. Розробка 2 розділу	26.03.2021 – 02.04.2021
5. Розробка 3 розділу	03.04.2021 – 25.04.2021
6. Оформлення атестаційної роботи	26.04.2021 – 02.05.2021

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект *Зниження імовірності виникнення загроз за допомогою математичної моделі експертної оцінки інформаційних систем*

Соціальний ефект *Покращення стану захищеності інформаційних систем на національному рівні*

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ _____
(підпис) (прізвище, ініціали)

Завдання прийняв
до виконання _____ _____
(підпис) (прізвище, ініціали)

Дата видачі завдання: _____

Термін подання дипломної роботи до ЕК _____

РЕФЕРАТ

Пояснювальна записка: 69 с., 7 рис., 7 табл., 2 додатки, 52 джерела.

Об’єкт дослідження – процес розробки захищених інформаційних систем дистанційного навчання.

Мета роботи – розробка математичної моделі експертної оцінки захищеної системи дистанційного навчання.

Методи дослідження – методи порівняння, структурний аналіз, системний підхід.

У роботі досліджено сучасні системи дистанційного навчання, комплекс вимог до їх функціоналу; комплекс вимог до структури захищеної інформаційної системи дистанційного навчання; вимоги до математичної моделі експертної оцінки захищеної системи дистанційного навчання.

Практичне значення роботи полягає у використанні математичної моделі для експертної оцінки захищеності інформаційних систем. Результати здійснених у дипломній роботі досліджень можуть бути використані на підприємствах будь-якого типу та розміру для експертної оцінки захищеності інформаційних систем.

Наукова новизна дослідження полягає у розробці математичної моделі розрахунку рейтингу експертів та математичної моделі оцінювання захищеності складної системи з урахування рейтингу експертів.

Напрямки подальших досліджень: вдосконалення математичної моделі експертної оцінки захищеної інформаційної системи.

Ключові слова: системи дистанційного навчання, експерти, експертна оцінка, математична модель, персональні дані.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БД	база даних
ІБ	інформаційна безпека
ІС	інформаційна система
ІТС	інформаційно-телекомунікаційна система
КСЗІ	комплексна система захисту інформації
КЗІ	криптографічний захист інформації
КЗЗ	комплекс засобів захисту
ОС	операційна система
СДН	система дистанційного навчання

ЗМІСТ

ВСТУП

Протягом останніх років темпи життя суттєво зросли. Швидкість передачі інформації, доступність інформаційних ресурсів в мережі Інтернет для будь якого мешканця, зростання вимог до оперативності прийняття рішень, особливо у галузі інформаційної безпеки.

Як приклад можна навести – атака вірусу «PETIA» в активній фазі зайняла півгодини. Втрати для економіки України, за оцінками експертів, перевищили 1 мільярд доларів США. Ця сума набагато перевищує річні бюджети усіх систем онлайн навчання в Україні! Вірус «поклав» понад 12 тисяч комп'ютерів в різних державних і приватних установах, включаючи Кабмін, операторів мобільного зв'язку, енергетичні компанії та найважливіші транспортні підприємства [1].

Ці фактори призводять до необхідності переосмислення підходів до використання СДН та підвищення кваліфікації. Лише СДН спроможні оперативно здійснити перепідготовку та підвищення кваліфікації за сучасних умов інформаційних загроз.

Дистанційне навчання — це сукупність сучасних технологій, що забезпечують доставку інформації в інтерактивному режимі за допомогою використання інформаційно-комунікаційних технологій від тих, хто навчає, до тих, хто навчається [2].

Актуальність обраної теми визначається зростанням використанням СДН у процесі навчання. Дистанційні засоби навчання будуть мати основну роль в удосконаленні системи освіти. У світі накопичено значний досвід впровадження СДН, які використовують сучасні телекомунікаційні технології, комп’ютерні мережі та системи безпосереднього телевізійного мовлення. Вітчизняний та закордонний досвід розвитку системи освіти вказує на те, що майбутнє її пов’язано з використанням дистанційного навчання. Ефективна реалізація переваг, що надає дистанційне навчання можлива лише за умови надання процесам його

впровадження та розвитку ознак системності, керованості та прогнозованості. Вивчення СДН і використання систем захисту інформації у складі сучасних технологій навчання є важливою і актуальною проблемою, яка потребує вирішення [3].

Метою роботи є розробка математичної моделі експертної оцінки захищеної системи дистанційного навчання.

Мета обумовлена вирішенням наступних задач:

– провести аналіз сучасних систем підготовки та підвищення кваліфікації;

– визначити комплекс вимог до сучасних систем підготовки та підвищення кваліфікації фахівців у галузі ІБ;

– визначити вимоги до захищеної інформаційної технології підтримки та забезпечення функціонування сучасної системи підготовки та підвищення кваліфікації фахівців у галузі ІБ;

– визначити вимоги до математичної моделі експертної оцінки захищеної СДН;

– розробити математичну модель розрахунку рейтингу експертів та математичну модель оцінювання захищеності складної системи з урахування рейтингу експертів;

– розробити програмну реалізацію математичної моделі розрахунку рейтингу експертів та математичної моделі оцінювання захищеності складної системи з урахування рейтингу експертів.

Об’єктом дослідження є процес розробки захищених інформаційних систем дистанційного навчання.

Предметом дослідження є методи та засоби оцінки захищеності систем дистанційного навчання.

Методом дослідження є методи порівняння, структурний аналіз, системний підхід.

Практичне значення роботи полягає у використанні математичної моделі для експертної оцінки захищеності інформаційних систем. Результати здійснених у

дипломній роботі досліджень можуть бути використані на підприємствах будь-якого типу та розміру для експертної оцінки захищеності інформаційних систем.

Наукова новизна дослідження полягає у розробці математичної моделі розрахунку рейтингу експертів та математичної моделі оцінювання захищеності складної системи з урахування рейтингу експертів.

Апробація результатів роботи та публікації. Основні результати доповідалися та обговорювалися на міжнародній науково-технічній конференції "Вимірювальна та обчислювальна техніка в технологічних процесах" (ВОТТП-2020) та на міжнародній науково-практичній конференції «Прикладні системи та технології в інформаційному суспільстві» (AISTIS-2020). Роботи надаються в додатку А.

РОЗДІЛ 1
ПРОВЕДЕННЯ АНАЛІЗУ СУЧАСНИХ ВИМОГ ДО ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ПІДТРИМКИ ТА ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ СУЧАСНОЇ СИСТЕМИ ПІДГОТОВКИ ТА ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ ФАХІВЦІВ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В даний час система освіти переживає період реформування. В умовах, що склалися, стала актуальною потреба в компетентних, конкурентоспроможних фахівцях з високим рівнем професійної підготовки, орієнтованих на професійне зростання і особистісний розвиток протягом усього життя. Все вищевикладене призвело до необхідності зміни методів навчання і переходу від традиційних методів навчання до сучасних освітніх технологій.

Фахівці, що займаються вивченням стратегічних проблем освіти, називають дистанційне навчання освітньою системою 21 століття [4]. Саме на цю систему освіти в даний час робиться велика ставка.

Зростаюча роль дистанційної освіти пояснюється тим, що прогрес зі сфери технологій поступово переміщається в інформаційну сферу. В даний час активно розвиваються різні телекомунікаційні системи, які відкривають широкі можливості в різних сферах людського життя, в тому числі і в освіті. Комп'ютерні технології розширили і можливості освіти. В даний час професійні знання застарівають дуже швидко. Тому, щоб відповідати сучасному рівню необхідно їх постійно вдосконалювати [5].

Дистанційне навчання є тією формою, яка дає можливість в даний час створювати системи масового безперервного самонавчання, загального обміну інформацією, що не залежать від тимчасових і просторових поясів.

В даний час все більшої актуальності набирає необхідність отримання додаткової професійної освіти в галузі ІБ шляхом підвищення кваліфікації або перепідготовки за даним напрямком. Це пов'язано з кількома факторами.

По-перше, успішність діяльності будь-якої організації безпосередньо залежить від ступеня професійної підготовки її персоналу. Важливе значення має не тільки позиція працівників, що стосується розвитку професійних і особистісних факторів, а й позиція керівництва організації, що означає прямий взаємозв'язок між ефективною роботою і професійною підготовкою співробітників. Тобто для успішної діяльності організації необхідно мати кваліфікований штат. Тому роботодавець зацікавлений не тільки в найму грамотних фахівців, а й в підтримці їх професійного рівня. Особливо це стосується ІБ організації, так як без належної уваги до цієї сфери ставиться під сумнів вся інша її діяльність [6].

По-друге, підвищення кваліфікації з ІБ просто необхідно в умовах високої динаміки розвитку інформаційних технологій, що тягне за собою наростання кількості загроз безпеці інформації, і веде до вдосконалення існуючих методів і засобів їх нейтралізації. Тобто без актуальних знань в цій області не можна забезпечити необхідний рівень захисту інформації в організації.

Тому, підготовка фахівців в області ІБ стає не тільки актуальною, але й життєво необхідною для існування підприємства. Ризики для компанії, пов'язані з різними впливами на її інформаційну інфраструктуру, є невід'ємною частиною процесу управління безперервністю бізнесу. При цьому найчастіше, особливо в невеликих компаніях, в питаннях захисту інформації керівники покладаються на рядових співробітників, які не мають відповідної кваліфікації [7].

1.1 Аналіз сучасних систем підготовки та підвищення кваліфікації

В даний час існує велика кількість СДН, але ми розглянемо найпопулярніші сучасні СДН.

Articulate Storyline.

Один з найбільш популярних інструментів для створення електронних навчальних матеріалів – Articulate Storyline. Його відрізняє висока якість, як самої

програми, так і продукту, що з неї виходить. Саме тому Articulate Storyline часто вибирають для професійної розробки електронного навчального контенту, не бентежачись вартістю даного продукту (близько 1400 $). Слід мати на увазі, що програма встановлюється виключно на ОС Windows. Користувач іншої ОС знадобиться віртуальна машина [8].

Курс складається зі слайдів. Є редактор шаблону для слайдів і відгуків (діалогових вікон - повідомлень, що виникають у відповідь на дію того, хто навчається). Також є безліч готових шаблонів для різних типів слайдів (пояснення або тест). Як і в PowerPoint, тут є можливість налаштувати розмір слайдів, анімацію переходів між слайдами, і анімацію на самому слайді.

Потужним інструментом для створення серйозних курсів є можливість роботи зі змінними, в які можна зберігати дані, які введені тими, хто навчаються, а потім використовувати їх в іншому місці. Наприклад, зберегти ім'я того, хто навчається і далі звертатися до нього по імені.

Storyline можна успішно використовувати для створення тренажерів - симуляторів програмного забезпечення. Демонстрація роботи з програмним забезпеченням може бути виконана за допомогою вбудованого рекордера. Він записує те, що відбувається на екрані (області екрану) з можливістю паралельного захоплення аудіо. У режимі step-by-step (крок за кроком) кожна дія (клік миші, поворот колеса миші) автоматично забезпечується коментарями. При цьому можна створити не тільки демонстраційний матеріал, а й такий, де користувач сам повинен виконати необхідні дії (try mode, test mode) [9].

Розроблений в Articulate навчальний курс може бути опублікований у всіх популярних форматах навчальних матеріалів (SCORM, TinCan, AICC), HTML5, Word (як набір скріншотів), на CD, а також в «хмарну» середу Articulate Online. Плеєр курсу має гнучку настройку: можна змінити текст і колір елементів. Є можливість додати ресурси (додаткові файли або посилання), глосарій курсу і замітки.

Moodle.

Поставка Moodle здійснюється вільно, так як Moodle є програмним забезпеченням з відкритим вихідним кодом (відповідно до GNU Public License).

Moodle може бути встановлений на будь-якому комп'ютері на якому встановлений Web-сервер, що підтримує PHP, а також встановлена БД SQL-типу (наприклад, MySQL).

Основні можливості Moodle [10]:

- система реалізує філософію "Педагогіки соціального конструкціонізму" (співробітництво, дії, критичне осмислення і т.д.);
- на 100% підходить для організації online-класів, а також підходить для організації традиційного навчання;
- СДН Moodle є: простою, легкою, ефективною, сумісною з різними продуктами, пред'являючи невисокі вимоги до браузеру;
- система легко встановлюється на більшість платформ, що підтримують PHP;
- система вимагає тільки одну БД;
- список курсів, розміщених в СДН Moodle, містить опис для кожного курсу;
- можливий пошук за дистанційними курсами;
- особливу увагу приділено високому рівню безпеки системи;
- більшість сторінок можуть бути відредаговані за допомогою вбудованого редактора.

Дистанційні курси, розроблені з використанням засобів СДН Moodle можуть включати в себе:

- ресурси;
- активні елементи;
- завдання;
- робочий зошит;

- опитування;
- базу даних;
- семінари;
- уроки;
- тести.

СДН Moodle є класичним клієнт-серверним Web-додатком, побудованим з використанням триланкової архітектури. Використання в якості клієнта Moodle Web-браузера робить використання даної системи вкрай зручною для всіх учасників навчального процесу [11].

Основною перевагою СДН Moodle є можливість її безкоштовного використання. При цьому функціональність СДН Moodle не поступається комерційним аналогам.

Ще однією важливою перевагою СДН Moodle є те, що вона поширюється у відкритому вихідному коді, що дозволяє адаптувати її під специфіку завдань, які повинні бути вирішені з її допомогою.

Docebo.

До основних можливостей системи Docebo відносять: налаштування для підтримки декількох моделей навчання (самостійно, змішано, у співпраці). В наявності є авторський інструмент, який дає можливість управляти тестами, завантаженнями файлів будь-якого формату, Web-сторінок, FAQ, глосаріями, колекціями посилань.

Підтримує сторонні інтерфейси з управління людськими ресурсами (SAP, Cezanne) та інші сервіси компаній (LDAP, Active Directpry і інші персоніфецірованние рішення).

Основні переваги Docebo [12]:

- Інтеграція в соціальні мережі.
- Інтеграція в популярні додатки і сервіси, Web і відео конференцій: Webex, Onsync, BigBlueButton, Adobe Connect.

- Інтеграція в систему Пейпал, можливість продавати курси за допомогою кредитних карт.

Як і всі системи, Docebo, має свої недоліки. Серед них SaaS модель поширення (як послуга): велика вартість використання, недостатня документація і її локалізація, за додаткові функції потрібно доплачувати.

Ключовими психологічними і техніко-організаційними особливостями СДН Docebo є комплексність функціоналу і величезні можливості інтеграції в соціальні мережі, конструктори сайтів, популярні додатки і веб сторінки [13].

Geenio.

Web-додаток дозволяє реалізувати повний цикл процесу навчання, починаючи від створення самого контенту за допомогою вбудованого редактора сторінок і закінчуючи аналізом результатів оцінки знань для прийняття рішень.

Ключові модулі Geenio [14]:

- Система управління навчанням
- Редактор нелінійних інтерактивних тестів
- Конструктор тестів, з безліччю різних типів питань
- Інструмент зі збору статистики та звітності. Можливість спостереження за процесом навчання своїх учнів.

Важливою перевагою Geenio є модуль нелінійності, який представлений «Картою навчання». У цьому режимі можна додавати нові сторінки, уроки (набори сторінок), питання і тести (набори питань). «Карта Навчання» є візуалізацією всього процесу проходження курсу і дозволяє створювати альтернативні шляхи розвитку подій. Таким чином, творець курсу завжди бачить весь шлях навчання, від початку і до кінця, все відгалуження і переходи між різними гілками розвитку подій [15].

За результатами розгляду сучасних систем дистанційного навчання можливо зробити наступні зауваження:

– Навчальні програми і курси можуть бути недостатньо добре розроблені через те, що кваліфікованих фахівців, здатних створювати подібні навчальні посібники, на сьогоднішній день не так багато.

– Висока вартість побудови СДН, на початковому етапі створення системи, великі витрати на створення СДН, самих курсів дистанційного навчання і купівлю технічного забезпечення.

– Проблема з ідентифікацією учня. Викладачам складно простежити, чи самостійно студент виконує всі завдання, здає заліки чи ні.

– Залежність від технологій. Електронна база може виявитися вразливою для хакерів і при вторгненні в неї збоку можна втратити всю документальну базу - історію виконаних лабораторних робіт, навчальних посібників і матеріалів. Тому потрібно, щоб для СДН була добре розроблена система захисту.

– Відсутність окремого компоненту з БД матеріалів, де буде зібраний весь навчальний матеріал для допомоги учням. Тому потрібно, щоб була окремо створена єдина база навчальних матеріалів.

Отже, сучасні тенденції розвитку ринку СДН спрямовані в бік універсалізації і збільшення функціональності систем.

Використання комерційних систем управління електронним навчанням не доступно більшості вітчизняних вузів через їх високу вартість і необхідність продовження ліцензії на кожен навчальний рік.

Системи з відкритим вихідним кодом дозволяють реалізувати той же набір можливостей, що і комерційні з істотно меншими витратами і більшою ефективністю.

1.1.1 Додаткові сервіси, які необхідні системам дистанційного навчання

Згідно з аналізу сучасних СДН, можна розглянути деякий загальний функціонал, властивий сучасним СДН:

- реєстрація учнів і викладачів;
- доставка контенту;
- забезпечення різних видів взаємодії учнів між собою і з викладачами;
- контроль успішності;
- збір статистики в навчальному процесі;
- генерація звітів;
- створення питань і управління тестами;
- підтримка створення контенту;
- організація багаторазово використовуваного контенту;
- розробка засобів навігації для управління процесом створення контенту.

Однією з основних складових дистанційного навчання є БД навчально-довідкових і методичних матеріалів. До навчально-методичних матеріалів висуваються жорсткі вимоги, тому що ефективність дистанційного навчання істотно залежить від форми і якості надання навчальних матеріалів.

Для організації збереження великої кількості допоміжних матеріалів для самостійної роботи доцільно організовувати сховища, які побудовані за принципами репозиторію. Репозиторій — ресурс у мережі, де зберігаються і підтримуються публікації. Найчастіше дані в репозиторії зберігаються у вигляді файлів, доступних для подальшого поширення по мережі [16].

Зазвичай репозиторій надає доступ до дисертацій, монографій, наукових видань та праць науковців, навчально-методичних матеріалів, патентів та кваліфікаційних робіт студентів.

Репозиторій, виступаючи важливим компонентом інформаційної СДН, забезпечує доступ до широкого спектру інформаційних джерел в електронній формі. В особливості до електронної наукової, навчальної та навчально-методичної інформації. Процес формування електронних матеріалів вимагає створення системи, що забезпечує зберігання, оновлення, пошук і витяг необхідної інформації [17].

Репозиторій повинен забезпечувати [18]:

– розміщення і зберігання матеріалів певних тематик, створюючи умови для росту та професійного розвитку фахівців;

– накопичення, розповсюдження та забезпечення довготривалого та надійного доступу до професійної інформації;

– спадкоємність знань та досвіду;

– вільний доступ до матеріалів авторизованим користувачам.

Тож, репозиторій – це єдина база навчальних матеріалів, яка є справжнім джерелом знань. Завдяки їй можна зберігати та нарощувати внутрішню базу матеріалів.

Не менш важливою частиною СДН є рейтингові системи оцінки знань студентів, тому що в умовах становлення нових форм організації і діяльності навчальної сфери необхідно зберегти і удосконалювати систему творчих змагань студентів на всіх етапах навчального процесу.

Тому з метою виділення кожного студента із загальної маси, створення умов для прояву його індивідуальних здібностей необхідна гнучка система підготовки фахівців із застосуванням автоматизованої рейтингової системи контролю знань студентів. Контролююча функція рейтингової системи забезпечує безперервний контроль знань студентів протягом кожного семестру і всього періоду навчання, інтегральну оцінку знань і творчих здібностей студента, отримання показника якості підготовки майбутнього фахівця [19].

Рейтингова оцінка роботи викладача виражається інтегрованим показником участі викладача в навчальній, навчально-методичній, науково-методичній, науково-дослідницькій, організаційно-методичній та позанавчальній роботі з урахуванням якісних показників роботи.

Використання рейтингової системи у СДН забезпечує [20]:

– підвищення мотивації студентів до якісного засвоєння курсів шляхом більш високої диференціації оцінки їх навчальної роботи;

– підвищення рівня саморегулювання навчальної діяльності студента і процесу навчання;

– стимулювання регулярної самостійної навчальної роботи студентів в семестрі. З цією метою сумарну рейтингову оцінку з дисципліни доцільно формувати з рейтингової оцінки поточного контролю знань з дисципліни та підсумкового контролю;

– підвищення мотивації професорсько-викладацького складу до інтенсивної та якісній роботі з підготовки фахівців;

– оцінку діяльності викладача по розділах індивідуального плану і стимулювання якісного його виконання.

1.2 Визначення комплексу вимог до сучасних систем підготовки та підвищення кваліфікації фахівців в галузі інформаційної безпеки

СДН повинна відповідати наступним вимогам [21]:

– доступність: система повинна надавати доступ до навчальних матеріалів з будь-якої точки віддаленого доступу;

– адаптованість: система повинна бути адаптованою відповідно до вимог начальної програми;

– ефективність: система повинна мати можливість скорочувати час і витрати на доставку матеріалів для навчання, збільшуючи при цьому ефективність і продуктивність;

– довговічність: система повинна відповідати новим технологіям, що часто змінюються та вдосконалюються без додаткового доопрацювання;

– інтероперабельність: система повинна мати можливість використовувати матеріали для навчання незалежно від платформи, на якій вони створені;

– забезпечення доступу до системи з різних браузерів;

– наявність засобів розробки контенту (наповнення курсів навчальними матеріалами та можливість зміни матеріалів курсу в режимі онлайн);

– можливість використання в якості контенту файлів різних форматів, в тому числі аудіо, відео, анімації, графіки.

1.2.1 Визначення комплексу вимог до системи інформаційного забезпечення як компонента сучасної системи підготовки та підвищення кваліфікації фахівців

СДН повинна представляти собою центральне захищене сховище з базою знань та навчальних матеріалів, в якому користувач може отримати необхідні йому знання та підвищити кваліфікацію.

Повинні бути передбачені необхідні засоби автоматизованого контролю цілісності даних і несуперечності збереженої інформації, персоніфікації даних, створених різними користувачами, ведення журналу операцій, які виконуються.

Система повинна складатися з таких підсистем [21]:

– захищене сховище системи (ведення захищеної БД курсів, тестів, учбових та дидактичних матеріалів; ведення БД користувачів центрального сховища);

– інформаційно-аналітична система контролю якості навчання (здійснення вхідного контролю знань персоналу при призначенні, переводі на посади; здійснення періодичного контролю знань персоналу – за регламентом або за необхідності);

– система аудиту знань (забезпечення вирішення завдань щодо забезпечення вибіркового контролю знань для окремих категорій персоналу).

Методи захисту для зв’язку між підсистемами повинні здійснюватися з використанням криптографічних засобів захисту інформації, які забезпечать впровадження наступних механізмів [22]:

– строгу автентифікацію при доступі користувачів до БД системи;

– створення захищеного каналу доступу;

– забезпечення цілісності, достовірності інформації при обміні між підсистемами.

Система повинна включати програмні засоби моніторингу та механізми документування аварійних подій чи помилок. В разі виникнення аварійних подій чи помилок в роботі системи, помилка повинна реєструватися у відповідному електронному журналі, а адміністратор має отримати відповідне повідомлення із зазначенням типу помилки. При цьому повинна бути реалізована можливість отримання технічної довідкової інформації-допомоги з різним рівнем деталізації щодо ліквідації аварійних подій, чи виправлення помилки.

Збереженість інформації повинна бути забезпечена у разі виникнення наступних подій (аварій, відмов тощо):

– відмова обладнання сервера;

– вимкнення живлення на робочому місці та/або на сервері БД;

– відмова ліній зв’язку.

З метою забезпечення зберігання інформації повинно використовуватися:

– резервне копіювання;

– відновлення даних при збоях в роботі мережевого, програмного і апаратного забезпечення.

Інформаційне забезпечення повинне забезпечити [23]:

– забезпечення фізичної та логічної цілісності даних;

– мінімізацію надмірності даних, що зберігаються;

– стандартизацію представлення даних;

– достовірність та актуальність даних;

– розмежування доступу до даних, запобігання несанкціонованого доступу до них.

Інформаційне забезпечення повинно відповідати основним вимогам:

– забезпечувати копіювання і зберігання масивів інформації;

– забезпечувати можливість розширення масивів інформації з урахуванням перспектив розвитку системи.

Висновки за розділом 1

Отже, сьогодні СДН є дуже актуальною проблемою. Вибір систем великий, але узагальнено вони повинні відповідати таким вимогам, як:

- захищеність, захист персональних даних;
- доступність;
- адаптованість;
- ефективність;
- модульність;
- довговічність;
- інтероперабельність.

Системам дистанційного навчання властивий широкий функціонал додаткових сервісів, але найважливішим є єдина база навчальних матеріалів, яка є справжнім джерелом знань.

РОЗДІЛ 2
ОБҐРУНТУВАННЯ ВИМОГ ДО МОДЕЛІ ЗАХИЩЕНОЇ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ПІДТРИМКИ ТА ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ СУЧАСНОЇ СИСТЕМИ ПІДГОТОВКИ ТА ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ ФАХІВЦІВ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Будь-яка СДН використовує інформаційно-комунікаційні технології і мережі передачі даних для здійснення взаємодії між учасниками освітнього процесу, зберігання і обробки інформації. Для запобігання різних сценаріїв порушення ІБ необхідно здійснювати періодичний контроль над станом захищеності системи, виявляти потенційні ризики і своєчасно застосовувати механізми безпеки, спрямовані на запобігання загрозам [24].

Вважаємо за доцільне запропонувати структуру та вимоги до СДН.

Система повинна складатися з таких підсистем [25]:

- захищене центральне сховище системи (ведення захищеної БД курсів, тестів, учбових та дидактичних матеріалів; ведення БД користувачів центрального сховища);
- захищені корпоративні сховища системи (організація та забезпечення захищеної взаємодії корпоративної системи підвищення кваліфікації користувачів; забезпечення можливості створення та ведення окремих корпоративних курсів, тестів, без передачі даних до захищеного центрального сховища системи);
- захищена система інформаційного обміну між сховищами системи (захищений інформаційний доступ до ресурсів сховищ для адміністративного, технічного персоналу системи; використання криптографічних протоколів захищеної доставки інформаційних пакетів до відокремлених вузлів захищених корпоративних сховищ системи);
- інформаційно-аналітична система контролю якості навчання (здійснення вхідного контролю знань персоналу при призначенні, переводі на посади;

здійснення періодичного контролю знань персоналу – за регламентом або за необхідності);

- система аудиту знань (забезпечення вирішення завдань щодо забезпечення вибіркового контролю знань для окремих категорій персоналу).

Для виявлення ключових проблем ІБ, причин і джерел їх виникнення, а також оцінки їх наслідків, необхідно виявити в ній найбільш критичні і вразливі місця.

В СДН найбільш уразливими з точки зору ІБ є процеси [26]:

- передачі ідентифікаційних і аутентифікаційних даних користувача СДН;
- обмін даними між браузером віддаленого користувача і веб-сайтом СДН.
- авторизації користувача в СДН;
- витяг і запис даних в базі даних СДН і ІС вузу;
- обмін даними між сервером СДН і сервером ІС вузу.

Подібний висновок в першу чергу пов'язано з тим, що саме в процесі виконання даних дій, найбільш імовірна спроба зловмисника реалізувати атаку на СДН і отримати доступ до її ресурсів, сервісів і даних [27].

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

- отримання несанкціонованого доступу до ресурсів і сервісів СДН;
- перевищення привілеїв і отримання контролю над СДН;
- отримання через зламану СДН несанкціонованого доступу до внутрішньої ІС вузу;
- крадіжка матеріалів та інтелектуальної власності: навчальних матеріалів, оціночних матеріалів і матеріалів, що створюються колективно учасниками навчального процесу;
- отримання доступу до персональних даних студентів та співробітників вузу;
- крадіжка і розголошення персональних даних студентів та співробітників вузу;

- отримання несанкціонованого доступу та внесення змін до БД навчальних відомостей;
- отримання несанкціонованого доступу до внутрішньої службової та іншої конфіденційної інформації, що зберігається і оброблюється в системі
- отримання несанкціонованого доступу і крадіжка результатів науково-дослідної та інноваційної діяльності;
- порушення цілісності та / або знищення навчальних матеріалів і даних про навчальний процес;
- порушення доступності веб-сайту і сервера СДН;
- порушення доступності інформації і матеріалів навчальних курсів для користувачів СДН.

Підсумувавши, робимо висновок, що в системі циркулює:

1) технологічна інформація (системні налаштування та налаштування безпеки програмного та апаратного забезпечення, ідентифікатори користувачів та їх облікові записи). Технологічна інформація є інформацією з обмеженим доступом, яка доступна тільки адміністраторам системи згідно з їх службовими обов'язками.

2) конфіденційна інформація (інформація, що містить персональні дані користувачів, викладачів, персоналу, інформація про яких оброблюються, зберігаються та передаються в системі).

3) чутлива для СДН інформація (дані про результати навчання користувачів, дані викладачів, дані курсів навчання, дані тестових завдань)

Система складна, вона повинна бути призначена для вирішення наступних завдань:

- створення центрального захищеного сховища з базою знань та навчальних матеріалів;
- забезпечення можливості створення розгалуженої інформаційної інфраструктури серверів – Централізована система навчання, корпоративні системи навчання, відомчі системи навчання тощо.

- забезпечення можливості в межах корпоративних ІТС створювати власні корпоративні захищені бази знань та навчальних матеріалів, формування та ведення корпоративних систем підготовки та підвищення кваліфікації працівників.

Відповідно до цього, є необхідним забезпечити конфіденційність, цілісність та доступність інформації, яка зберігається в БД системи. Але для різної інформації різні вимоги.

2.1. Вимоги до захищеної інформаційної технології підтримки та забезпечення функціонування сучасної системи підготовки та підвищення кваліфікації фахівців в галузі інформаційної безпеки

Розробка системи повинна передбачати наступні вимоги [29]:

Впровадження механізмів захисту створення до складу захищеного центрального сховища системи – з метою побудови КСЗІ;

Розробку захищених корпоративних сховищ системи як комплексів засобів захисту КЗЗ, з метою подальшої побудови захищеної системи в корпоративних відомчих системах;

Створення висококваліфікованої команди фахівців в межах захищеного центрального сховища системи – з метою забезпечення підтримки користувачів, забезпечення підтримки системи, її розвитку, створення учбових курсів та матеріалів тощо;

Забезпечення можливості створення команд висококваліфікованих фахівців для обслуговування захищених корпоративних сховищ системи, забезпечення їх підготовки з використанням можливостей команди підтримки захищеного центрального сховища системи;

Захищена система інформаційного обміну між сховищами повинна забезпечувати можливість створення віртуальної захищеної системи зв’язку у

відкритому середовищі мережі Інтернет з досить жорсткими вимогами щодо забезпечення захисту;

Захищена система інформаційного обміну між сховищами повинна забезпечувати можливість взаємодії із захищеними корпоративними сховищами системи з безумовним виконанням політик безпеки корпоративних відомчих захищених мереж та систем.

Захищена інформаційно-аналітична система контролю якості навчання повинна використовувати найкращі рішення щодо забезпечення контролю знань, математичні методи оцінювання якості підготовки фахівців тощо.

2.1.1. Вимоги до функціоналу інформаційної системи дистанційного навчання

Як було згадано на початку другого розділу, сучасна СДН повинна складатися з п’яти компонентів, кожен з яких має забезпечувати вирішення різних складних завдань. Розглянемо функціонал кожної з них більш детально.

Захищене центральне сховище системи повинно забезпечувати вирішення наступних завдань:

- ведення захищеної БД курсів, тестів, учбових та дидактичних матеріалів;
- ведення БД користувачів центрального сховища;
- ведення централізованого обліку захищених корпоративних сховищ, переліку курсів, учбових матеріалів, що передавались до захищених корпоративних сховищ;
- організація та забезпечення захищеної взаємодії з захищеними корпоративними сховищами;
- облік та ведення БД відгуків на курси, учбові матеріали.

Захищені корпоративні сховища системи повинні забезпечувати вирішення наступних завдань:

- ведення захищеної БД курсів, тестів, учбових та дидактичних матеріалів, які розташовані у корпоративному сховищі;
- ведення БД користувачів корпоративного сховища;
- ведення централізованого обліку курсів, матеріалів, які надійшли від центрального сховища;
- ведення централізованого обліку фахівців, які завершили курси та отримали сертифікати з підвищення рівня знань;
- організація та забезпечення захищеної взаємодії корпоративної системи підвищення кваліфікації користувачів;
- забезпечення можливості створення та ведення окремих корпоративних курсів, тестів, без передачі даних до захищеного центрального сховища системи;
- забезпечення можливості тестування рівня знань при призначенні на посади;
- облік та ведення корпоративної БД відгуків на курси, учбові матеріали.

Захищена система інформаційного обміну між сховищами системи повинна забезпечувати вирішення наступних завдань:

- захищену взаємодію між сховищами;
- захищений інформаційний доступ до ресурсів сховищ для адміністративного, технічного персоналу системи;
- використання криптографічних протоколів захищеної доставки інформаційних пакетів до відокремлених вузлів захищених корпоративних сховищ системи.

Захищена інформаційно-аналітична система контролю якості навчання повинна забезпечувати вирішення наступних завдань:

- здійснення вхідного контролю знань персоналу при призначенні, переводі на посади;
- здійснення періодичного контролю знань персоналу – за регламентом або за необхідності;

- ведення корпоративної БД обліку персоналу, курсів, результатів підготовки тощо;
- забезпечення можливості організації виборок та пошуку інформації за певними критеріями.

Захищена система аудиту знань повинна забезпечувати вирішення наступних завдань щодо забезпечення вибіркового контролю знань для окремих категорій персоналу:

- експертів з питань забезпечення безпеки інформації;
- кандидатів на зарахування на керівні посади;
- кандидатів на призначення на посади з підвищеною відповідальністю.

2.1.2. Вимоги щодо захисту персональних даних та чутливої для інформаційної системи дистанційного навчання інформації

Основними вимогами захисту персональних даних інформаційної СДН є [30]:

- реєстрація усіх користувачів відповідно до встановленої політики безпеки;
- можливість здійснення однозначної ідентифікації та автентифікації кожного зареєстрованого користувача;
- створення захищеного середовища обробки інформації, в якому всі дії користувачів контролюються системою захисту інформації;
- запобігання несанкціонованому доступу до приміщень, фізичних та інформаційних ресурсів;
- блокування доступу до ресурсів ІС користувачів, які порушили встановлені правила розмежування доступу;
- контроль цілісності програмно-технічного середовища ІС;
- комплексне застосування механізмів захисту інформації.

Інформація в процесі обробки в ІС не повинна підлягати неконтрольованому та несанкціонованому ознайомленню, копіюванню, відновленню, а також неконтрольованій та несанкціонованій модифікації.

Під час визначення особи як користувача повинен створюватися його обліковий запис шляхом формування:

– інформації ідентифікації – ім’я (псевдонім) користувача;

– інформації автентифікації – пароль для входу до системи та/або інші ідентифікатори користувача.

Надання доступу до інформації повинно здійснюватися за умови достовірного розпізнання користувачів з урахуванням наданих повноважень.

Повинна бути забезпечена можливість своєчасного доступу зареєстрованих користувачів до інформації.

Інформація під час обробки в ІС повинна мати атрибути з визначенням встановленого ступеня обмеження доступу до неї.

Повинен бути забезпечений облік дій всіх користувачів щодо обробки інформації. Повинен здійснюватися періодичний контроль за всіма обліковими діями.

Спроби порушення встановленого порядку доступу до інформації повинні підлягати реєстрації з забезпеченням можливості розслідування інцидентів з боку уповноважених осіб. У цьому випадку повинна забезпечуватися можливість блокування доступу до інформації.

2.1.3. Вимоги щодо захисту технологічної інформації, яка має конфіденційний характер в системі дистанційного навчання

Основними вимогами щодо захисту технологічної інформації, яка має конфіденційний характер в СДН, є:

- класифікація активів системи, що підлягають захисту в ІС;

- встановлення категорій користувачів та визначення їх повноважень щодо доступу та використання обчислювальних ресурсів та інформації;
- реєстрація та аналіз подій, пов’язаних з безпекою інформації;
- реагування на події ІБ;
- антивірусний захист інформації;
- дублювання критичних компонентів системи та їх вузлів.
- резервне копіювання інформації;
- контроль за станом захисту інформації в системі відносно актуальних ризиків виникнення інформаційних загроз.

У складі ІС мають використовуватися ліцензійні антивірусні програмні забезпечення, які пройшли державну експертизу у сфері технічного захисту інформації.

Встановлення, налаштування, оновлення антивірусних програмних забезпечень повинно здійснюватися уповноваженими адміністраторами відповідно до документації або рекомендацій, що поставляються з програмним забезпеченням.

Оновлення БД антивірусних програмних забезпечень має здійснюватися регулярно.

Порядок забезпечення політики антивірусного захисту адміністраторами та користувачами системи має визначатися інструкцією з антивірусного захисту та відповідними інструкціями адміністраторів.

У ході функціонування ІС на регулярній основі повинно забезпечуватися резервне копіювання інформації, що обробляється в системі, та програмних засобів з метою швидкого її відновлення на випадок несанкціонованих дій, впливу комп’ютерних вірусів, аварій та відмов обладнання, інших подій, що можуть призвести до знищення чи пошкодження інформації.

Обов’язковому резервному копіюванню повинна підлягати технологічна інформація, що обробляється в ІС.

Резервне копіювання повинно здійснюватися не рідше одного разу на тиждень.

2.2. Побудова моделі захищеної інформаційної системи дистанційного навчання

Як було згадано в першому розділі, в даний час існує безліч СДН. Це готові програмні продукти – «Articulate Storyline», «Moodle», «Docebo», «Geenio» та інші.

Можна з упевненістю сказати про те, що ринок СДН активно розвивається у всьому світі. Це пов'язано в першу чергу з підвищеним попитом на освітні послуги і розвитком інформаційних технологій. До того ж з року в рік кількість користувачів в Інтернеті збільшується [28].

СДН в Україні тільки починають формуватися, багато компаній і фірм створюють свої СДН для персоналу.

Однією з таким систем є СДН Playgarden, яка побудована на платформі віддаленого навчання Opigno. Opigno – це система управління навчанням заснована на Drupal. Вона була розроблена таким чином, щоб повністю інтегруватися з будь-якою платформою Drupal (веб-сайт, Інтранет, екстранет) і пропонує максимальну гнучкість для розширення [31].

СДН Playgarden включає в себе [32]:

- Тренінги: цей розділ дає користувачеві огляд всіх курсів, до яких він має доступ.
- Каталог тренінгів: каталог відображає користувачеві всі курси (згруповані по класах, якщо є), на які він може підписатися. Це означає, що курси, що відображаються повинні бути загальнодоступними, а курси, на які користувач уже підписався, приховані.
- Форум: відображає користувачеві все форуми, до яких він має доступ. Це означає глобальний форум (рівень платформи, доступний для всіх користувачів незалежно від курсів, до яких вони мають доступ) і один форум за курсом, до якого користувач має доступ (якщо інструмент форуму був активований для курсу).

- Календар: календар об'єднує всі події, які застосовуються для користувача, що означає глобальні події та події для кожного з курсів, до яких користувач має доступ. Таким чином, користувач має огляд всіх своїх навчальних заходів.

- Повідомлення: Playgarden пропонує внутрішню систему обміну повідомленнями, що дозволяє користувачам спілкуватися в залежності від певних дозволів. Базові настройки дозволяють тільки менеджерам, вчителям і тренерам зв'язуватися зі своїми учнями. Потім учні можуть відправляти повідомлення і відповідати на них іншим учасникам (студентам, викладачам) свого класу або курсу.

- Мої досягнення: цей розділ дає студенту огляд всіх його результатів для класів і курсів, а також для завантаження його сертифікатів, якщо він пройшов тест з мінімальним рахунком, визначеним в налаштуваннях класу / курсу. Також користувач може детально деталізувати результати з курсу, уроку, тесту.

- Статистика: цей розділ містить графічні панелі моніторингу зі статистикою використання глобальної платформи, статистикою по курсу і статистикою по користувачах.

- Адміністрування: цей розділ не відображається для учнів. Менеджери, вчителі, тренери і, звичайно, адміністратори платформи, мають доступ до цього розділу. Деякі частини приховані в залежності від їх профілів. Менеджери, викладачі та тренери знайдуть посилання для управління користувачами (переглянуть їх результати, відправлять повідомлення), а адміністратор платформи знайде додатково деякі інтерфейси для визначення загальних параметрів платформи.

Загальний принцип застосування Playgarden представлений на рисунку 2.1:

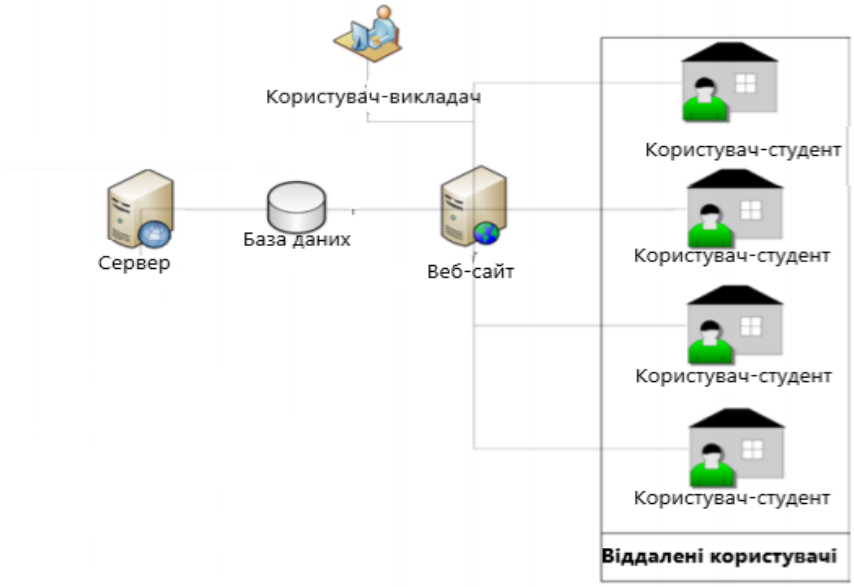

Рисунок 2.1 – Функціональні компоненти Playgarden

В якості основних функціональних компонентів Playgarden можна виділити [33]:

1) веб-додаток - зовнішній інтерфейс, призначений для організації віддаленого доступу студентів до змісту навчальних курсів, презентацій, мультимедійних продуктів, тестів та інтерактивної взаємодії з викладачем;

2) БД, в якій зберігатися наповнення навчальних курсів, розміщуються оціночні матеріали, електронні підручники, інформація для студентів і дані про успішність;

3) сервер Playgarden, є ядром системи і забезпечує наступні функціональні можливості:

- реєстрація та управління обліковими записами користувачів в системі;
- розмежування прав доступу до функцій і наповненню системи;
- надання доступу до ресурсів;
- адміністрування та захист системи;
- облік учнів;
- створення і імпорт навчальних матеріалів;
- управління каталогами курсів;
- відстеження результатів навчання і тестування;

– реєстрація інформації про події в системі.

Основними суб'єктами взаємодії в рамках системи Playgarden є внутрішні і зовнішні користувачі, яких можна розділити на наступні групи:

1) викладачі - створюють навчальні курси, контролюють навчальний процес;

2) адміністратори, програмісти, фахівці з ІБ – забезпечують адміністрування та захист системи, відстежують події та інциденти, пов'язані з функціонуванням системи;

3) студенти - вивчають курси, проходять тестування, освоюють навчальний план.

Відповідно до виділених функціональних підсистем і суб'єктів типовий технологічний процес обробки інформації в системі Playgarden допустимо представити таким чином:

1) підключення користувача до веб-сайту системи;
2) авторизація користувача на сервері системи;
3) запит на сервер системи на надання інформації та доступу до ресурсів курсів і підсистем системи;
4) введення, модифікація або висновок інформації відкритого і / або обмеженого доступу;
5) отримання користувачем запитаного матеріалу і даних;
6) відключення користувача від ресурсів СДН.

2.2.1. Вимоги до структури захищеної інформаційної системи дистанційного навчання Playgarden

Структура захищеної інформаційної СДН Playgarden повинна бути формалізована таким чином, щоб була можливість оцінки достатності комплексу засобів захисту і нормативних документів, що використовуються в ній [34].

Формальний опис структури захищеної ІС має спиратися на кілька моделей:

- модель системи документообігу;
- модель ІС;
- модель загроз інформації та ІС;
- модель загроз засобів захисту інформації.
- модель експертної оцінки захищеної ІС.

Модель системи документообігу дозволить визначити, в рамках яких середовищ циркулює інформація в ІС, а також об'єкти та суб'єкти, яким дозволено зберігання, обробка та передача інформації.

Модель ІС дозволить врахувати типи каналів передачі інформації та багаторівневість зон роботи з інформацією, визначивши необхідну кількість рубежів захисту.

Модель загроз інформації повинна включати весь можливий перелік загроз, для кожної з яких будуть визначені методи і засоби захисту в рамках кожної середи.

Модель загроз засобів захисту дозволить враховувати в структурі системи захисту заходи, необхідні для забезпечення безперервної роботи захищеної ІС.

Модель експертної оцінки захищеної ІС дозволить провести аналіз стану захищеності ІС за рахунок залучення компетентних експертів в галузі ІБ.

При цьому структура захищеної ІС повинна бути заснована на єдиному описі програмно-технічного і нормативного елемента системи захисту, дозволяючи комплексно оцінити якість захисту від кожної загрози [35].

2.2.2. Розробка рекомендацій до захищеної інформаційної системи дистанційного навчання Playgarden

При функціонуванні захищеної інформаційної СДН Playgarden повинно забезпечуватись виконання наступних вимог:

- захищене функціонування ІС з використанням мережі Інтернет;

- неможливість стороннього втручання в проведення транзакцій при обміні інформацією функціональними компонентами ІС;

- ведення захищеного аудиту інформаційної взаємодії функціональних компонентів;

- побудова транзакцій при інформаційному обміні між функціональними компонентами з використанням криптографічних протоколів строгої автентифікації, криптографічних протоколів інформаційного обміну з підтвердженням не лише отримання інформації, а й факту імплементації інформації до ІС без пошкоджень та колізій;

- забезпечення надійного та безпечного захищеного накопичення та зберігання транзакцій інформаційної взаємодії функціональних компонентів з метою забезпечення можливості незалежного та повного відтворення ІС у аварійних випадках (наприклад, після пошкодження ІС комп'ютерним вірусом на кшталт віруса «PETIA»);

- забезпечення функціонування системи інформаційної взаємодії функціональних компонентів за принципом «24*7*365».

Висновки за розділом 2

На підставі матеріалу другого розділу вважаємо за доцільне зробити наступні висновки.

1. В СДН циркулює технологічна інформація та персональні дані користувачів.

2. Формальний опис структури захищеної ІС має спиратися на кілька моделей:

- модель системи документообігу;
- модель ІС;
- модель загроз інформації та ІС;

- модель загроз засобів захисту інформації.
- модель експертної оцінки захищеної ІС.

3. Побудова захищеної інформаційної СДН повинна здійснюватись з використанням криптографічних засобів захисту інформації, які забезпечать впровадження наступних механізмів:

- строгу автентифікацію при доступі користувачів до бази даних ІС;
- створення захищеного каналу доступу;
- забезпечення цілісності, достовірності інформації при обміні.

РОЗДІЛ 3
МАТЕМАТИЧНА МОДЕЛЬ ЕКСПЕРТНОЇ ОЦІНКИ ЗАХИЩЕНОЇ СИСТЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ

Експертне оцінювання - одна з найбільш поширених технологій, що привертає увагу широкого кола фахівців. В даний час сфера застосування експертного оцінювання постійно розширюється [36-40].

Останнім часом експертне оцінювання знаходить інтенсивне застосування в області експлуатації корпоративних і телекомунікаційних мереж, завдяки простоті і оперативності отримання потрібних відомостей про їх фактично технічній стан. Це пояснюється тим, що експлуатація корпоративних і телекомунікаційних мереж відносно нова сфера людської діяльності, в якій йде процес накопичення і осмислення різнопланової інформації. Застосування методів експертного оцінювання особливо поширене на завданнях: проектування корпоративних мереж [41], при побудові комплексних систем захисту [42], при експлуатації корпоративних мереж [43], обчислення інформаційних ризиків та інше [44].

Методи експертних оцінок, засновані на знаннях фахівців і накопиченому ними досвіді при проведенні оцінки захищеності системи є важливим інструментом визначення загальних тенденцій захисту і технічного рівня складних автоматизованих систем 3 класу [45].

При формуванні експертних оцінок основним джерелом інформації є експерт, а для підвищення ступеня об'єктивності та якості процедури прийняття рішення доцільно враховувати думки декількох експертів. Таким чином, експертні методи ґрунтуються виключно на оцінках експертів, зроблених стосовно проблеми або завдання, яку вони знають краще за інших.

Основними факторами при проведенні експертних оцінок, що визначають надійність і точність оцінки, є підбір експертів і їх компетентність. Визначити

необхідний чисельний склад експертної групи дуже важливо. При недостатньому числі експертів, а також при їх різній кваліфікації результати їх діяльності не будуть надійні. Потрібно враховувати всі фактори, що впливають на точність результатів.

Тому є необхідність розробки математичної моделі експертної оцінки, яка, враховуючи всі фактори, що впливають на точність результатів, а саме – кількість експертів, рівень їх компетентності та їх різна кваліфікація, буде найбільш точно показувати рівень захищеності ІС.

3.1. Вимоги до математичної моделі експертної оцінки захищеної системи дистанційного навчання

Як вже було зазначено, визначити необхідний чисельний склад експертної групи дуже важливо. При недостатньому числі експертів результати їх діяльності не будуть надійні. Численну групу кваліфікованих експертів важко сформувати і організувати її роботу. Тому необхідно взяти невелику кількість експертів, наприклад – три, які мають високі знання в потрібних напрямках щодо захисту інформації.

Розроблено метод оцінки технічного рівня систем за участю експертів, основні положення якого наведені в роботах [46-48]. В даному випадку при оцінці технічного рівня системи експерти зазвичай залучаються для формування показників і визначення вагомості (важливості) оціночних показників, рангів досліджуваних об'єктів. Важливою обставиною для дослідника є обґрунтований підбір експертів.

Формування експертних робочих груп є відповідальним етапом у процедурі експертної оцінки [49].

Експерт повинен відповідати таким вимогам:

- оцінки експерта повинні бути стабільними протягом проведення експертизи;
- експерт повинен бути компетентним у своїй галузі знань, тобто бути визнаним спеціалістом з питань ІБ.

Для оцінки якості захищеної СДН повинна проводитись процедура оцінки із застосуванням опитування. Даний метод повинен включати наступні основні етапи:

- вибір певної кількості експертів, яку будуть брати участь в опитуванні;
- формування рейтингу експертів на основі самооцінки та оцінки один одного взаємно з іншими експертами;
- формування основних напрямків, по яким експерти повинні мати високі знання;
- використання опитувальних листів на основі вимог з ІБ;
- формування на основі вимог і рекомендацій з інформаційної безпеки і на основі відповідей залучених фахівців рівень захищеності ІС.

Вимоги до математичної моделі експертної оцінки захищеної СДН:

- створення збалансованого рейтингу кваліфікації експертів;
- створення опитувального листа для експертів;
- забезпечення можливості розрахунку виваженої експертної оцінки на основі рейтингу кваліфікації експертів та відповідей на опитувальний лист.

3.1.1. Математична модель розрахунку рейтингу експертів

Підвищення достовірності експертних оцінок, за рахунок залучення в групу найбільш компетентних експертів для проведення експертизи є актуальною проблемою.

Для оцінювання компетентності експертів потрібно розробити модель оцінювання експертів, яка допоможе визначити рівень компетентності експерта.

Для прикладу, при оцінюванні захищеності ІТС, можна визначити п’ять основних напрямків, по яким експерти повинні мати високі знання [50]:

– знання вимог нормативних документів у галузі захисту інформації (далі – Норм. док.);

– знання вимог з питань криптографічного захисту інформації (далі – КЗІ);

– знання вимог щодо побудови системи захисту інформації (далі – КСЗІ);

– знання вимог щодо порядку організації та проведення робіт у відповідності до вимог міжнародних та державних стандартів (далі – Міжн./Держ. станд.);

– знання вимог щодо підготовки системи до введення в експлуатацію(далі – Експл.).

Кожен експерт має володіти рейтингом за кожним напрямком.

Запропонована математична модель обчислення.

Для оцінки компетентності експертів, можна використовувати такі коефіцієнти: K_c - коефіцієнт відносної самооцінки; $K_в$ - коефіцієнт взаємної оцінки [51].

Рейтинг експерта формується виходячи з його власної оцінки (K_c) та оцінок його знань іншими експертами ($K_в$).

Перш за все, кожен експерт оцінює свій рівень знань в кожній області, ставлячи собі такі питання:

1. На скільки відсотків я розуміюся в нормативних документах у галузі захисту інформації?

2. На скільки відсотків я розуміюся з питань КЗІ?

3. На скільки відсотків я розуміюся в питаннях КСЗІ?

4. На скільки відсотків я розуміюся в організації та проведення робіт у відповідності до вимог міжнародних та державних стандартів?

5. На скільки відсотків я розуміюся в питаннях підготовки системи до введення в експлуатацію?

Після відносної самооцінки отримуємо такі результати, для прикладу:

Таблиця 3.1 – Приклад відносної самооцінки експертів

	Норм. док.	КЗІ	КСЗІ	Міжн./Держ. станд.	Експл.
Екс. 1 (K_c)	68%	95%	65%	87%	70%
Екс. 2 (K_c)	75%	90%	85%	65%	93%
Екс. 3 (K_c)	60%	76%	90%	79%	89%

Далі відбувається взаємна оцінка експертами один одного. Питання ставляться по тим самим напрямкам:

1. На скільки відсотків експерт 1/2/3 розуміється в нормативних документах у галузі захисту інформації?
2. На скільки відсотків експерт 1/2/3 розуміється з питань КЗІ?
3. На скільки відсотків експерт 1/2/3 розуміється в питаннях КСЗІ?
4. На скільки відсотків експерт 1/2/3 розуміється в організації та проведення робіт у відповідності до вимог міжнародних та державних стандартів?
5. На скільки відсотків експерт 1/2/3 розуміється в питаннях підготовки системи до введення в експлуатацію?

Таблиця 3.2 – Експерт 1 оцінює експерта 2 і експерта 3

Екс. 2 ($K_{в1}$)	73%	88%	82%	60%	90%
Екс. 3 ($K_{в1}$)	60%	75%	85%	77%	88%

Таблиця 3.2 – Експерт 2 оцінює експерта 1 і експерта 3

Екс. 1 ($K_{в2}$)	65%	95%	63%	85%	70%
Екс. 3 ($K_{в2}$)	61%	75%	90%	75%	89%

Таблиця 3.3 – Експерт 3 оцінює експерта 1 і експерта 2

Екс. 1 ($K_{вз}$)	68%	91%	62%	86%	70%
Екс. 2 ($K_{вз}$)	75%	87%	85%	60%	90%

На підставі оцінки експертами самих себе і інших експертів, отримуємо рядок матриці оцінки. Застосувавши середнє арифметичне отримуємо зважену оцінку експерта: $\bar{x} = \frac{1}{n} \sum_{i=1}^{n} x_i = \frac{1}{n} (x_i + \ldots + x_n)$

3.1.2. Математична модель оцінювання захищеності складної системи з урахування рейтингу експертів

Ми розглядаємо існуючу ІС [52], до якої існують перелік вимог:

- по нормативним документам у галузі захисту інформації,
- по КЗІ,
- по побудові КСЗІ,
- по порядку організації та проведення робіт у відповідності до вимог міжнародних та державних стандартів,
- по підготовці системи до введення в експлуатацію.

ІС складається з компонентів, які забезпечують роботу цієї системи (Рисунок 3.1).

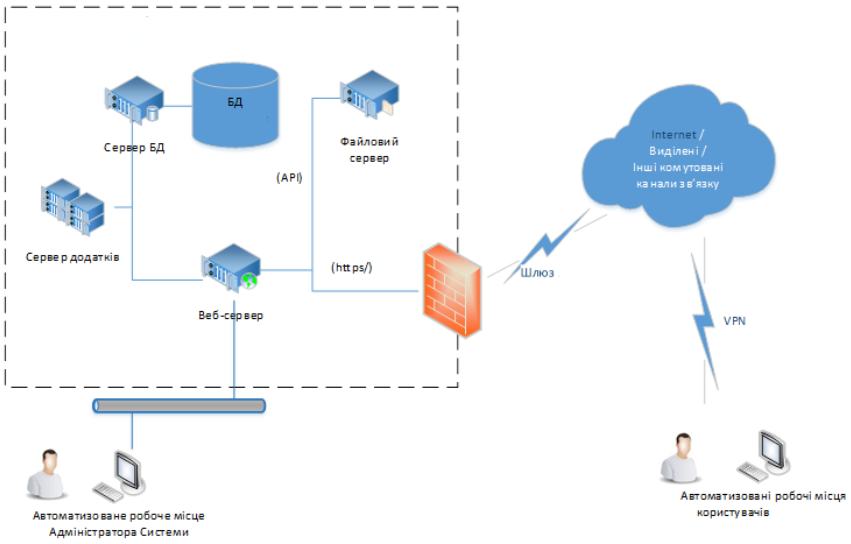

Рисунок 3.1 - Структурна схема апаратно-програмного комплексу ІС

В системі є наступні ролі адміністративного персоналу, який приймає безпосередню участь у вирішенні завдань забезпечення безпеки та надійного функціонування системи.

– Адміністратор системи ІС з виконанням функцій:

- налаштування системних параметрів ІС;
- розгортання, формування та налаштування БД;
- супровід та технічна підтримка БД (резервне копіювання, відновлення інформації);
- налаштування бізнес-процесів.

– Технічний адміністратор ІС з виконанням функцій:

- налаштування довідників;
- створення облікових записів користувачів;
- формування звітів;
- налаштування планувальника завдань;
- перегляд конфігураційних параметрів.

– Адміністратор безпеки ІС з виконанням функцій:

- керування засобами КЗІ;

- підключення зовнішніх користувачів з точки зору виконання положень політики безпеки;
- контроль стану ІБ в системі та її компонентів.

– Адміністратор технічного забезпечення ІС з виконанням функцій:

- технічне обслуговування апаратного забезпечення системи;
- виконує заявки щодо включення додаткових потужностей у систему;
- виконання профілактичних робіт;
- виконує завдання щодо підтримки працездатності апаратного забезпечення, в середовищі якого функціонує система та її компоненти.

Для створення системи криптографічного захисту та забезпечення корпоративної ІБ виконуються певні вимоги щодо реалізації криптографічних алгоритмів засобами криптографічного захисту; щодо забезпечення шлюзом захисту фільтрації та захисту трафіку; щодо забезпечення системи керування VPN Manager.

Для криптографічного захисту інформації з обмеженим доступом в системі використовуються засоби КЗІ, які мають позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації.

В моделі порушника визначено:

– Потенційні порушники.

– Категорії порушників, які мають потенційну можливість порушення конфіденційності та цілісності вважаються найбільш небезпечними, спостереженості - менш небезпечними, доступності - найменш небезпечними.

– Специфікація моделі порушника за мотивами здійснення порушень.

– Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІС.

– Профілі можливостей порушників.

– Характер дій порушника.

– Мотив порушення, кваліфікація та можливості порушника, час дії порушника.

– Ефективність рівень загроз - рейтингова оцінка загроз порушника з відповідними характеристиками.

– Спроби несанкціонованого доступу.

В системі є узагальнені відомості про інформацію, що обробляється, зберігається та передається в ІС та перелік відомостей щодо фізичних осіб, дані яких оброблюються в ІС та у сукупності або окрему містять конфіденційну інформацію(персональні дані фізичних осіб).

В моделі загроз наведено формалізований опис можливих дій порушника щодо реалізації потенційних сценаріїв загроз, який базується на його практичних та теоретичних можливостях, апріорних знаннях, часі та місцю дії тощо, в якому з достатнім рівнем деталізації визначено: можливі цілі порушника та їх градація за ступенями небезпечності для ІС; категорії персоналу, користувачів ІС та сторонніх осіб, із числа яких може бути порушник; припущення щодо кваліфікації порушника; припущення щодо характеру його дій, зведена модель порушника визначає імовірні типи та характеристики суб’єктів шкідливого впливу на систему.

В складі документації КСЗІ підготовлено експлуатаційну документацію визначених засобів та механізмів захисту, що входять в КЗЗ. Склад та зміст експлуатаційної документації компонентів (складових частин) КЗЗ, наданої для випробувань в складі об’єкта випробувань, відображає програмно-технічний комплекс засобів захисту КСЗІ і дозволяє адміністративному персоналу виконувати свої посадові обов’язки з обслуговування КЗЗ.

Розроблений набір тестів, з метою перевірки що реалізовані функціональні підсистеми комплексу засобів захисту інформації від несанкціонованого доступу КСЗІ в ІС забезпечують в рамках компонентів ІС реалізацію послуг функціонального профілю відповідно до вимог технічного завдання.

Для більш детального ознайомлення з ІС, Технічне завдання на КСЗІ в ІС наведено в Додатку Б.

При проведенні обстеження середовищ функціонування ІС розглядається як організаційно-технічна система, яка поєднує обчислювальну систему, фізичне середовище, оброблювану інформацію і технологію її обробки.

При проведенні обстеження середовищ функціонування ІС експертно-документальним методом на підставі представлених робочої конструкторської та експлуатаційної документації, матеріалів, документів, актів, сертифікатів було складено лист опитування, за яким буде оцінено захищеність ІС.

Як було визначено в попередньому підрозділі, використовуються п’ять напрямків, по яким створено лист опитування для захищеності ІС:

1. Відповідність системи вимогам нормативних документів у галузі захисту інформації.
2. Відповідність системи вимогам з питань КЗІ.
3. Відповідність системи вимогам щодо побудови КСЗІ.
4. Відповідність системи вимогам щодо порядку організації та проведення робіт у відповідності до вимог міжнародних та державних стандартів.
5. Виконання заходів щодо підготовки системи до введення в експлуатацію.

Відповіді на питання можуть бути такими:

Таблиця 3.5 – Відповіді на питання у відсотках

"Так"	100%
Виконано майже повністю	75%
Виконано частково	50%
Майже не виконано	25%
"Ні"	0%

Таблиця 3.6 – Лист опитування для експертів

Питання	**Так**	**Виконано майже повністю**	**Виконано частково**	**Майже не виконано**	**Ні**
Відповідність системи вимогам нормативних документів у галузі захисту інформації					
Чи утворена служба захисту інформації або призначені особи, на яких покладається забезпечення захисту інформації та контролю за ним, власником системи, в якій обробляється інформація з обмеженим доступом?					
Чи проведені повні і достатні випробування КСЗІ, її систем?					
Чи проведена інвентирізація усіх компонентів системи?					
Відповідність системи вимогам з питань криптографічного захисту інформації					
Чи реалізують засоби КЗІ криптографічні алгоритми, необхідні для захищеності ІС?					
Чи розроблена і впроваджена політика використання криптографічних контролів для захисту інформації?					
Чи мають позитивний експертний висновок за результатами державної експертизи у сфері КЗІ використані для захисту інформації в системі засоби КЗІ?					

продовження табл.3.6

Відповідність системи вимогам щодо побудови комплексної системи захисту інформації					
Чи визначено в моделі порушника з достатнім рівнем деталізації визначено: можливі цілі порушника та їх градація за ступенями небезпечності для ІС; категорії персоналу, користувачів ІС та сторонніх осіб, із числа яких може бути порушник; припущення щодо кваліфікації порушника; припущення щодо характеру його дій?					
Чи забезпечують специфікація та рівні послуг безпеки, визначені в Технічному завданні, можливості попередження, протидії та реагування на актуальні загрози інформації, описані в моделі політики безпеки?					
Чи узагальнені відомості щодо забезпечення властивостей (конфіденційності, цілісності, доступності та спостережності) інформації, що зберігається та обробляється в ІС?					
Відповідність системи вимогам щодо порядку організації та проведення робіт у відповідності до вимог міжнародних та державних стандартів					
Чи регулярно перевіряється ІС на відповідність стандартам впровадження безпеки?					
Чи ретельно сплановані та погоджені вимоги аудиту та діяльність, що охоплює перевірки ОС, щоб мінімізувати ризик порушення бізнес процесів?					

продовження табл.3.6

Чи забезпечене керівниками коректне виконання всіх процедур безпеки в сфері їх відповідальності для досягнення відповідності політикам та стандартам безпеки?					
Виконання заходів щодо підготовки системи до введення в експлуатацію					
Наданий в моделі загроз опис можливих джерел виникнення загроз, а також сценарії їх реалізації в системі базується на визначених параметрах потенційних можливостей порушника, враховує конструктивні та технологічні вразливості реалізації ІС відповідно до розробленої архітектури реалізації та відповідає умовам і характеристикам середовищ експлуатації?					
Чи відображає склад та зміст експлуатаційної документації компонентів комплексу заходів захисту програмно-технічний комплекс засобів захисту КСЗІ та чи дозволяє адміністративному персоналу виконувати свої посадові обов'язки з обслуговування КЗЗ?					
Чи розроблений набір тестів, з метою перевірки що реалізовані функціональні підсистеми комплексу засобів захисту інформації від несанкціонованого доступу КСЗІ в ІС забезпечують в рамках компонентів ІС реалізацію послуг функціонального профілю відповідно до вимог Технічного завдання?					

При підрахунку числового значення узагальненої думки експертів, які відповіли на запитання, враховуються:

– рівень знань експерта по напрямку, яке відповідає напрямку питання;

– оцінка даного питання.

Результат оцінювання - цифрова оцінка ІС, яка отримана з урахуванням думок всіх експертів. Цифровий профіль безпеки системи формується таким чином:

За результатами експертного оцінювання ІТС отримано наступні виважені коефіцієнти:

Таблиця 3.7 – Результати експертного оцінювання

№	Зміст	Оцінка відповідності, в %
1.	відповідність системи вимогам нормативних документів у галузі захисту інформації	
2.	відповідність системи вимогам з питань криптографічного захисту інформації	
3.	відповідність системи вимогам щодо побудови системи захисту інформації	
4.	відповідність системи вимогам щодо порядку організації та проведення робіт у відповідності до вимог міжнародних та державних стандартів	
5.	виконання заходів щодо підготовки системи до введення в експлуатацію	

3.2. Апробація моделі та інтерпретація отриманих результатів

Математична модель експертної оцінки захищеної ІС може застосовуватися до будь-якої ІС, побудованої згідно вимог стандартів і міжнародних документів. В тому числі така модель може застосовуватися до СДН, які розглядаються як ІС.

Запропонована модель експертної оцінки захищеної СДН має програмну реалізацію математичних методів розрахунку, яка в подальшому може бути

корисною для проведення аудиту та оцінки стану захищеності СДН, що є дуже актуальним питанням в наш час.

Програмна реалізація пропонує такі можливості:

- введення кількості експертів;
- введення рейтингу експертів;
- розрахунок рейтингу експертів на підставі опитування;
- введення переліку питань;
- внесення оцінок експертів за питаннями;
- розрахунок підсумкового рейтингу ІС;
- формування таблиці з оцінкою системи.

При проведенні розробки моделі захищеності ІС було взято три реальних експерта, які ознайомилися з документацією по ІС, та пройшли опитування. Система, інформація по якій була наведена в п. 3.1.2, - це ІТС, яка існує та функціонує в межах міста Києва.

Програмна реалізація представлена на рисунку 3.2.

	Норм.док	КЗИ	КСЗИ	Міжн.Держ.Станд.	Введення в експлуат.	Середня оцінка
Експерт 1						#ДЕЛ/0!
Експерт 2						#ДЕЛ/0!
Експерт 3						#ДЕЛ/0!
	Оцінка інших експертів першим експертом					
Експерт 2						
Експерт 3						
	Оцінка інших експертів другим експертом					
Експерт 1						
Експерт 3						
	Оцінка інших експертів третім експертом					
Експерт 1						
Експерт 2						
	Середня оцінка експертів по дисциплінам					Середня оцінка
Експерт 1	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!
Експерт 2	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!
Експерт 3	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!	#ДЕЛ/0!

Експерт 1	
1. відповідність системи вимогам нормативних документів у галузі захисту інформації	
2. відповідність системи вимогам з питань криптографічного захисту інформації	
3. відповідність системи вимогам щодо побудови системи захисту інформації	
4. відповідність системи вимогам щодо порядку організації та проведення робіт у відповідності до вимог міжнародних та державних стандартів	
5. виконання заходів щодо підготовки системи до введення в експлуатацію	
Експерт 2	
1. відповідність системи вимогам нормативних документів у галузі захисту інформації	
2. відповідність системи вимогам з питань криптографічного захисту інформації	
3. відповідність системи вимогам щодо побудови системи захисту інформації	
4. відповідність системи вимогам щодо порядку організації та проведення робіт у відповідності до вимог міжнародних та державних стандартів	
5. виконання заходів щодо підготовки системи до введення в експлуатацію	
Експерт 3	
1. відповідність системи вимогам нормативних документів у галузі захисту інформації	

Рисунок 3.2 – Програмна реалізація математичної моделі

Експертами заповнюється таблиця з визначеним рівнем кваліфікація за п’яти напрямками. Середня оцінка рахується застосувавши середнє арифметичне.

Потім проставляється взаємна оцінка експертами один одного. Та заповнюється відповідно в таблицю. Ми отримуємо зважену середню оцінку експерта. Вона рахується так – складається відносна самооцінка експерта та дві оцінки іншими експертами, отриманий результат ділиться на кількість експертів (на три). Результат представлено на рисунку 3.3.

	A	B	C	D	E	F	G
1		Норм.док	КЗИ	КСЗИ	Міжн.Держ.Станд.	Введення в експлуат.	Середня оцінка
2	Експерт 1	68%	95%	65%	87%	70%	77%
3	Експерт 2	75%	90%	85%	65%	93%	82%
4	Експерт 3	60%	76%	90%	79%	89%	79%
5							
6							
7		Оцінка інших експертів першим експертом					
8	Експерт 2	73%	88%	82%	60%	90%	
9	Експерт 3	60%	75%	85%	77%	88%	
10		Оцінка інших експертів другим експертом					
11	Експерт 1	65%	95%	63%	85%	70%	
12	Експерт 3	61%	75%	90%	75%	89%	
13		Оцінка інших експертів третім експертом					
14	Експерт 1	68%	91%	62%	86%	70%	
15	Експерт 2	75%	87%	85%	60%	90%	
16		Середня оцінка експертів по дисциплінам					Середня оцінка
17	Експерт 1	67%	94%	63%	86%	70%	76%
18	Експерт 2	74%	88%	84%	62%	91%	80%
19	Експерт 3	60%	75%	88%	77%	89%	78%
20							

Рисунок 3.3 – Оцінювання рівня експертів

Далі експерти переходять до листа опитування (розділ 3.1.2. табл.3.6). За питаннями, експерти оцінюють стан захищеності системи, та результат заносять до таблиці (Рисунок 3.4):

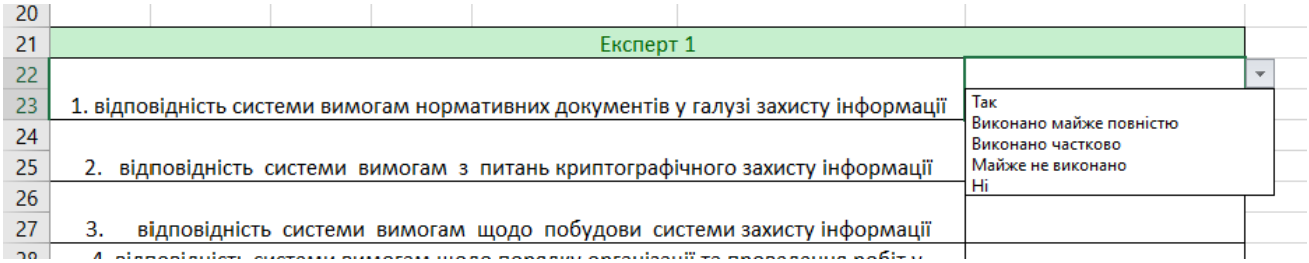

Рисунок 3.4 – Лист опитування

Отримуємо таблицю з результатами опитування експертів (Рисунок 3.5).

Експерт 1	
1. відповідність системи вимогам нормативних документів у галузі захисту інформації	Так
2. відповідність системи вимогам з питань криптографічного захисту інформації	Виконано майже повністю
3. відповідність системи вимогам щодо побудови системи захисту інформації	Виконано майже повністю
4. відповідність системи вимогам щодо порядку організації та проведення робіт у відповідності до вимог міжнародних та державних стандартів	Так
5. виконання заходів щодо підготовки системи до введення в експлуатацію	Виконано майже повністю
Експерт 2	
1. відповідність системи вимогам нормативних документів у галузі захисту інформації	Виконано майже повністю
2. відповідність системи вимогам з питань криптографічного захисту інформації	Виконано майже повністю
3. відповідність системи вимогам щодо побудови системи захисту інформації	Так
4. відповідність системи вимогам щодо порядку організації та проведення робіт у відповідності до вимог міжнародних та державних стандартів	Так
5. виконання заходів щодо підготовки системи до введення в експлуатацію	Так
Експерт 3	
1. відповідність системи вимогам нормативних документів у галузі захисту інформації	Так
2. відповідність системи вимогам з питань криптографічного захисту інформації	Так
3. відповідність системи вимогам щодо побудови системи захисту інформації	Виконано майже повністю
4. відповідність системи вимогам щодо порядку організації та проведення робіт у відповідності до вимог міжнародних та державних стандартів	Так
5. виконання заходів щодо підготовки системи до введення в експлуатацію	Виконано частково

Рисунок 3.5 – Результати опитування експертів

При підрахунку результатів ми множимо коефіцієнт з середньою зваженою оцінкою експерта на коефіцієнт, який відповідає певній відповіді за листом опитування. І рахуємо середню оцінку за коефіцієнтами по трьом експертам. Отримуємо оцінку відповідності системи напрямкам з ІБ у відсотках (Рисунок 3.6).

№	Зміст	Оцінка відповідності в %
1	Відповідність системи вимогам нормативних документів у галузі захисту інформації	61%
2	Відповідність системи вимогам з питань криптографічного захисту інформації	71%
3	Відповідність системи вимогам щодо побудови системи захисту інформації	66%
4	Відповідність системи вимогам щодо порядку організації та проведення робіт у відповідності до вимог міжнародних та державних стандартів	75%
5	Виконання заходів щодо підготовки системи до введення в експлуатацію	68%

Команда експертів із зваженим рейтингом	78%	**здійснила експертну оцінку системи на**	68%	

Рисунок 3.6 – Оцінка відповідності системи напрямкам з ІБ

На підставі проведених обчислень при оцінці даної ІС ми можемо отримати наступні результати:

1. Поточна команда експертів оцінила захищеність системи на 68%. При цьому за показниками, які виділені при проведенні оцінювання, можна побачити більш детальний результат:

- відповідність системи вимогам нормативних документів у галузі захисту інформації – 61%;
- відповідність системи вимогам з питань КЗІ – 71%;
- відповідність системи вимогам щодо побудови КСЗІ – 66% ;
- відповідність системи вимогам щодо порядку організації та проведення робіт у відповідності до вимог міжнародних та державних стандартів – 75%;
- виконання заходів щодо підготовки системи до введення в експлуатацію – 68%.

2. Рівень команди експертів, які приймали участь у оцінюванні системи складає 83%.

При прийнятті рішення щодо відповідності системи вимогам захищеності необхідно брати до уваги рівень експертів.

Більш достовірну оцінку можливо отримати за рахунок залучення експертів з більш високим рівнем підготовки.

3. Як видно з таблиці (з рівнем експертів) є занижені показники рівня експертів з питань відповідності системи вимогам нормативних документів у галузі захисту інформації та відповідності системи вимогам щодо порядку організації та проведення робіт у відповідності до вимог міжнародних та державних стандартів.

Доцільно підібрати команду експертів, яка відповідає вимогам щодо оцінювання системи.

Наприклад, взяти команду експертів з високим рівнем знань у галузях:

- виконання заходів щодо порядку проведення експертизи;

- знання вимог щодо порядку оформлення документації на ІТС, на експертизу;
- знання державних стандартів України 34серії,

якщо саме ці галузі є критичними при оцінюванні системи.

Висновки за розділом 3

1. Складність сучасних ІС не дає можливість однозначно зробити висновок про їх захищеність.
2. ІС розвиваються, оновлюється софт, змінюється компоненти ОС, апаратне забезпечення. Гарантувати її захищеність при таких умовах складно.
3. Постійно змінюються загрози ІС. З'являються нові, змінюється рівень кваліфікації персоналу і т.д.
4. Необхідні математичні методи експертної оцінки захищеності інформаційних систем при їх створенні або в умовах експлуатації (вимоги ДСТУ / ISO 27001, 27002). І, відповідно, програмні реалізації математичних методів розрахунку.

ВИСНОВОК

У зв'язку з активним вдосконаленням інформаційних технологій і поширенням локальних і глобальних мереж, все більшого значення набуває наявність системи дистанційної освіти. Це життєва необхідність, оскільки «... сучасна дистанційна освіта дає рівні можливості всім людям незалежно від соціального стану (студентам, цивільним і військовим, безробітними та т. д.) в будь-яких районах країни і за кордоном реалізувати права людини на освіту і отримання інформації ».

Системи дистанційної освіти представляють собою додатки, які будуються на базі ІС і активно використовують веб-ресурси для організації інтерактивної взаємодії учнів і викладача. В процесі свого функціонування дана система піддається ряду негативних впливів випадкового і навмисного характеру, що в результаті може привести до порушення інформаційної безпеки СДН.

Тому у дипломній роботі розв’язано актуальне наукове завдання щодо розробки математичної моделі експертної оцінки захищеної СДН.

В ході розв’язання поставленої задачі були отримані наступні наукові та практичні результати:

1. Проведено аналіз сучасних систем підготовки та підвищення кваліфікації.
2. Визначено комплекс вимог до сучасних систем підготовки та підвищення кваліфікації фахівців у галузі ІБ.
3. Визначено вимоги до захищеної інформаційної технології підтримки та забезпечення функціонування сучасної системи підготовки та підвищення кваліфікації фахівців у галузі ІБ.
4. Побудовано модель захищеної інформаційної СДН Playgarden.
5. Визначено вимоги до математичної моделі експертної оцінки захищеної СДН.

6. Розроблено математичну модель розрахунку рейтингу експертів та математичну модель оцінювання захищеності складної системи з урахування рейтингу експертів.

7. Розроблено програмна реалізацію, яка пропонує такі можливості:

- введення кількості експертів;
- введення рейтингу експертів;
- розрахунок рейтингу експертів на підставі опитування;
- введення переліку питань;
- внесення оцінок експертів за питаннями;
- розрахунок підсумкового рейтингу ІС;
- формування таблиці з оцінкою системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Україна стала першою ціллю принципово нового виду кіберзброї [Електронний ресурс]. – Режим доступу: https://www.ukrinform.ua/rubric-technology/2259655-ukraina-stala-persou-cillu-principovo-novogo-vidu-kiberzbroi.html
2. Дистанційне навчання [Електронний ресурс]. – Режим доступу: https://cpto.pl.ua/administraciya-11-23-40-15-10-2020/
3. Делик І.С. Зарубіжний досвід дистанційного навчання студентів з особливими потребами. / І.С. Делик, О.В. Діденкот // [Електронний ресурс]. – Режим доступу: www.irbis-nbuv.gov.ua/cgibin/irbis.../cgiirbis_64.exe?
4. Пріоритети дистанційного навчання іноземної мови в сучасному світі інноваційних технологій [Електронний ресурс]. – Режим доступу: https://core.ac.uk/download/pdf/32612157.pdf
5. Околелов, О.П. Процесс обучения в системе дистанционного образования Текст. / О.П. Околелов // Дистанц. образование. 2000. - № 3. - С. 3743.
6. Андрєєв А.А. Засоби сучасних інформаційних технологій в системі освіти: систематизація та тенденції розвитку -М .: ВУ, 1995 г. с. 48-43.
7. Peter Brusilovsky. Adaptive Systems // User Modeling and UserAdapted Functions 11: 87 - 110, 2001
8. Articulate Storyline [Електронний ресурс]. – Режим доступу: https://articulate.com/perpetual/storyline-3
9. Articulate Storyline 360 [Електронний ресурс]. – Режим доступу: https://soware.ru/products/articulate-storyline-360
10. Moodle [Електронний ресурс]. – Режим доступу: https://moodle.org/
11. Система електронного навчання і тестування Moodle: огляд можливостей [Електронний ресурс]. – Режим доступу: https://www.ispring.ru/elearning-insights/moodle

12. Обзор СДО Docebo: возможности и решаемые бизнес-задачи [Електронний ресурс]. – Режим доступу: https://lmslist.ru/sdo/obzor-docebo/

13. Docebo Review [Електронний ресурс]. – Режим доступу: https://www.pcmag.com/reviews/docebo

14. Geenio LMS [Електронний ресурс]. – Режим доступу: https://elearningindustry.com/directory/elearning-software/geenio-lms

15. Geenio LMS [Електронний ресурс]. – Режим доступу: https://www.lms.org/reviews/geenio/

16. Репозиторій [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/%D0%A0%D0%B5%D0%BF%D0%BE%D0%B7%D0%B8%D1%82%D0%B0%D1%80%D1%96%D0%B9

17. Институционный репозиторий как средство повышения научного рейтинга преподавателя [Електронний ресурс]. – Режим доступу: https://core.ac.uk/download/pdf/19668552.pdf

18. Положення про репозиторій. [Конфіденційно]

19. Положення про дистанційне навчання [Електронний ресурс]. – Режим доступу: http://uiite.kpi.ua/2019/06/03/polozhennya-pro-distancijne-navchannya/

20. Морзе Н. Яким має бути «розумний» університет в «розумному» суспільстві? //Сучасні стратегії університетської освіти: якісний вимір; матерілі міжнародної науково-практ. конф. (Київ, 28-29 березня 2012 р. ЗВ'ЯЗОК). - К., 2012. - С. 87-99. [Електронний ресурс]. – Режим доступу: http://elibrary.kubg.edu.ua/892/1/N_Morze_KONF_2_NDLIO.pdf

21. Технічні вимоги до системи дистанційного навчання для корпоративного замовника з підвищеними вимогами щодо забезпечення інформаційної безпеки [Конфіденційно]

22. Модель оценки защищенности систем дистанционного образования вузов [Електронний ресурс]. – Режим доступу: https://cyberleninka.ru/article/n/model-otsenki-zaschischennosti-sistem-distantsionnogo-obrazovaniya-vuzov/viewer

23. Брусилівський, П.Л. Адаптивні і інтелектуальні технології в мережевому навчанні / П.Л. Брусилівський // Новини штучного інтелекту. 2002. - №5. - С.25-31.

24. Брусилівський, П.Л. Інтелектуальні навчальні системи / П.Л. Брусилівський // Информатика. Інформаційні технології. Засоби і системи. 1990. - №2. - С.3-22.

25. Власенко А.А. Разработка системы адаптивного контроля знаний в высшем учебном заведении / Власенко А.А., Орлов Д.С. // Управление в социальных и экономических системах: сборник трудов всероссийской конф. – Воронеж: ВИВ. – 2009. – С. 112–114.

26. Глобальне дослідження витоків конфіденційної інформації в I півріччі 2015 року [Електронний ресурс]. – Режим доступу: http://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2015_half_year.pdf

27. Колгатін А.Г. Інформаційна безпека в системах відкритої освіти // Освітні технології і суспільство. - 2014. -Т.17, №1. - С. 417 - 425.

28. Глобальная архитектура Opigno LMS [Електронний ресурс]. – Режим доступу: http://drupal.lluvia.ru/opigno/%D0%B3%D0%BB%D0%BE%D0%B1%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F-%D0%B0%D1%80%D1%85%D0%B8%D1%82%D0%B5%D0%BA%D1%82%D1%83%D1%80%D0%B0

29. Власенко А.А. Разработка структуры адаптивной системы обучения / Власенко А.А. // Вестник Воронежского Государственного технического университета. – 2011. – № 6.– С. 50–52.

30. Колгатін А.Г. Інформаційна безпека в системах відкритої освіти // Освітні технології і суспільство. - 2014. -Т.17, №1. - С. 417 - 425.

31. Opigno LMS [Електронний ресурс]. – Режим доступу: http://drupal.lluvia.ru/opigno/opigno-lms

32. Опис системи дистанційного навчання Playgarden [Конфіденційно]

33. Усков А. В. Іванніков А. Д. Усков В. Л. Технології забезпечення інформаційної безпеки корпоративних освітніх мереж // Освітні технології і суспільство. - 2008. -Т.11, №1. - С. 472 - 479.

34. Оладько В.С., Микова С.Ю., Нестеренко М.А. Технологии защиты интернет-технологий и web-приложений [Електронний ресурс]. – Режим доступу: http://www.inter-nauka.com/issues/2015/8/476

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

36. Аткина В.С. Модель оценки защищенности организаций банковской системы Российской Федерации// Известия ЮФУ. Технические науки. – 2013. - №12 (149). - С. 184-193.

37. Пятков А.Г., Лубкин И.А. Оценка уровня защищенности компьютерных сетей при помощи метрик безопасности на основе общего графа//Актуальные проблемы авиации и космонавтики. Информационные технологии. – 2010. – Т.1., №6. – С. 396-397.

38. Дмитриева Е.Ю. Паниткин Д.В. К вопросу об оценке защищенности локальной вычислительной сети//Информация и Безопасность. - 2008. – Т11, №3. - С. 465 – 466.

39. Остапенко О.А., Нартов А.Н., Боев С.А. Непрерывное бетта-распределение плотности вероятностей ущерба систем при оценке их рисков и ущерба//Информация и Безопасность.-2006. –Т.9., №2. – С. 94-97.

40. Петриченко Г.С., Григорян Н.К., Медовщиков М.И. Методика разработки экспертной системы руководителя для принятия управленческих решений. Научнотехнические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2012. Т. 1. № 140. С. 60- 66.

41. Петриченко Г.С., Нарыжная Н.Ю., Гоголев В.Н. Моделирование управленческих ситуаций по защите информации с применением иерархической

системы неисправностей. Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2008. Т. 2. № 55. С. 103-107.

42. Петриченко Г.С. Анализ состояния вопросов эксплуатации корпоративных сетей на современном этапе. Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2014. № 100. С. 378-395

43. Петриченко Г.С., Дудник Л.Н., Срур М.Ю. Методика оценки финансового риска при проектировании и монтаже компьютерной сети предприятия. Научнотехнические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2011. Т. 2. № 120. С. 18- 25.

44. Кошкина Е.Н. SWOT- анализ дистанционного обучения в России // Вестник Международного института экономики и права. 2013. С.28-31.

45. Ямпольский С.М., Лисичкин В.А. Прогнозирование научно-технического прогресса, – М.:Экономика, 1974. – 207 с.

46. Семенов С.С. Оценка технического уровня систем наведения управляемого авиационного оружия класса «воздух-поверхность» // Вестник компьютерных и информационных технологий. – 2006. – №8 – С. 7-11.

47. Семенов С.С.Щербинин В.В. Метод оценки технического уровня систем наведения управляемых авиационных бомб / Материалы четвертой научно-практической конференции «Перспективные системы и задачи управления» и первой молодежной школы семинара «Управление и обработка информации в технических системах». Таганрог. ТФЮУ, 2009 г. – 291 с. – С. 160-167.

48. Семенов С.С.Щербинин В.В. Метод оценки технического уровня систем наведения управляемых авиационных бомб // Вопросы оборонной техники. Сер. 9. Специальные системы управления, следящие приводы и их элементы.. – М.: ФГУП «НТЦ «Информтехника», 2010. – Вып. 1 (242) – 2 (243). – 108 с. – С. 29-32.

49. Методика оцінки компетентності експертів [Електронний ресурс]. – Режим доступу: http://ej.kubagro.ru/2015/05/pdf/04.pdf

50. Підготовка інформації для автоматизованих навчальних систем / А.Я.Савельев, В.А.Новіков, Ю.І.Лобанов (під ред. А.Я.Савельева) // М .: Вища школа, 1986.- 175 с.

51. Гончаров М.М., Борисов В.В. Розробка моделі аналізу ризиків інформаційної безпеки комп'ютерних систем на основі нечіткої логіки [Електронний ресурс]. – Режим доступу: http://networkjournal.mpei.ac.ru/cgibin/main.pl?l=ru&n=18&pa=9&ar=1

52. Технічне завдання на ІТС [Конфіденційно]

ДОДАТКИ

ДОДАТОК А

(копії наукових публікацій)

ПІДХІД ДО ПОКРАЩЕННЯ СИСТЕМ ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ НА ПРИКЛАДІ ВЗАЄМОДІЇ ДЕРЖАВНИХ РЕЄСТРІВ

Хижняк Анна Олександрівна
Магістр кафедри кібербезпеки та захисту інформації
Оксіюк Олександр Глібович
Доктор технічних наук, професор, завідувач кафедри кібербезпеки та захисту інформації
vetrafiar@gmail.com

Анотація *– представлено аналіз загального функціонування інформаційних реєстрів та внесено пропозиції щодо покращення системи інформаційної взаємодії на прикладі взаємодії державних реєстрів.*

Ключові слова: *інформаційна система, взаємодія, інформаційні реєстри.*

1. ВСТУП / INTRODUCTION

Сучасне суспільство існує в умовах, коли інформація є необхідним інструментом для забезпечення суспільного ладу та правопорядку, наприклад, інформація про платників податків; власників зброї, транспортних засобів, нерухомості; наділених спеціальними повноваженнями осіб – нотаріусів, арбітражних керуючих тощо є необхідною для таких цілей. Вся потрібна інформація про таких осіб чи об’єктів міститься у спеціальних реєстрах, тобто вона систематизована та універсальна для зручності користування нею.

Для того, щоб системи інформаційної взаємодії безпечно функціонували, необхідно забезпечити повний захист інформації. В цій роботі наводяться пропозиції щодо покращення систем інформаційної взаємодії на прикладі взаємодії державних реєстрів.

2. ОСНОВНА ЧАСТИНА / MAIN PART

Створення інформаційних реєстрів вимагає неперервного системного аналізу національних інформаційних ресурсів, їх взаємозв’язків та захищеності. При цьому інформаційні реєстри слід розглядати як розподілену складну інформаційну систему, оскільки вона наділена усіма властивостями складних систем, а саме: великою кількістю складових компонентів, взаємодією з навколишнім середовищем, ієрархічною структурою та мінливістю у часі.

Загальними засадами створення та функціонування інформаційних реєстрів є: єдність методології створення, ведення, адміністрування, реєстрації та взаємодії реєстрів; обов'язковість та публічність реєстрації у реєстрах їх об’єктів та внесення даних (змін до них) про зареєстровані об’єкти; технологічна нейтральність та заборона преференцій для конкретних технологій; забезпечення доступу до відкритих даних; організація електронного інформаційного обміну між реєстрами за принципом «запит – відповідь» [1].

Розглянемо Реєстр територіальної громади міста Києва (далі – РТГК) [2], Державний реєстр виборців [3] та Міністерство Юстиції України [4].

За відкритими даними у м. Києві знаходиться не більш, ніж 10 реєстрів, які взаємодіють з РТГК. Вважатимемо, що взаємодія реєстрів повинна здійснюватися з використанням технологій інформаційних транзакцій, на кшталт банківських.

Це надає можливість для проведення аналізу системи захисту інформації у РТГК зробити допущення:

- розглядаємо систему інформаційної взаємодії реєстрів як АС класу 2, де сервером системи є інформаційна система РТГК, а зовнішні інформаційні системи – звичайними користувачами;
- при здійсненні обміну з метою недопущення стороннього втручання використовується криптографічний захист каналів зв’язку;
- висуваються високі вимоги щодо забезпечення цілісності та достовірності інформації при здійсненні інформаційного обміну.

На сьогодні спостерігається значна ступінь дублювання інформації в реєстрах. При порівнянні даних РТГК, Державного реєстру виборців та реєстрів Міністерства Юстиції України можна виявити достатню кількість схожих даних, а саме: прізвище, ім’я та по-батькові; дата народження; місце проживання; відомості про громадянство або його відсутність; унікальний номер запису в Єдиному державному демографічному реєстрі). Отже, можна зробити висновок, що близько 50% тотожних полів наявні в Державному реєстру

виборців, реєстру територіальної громади міста Києва та реєстрах Міністерства Юстиції України.

Тож, вважається за доцільне зробити висновки, що:

1. Велика кількість тотожних полів у реєстрах зумовлена тим, що досі нормативно не визначено перелік базових державних реєстрів, поля яких повинні виступати першоджерелами для використання в інших інформаційних ресурсах і забезпечення взаємодії між державними реєстрами.
2. Відсутність поняття базових державних реєстрів призводить до того, що поля з тотожною інформацією дублюються в різних реєстрах, а також мають рівнозначний пріоритет.
3. Питання щодо забезпечення взаємодії реєстрів в частині синхронізації даних між ними, з впровадженням протоколів взаємодії з використанням криптографічних механізмів, створює передумови для накопичення розбіжностей та, як результат, втрати актуальності даних.

Розглянемо принципи забезпечення безпеки при інформаційній взаємодії реєстрів на прикладі взаємодії РТГК з Державним реєстром виборців України.

Як було зазначено, при взаємодії інформаційних реєстрів існують значні перекриття даних реєстрів. Розглянемо питання щодо перекриття даних реєстрів більш уважно.

Реєстром-джерелом є Державний реєстр виборців України. РТГК утворено шляхом експорту даних. Верифікація даних Державного реєстру виборців виконується підрозділами Центральною виборчою комісією.

Водночас, РТГК використовується: працівниками Міністерства юстиції України, нотаріусами, при вчиненні нотаріальних дії. При цьому нотаріуси зобов’язані здійснювати перевірку оригіналів документів; працівниками органів призначення субсидій – для внесення даних про призначення субсидій тощо.

Підсумовуючі, існує можливість додаткової та незалежної верифікації даних, які отримані з Державного реєстру виборців, під час повсякденної роботи з реєстром територіальної громади міста Києва.

Розглянемо інформаційні потоки при взаємодії реєстрів.

З Державного реєстру виборців України:

1. Створення реєстру як експорт даних.

2. Отримання з Державного реєстру виборців оновлень даних для РТГК.

До Державного реєстру виборців України:

3.Отримання з РТГК даних про виявленні неточності в записах.

Тому система безпечної взаємодії між реєстрами повинна:

- підтримувати легку та уніфіковану розробку та впровадження взаємодій між інформаційними системами;
- гарантувати високий рівень безпеки шляхом використання електронно-цифрового підпису, шифрування даних, реєстрації подій, контролю доступу до електронних послуг та механізмів "відмови в обслуговуванні";
- забезпечувати стійкість до відмов;
- надавати доступ до даних різним установам відповідно до наданих їм прав доступу.

Система також має забезпечувати достовірність і цілісність інформації, а також чітке дотримання своїх обов'язків учасниками процесу обміну даними. Усі дані, що надсилаються через систему підписуються цифровим підписом та зашифровуються, автентифікуються та фіксуються, а вся інформація, що надходить у неї, проходить процедуру аутентифікації та реєструється [5].

Отже, система інформаційної взаємодії реєстрів повинна функціонувати як окрема захищена система. При цьому повинно забезпечуватись виконання наступних вимог:

- захищена взаємодія між інформаційними системами реєстрів державних органів України з використанням мережі Інтернет;
- забезпеченням безпеки взаємодії, неможливість стороннього втручання в проведення транзакцій при обміні інформацією між реєстрами;
- веденням захищеного аудиту інформаційної взаємодії реєстрів;
- побудова транзакцій при інформаційному обміні між реєстрами з використанням криптографічних протоколів строгої автентифікації, криптографічних протоколів інформаційного обміну з підтвердженням не лише отримання інформації, а й факту імплементації інформації до реєстру без пошкоджень та колізій;
- забезпечення надійного та безпечного захищеного накопичення та зберігання транзакцій інформаційної взаємодії державних реєстрів з метою забезпечення можливості незалежного та повного відтворення реєстру у аварійних випадках;
- забезпечення функціонування системи інформаційної взаємодії реєстрів за принципом «24*7*365».

Тож, побудова системи інформаційної взаємодії реєстрів не є простим завданням та потребує ретельного опрацювання питань взаємодіє реєстрів, які:

– побудовані з використанням різних баз даних;
– підтримують різні концепції забезпечення безпеки;
– мають різні рівні обслуговування та забезпечення безпеки.

3. ВИСНОВКИ / CONCLUSIONS

Наведений аналіз і внесені пропозиції спрямовано на покращення систем інформаційної взаємодії на прикладі взаємодії державних реєстрів.

4. ЛІТЕРАТУРА / REFERENCES

1. Реформа системи електронних публічних реєстрів [Електронний ресурс]. – Режим доступу: https://tsdea.archives.gov.ua/wp-content/uploads/2018/02/Draft-Law-22022018.pdf

2. Про затвердження Положення про інформаційну систему «Реєстр територіальної громади міста Києва» [Електронний ресурс]. – Режим доступу: http://kmr.ligazakon.ua/SITE2/l_docki2.nsf/alldocWWW/46766F58E7709751C22581BC0068743A?OpenDocument

3. Закон України «Про Державний реєстр виборців» [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/698-16

4. Про затрвердження Положення про Міністерство Юстиції України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/395/2011#n10

5. Петраков А.В. Основи практичного захисту інформації. - М .: Радіо та зв'язок, 1999. - 360 с.

THE APPROACH TO THE IMPROVEMENT OF INFORMATION INTERACTION SYSTEMS BASED ON THE EXAMPLE OF STATE REGISTERS INTERACTION

Khyzhniak Anna Alexandrovna
Master of the department of Cyber Security and Information Protection
Oksiiuk Oleksandr Glebovish
Doctor of technical science, professor, head of the department of Cyber Security and Information Protection
vetrafiar@gmail.com

Abstract — the analysis of the general functioning of information registers is presented. Proposals were made for the improvement of information interaction systems on the example based on the example of state registers interaction.

Key words: information system, interaction, information registers

Хижняк Анна
Київський національний університет імені Тараса Шевченка
vetrafiar@gmail.com

ОСНОВНІ КРИТЕРІЇ ГОТОВНОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ НЕПЕРЕРВНОСТІ РОБОТИ БІЗНЕСУ

Abstract: the main criteria for the readiness of information and communication technology for business continuity is presented. These criteria should be based on the requirements of information and communication technology readiness to ensure business continuity, as well as on common goals in terms of incident response and continuity requirements.

Key words: information and communication technology; business continuity.

Інформаційно-комунікаційні технології (ІКТ) з часом стали складовою частиною багатьох видів діяльності, які є елементами критичних інфраструктур у всіх секторах: державному, приватному чи громадському.

Для багатьох організацій готовність ІКТ є найважливішою складовою в реалізації менеджменту безперервності бізнесу і менеджменту інформаційної безпеки.

В результаті ефективність менеджменту безперервності бізнесу часто залежить від фактичної готовності ІКТ, що забезпечує впевненість у тому, що в період порушення продовжують виконуватися мети організації. Це особливо важливо у зв'язку з тим, що наслідки порушень ІКТ часто мають додаткові ускладнення, будучи прихованими і (або) важко виявляються.

Готовність ІКТ до забезпечення безперервності бізнесу ґрунтується на наступних ключових принципах:

– попередження інцидентів - захист послуг ІКТ від таких загроз, як несприятливий вплив зовнішнього середовища і апаратні збої, операційні помилки, зловмисні атаки і природні лиха, є вкрай важливим для підтримки бажаних рівнів доступності систем в організації;

- виявлення інцидентів - найшвидше виявлення інцидентів буде зводити до мінімуму їх вплив на послуги, скорочувати роботи по відновленню і зберігати якість послуг;
- реагування - реагування на інцидент найбільш підходящим способом призведе до більш ефективного відновлення і зменшить будь-які простої. Невдале реагування може привести до переростання незначного інциденту в щось більш серйозне;
- відновлення - визначення і реалізація відповідної стратегії відновлення забезпечуватиме впевненість у своєчасному відновленні послуг і підтримки цілісності даних. Розуміння пріоритетів відновлення дозволить відновлювати в першу чергу найкритичніші послуги. Послуги, що носять менш критичний характер, можуть відновлюватися пізніше або, за деяких умов, взагалі не відновлюватися;
- вдосконалення - уроки, засвоєні з реагування на дрібні і великі інциденти, повинні документуватися, аналізуватися і переглядатися. Розуміння цих уроків дасть можливість організації краще готуватися, контролювати і уникати інцидентів і порушень.

Рисунок 1 ілюструє, яким чином відповідний елемент готовності ІКТ до забезпечення безперервності бізнесу підтримує типову тимчасову послідовність відновлення ІКТ після лиха і, в свою чергу, підтримує діяльність щодо забезпечення безперервності бізнесу. Реалізація готовності ІКТ до забезпечення безперервності бізнесу дає можливість організації ефективно реагувати на нові і виникаючі загрози, а також реагувати на порушення і відновлюватися після них.

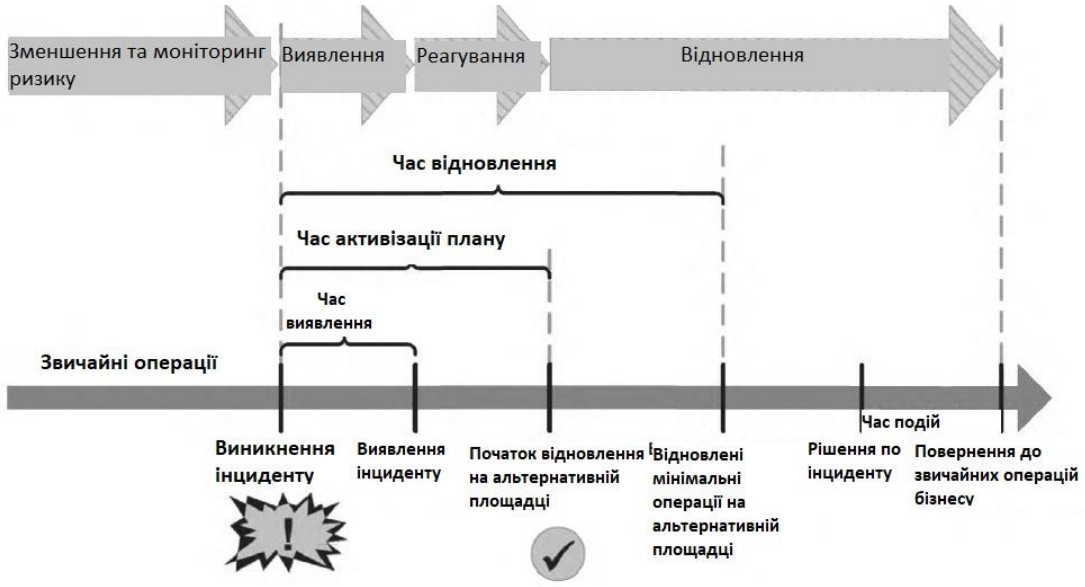

Рисунок 1

Ключові елементи готовності ІКТ до забезпечення безперервності бізнесу можна узагальнити наступним чином:

– кадри: фахівці, що володіють відповідними навичками та знаннями, і компетентний резервний персонал;
– споруди: фізичне середовище, в якому розташовані ресурси ІКТ;
– технічне оснащення:
  1. апаратні засоби (сервери, дискові масиви, накопичувачі на магнітній стрічці і прилади);
  2. мережі (включаючи послуги передачі даних і голосу), комутатори та маршрутизатори;
  3. програмні засоби, включаючи операційну систему і прикладні програми, зв'язок або інтерфейси між прикладними програмами і підпрограми пакетної обробки даних;
– дані: дані прикладних програм, голосові дані та інші види даних;
– процеси: відновлення і підтримки послуг ІКТ, включаючи підтримуючу документацію для опису конфігурації ресурсів ІКТ і створення можливості ефективного функціонування;

– постачальники: компоненти ланцюжка постачання послуг, де надання послуг ІКТ залежить від зовнішнього постачальника послуг або іншої організації, що беруть участь в ланцюжку поставок, наприклад, постачальник даних з фінансових ринків, постачальник телекомунікаційних послуг або постачальник Інтернет-послуг.

Готовність ІКТ до забезпечення безперервності бізнесу, ймовірно, буде більш ефективною і рентабельною, коли вона спроектована і вбудована в послуги ІКТ з самого початку, як частина стратегії готовності ІКТ до забезпечення безперервності бізнесу, що підтримує цілі забезпечення безперервності бізнесу організації. Це забезпечить впевненість в тому, що послуги ІКТ будуть краще створені, краще зрозумілі і більш стійкі. Зміна готовності ІКТ до забезпечення безперервності бізнесу може бути складною та дорогою задачею, що викликає порушення.

Організація повинна розробляти, реалізовувати, підтримувати і постійно удосконалювати сукупність документально оформлених процесів, які будуть підтримувати готовність ІКТ до забезпечення безперервності бізнесу.

Ці процеси повинні забезпечувати впевненість в тому, що цілі готовності ІКТ до забезпечення безперервності бізнесу чітко викладені, зрозумілі і доведені до відома, а також демонструвати зацікавленість вищого керівництва в готовності ІКТ до забезпечення безперервності бізнесу.

Рисунок 2 графічно показує види діяльності, що відбуваються на різних етапах забезпечення готовності ІКТ до забезпечення безперервності бізнесу. Готовність ІКТ до забезпечення безперервності бізнесу передбачає створення в організації процесів розробки і вдосконалення ключових елементів готовності ІКТ до забезпечення безперервності бізнесу, щоб підвищити їх здатність реагувати на порушення будь-якого виду, включаючи мінливі ситуації ризику, за допомогою використання підходу «Планування-Здійснення-Перевірка-Дія».

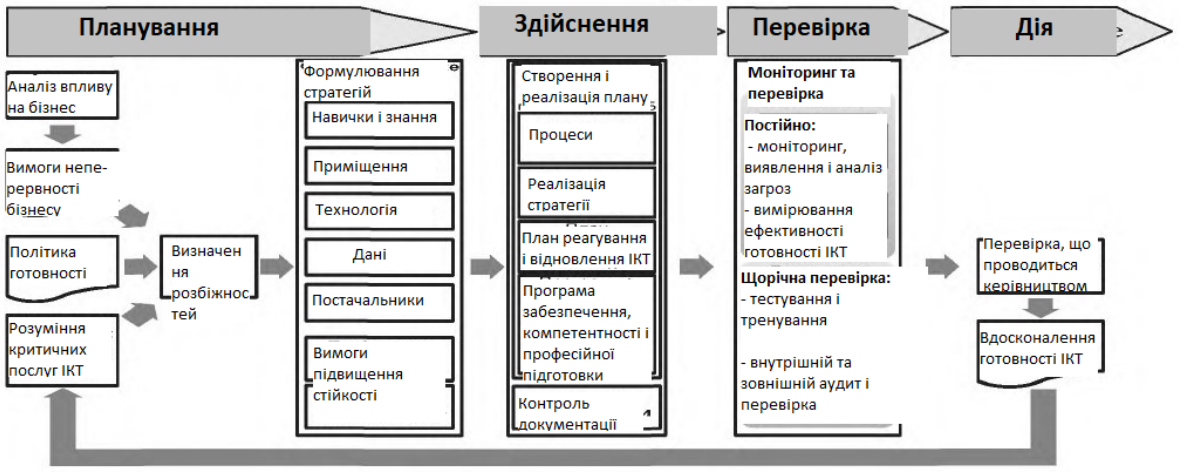

Рисунок 2

Оскільки ефективність готовності ІКТ до забезпечення безперервності бізнесу різниться в різних організаціях, кожна організація повинна розробити власні критерії ефективності готовності ІКТ до забезпечення безперервності бізнесу і підтримувати їх як частину процесу постійного вдосконалення.

Основний підхід полягає у використанні відомих сценаріїв інцидентів і взаємопов'язаних подій, щоб встановити базовий рівень реагування для кожної категорії інцидентів і пов'язаних з ними подій наступним чином:

- встановлення в рамках процесів СМІБ відомих інцидентів і індикаторів подій в якості вхідних даних для подальших етапів;
- встановлення сукупності відомих інцидентів (наприклад, атака злому пароля, відмова сервера через нестачу місця на жорсткому диску);
- визначення подій, що ведуть до цих інцидентів (наприклад, невдала спроба входу в систему, використання жорсткого диска);
- визначення відповідного часу виявлення (наприклад, граничне значення для подій, про які повинні бути повідомлені та попереджені система / адміністратор);

- визначення відповідного часу реагування (наприклад, період часу для прийняття адміністратором заходів з метою запобігання реалізації інциденту);
- розподіл подій по групах, виходячи з необхідного часу реагування та видів заходів реагування;
- уточнення матриць і значень за допомогою тестування сценаріїв і навчань / тренувань;
- проведення тестування для визначення того, чи є заходи реагування здійсненними, а цілі досяжними;
- уточнення груп очікуваного часу реагування на подію і очікуваних заходів реагування на події (наприклад, пошук альтернативного методу моніторингу, виявлення та дій);
- вдосконалення шляхом збору інформації про нові інциденти і сценаріях відмови і повторення процесу [1].

Таким чином, можна зробити висновки, що організація повинна визначити критерії для вимірювання ефективності готовності її ІКТ. Такі критерії можуть використовуватися для визначення бажаної якості реагування на порушення, як в термінах ефективності, так і в термінах результативності.

Критерії ефективності готовності ІКТ до забезпечення безперервності бізнесу повинні бути засновані на вимогах готовності ІКТ до забезпечення безперервності бізнесу, а також на спільних цілях з точки зору реагування на інциденти і вимог забезпечення безперервності.

ЛІТЕРАТУРА

1. ДСТУ ISO/IEC 27031:2015 Інформаційні технології. Методи захисту. Настанови щодо готовності інформаційно-комунікаційних технологій для неперервності роботи бізнесу. [Електронний ресурс]. – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=81330

ДОДАТОК Б

Технічне завдання на КСЗІ для ІС

Загрози конфіденційності інформації

Порушення конфіденційності інформації, що обробляється та зберігається в ІТС

Розглядаються наступні шляхи порушення конфіденційності інформації, що обробляється та зберігається в ІС:

К.1.1. Отримання несанкціонованого доступу сторонніх осіб до інформації, що обробляється та зберігається в ІС, внаслідок несанкціонованого фізичного доступу до обладнання.

Імовірність реалізації: середня

Втрати внаслідок реалізації: високі

Ефективний рівень: високий

К.1.2. Отримання несанкціонованого доступу сторонніх осіб до інформації, що обробляється та зберігається в ІС, під час її обробки внаслідок навмисного підключення до обладнання, помилок при настроюванні комутаційного обладнання або апаратних збоїв.

Імовірність реалізації: низька

Втрати внаслідок реалізації: високі

Ефективний рівень: середній

К.1.3. Отримання несанкціонованого доступу сторонніх осіб до інформації, що обробляється та зберігається в ІС, внаслідок навмисного підключення до каналів зв'язку чи обладнання з наступним використанням для несанкціонованого доступу відомих вразливостей програмно-технічних засобів системи.

Імовірність реалізації: низька

Втрати внаслідок реалізації: високі

Ефективний рівень: середній

К.1.4. Отримання несанкціонованого доступу сторонніх осіб до інформації, що обробляється та зберігається в ІС, внаслідок навмисного підключення до каналів зв'язку чи обладнання з наступним використанням для несанкціонованого доступу (далі – НСД) перехоплених атрибутів доступу авторизованих користувачів.

Імовірність реалізації: низька

Втрати внаслідок реалізації: високі

Ефективний рівень: середній

К.1.5. Отримання несанкціонованого доступу сторонніх осіб до інформації, що обробляється та зберігається в ІС, внаслідок фізичного доступу до носіїв інформації (змінних носіїв, носіїв, що вийшли з ладу, носіїв, що підлягають утилізації).

Імовірність реалізації: середня

Втрати внаслідок реалізації: високі

Ефективний рівень: високий

Порушення конфіденційності технологічної інформації

К.2.1 Порушення конфіденційності технологічної інформації (атрибутів доступу користувачів) сторонніми особами внаслідок необережного поводження авторизованих користувачів з атрибутами доступу (розглядається як частина реалізації атак **К.1.1**, **К.1.4**, спрямованих на порушення конфіденційності інформації).

Імовірність реалізації: середня

Втрати внаслідок реалізації: середні

Ефективний рівень: середній

К.2.2. Порушення конфіденційності технологічної інформації (атрибутів доступу користувачів) з боку авторизованих користувачів системи внаслідок необережного поводження з ними (як мета такого порушення розглядається ескалація прав доступу до ресурсів ІС та виконання несанкціонованих дій від імені іншого користувача, розглядається як частина атак **Ц.1.3**, **Ц.2.1**, **Ц.2.2**, спрямованих на порушення цілісності інформації).

Імовірність реалізації: висока

Втрати внаслідок реалізації: середні

Ефективний рівень: високий

К.2.3. Порушення конфіденційності технологічної інформації (атрибутів доступу користувачів системи) з боку авторизованих користувачів системи з застосуванням відомих вразливостей програмно-технічних засобів ІС (розглядається як частина атак **Ц.1.3**, **Ц.2.1**, **Ц.2.2**, спрямованих на порушення цілісності інформації).

Імовірність реалізації: висока

Втрати внаслідок реалізації: середні

Ефективний рівень: високий

К.2.4. Отримання несанкціонованого доступу сторонніх осіб до технологічної інформації (атрибути доступу, конфігураційні настроювання), що зберігається та обробляється в ІС, внаслідок фізичного доступу до носіїв інформації (змінних носіїв, носіїв, що вийшли з ладу, носіїв, що підлягають утилізації).

Імовірність реалізації: середня

Втрати внаслідок реалізації: низькі

Ефективний рівень: середній

Загрози цілісності інформації

Загрози цілісності інформації, що обробляється та зберігається в ІТС

Ц.1.1. Порушення цілісності інформації, що обробляється та зберігається в ІС, внаслідок апаратного або програмного збою.

Імовірність реалізації: середня

Втрати внаслідок реалізації: дуже високі

Ефективний рівень: високий

Ц.1.2. Порушення цілісності інформації, що обробляється та зберігається в ІС, сторонніми особами внаслідок отримання фізичного доступу до обладнання (навмисне чи внаслідок необережного поводження з обладнанням або системами, що забезпечують його функціонування).

Імовірність реалізації: низька

Втрати внаслідок реалізації: високі

Ефективний рівень: середній

Ц.1.3. Порушення цілісності інформації, що обробляється та зберігається в ІС, внаслідок навмисних дій авторизованого користувача будь-якого рівня в межах його повноважень.

Імовірність реалізації: середня

Втрати внаслідок реалізації: дуже високий

Ефективний рівень: високий

Ц.1.4. Порушення цілісності інформації, що обробляється та зберігається в ІС, внаслідок ненавмисних (помилкових) дій авторизованого користувача будь-якого рівня.

Імовірність реалізації: середня

Втрати внаслідок реалізації: середні

Ефективний рівень: середній

Ц.1.5. Порушення цілісності інформації, що обробляється та зберігається в ІС, внаслідок ураження комп'ютерним вірусом.

Імовірність реалізації: низька

Втрати внаслідок реалізації: середні

Ефективний рівень: середній

Загрози цілісності технологічної інформації

Ц.2.1. Порушення цілісності технологічної інформації (журнали реєстрації подій) сторонніми особами або авторизованими користувачами з застосуванням відомих вразливостей програмно-технічних засобів ІС або перехоплених атрибутів доступу співробітників з адміністративними правами (як мета реалізації даної загрози розглядається приховування несанкціонованих дій в системі в рамках реалізації інших загроз, спрямованих на порушення цілісності або конфіденційності інформації).

Імовірність реалізації: низька

Втрати внаслідок реалізації: високі

Ефективний рівень: середній

Ц.2.2. Порушення цілісності технологічної інформації (конфігураційні файли, виконувані файли програмного забезпечення) сторонніми особами або авторизованими користувачами з застосуванням відомих вразливостей програмно-технічних засобів ІС або перехоплених атрибутів доступу співробітників з адміністративними правами (як мета реалізації даної загрози розглядається створення умов для подальшого несанкціонованого доступу до інших компонент системи в рамках реалізації загроз **К.1.1** – **К.1.4**, **Ц.1.3** (для авторизованих користувачів)).

Імовірність реалізації: низька

Втрати внаслідок реалізації: середні

Ефективний рівень: середній

Ц.2.3. Порушення цілісності технологічної інформації (конфігураційні файли, виконувані файли програмного забезпечення) внаслідок ураження системи комп'ютерним вірусом.

Імовірність реалізації: низька

Втрати внаслідок реалізації: середні

Ефективний рівень: середній

Загрози доступності інформації

Загрози доступності інформації, що зберігається в ІТС

Д.1.1. Втрата доступності інформації, що зберігається в ІС, внаслідок виходу з ладу комутаційного або серверного обладнання, або елементів, що забезпечують їх роботу (найбільш імовірним вважається вихід з ладу системи електроживлення).

Імовірність реалізації: висока

Втрати внаслідок реалізації: низькі

Ефективний рівень: середній

Д.1.2. Втрата доступності інформації, що зберігається в ІС, внаслідок ураження системи комп'ютерним вірусом (перевантаження каналів зв'язку віддалених користувачів інтенсивним трафіком, що генерується вірусами типу "хробак" при розповсюдженні, вичерпання дискового простору або процесорного часу на уражених деякими типами вірусів серверах, що призводить до неможливості обробки запитів та виникнення відмов в обслуговуванні).

Імовірність реалізації: середня

Втрати внаслідок реалізації: низькі

Ефективний рівень: середній

Вимоги до КСЗІ

Керування доступом користувачів до інформації

В ІС повинен бути реалізований адміністративний принцип керування доступом.

Потоки інформації всередині ІС встановлюються відповідними адміністраторами і не можуть бути змінені іншими користувачами. В ІС повинні бути виділені посади зазначених адміністраторів, повноваження та обов'язки яких зафіксовані в посадових інструкціях.

Підходи щодо адміністрування комплекс засобів захисту (КЗЗ)

Управління засобами захисту, що використовуються в ІС, а також моніторинг їх стану здійснюється з використанням локального або віддаленого доступу до відповідного обладнання.

Вимоги щодо взаємодії з глобальними мережами та мережевого захисту

Засоби мережевого захисту ІС повинні забезпечувати виконання наступних функцій:

– здійснення фільтрації мережевого трафіку за протоколами, портами і IP-адресами згідно з визначеною політикою безпеки;

– розмежування мережевого доступу між ІС та мережею Інтернет;

– інспекція мережевого трафіку та блокування пакетів або сесій, що є підозрілими;

– забезпечення проходження між ІС та Інтернет лише дозволених інформаційних потоків згідно визначених протоколів;

– виявлення та протидію мережевим атакам;

– забезпечення завершення з'єднання з вузлом, у разі атаки;

– реєстрація подій, що мають відношення до безпеки.

Основні атрибути доступу користувачів, процесів і об'єктів

Основними атрибутами доступу користувачів, що використовуються для проведення ідентифікації, автентифікації та авторизації засобами комплексу засобів захисту інформації від несанкціонованого доступу ІС, в загальному випадку є:

– умовне ім'я в ІС (логін);

– пароль.

Атрибутами мережевих об'єктів, що використовуються для розмежування доступу, є:

– IP-адреса мережі, до якої належить об'єкт;

– мережеве ім'я.

Атрибутами інформаційних об'єктів, що використовуються для розмежування доступу, є:

- в файлових системах: ім'я, розширення, атрибути доступу (читання, модифікація, знищення);

- для об'єктів баз даних: ім'я об'єкта, атрибути доступу (читання, модифікація, знищення);

- при передачі інформаційних об'єктів засобами обчислювальної мережі додатковими атрибутами, за якими виконують розмежування доступу мережеві засоби захисту, є: IP-адреса відправника IP-пакету, IP-адреса отримувача IP-пакету, TCP/UDP-порт прикладного процесу-відправника, TCP/UDP-порт прикладного процесу-отримувача, номер пакету у послідовності (тільки для TCP), значення,

визначені в службових полях заголовків різних рівнів (TTL, прапори та ін.), команда протоколу прикладного рівня.

Атрибутами процесів є:

- назва виконуваного програмного модуля;
- ідентифікатор процесу в ОС.

Для процесів, що призначені для мережевої взаємодії, додатковими атрибутами, за якими виконують розмежування доступу мережеві засоби захисту, є:

- тип протоколу транспортного рівня, що використовується процесом;
- TCP/UDP–порт (діапазон портів) призначення;
- TCP/UDP–порт (діапазон портів) відправника;
- тип протоколу прикладного рівня, що використовується процесом.

Вимоги до реєстрації дій користувачів по відношенню до інформації, яка обробляється та зберігається в ІТС

КЗЗ повинен дозволяти однозначно ідентифікувати користувача, що сформував запит на будь-яку транзакцію, пов’язану зі зміною інформації, яка зберігається в базі даних (створення, модифікація, знищення), та відстежити історію таких транзакцій.

Вимоги до реєстрації дій користувачів по відношенню до технологічної інформації.

КЗЗ повинен забезпечувати реєстрацію наступних дій користувачів по відношенню до технологічної інформації:

1. Отримання авторизованими користувачами доступу до ІС (вхід/вихід).
2. Невдалі спроби отримання доступу до ІС внаслідок непроходження користувачем автентифікації.
3. Зміни конфігураційних налаштувань компонент ІС.
4. Отримання авторизованими користувачами доступу до об’єктів захисту ІС.

Загальні вимоги до КСЗІ

Для забезпечення захисту від загроз, компоненти КСЗІ повинні реалізовувати наступні основні функції захисту.

1) Забезпечення стійкості ІС в цілому до відмов та унеможливлення втрати інформації, що повинно забезпечуватися шляхом резервування елементів системи збереження даних, засобів комутації та електроживлення. Також повинно забезпечуватися періодичне резервне копіювання баз даних ІС. Необхідна періодичність резервного копіювання визначається на етапі техноробочого проекту та відображається у відповідних інструкціях обслуговуючому персоналу.

2) Розмежування доступу користувачів ІС до інформації, що обробляється та зберігається в ІС, відповідно до їх повноважень згідно технологічного процесу обробки інформації.

3) Забезпечення однозначної ідентифікації користувачів ІС.

4) Забезпечення можливості відстежити історію запитів, спрямованих на внесення змін до інформації, що зберігається в базах даних ІС, та однозначної ідентифікації користувачів ІС, що виконували такі зміни (внесення, модифікація, видалення).

5) Забезпечення захисту від несанкціонованого доступу до інформації при її обробці засобами ІС організаційними заходами.

6) Забезпечення на мережевому рівні проходження тільки дозволених інформаційних потоків з боку телекомунікаційних мереж до ІС, а також в зворотному напрямку.

7) Забезпечення реєстрації подій, пов’язаних з отриманням користувачами доступу до ресурсів ІС (проходження/непроходження автентифікації), дій адміністраторів щодо зміни настроювань серверів та комутаційного обладнання.

8) Наявність засобів перегляду та аналізу подій.

9) Наявність засобів для резервування конфігураційних файлів та критично важливих для функціонування обладнання ІС системних файлів (створення образів дисків, резервування операційних систем серверів та комутаційного обладнання) з метою їх наступного швидкого відновлення в разі збоїв.

10) Забезпечення цілісності інформації, що передається каналами зв’язку між компонентами ІС через незахищене середовище.

11) Забезпечення антивірусного захисту в такому обсязі:

- на всіх електронних обчислювальних машинах (ЕОМ), включених до ІС, повинні бути встановлені засоби антивірусного захисту, що повинні регулярно оновлюватися; оновлення повинно здійснюватися в автоматичному або ручному режимі централізовано;

- в ІС повинно використовуватися програмне забезпечення тільки згідно специфікації, визначеної на етапі техноробочого проекту;

- інсталяція програмного забезпечення на ЕОМ, включених до ІС, або відновлення (відкат) системних та конфігураційних файлів з резервних копій повинна здійснюватися тільки з контрольних носіїв у встановленому порядку.

12) Організація захисту інформації в ІС має визначатися Планом захисту інформації, який оформлюється та затверджується встановленим порядком.

Вимоги до фізичного середовища

Вхід до приміщень, в яких розміщуються компоненти ІС, повинен бути обмежений.

Серверне обладнання ІС повинно розташовуватись в окремих виділених приміщеннях з метою мінімізації доступу до цих приміщень осіб, що не мають відношення до обслуговування та експлуатації такого обладнання.

Доступ до виділених приміщень повинен бути дозволений тільки адміністраторам. При необхідності доступу до апаратного приміщення відвідувачів, останні повинні знаходитися в приміщеннях тільки у супроводженні співробітника з числа цих адміністраторів та за умови реєстрації таких відвідувань у відповідних журналах доступу до таких приміщень з обов’язковим вказанням проміжку часу перебування у приміщенні, інформації про особу, що перебувала у приміщенні, описом робіт, які проводила така особа.

Приміщення, в яких розташовані компоненти ІС, повинні бути обладнані системами вентиляції. Повинно здійснюватися постійне зовнішнє спостереження за приміщеннями з метою раннього виявлення ознак, що можуть призвести до несанкціонованого доступу.

Розміщення компонентів ІС має виконуватися, виходячи з:

- унеможливлення ознайомлення сторонніми особами з інформацією, що відображається на моніторах;

- технічних характеристик обладнання і вимог щодо його встановлення та умов експлуатації, визначених їх виробником.

Вимоги до організаційного забезпечення

Експлуатація ІС, що входять до складу ІС, повинна здійснюватися лише за умови наявності затвердженого встановленим порядком Плану захисту інформації.

Дії користувачів повинні визначатися відповідними настановами (інструкціями).

Повинен бути розроблений порядок дій користувачів категорії 1 у разі відмови КСЗІ (окремого її компоненту) ІС, та затверджені відповідні настанови кожного користувача.

Повинні бути розроблені нормативні та розпорядчі документи, що визначають правила режиму доступу у приміщення, в яких розміщені компоненти ІС, та порядок доступу відвідувачів до цих компонентів.

Вимоги до системи електроживлення

Для забезпечення працездатності технічних засобів ІС вони повинні бути обладнані джерелами безперебійного живлення. Потужність джерел безперебійного живлення має бути достатньою для коректного завершення роботи компонентів ІС.

Вимоги до антивірусного захисту

ІС повинна мати у своєму складі систему антивірусного захисту (далі – САЗ), яка має забезпечувати захист програмного забезпечення від комп'ютерних вірусів, шкідливого програмного забезпечення та зловмисних мобільних програм, у

фоновому режимі або за запитом адміністратора серверів.

Програмне забезпечення САЗ повинно вибиратись зважаючи на такі чинники:

- максимальне зменшення можливих помилок при обробці зашифрованих даних, зважаючи на можливу тотожність з сигнатурами вірусів;

- наявність сертифікатів відповідності (експертних висновків), отриманих для САЗ за відповідними результатами сертифікації (державної експертизи в сфері технічного захисту інформації).

Система антивірусного захисту ІС повинна відповідати наступним вимогам:

- керування САЗ має здійснюватися централізовано адміністратором серверів;

- контроль стану програмного забезпечення, з точки зору можливості його зараження вірусами, технічних засобів центрального вузла ІС має здійснюватися також централізовано адміністратором серверів;

- поновлення антивірусної бази даних повинно здійснюватися централізовано, за участю спеціально уповноваженої на це особи.

КЗЗ, який здійснює розмежування прав доступу, має забезпечити захист від несанкціонованого доступу до програмного забезпечення САЗ, включаючи його інформаційну базу, для всіх посадових осіб, крім адміністратора серверів.

Для створення системи криптографічного захисту та забезпечення корпоративної інформаційної безпеки в ІС повинні виконуватись наступні вимоги:

- *засоби криптографічного захисту інформації* повинні реалізувати наступні криптографічні алгоритми

- алгоритм шифрування даних відповідно до ДСТУ ГОСТ 28147:2009 режимі гамування із зворотнім зв’язком;

- алгоритм шифрування даних з контролем цілісності відповідно до ДСТУ ГОСТ 28147:2009 у режимі імітовставки для розподілу ключових даних;

- алгоритм гешування інформації відповідно до ГОСТ 34.311-95;

- алгоритм обчислення та перевірки електронного цифрового підпису, використання еліптичних кривих, генерація псевдовипадкових послідовностей,

генерація ключових даних, перевірка правильності генерації ключових даних, а також обчислювальні процедури в поліноміальному базисі відповідно до ДСТУ 4145-2002.

- *шлюз захисту* повинен забезпечувати:

- пакетну фільтрацію трафіку з використанням інформації в полях заголовків мережевого і транспортного рівнів;
- реалізацію заданого протоколу взаємодії (автентифікація та / або захист трафіку) для кожного захищеного з'єднання, доступ в заданому захищеному режимі тільки для зареєстрованих партнерів по взаємодії;

- *система керування* VPN Manager повинна забезпечувати

- моніторинг та оперативне керування криптграфічно захищеною корпоративною мережею VPN;
- збір інформації про стан та роботоспроможність елементів системи криптографічного захисту VPN-мережі;
- відображення стану елементів мережі та історії змін параметрів;
- аналіз стану мережі та забезпечення підтримки прийняття рішень про зміну конфігурації мережі к випадках різних ситуацій;
- протоколювання подій в мережі.