ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙІНСТИТУТ МЕНЕДЖМЕНТУ ТА ПІДПРИЄМНИЦТВА
КАФЕДРА ДОКУМЕНТОЗНАВСТВА ТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

КВАЛІФІКАЦІЙНАРОБОТА

на тему: «Можливості інформаційних технологій в системі управління безпеки е-документообігу на підприємстві»

на здобуття освітнього ступеня магістра
зі спеціальності 029 Інформаційна, бібліотечна та архівна справа
освітньо-професійної програми Управління інформаційно-комунікаційною діяльністю

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Андрій КАРНАСЮК

Виконав: здобувач вищої освіти
гр. ДЗДМ-61
Андрій КАРНАСЮК

Керівник:
к. філол. наук, доцент Алла ОВСІЄНКО

Рецензент:
доктор філософії, доцент Оксана ПЛУЖНИК

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут менеджменту та підприємництва

Кафедра документознавства та інформаційної діяльності
Ступінь вищої освіти магістр
Спеціальність 029 Інформаційна, бібліотечна та архівна справа
Освітньо-професійна програма Управління інформаційно-комунікаційною діяльністю

ЗАТВЕРДЖУЮ
Завідувач кафедри документознавства
та інформаційної діяльності
_____ Тетяна СИДОРЕНКО
«___»_____20__р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Карнасюка Андрія В'ячеславовича

1. **Тема кваліфікаційної роботи:** «Можливості інформаційних технологій в системі управління безпеки е-документообігу на підприємстві».
керівник кваліфікаційної роботи Алла ОВСІЄНКО к.філол.н.
затверджені наказом Державного університету інформаційно-комунікаційних технологій №320 від 15.10.2024
2. **Строк подання кваліфікаційної роботи** «15» грудня 2024р.
3. **Вихідні дані до кваліфікаційної роботи:**
Мета дослідження: комплексне дослідження та аналіз сучасних інформаційних технологій, їх можливостей і методів для забезпечення надійного захисту електронного документообігу на підприємстві.
Об'єкт дослідження: система управління безпекою електронного документообігу на підприємстві.
Предмет дослідження: можливості інформаційних технологій та методи їх застосування для забезпечення безпеки електронного документообігу на підприємстві.
4. **Перелік питань, які потрібно розробити:**
1. Теоретичні основи безпеки е-документообігу
2. Можливості інформаційних технологій в забезпеченні безпеки е-документообігу
3. Практичне впровадження інформаційних технологій для безпеки е-документообігу на підприємстві
5. **Перелік ілюстративного матеріалу:** презентація
6. **Дата видачі завдання** «07» вересня 2024 р.

КАЛЕНДАРНИЙПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Визначення тематики, вибір наукового керівника, уточнення теми	09.09.2024	*виконано*
2	Розроблення та складання плану кваліфікаційної магістерської роботи	17.09.2024	*виконано*
3	Підготовка 1 розділу	08.10.2024	*виконано*
4	Підготовка 2 розділу	29.10.2024	*виконано*
5	Підготовка 3 розділу	22.11.2024	*виконано*
6	Висновки	29.11.2024	*виконано*
7	Підготовка остаточного варіанта роботи	12.12.2024	*виконано*
8	Написання відгуку науковим керівником	13.12.2024	*виконано*
9	Оформлення та представлення роботи на кафедру та перевірка на плагіат	16.12.2024	*виконано*
10	Підготовка доповіді, презентації та ілюстративного матеріалу, рецензія	18.12.2024	*виконано*
11	Попередній захист роботи	20.12.2024	*виконано*
12	Основний захист кваліфікаційної магістерської роботи	22.01.2025	*виконано*

Здобувач вищої освіти _____ Андрій КАРНАСЮК

Керівник кваліфікаційної роботи _____ Алла ОВСІЄНКО

ЗМІСТ

ВСТУП

Актуальність дослідження. У сучасних умовах стрімкого розвитку інформаційних технологій електронний документообіг (ЕДО) стає важливою складовою ефективного функціонування підприємств. Збільшення обсягів інформації, що обробляється, вимагає швидкості, точності та доступності даних, які забезпечуються впровадженням ЕДО. Однак разом із зростанням використання цифрових рішень зростають і загрози, пов'язані з безпекою інформації.

Захист електронного документообігу є критичним аспектом у забезпеченні конфіденційності, цілісності та доступності даних. Небезпека витоків інформації, кіберзагрози, спроби несанкціонованого доступу ставлять перед підприємствами нові виклики, які потребують застосування сучасних технологій безпеки.

Таким чином, дослідження можливостей інформаційних технологій у системі управління безпекою електронного документообігу є надзвичайно актуальним для підвищення стійкості підприємств до сучасних викликів, забезпечення відповідності нормативним вимогам і покращення управління бізнес-процесами.

Стан наукової розробки проблеми.

Наукова розробка проблеми використання інформаційних технологій у забезпеченні безпеки електронного документообігу на підприємствах перебуває у фазі активного розвитку, зумовленого зростанням обсягів даних, цифровізацією бізнес-процесів та необхідністю захисту інформації від зовнішніх і внутрішніх загроз.

Серед видатних дослідників, які присвячують свої наукові та практичні зусилля аналізу цієї проблематики, варто відзначити праці Мазниченко Н. І. досліджував захист інформації в системах електронного документообігу, акцентуючи на системах ідентифікації [30]. Майстренко А. А. зосередилася на нормативно-правовому забезпеченні електронного документообігу в

Україні, проводячи інформаційно-аналітичний огляд [31]. Мізіна О.,

Вощенко В., Вдовіна О. аналізували законодавче регулювання електронного документообігу в Україні [32]. Писаренко В. П. досліджував міжнародний досвід та зарубіжне законодавство в сфері регулювання електронного документообігу, розглядаючи можливості його впровадження в електронній комерції [39].

Каланча І. займалася вивченням міжнародного досвіду використання електронного сегмента в кримінальній процесуальній діяльності суду [22]. Ковбасюк Ю.В. в своїй роботі розглядав аспекти державного управління, зокрема електронний документообіг та захист інформації [24]. Королюк Т. зосереджувалася на аспектах діджиталізації документообігу, включаючи законодавчі аспекти, переваги, недоліки та ефективність впровадження [27].

Радченко С. В. та Лиско Н. А. у своїх публікаціях описали особливості роботи різних систем документообігу, а саме «Megapolis», «OPTIMA-WorkFlow», «ДокПроф» та інші. Автори вважають, що розвиток електронного урядування – це складний процес, що потребує значних матеріальних, інтелектуальних і фінансових ресурсів та вимагає вирішення комплексу правових, організаційних і технічних проблем [44].

Ця активність дослідження відображає важливість проблеми та прагнення науковців з’ясувати перспективи розвитку та вдосконалення системи електронного документообігу в Україні. Враховуючи накопичений науковий досвід, можна зробити висновок про актуальність та важливість подальших наукових досліджень у цій сфері з метою оптимізації управлінських процесів та підвищення рівня ефективності використання електронного документообігу в Україні.

Стан вивчення теми. Серед сучасних досліджень можна виділити роботи, присвячені аналізу конкретних випадків впровадження систем управління безпекою е-документообігу на підприємствах. Такі дослідження надають цінну інформацію про практичний досвід підприємств у впровадженні засобів захисту, а також про ефективність різних методів та технологій.

Метою кваліфікаційної роботи є комплексне дослідження та аналіз сучасних інформаційних технологій, їх можливостей і методів для забезпечення надійного захисту електронного документообігу на підприємстві.

Завдання кваліфікаційної роботи:

– вивчити теоретичні основи електронного документообігу на підприємстві, його значення для підвищення ефективності бізнес-процесів та основні вимоги до безпеки;

– дослідити ключові загрози та ризики, пов’язані з електронним документообігом, включаючи кіберзлочини, витік даних та зловмисне втручання;

– описати принципи та методології забезпечення безпеки електронного документообігу, враховуючи сучасні підходи до управління інформаційною безпекою;

– розглянути можливості застосування сучасних інформаційних технологій для забезпечення захисту е-документообігу, таких як шифрування, цифрові підписи, аутентифікація та авторизація;

– проаналізувати функціонування систем моніторингу та виявлення загроз (IDS/IPS) як складової безпеки інформаційних систем підприємства;

– дослідити переваги та ризики використання хмарних технологій у системах е-документообігу з точки зору безпеки;

– проаналізувати стан безпеки системи електронного документообігу на підприємстві, включаючи виявлення слабких місць і загроз;

– розробити практичні рекомендації для вдосконалення системи управління безпекою електронного документообігу, враховуючи використання сучасних ІТ-рішень;

– запропонувати заходи впровадження інформаційних технологій на підприємстві для підвищення рівня безпеки е-документообігу, зокрема шляхом інтеграції інноваційних методів захисту.

Об'єкт дослідження: система управління безпекою електронного документообігу на підприємстві.

Предмет дослідження: можливості інформаційних технологій та методи їх застосування для забезпечення безпеки електронного документообігу на підприємстві.

Методи дослідження. Для досягнення мети дослідження та вирішення поставлених завдань у кваліфікаційній роботі застосовуються наступні методи дослідження. Аналіз наукових джерел та літератури з тематики інформаційної безпеки та е-документообігу. Синтез отриманих даних для визначення основних проблем та розробки рекомендацій щодо вдосконалення системи безпеки. Вивчення елементів системи управління безпекою е-документообігу та їх взаємозв'язків. Розробка комплексного підходу до забезпечення безпеки з урахуванням технічних, організаційних та правових аспектів. Аналіз переваг та недоліків існуючих методів і засобів забезпечення безпеки е-документообігу. Дослідження реальних випадків впровадження інформаційних технологій для забезпечення безпеки е-документообігу на підприємствах. Аналіз успішних практик та вивчення досвіду підприємств.

Застосування цих методів дослідження дозволяє провести всебічний аналіз можливостей інформаційних технологій у системі управління безпекою е-документообігу на підприємстві та розробити ефективні заходи для підвищення рівня захищеності інформаційних систем.

Наукова новизна та практична значущість отриманих результатів дослідження дозволить у загальному підході до вирішення проблем безпеки е-документообігу на підприємствах з використанням сучасних інформаційних технологій, що дозволяє значно підвищити рівень захищеності інформаційних систем та забезпечити ефективне управління безпекою в умовах.

Джерельна база дослідження складається з наукових та практичних матеріалів, які висвітлюють різні аспекти інформаційних технологій та їх застосування для забезпечення безпеки електронного документообігу на підприємствах. Основними джерелами інформації є: монографіїта книги; наукові статті та журнали; конференційні матеріали, законодавчі та нормативні акти; Інтернет-ресурси; дисертації та дипломні роботи.

Ці джерела забезпечують комплексний підхід до вивчення можливостей інформаційних технологій у системі управління безпекою е-документообігу на підприємствах, дозволяючи провести всебічний аналіз та розробити ефективні рекомендації для практичного впровадження.

Апробація результатів дослідження. Аналіз окремих аспектів досліджуваної теми був викладений у науковій публікації «Основні аспекти безпеки електронного документообігу» на ІІ всеукраїнській науково-практичній Інтернет-конференції «Соціальні комунікації в умовах глобалізації суспільства: виклики та перспективи», яка відбулась у Державному університету інформаційно-комунікаційних технологій, 07 листопада 2024 р.

Структура кваліфікаційної магістерської роботи. Робота складається зі вступу, трьох розділів, 9 підрозділів, переліку посилань.

РОЗДІЛ 1: ТЕОРЕТИЧНІ ОСНОВИ БЕЗПЕКИ Е-ДОКУМЕНТООБІГУ

1.1. Поняття і значення е-документообігу на підприємстві

Документообіг – це рух документів в компанії від їхнього створення (чи отримання від контрагента) до передачі в архів.

Електронний документообіг – це, відповідно, такий же процес, тільки з документами в електронному вигляді.

Кожна установа має свої процеси роботи з документами, але зазвичай, до них належить створення чи одержання документа, обробка та редагування, узгодження й підписання, надсилання контрагенту чи передача на виконання, архівування. Залежно від виду документа, компанії, налаштованих процесів ці етапи можуть доповнюватись та відрізнятись. Всі процеси, які відбуваються з паперовими документами, можуть бути і в електронному форматі, завдяки чому оптимізуються, стають швидшими та дешевшими [4].

Електронний документообіг у компаніях зазвичай реалізується через спеціальну систему – для корпоративного документообігу, як, наприклад, Megapolis.DocNet, або ж для зовнішнього документообігу, як Deals чи Вчасно. Іноді невеликі компанії обмінюються електронними документами через звичайну електронну пошту чи навіть месенджери, але такий спосіб незахищений та ненадійний [11].

Системи електронного документообігу ж дозволяють бути впевненими в захисті документів, відслідковувати всі дії, які з ними відбувались (бачити, хто, коли і що саме робив з документом), підписувати документи за допомогою КЕП, УЕП чи хмарних підписів, а також забезпечують повноцінну організацію роботи з документами.

Про види систем документообігу та їхні функції ми розповімо трохи нижче, а поки поговоримо про те, яким може бути електронний документообіг.

Документообіг буває внутрішній та зовнішній. Внутрішній документообіг (його ще іноді називають корпоративним) – це рух документів всередині компанії, тобто обмін документами між різними підрозділами та співробітниками однієї організації.

В межах однієї компанії відбувається створення, узгодження та підписання великої кількості документів – наказів, службових записок, заяв, інструкцій, статутів і багато іншого. Все це можна вести в електронному вигляді та автоматизувати. ЕДО дозволяє не лише перевести документи в електронний формат, а налаштувати процеси та організувати роботу з документами максимально зручно і швидко [45].

Внутрішній електронний документообіг дозволяє значно оперативніше створювати, узгоджувати та шукати документи, мати історію всіх файлів, організувати легкий доступ відповідальних співробітників до документів, контролювати, де знаходяться документи та на якому етапі виконання завдань із ними тощо.

Зовнішній документообіг – це рух документів за межами компанії, тобто обмін документами із контрагентами, клієнтами, партнерами, державними органами та іншими зовнішніми організаціями.

Зазавичай зовнішній документообіг передбачає погодження рахунків, актів виконаних робіт, звітів, накладних тощо. Електронний зовнішній документообіг дозволяє миттєво передавати документи контрагентам, не витрачаючи часу й коштів на друк та пересилку [21]. А також ЕДО підвищує захист документів, тож обмін стає значно безпечнішим.

Система електронного документообігу – це програмне рішення, яке дозволяє організувати роботу з е-документами та обмін ними всередині компанії чи з зовнішніми отримувачами.

В системі ЕДО можна створювати документи, відправляти та отримувати їх на узгодження, підписувати, керувати рухом документів, розмежовувати доступ до них, зберігати та відправляти в архів тощо.

Залежно від виду документообігу системи теж діляться на внутрішні (корпоративні) та зовнішні.

Системи внутрішнього (корпоративного) документообігу дозволяють обмінюватися документами всередині компанії. А системи зовнішнього електронного документообігу – це рішення для обміну та підписання документів з контрагентами, клієнтами та іншими користувачами поза межами компанії.

Деякі провайдери дозволяють інтегрувати зовнішні та внутрішні системи між собою, щоб працювати в одному середовищі й не перемикатися між різними сервісами. Наприклад, ви можете інтегрувати Megapolis.DocNet з Deals, Вчасно і ПТАХ, щоб працювати з усіма документами в інтерфейсі Megapolis.DocNet [13].

Системи електронного документообігу повинні давати можливість організувати повноцінну роботу з документами в компанії. Детальніше про функції розповідаємо на прикладі можливостей системи Megapolis.DocNet.

Управління документами. Документи в системі відсортовані так, як вам зручно, їх можна згрупувати та відфільтрувати, а вся інформація про кожен документ зберігається в картках. Гнучкий пошук ElasticSearch дозволяє миттєво знайти документи за словами (як в Google) або за будь-якими параметрами.

Спільна робота з колегами. В системі ви можете працювати над документами разом з іншими співробітниками, обговорювати зміни чи допрацювання у чаті, прив'язаному до конкретного документа, підключати будь-яку кількість колег до роботи [30, с. 2].

Керівники бачать завдання співробітників та можуть слідкувати за всіма подіями в календарі. Сповіщення допомагають не пропустити дедлайн та вчасно опрацьовувати всі документи.

Всі документи можна зберігати в архіві на сервері чи у хмарі, при цьому доступ до них такий же швидкий та простий, як і до неархівованих документів.

Автоматизація процесів. Ви можете налаштувати маршрути узгодження документів будь-якої складності. А також в Megapolis.DocNet можна автоматизувати та оптимізувати будь-який процес, пов'язаний з документами, завдяки конструктору процесів, що працює на рушію Camunda та створений на базі визнаних світових стандартів: специфікації процесу BPMN™ 2.0, управління справами CMMN™ і моделювання рішень DMN™.

Це неповний перелік функцій та можливостей, доступних в системі електронного документообігу. Саме СЕД дозволяє адаптувати роботу з документами під потреби вашої компанії та організувати її максимально зручно саме для вас.

Електронний документообіг зручніший за паперовий, адже не потрібно друкувати документи та відправляти їх чи носити по кабінетах на підпис.

Документи відправляються миттєво, навіть якщо контрагент знаходиться в іншій країні. Процес узгодження та підписання документів не зупиняється, навіть якщо керівник у відрядженні. До того ж деякі вендори пропонують системи, що мають мобільні застосунки [36, с. 480-482]. Тож керівник чи керівниця можуть зайти в робочий кабінет навіть у відпустці та за кілька хвилин підписати всі потрібні документи навіть без ноутбуку .

Можна відправити документи кількох адресатам одночасно. Узгоджувати документи можна послідовно чи паралельно, ви можете легко зробити такі маршрути погодження, як вам потрібно. Наприклад, один і той самий документ може узгодити дві людини – якщо перша це зробить, то з другої це завдання знімається автоматично. У випадку з паперовими документами для цього треба було б друкувати дві копії, відносити їх кожному співробітнику та робити зайву роботу [54, с. 182]. Електронний документообіг же значно спрощує цей процес.

Доступні шаблони документів, які ви робите один раз, і потім всі співробітники ними користуються, щоб швидко і без помилок створювати документи. Шаблони вже мають обов’язкові поля, тому неможливо забути внести важливу інформацію – система не збереже документ без неї.

Економія коштів на друці та пересилці документів. Великі компанії витрачають багато грошей на те, щоб відправити документи контрагенту кур’єром та отримати їх назад. Крім того, що електронний документообіг значно пришвидшує цей процес, він ще й робить його значно дешевшим.

Кращий рівень конфіденційності, адже доступ до документів в системі контролюється адміністратором. Це гарантує, що документ побачать тільки ті співробітники/відділи, які мають на це право. Для зберігання електронних документів не потрібен фізичний архів, що дуже зручно для великих компаній, яким потрібні великі приміщення, щоб вмістити всі документи й організувати роботу з ними. Електронний документообіг в архіві дозволяє зберігати безліч документів в е-форматі, миттєво їх вивантажувати та шукати [6, с.123].

Якщо говорити про недоліки електронного документообігу, до них можна віднести небезпеку проникнення вірусів в документи. Але зазвичай ця проблема вирішується завдяки надійним системам документообігу. Наприклад, Megapolis.DocNet має вбудований антивірус, який автоматично перевіряє всі вхідні документи та поміщає небезпечні в карантин.

Також до недоліків можна віднести вартість систем ЕДО, але якщо порахувати вигоди від автоматизації роботи з документами та економію часу співробітників, то виходить, що впровадження е-документообігу навпаки економить кошти компанії.

Для того, щоб впровадити ЕДО, потрібно зробити кілька обов'язкових дій. Розробити інструкцію про електронні документи та електронне діловодство на підприємстві [12]. Там потрібно зафікусувати назви е-документів, електронних облікових документів та архівних електронних документів.

Отримати кваліфікований електронний підпис (КЕП) для директора та головного бухгалтера, а також КЕП або УЕП (удосконалений електронний підпис) для інших співробітників, які працюють з документами.

Повідомити контрагентів та партнерів, що ви переходите на ЕДО, зафіксувати їхню згоду щодо е-документів та використання ЕЦП в договорах.

Видати наказ про перехід підприємства на електронний документообіг з певної дати.

Крім того, важливий етап – вибір системи ЕДО та навчання співробітників. Перш за все визначте ваші потреби, пріоритети та важливі функції, які повинне мати рішення. Пропишіть критерії вибору, кількість людей, які працюватимуть в системі, кількість документів, з якими працюватимуть одночасно. Це допоможе обрати систему за технічними характеристиками.

Після вибору рішення підлаштуйте його під свої потреби та організуйте навчання співробітників. Збирайте зворотній зв'язок від працівників, щоб покращити систему та побороти недовірливе ставлення до нововведення.

В цьому розділі ми обговоримо законність електронного документообігу. В цьому питанні сумніватись не доводиться, адже ЕДО поширений не лише у

приватних компаніях. Електронний документообіг в органах державної влади впроваджений вже давно і регулюється відповідним законодавством [15].

По-перше, Законом України «Про електронні документи та електронний документообіг», який функціонує з 2003 року [42].

По-друге, Законом України «Про електронні довірчі послуги», що закріплює юридичну силу е-документообігу [17].

Також Законом України «Про електронну комерцію», Наказом Міністерства фінансів України «Про затвердження Порядку обміну електронними документами з контролюючими органами», Постановою Правління НБУ «Про затвердження Положення про застосування електронного підпису в банківській системі України» та багатьма іншими [18].

Отже, система електронного документообігу є ключовим елементом сучасного підприємства, сприяючи автоматизації бізнес-процесів, підвищенню продуктивності праці та зменшенню витрат. Е-документообіг дозволяє підприємствам ефективніше організовувати обробку, зберігання та передачу інформації, що сприяє досягненню стратегічних цілей.

1.2. Основні загрози та ризики в системах е-документообігу

Серед переваг електронного документообігу не лише зручність, але й безпека. Адже електронні документи зберігаються у захищених хмарних сховищах, пересилаються виключно захищеними каналами, а також можна налаштувати обмежений доступ до кожного з них. Це значно надійніше, ніж працювати з документами в паперовому вигляді та тримати їх у звичайному архіві.

Але для того, щоб на 100% бути переконаним у надійності ЕДО, треба обрати безпечну систему. У цьому блозі ми розповімо про основні фактори та критерії, що вказують на захист та безпеку такого ПЗ. Отже, що варто перевірити під час вибору системи електронного документообігу.

Коли ви обираєте систему, перевірте наявність у неї сертифікатів, що підтверджують відповідність стандартам інформаційної безпеки.

Безпека системи часто залежить від захисту платформи, на якій вона створена. Наприклад, якщо платформа отримала сертифікат Г2 згідно стандартів захисту інформації України, то вона відповідає рівню EAL 3 міжнародного стандарту [20, с. 177]. Такий сертифікат забезпечує відповідний захист персональних даних у системі, а також свідчить про те, що рішення може використовуватись в державних органах України.

Також можна дивитися на інші параметри, що вказують на безпеку. Наприклад, на відповідність всім вимогам безпеки GDPR (загального регламенту про захист даних Європейського Союзу).

Penetration-тести. Penetration-тест або тест на проникнення – це перевірка системи так званими «білими хакерами». Під час такого тестування спеціаліст намагається знайти вразливості, використати їх, щоб зламати програму, вивести її з ладу, вкрасти конфіденційну інформацію і так далі. Якщо йому це не вдається – це означає, що система пройшла тест і є надійною.

Звіти про проходження таких penetration-тестів ви можете запросити у розробника системи. Також можна організувати перевірку за допомогою незалежних компаній, що надають такі послуги, або силами власних спеціалістів і переконатися, що система витримає «атаку». Також безпечну систему можна визначити за такими факторами [29, с. 231-234]:

Надійність дата-центру. Інформаційна безпека хмари (дата-центру), у якому розгорнута система, має відповідати як українським вимогам у галузі захисту інформації так і міжнародним стандартам, наприклад такому як стандарт ISO 27001.

Двофакторна аутентифікація. Це найбільш надійний спосіб входу до облікового запису. Його суть в тому, що доступ до акаунту можна отримати, підтвердивши свою особистість у кілька етапів. Наприклад, за допомогою отриманого листа на електронну пошту, смс-повідомлення або push-повідомлення.

Захищене з'єднання. Система повинна використовувати захищене з'єднання між сервером та клієнтом з використанням https протоколу обміну даними, що забезпечує

шифрування даних, які передаються між клієнтом та сервером. Завдяки шифруванню сторонні особи не зможуть прочитати інформацію, навіть якщо перехоплять її.

Резервне копіювання. Щоб не втратити документи, необхідне резервне копіювання. Найбільш надійні системи – ті, які виконують регулярне резервування даних та зберігають їх в захищеному хмарному середовищі у кількох дата-центрах.

Політика захисту контенту (Content security policy). Використання Content security policy у повідомленнях, що надходять від сервера. Це унеможливлює використання зловмисниками Cross Site Scripting атак на пристрої користувача.

Налаштування прав доступу. В системі повинна бути можливість розмежувати права доступу. Тобто, працювати з документами можуть виключно співробітники згідно встановленого переліку. Це стосується як перегляду документів, так і дозволу на їх підписання.

Шифрування даних. Всі документи, що є в системі, повинні зберігатися у файловому сховищі в зашифрованому вигляді. Якщо зловмисник отримає фізичний доступ безпосередньо до файлового сховища, він не зможе розшифрувати дані без відповідних ключів.

Перевірка документів. Система має перевіряти документи, що завантажуються користувачами, на наявність вірусів, тим самим унеможливлюється зараження інших документів в системі, що може призвести до небажаних наслідків.

Захищений електронний підпис. Все підписання документів КЕП проводиться на пристрої клієнта. Сам ключ підпису та його паролі не передаються на сервер, тому перехопити їх неможливо.

Тож не варто боятися переходити на електронний документообіг. Нюанси використання е-документів давно прописані в законодавстві, а самі системи забезпечують надійний захист вашої інформації. Це дозволяє уникнути більшості ризиків, які є при роботі з паперовими документами: до цифрових документів не можуть отримати несанкціонований доступ сторонні користувачі, а також їх майже неможливо втратити чи підробити. Тому обирайте електронний документообіг – тільки він може забезпечити найвищий рівень захисту та надійності [28, с.89].

Отже, електронний документообіг є вразливим до кіберзлочинів, які включають крадіжку даних, витоки інформації, несанкціонований доступ до системи, зловмисне втручання та атаки на інфраструктуру. Також важливим фактором є людський фактор, який може спричинити випадкові помилки чи ненавмисне розголошення інформації. Ці ризики вимагають комплексного підходу до їх виявлення та мінімізації.

1.3. Принципи та підходи до забезпечення безпеки е-документообігу

Принципи забезпечення безпеки е-документообігу: конфіденційність, цілісність: доступність: аутентичність, непідробність, контроль доступу.

Гарантування того, що інформація доступна лише тим користувачам, які мають на це право. Реалізується через шифрування даних та управління доступом. Забезпечення точності та повноти даних. Це означає, що інформація не може бути змінена або знищена неавторизованими особами. Використовуються методи контрольних сум та цифрових підписів.

Гарантія того, що авторизовані користувачі можуть отримати доступ до інформації та ресурсів, коли це необхідно. Застосовуються резервні копії та відновлення після збоїв. Підтвердження особи користувача або джерела даних. Реалізується через аутентифікацію користувачів за допомогою паролів, біометричних даних, смарт-карток тощо.

Гарантія того, що відправник не може відмовитись від відправлення повідомлення, а отримувач – від його отримання. Забезпечується використанням цифрових підписів. Обмеження доступу до інформації та ресурсів лише тим користувачам, які мають відповідні права. Реалізується через політики безпеки та механізми управління доступом.

Підходи до забезпечення безпеки е-документообігу: Криптографічний захист, аутентифікація та авторизація, моніторинг та аудит, системи виявлення та запобігання вторгнень (IDS/IPS), захист від шкідливого ПЗ, управління ризиками, навчання та підвищення обізнаності, резервне копіювання та відновлення [33, с.18]:

Використання шифрування для захисту даних як у стані спокою, так і під час передачі. Це включає симетричне та асиметричне шифрування, цифрові підписи, сертифікати та інші криптографічні методи.

Застосування багатофакторної аутентифікації (МФА) для підтвердження особи користувачів. Використання ролей та політик доступу для контролю прав користувачів.

Постійний моніторинг системи для виявлення аномалій та загроз. Ведення журналів аудиту для відстеження дій користувачів та забезпечення можливості проведення розслідувань [32].

Використання систем для виявлення та блокування неавторизованих спроб доступу та інших загроз. Використання антивірусного програмного забезпечення, фільтрів електронної пошти, систем запобігання вторгнень для захисту від вірусів, троянів та іншого шкідливого ПЗ.

Ідентифікація, оцінка та управління ризиками, пов'язаними з е-документообігом. Включає проведення оцінок вразливостей, тестування на проникнення та інші методи управління ризиками.

Регулярне навчання персоналу з питань інформаційної безпеки та підвищення обізнаності про актуальні загрози та методи їх уникнення. Регулярне створення резервних копій даних та планування процедур відновлення після збоїв для забезпечення доступності та цілісності інформації.

Застосування цих принципів та підходів у комплексі дозволяє ефективно забезпечити безпеку е-документообігу на підприємстві, мінімізуючи ризики та загрози для інформації та бізнес-процесів [22, с.225].

Отже, Сучасні принципи забезпечення безпеки е-документообігу базуються на системності, багаторівневому захисті та дотриманні міжнародних стандартів інформаційної безпеки. Ефективна система безпеки повинна включати ідентифікацію користувачів, регулярний моніторинг, політику управління доступом, а також періодичну оцінку ризиків.

РОЗДІЛ 2: МОЖЛИВОСТІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ Е-ДОКУМЕНТООБІГУ

2.1. Шифрування даних та цифрові підписи як основні технології захисту

В умовах сучасної інформаційної епохи, де обсяги даних зростають з кожним днем, питання захисту інформації набуває особливої актуальності. Шифрування даних та цифрові підписи є двома основними технологіями, що забезпечують конфіденційність, цілісність і автентичність інформації. У цьому розділі буде розглянуто принципи роботи цих технологій, їх застосування, а також переваги і недоліки.

Шифрування — це процес перетворення інформації у форму, що робить її недоступною для неавторизованих користувачів. Основна мета шифрування полягає у забезпеченні конфіденційності даних. Відомо кілька основних методів шифрування, зокрема симетричне та асиметричне шифрування [24, с.324].

При симетричному шифруванні використовується один і той же ключ для шифрування та розшифрування даних. Це робить його швидким і ефективним для обробки великих обсягів інформації. Однак, ключ повинен бути безпечно переданий між сторонами, що ускладнює його використання в певних випадках. Прикладами алгоритмів симетричного шифрування є AES (Advanced Encryption Standard) та DES (Data Encryption Standard).

Асиметричне шифрування використовує пару ключів: публічний та приватний. Публічний ключ може бути відомим усім, тоді як приватний ключ повинен зберігатися в таємниці. Цей метод дозволяє здійснювати безпечний обмін ключами для симетричного шифрування [26]. Зазвичай, алгоритми асиметричного шифрування, такі як RSA (Rivest-Shamir-Adleman) або ECC (Elliptic Curve Cryptography), застосовуються для шифрування малих обсягів даних, зокрема для обміну ключами.

Шифрування даних використовується в багатьох сферах: від захисту особистих даних у соціальних мережах до забезпечення безпеки транзакцій у

фінансових установах. Системи шифрування є невід'ємною частиною VPN (Virtual Private Network), що дозволяє забезпечити безпечний доступ до мережі.

Цифровий підпис — це криптографічний метод, що забезпечує автентичність та цілісність електронних документів. Він використовує асиметричне шифрування, де особа, що підписує документ, використовує свій приватний ключ для створення підпису. Інші користувачі можуть перевірити підпис, використовуючи публічний ключ підписувача [8].

Процес створення цифрового підпису включає кілька етапів [5]:

1. Генерація хешу документа: Спочатку створюється хеш-код документа за допомогою криптографічної хеш-функції (наприклад, SHA-256).

2. Шифрування хешу: Хеш-код шифрується за допомогою приватного ключа підписувача, створюючи цифровий підпис.

3. Передача документа: Документ надсилається разом з цифровим підписом.

Перевірка підпису виконується шляхом розшифрування підпису за допомогою публічного ключа і порівняння отриманого хешу з хешем документа.

Цифрові підписи широко використовуються в електронних торгах, електронному урядуванні та в банківських системах. Вони забезпечують юридичну силу електронних документів і знижують ризики шахрайства.

Основними перевагами шифрування даних та цифрових підписів є [5]:

• Конфіденційність – забезпечує захист інформації від несанкціонованого доступу.

• Цілісність – гарантує, що дані не були змінені під час передачі.

• Автентичність – підтверджує особу відправника або джерела даних.

Однак існують і недоліки:

• Складність управління ключами: Особливо у випадку асиметричного шифрування, де важливо забезпечити безпеку приватного ключа.

• Витрати ресурсів: Шифрування може вимагати значних обчислювальних ресурсів, що особливо критично в умовах великих обсягів даних.

• Проблеми з інтеграцією: Впровадження нових технологій шифрування і підпису може вимагати значних зусиль для інтеграції в існуючі системи.

Отже, шифрування даних та цифрові підписи є критично важливими інструментами для забезпечення безпеки інформації в сучасному світі. Вони забезпечують захист особистих даних, фінансових транзакцій і юридичних документів, що робить їх незамінними у багатьох сферах діяльності. Однак, для їх ефективного використання необхідно враховувати можливі недоліки та виклики, пов'язані з управлінням ключами та ресурсами. Підвищення рівня обізнаності користувачів про ці технології та їх належне впровадження допоможе знизити ризики і забезпечити належний рівень захисту даних.

2.2. Аутентифікація та авторизація користувачів

У сучасному світі, де дані стали ключовим ресурсом, забезпечення їхньої безпеки стає дедалі важливішим. Один з основних аспектів цього – правильне розуміння процесів аутентифікації та авторизації. У цій статті ми розберемо, яка різниця між авторизацією та автентифікацією і що вони собою являють.

Щоб наочно зрозуміти важливість цих процесів, уявімо собі ситуацію, коли несанкціонований користувач отримує доступ до банківського акаунту через недостатню аутентифікацію. Це може призвести до фінансових втрат, крадіжки особистих даних і навіть загрози безпеці. Саме тому правильна автентифікація та авторизація є невід'ємною частиною захисту наших особистих і фінансових інтересів в онлайн-світі [2, с.18].

Визначення аутентифікації. Це процедура перевірки та підтвердження особи користувача перед наданням доступу до певної системи, додатку або ресурсу. Її мета полягає в тому, щоб переконатися, що людина, яка намагається отримати доступ, дійсно є тим, за кого вона себе видає. Це забезпечує безпеку, запобігає несанкціонованому доступу та захищає конфіденційні дані від несанкціонованого використання.

Процес автентифікації починається з того, що користувач надає системі унікальну інформацію, яка ідентифікує його, наприклад, логін і пароль. Після

введення цих даних система перевіряє їх наявність у базі даних. Якщо введені дані відповідають даним у системі, користувач вважається успішно аутентифікованим і отримує доступ [9]. У разі помилки, користувачеві може бути відмовлено в доступі.

Існує кілька методів такої перевірки, призначених для підвищення безпеки [14]:

1. Введення логіна і пароля: від користувача вимагається ввести унікальний логін і пароль, які пов’язані з його акаунтом. Це один із найпоширеніших способів аутентифікації.

2. Багатораторна автентифікація (MFA): користувач повинен надати кілька форм підтвердження своєї особи. Наприклад, після введення логіна і пароля, він може отримати одноразовий код на свій телефон або електронну пошту, який також необхідний для входу.

3. Біометричні дані: цей метод уже використовує унікальні фізіологічні або поведінкові характеристики користувача, такі як відбитки пальців, розпізнавання обличчя або голосу. Має високий рівень безпеки, оскільки біометричні дані складно підробити або вкрасти.

4. Перевірка через соціальні мережі: дає змогу користувачам увійти на сайт або в застосунок, використовуючи свої облікові дані із соціальних мереж, як-от Facebook або Google.

Вибір конкретного методу залежить від рівня безпеки, який потрібен для конкретної системи, і зручності використання для кінцевого користувача.

Визначення авторизації. Авторизація, з іншого боку, пов’язана з визначенням того, до яких ресурсів або функціональності користувач має доступ. Після успішної перевірки система визначає рівень доступу користувача: які файли він може бачити, які дії він може виконувати тощо. Це включає визначення рівнів доступу, дозволів на виконання певних операцій і тимчасових обмежень на доступ до ресурсів [12].

Цей процес включає в себе такі аспекти:

• Рівні доступу: різні користувачі можуть мати різні рівні доступу в системі. Наприклад, у системі управління проектами звичайні користувачі можуть мати доступ лише до читання даних, тоді як адміністратори мають повний доступ до редагування та видалення інформації. Або, скажімо, у системі електронної медичної документації, лікарі можуть мати вищий рівень доступу, ніж медичні сестри чи адміністративний персонал.

• Дозволи на доступ. Перевірка також визначає конкретні дії, які користувач може здійснювати. Це можуть бути дозволи на читання, запис, зміну або видалення певних даних. Наприклад, в онлайн-магазинах, адміністратори мають дозвіл на управління асортиментом товарів, тоді як звичайні користувачі можуть лише переглядати товари та робити замовлення.

• Часові обмеження. Мистецтво про тимчасові рамки доступу. Наприклад, деякі користувачі можуть мати доступ тільки в певний час доби або в певні дні тижня.

Цей процес перевірки не тільки забезпечує безпеку даних, а й допомагає ефективно використовувати ресурси, надаючи користувачам тільки ті можливості, які необхідні для їхньої роботи, і встановлюючи необхідні обмеження для підтримки безпеки системи.

Порівняння. Основна відмінність між обома процесами полягає в тому, що перша підтверджує особу користувача, тоді як друга визначає, що цей користувач може робити після того, як його особу підтверджено. Розуміння цієї відмінності є ключовим, бо без правильної автентифікації авторизація стає безглуздою – система не зможе переконатися в тому, що користувач із правильними дозволами справді той, за кого себе видає.

Розглянемо табличку, в якій детально розглядаються основні відмінності та схожості (рис. 2.1) [20, с.178]:

Аспект	Автентифікація	Авторизація
Визначення	Перевірка особистості користувача.	Керування доступом користувача до ресурсів після перевірки.
Ціль	Посвідчення, що користувач є тим, за кого він себе видає.	Керування діями та доступом користувача в системі.
Процес	Підтвердження особи через введення даних (логіна, пароля), біометричні дані тощо.	Визначення дозволів і рівня доступу користувача до ресурсів.
Фокус	Посвідчення особи користувача.	Визначення прав доступу та контроль над функціональністю.
Ключові моменти	Логін, пароль, біометричні дані, одноразові коди тощо.	Рівні доступу, дозволи на дії, тимчасові обмеження тощо.
Припускає	Попередню аутентифікацію для визначення особи.	Успішну аутентифікацію для встановлення доступу до ресурсів.
Чому важливо	Запобігає несанкціонованому доступу до системи та даних.	Контролює, що користувач може робити в системі після аутентифікації.
Приклад у житті	Введення пароля під час входу в акаунт, використання відбитків пальців або розпізнавання обличчя.	Після входу в пошту, визначення, чи може користувач писати, читати, видаляти листи.
Схожості	Обидва процеси пов’язані з безпекою даних і контролем доступу.	Обидва процеси працюють у парі, визначаючи, хто має доступ до чого.

Рисунок 2.1. Основні відмінності та схожості аутентифікації та авторизації користувачів

• Онлайн-магазини: Коли ви оформляєте замовлення в інтернет-магазині, система аутентифікує вас і потім авторизує певні дії, такі як додавання товарів у кошик, оплата та управління замовленнями.

• Медичні інформаційні системи: лікарі можуть автентифікувати себе, щоб отримати доступ до медичної історії пацієнтів, при цьому авторизація визначає, які дані вони можуть бачити та змінювати.

Отже, обидві системи забезпечують безпеку особистих даних, підтримують конфіденційність приватної інформації, дають змогу системам контролювати доступ і забезпечують зручність та ефективність у використанні різних сервісів і систем.

2.3. Системи моніторингу та виявлення загроз (IDS/IPS)

У сучасному світі системи виявлення та запобігання вторгнень (Intrusion detection system / Intrusion prevention system, IDS / IPS) - необхідний елемент захисту від мережевих атак. Основне завдання даних систем - виявлення фактів несанкціонованого доступу в корпоративну мережу або несанкціонованого управління нею, з виконанням відповідних заходів протидії (інформування адміністраторів про факт вторгнення, обрив з'єднання або перенастроювання брандмауера для блокування подальших дій зловмисника і т.д.).

Існує багато систем виявлення та запобігання вторгнень. Актуальною є задача вибору однієї з них. У роботі проводиться порівняльний аналіз систем виявлення вторгнень, робиться висновок про те, що система Suricata є більш швидким та надійним детектором атак [23].

IDS / IPS системи - це унікальні інструменти, створені для захисту мереж від несанкціонованого доступу. Вони являють собою апаратні або комп'ютерні засоби, які здатні оперативно виявляти і ефективно запобігати вторгненням. Серед заходів, які приймаються для досягнення ключових цілей IDS / IPS, можна виділити інформування фахівців з інформаційної безпеки про факти спроб хакерських атак і впровадження шкідливих програм, обрив з'єднання зі зловмисниками і перенастроювання мережевого екрану для блокування доступу до корпоративних даних.

Кібератаки – одна з основних проблем, з якими стикаються суб'єкти, які мають інформаційними ресурсами. Відомі антивірусні програми і брандмауери ефективні лише для захисту очевидних місць доступу до мереж [24]. Однак зловмисники здатні знаходити шляхи обходу і вразливі сервіси навіть в

найдосконаліших системах безпеки. При такій небезпеці не дивно, що закордонні та українські.

UTM-рішення отримують все ширшу популярність серед організацій, що бажають виключити можливість вторгнення і поширення шкідливого ПЗ (хробаків, троянів і комп'ютерних вірусів). Багато компаній приймають рішення купити сертифікований міжмережевий екран або інший інструмент для комплексного захисту інформації.

Всі існуючі сьогодні системи виявлення та запобігання вторгнень об'єднані кількома загальними властивостями, функціями і завданнями, які з їх допомогою вирішують фахівці з інформаційної безпеки [61]. Такі інструменти за фактом здійснюють безперервний аналіз експлуатації певних ресурсів і виявляють будь-які ознаки нетипових подій.

Організація безпеки корпоративних мереж може ґрунтуватися на кількох технологіях, які відрізняються типами виявлених інцидентів і методами. Крім функцій постійного моніторингу та аналізу того, що відбувається, IDS системи виконують такі функції [56]:

– збір і запис інформації;

– оповіщення адміністраторів мереж про зміни, що відбулися;

– створення звітів для підсумовування логів.

Технологія IPS в свою чергу у додачу до вище сказаного, здатна не тільки визначити загрозу і її джерело, а й здійснити їх блокування. Це говорить про розширений функціонал подібного рішення. Вона здатна здійснювати наступні дії:

– обривати шкідливі сесії і запобігати доступу до найважливіших ресурсів;

– змінювати конфігурацію «підзахисної» середовища;

– проводити дії над інструментами атаки (наприклад, видаляти заражені файли).

Варто відзначити, що UTM-міжмережевий екран і будь-які сучасні системи виявлення та запобігання вторгнень є оптимальною комбінацію технологій систем IDS і IPS.

Одним з рішень IPS запобігання вторгнень є детектори атак, які призначені для своєчасного виявлення безлічі шкідливих загроз. В Інтернет Контроль Сервері вони реалізовані у вигляді системи Suricata - багатозадачного і продуктивного інструменту, розробленого для захисту мереж, а також збору і зберігання інформації про будь-які сигнали, що надходять. Робота детектора атак заснована на аналізі сигнатур і евристиці, а зручність його обумовлено наявністю відкритого доступу до вихідного коду. Такий підхід дозволяє налаштовувати параметри роботи системи для вирішення індивідуальних завдань.

До редагованих параметрів Suricata відносяться правила, яким буде підпорядковуватися аналіз трафіку, фільтри, що обмежують висновок попередження адміністратора, діапазони адрес різних серверів, активні порти і мережі.

Таким чином, Suricata (рис. 2.2) [53], як IPS-рішення - це досить гнучкий інструмент, функціонування якого підлягає змінам в залежності від характеру атаки, що робить його максимально ефективним.

В ІКС фіксується і зберігається інформація про підозрілу активність, блокуються ботнети, DOS- атаки, а також TOR, анонімайзери, P2P і торрент-клієнти.

У вкладці налаштувань (рис. 2.2.) [42] можна редагувати параметри роботи детектора атак. Тут можна вказати внутрішні, зовнішні мережі, діапазони адрес різних серверів, а також порти, що використовуються. Всім цим змінним присвоєно значення за замовчуванням, з якими детектор атак може коректно запуститися. За замовчуванням, аналізується трафік на зовнішні інтерфейси.

Детектору атак можна підключати правила, за допомогою яких він буде аналізувати трафік. На вкладці на рис.2.3 [42] можна подивитися наявність і вміст того чи іншого файлу з правилами, а також включити або виключити його дію (за допомогою прапорців праворуч). У правому верхньому куті розташовується пошук за назвою або за кількістю правил у файлі. Порівняння Suricata та Snort.

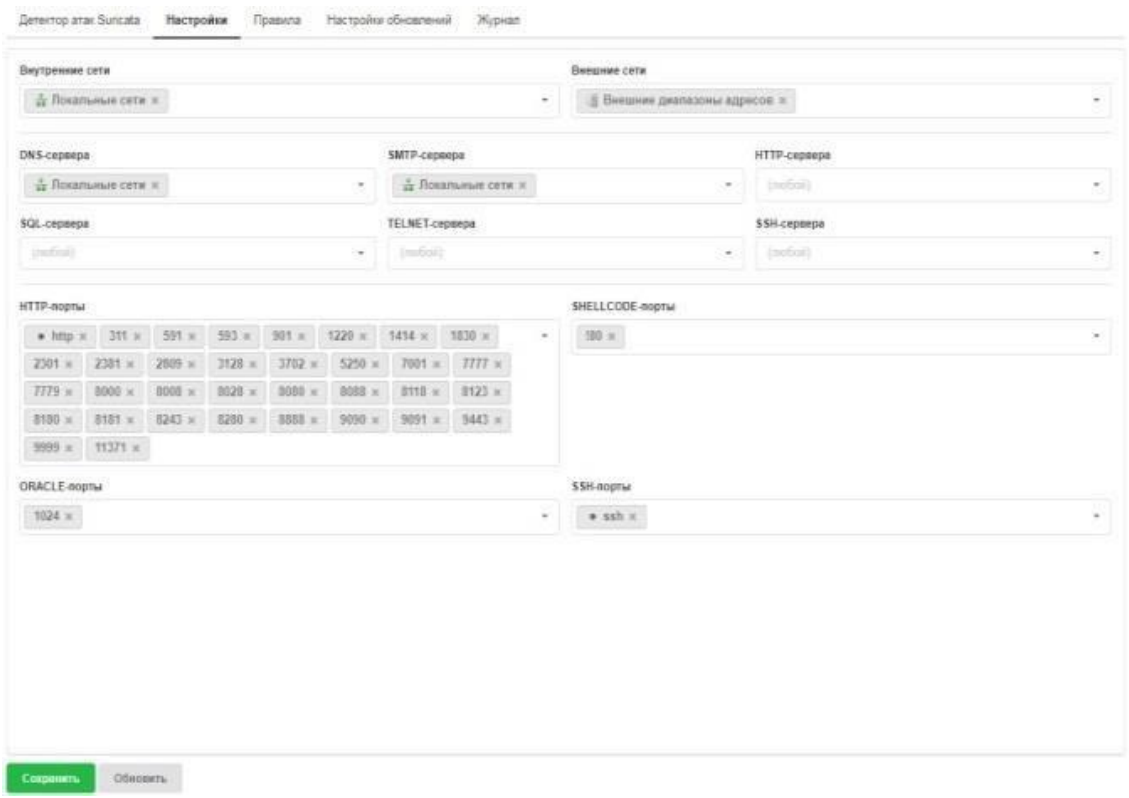

Рисунок 2.2. Настройка –Suricata‖

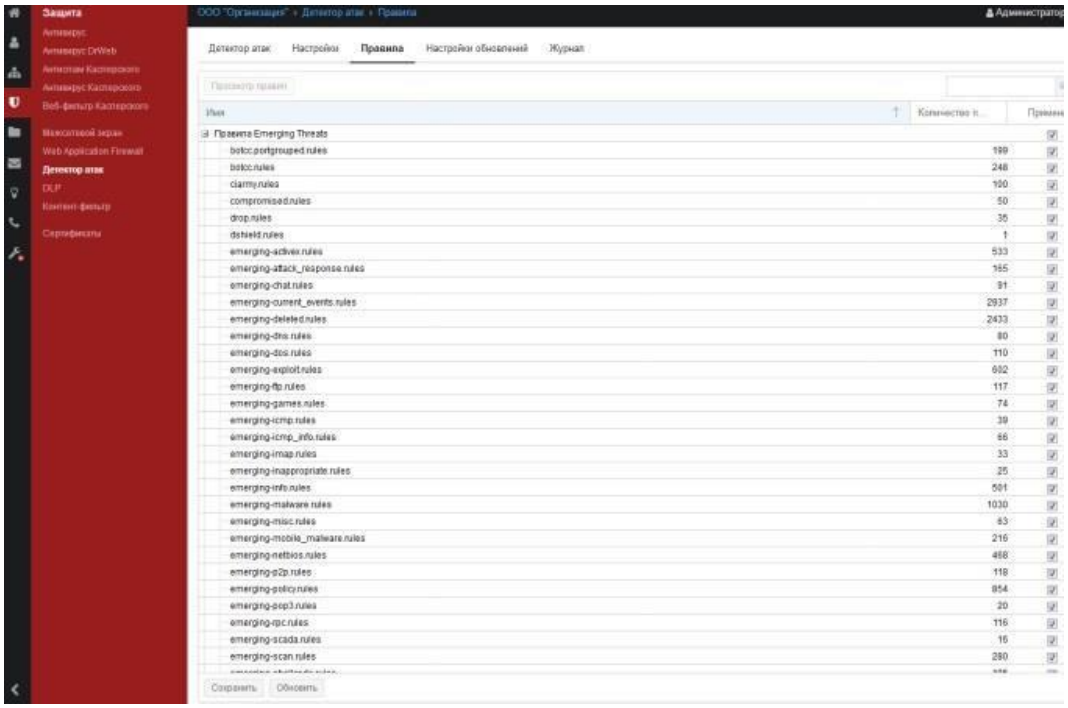

Рисунок 2.3. Правила –Suricata‖

Більше 250 одиничних тестів було проведено проти Suricata та Snort, дотримуючись методології, результати наведені в таблиці 1.1 [44]

Таблиця 2.1.

Результати тестів

Тестова група	**Кількість тестів**	**Оцінка suricata**	**Оцінк snort**
Поганий трафік	4	1	1
Роздроблені пакети	2	1	3
Шкідливі програми та віруси	14	9	7
Відмова в обслуговуванні (DoS)	3	3	3
Атаки з боку клієнта	257	157	127
Оболонки	12	12	7
Продуктивність	0	2	1
Всього	297	185	149

Випробування були проведені на 14 шкідливих програмах та вірусах. Suricata має кращий рівень виявлення шкідливих програм та вірусів, ніж Snort.

На наборі з 11 оболонок (вірус схований в іншому файлі), Suricata виявив 9 shellcodes, а Snort виявив 7 shellcodes.

У наборі з 3 тестів і Suricata, і Snort виявили 3 спроби DoS проти служб SSH та MSSQL. Тести продемонстрували, що Suricata краща, ніж Snort для виявлення нападів на стороні клієнта, зі швидкістю виявлення 82% проти 49%.

Отже, системи моніторингу та виявлення загроз забезпечують своєчасне виявлення спроб зловмисного впливу, несанкціонованих доступів чи інших загроз. Інтеграція IDS/IPS у системи е-документообігу дозволяє підвищити безпеку шляхом проактивного реагування на потенційні ризики. Такі системи ефективні для запобігання DDOS-атак, сканування вразливостей та фішингових загроз.

2.4. Використання хмарних технологій для забезпечення безпеки документів

Спочатку наведено визначення хмарних обчислень, їх призначення та основні характеристики. Під хмарними обчисленнями розуміється результат розвитку багатьох різних технологій, які в комбінації змінили організаційний підхід до побудови інформаційної інфраструктури організації. Хмарні обчислення (cloud computing) – модель надання можливості повсюдного і зручного мережевого доступу на вимогу до пулу налаштованих обчислювальних

ресурсів, які підлягають конфігурації (наприклад, мережі, сервери, засоби зберігання, застосунки і сервіси), що можуть оперативно надаватися і звільнятися при мінімальному зусиллі управління або взаємодії з провайдером (постачальником) [3].

Основними характеристиками хмарних обчислень, які відрізняють їх від інших типів обчислень є: самообслуговування на вимогу, об'єднання ресурсів, миттєва еластичність ресурсів, вимірюваний сервіс. Розглянемо кожну з характеристик окремо [3].

Самообслуговування на вимогу. Споживач зам необхідності автоматично, без взаємодії з кожним постачальником послуг, може самостійно визначати і змінювати обчислювальні потужності, як-от серверний час, обсяг сховища даних; широкий (універсальний) мережевий доступ. Обчислювальні можливості доступні на великій відстані мережею через стандартні механізми, що сприяє широкому використанню різнорідних платформ клієнта (термінальних пристроїв).

Об'єднання ресурсів. Конфігуруванні обчислювальні ресурси постачальника об'єднані в єдиний пул для спільного використання розподілених ресурсів великою кількістю споживачів.

Миттєва еластичність ресурсів (миттєва масштабованість). Хмарні послуги можуть швидко надаватися, розширюватися, стискатися і звільнятися, виходячи з потреб споживача.

Вимірюваний сервіс (облік споживаного сервісу і можливість оплати послуг, які були реально використані). Хмарні системи автоматично керують і оптимізують використання ресурсів завдяки здійснення вимірювань на деякому рівні, що відповідає типу сервісу.

Проаналізувавши загальне визначення хмарних обчислень та їх основні характеристики можна сформулювати основні переваги й недоліки під час роботи з ними [3]. Хмарні обчислення мають ряд важливих переваг: вся інформація доступна з будь-якого пристрою, (комп'ютер, планшет, смартфон, тощо) підключеного до інтернету. Користувач не прив'язаний до певного

робочого місця; скорочення витрат на придбання дорогих потужних комп'ютерів, серверів, немає потреби оплачувати роботу IT-фахівця для обслуговування локального дата-центру; необхідні інструменти для роботи надаються автоматично веб сервісом; високий рівень технологічності обчислювальних потужностей, який надається користувачу, дозволяє зберігати, аналізувати і обробляти дані; оплата сервісів відбувається тільки за необхідності їх використання, при цьому оплата відбувається тільки за необхідний пакет послуг; сучасні хмарні обчислення можуть забезпечувати найвищу надійність, до того ж лише невелика кількість організацій можуть дозволити собі утримувати повноцінний дата-центр; висока відмово стійкість.

Недоліки хмарних обчислень: для роботи з «хмарою» потрібне постійне підключеннядо Інтернету; користувач не завжди може налаштувати програмне забезпечення, яке використовується за індивідуальними потребами; створення власної «хмари» потребує значних коштів; «хмара» – сховище даних, до яких, використовуючи вразливості системи, можуть отримати доступ зловмисники [9].

Визначивши важливі переваги та основні недоліки хмарних обчислень перейдемо до класифікації та аналізу організацій та органів, які розробляють нормативно-правові документи для хмарних обчислень. Вони створюють міжнародні стандарти і мають наступнуієрархію рівнів:

1. Міжнародний (ISO/IEC [3]);»
2. Міждержавний (форуми і консорціуми (Cisco, CSA));
3. Регіональний (європейські органи ETSI, CEN / CENELEC);
4. Національний (закони та державні стандарти, відомчі нормативні документи, керівництва, інструкції, наприклад: (NIST) [10].

При стандартизації хмарних технологій кордони держав втрачають обмежувальну роль,так як учасники процесу надання послуг часто знаходяться в різних країнах і на різних континентах. У силу актуалізації забезпечення інформаційної безпеки та відсутності міжнародних стандартів зі сертифікації елементів хмарної інфраструктури, такі елементи (дата-центри, канали і мережі комунікацій) використовують сертифікати безпеки стандартів суміжних

напрямів (як міжнародних, так і інших країн).

У сфері управління конфігурацією хмарних технологій багато організацій прагнуть розробляти специфікації для стандартного інтерфейсу прикладного програмування (API), тобто інтерфейсу через який користувачі та оператори керують хмарними обчисленнями та сховищами. Робоча група Відкритого інтерфейсу хмарних обчислень (Open Cloud Computing Interface Working Group – OCCI-WG) організації Open Grid Forum (OGF) визначила та випустила API для управління інфраструктурою як сервісом (IaaS). Інкубатор Open Cloud Standards Incubator (OCSI) робочої групи розподіленого управління (DMTF) також визначив API керування IaaS. А асоціація виробників мереж зберігання даних (SNIA) сформулювала специфікації Cloud Data Management Interface (CDMI – Управління інтерфейсом хмарних даних), яка є API для управління блоками зберігання даних [13].

Організація нестандартних послуг також активно працює в цій галузі. Спільнота з відкритим кодом під назвою «OpenStack», створена переважно Rackspace і NASA зробила вихідний код програмного забезпечення для керування IaaS відкритим.

Стандартизація хмарних обчислень розпочата промисловими організаціями, які розробляють так звані «стандартні стандарти». Почали діяти органи стандартизації, такі як MCE-T та ISO/IEC JTC1, а також стандартні органи, орієнтовані на інформаційно-телекомунікаційні технології, як-от Інститут інженерів електротехніки та електроніки (IEEE) та Інтернет-технічна робоча група (IETF). У США та Європі стандартизація хмарних обчислень також обговорюються урядовими організаціями.

Існує дві групи органів стандартів форуму, пов’язані з хмарними обчисленнями. Ті, що входять до складу першої групи, включаючи DMTF, OGF і SNIA, активно працюють у сфері мереж та керування розподіленим процесом, а останнім часом додають хмарні обчислення до своїх завдань. Органи другої групи, включаючи OCC, CSA та GICTF, нещодавно засновані для роботи з хмарними обчисленнями.

DMTF (Distributed Management Task Force – Робоча група розподіленого управління). DMTF визначила Open Virtualization Format (OVF), який є стандартним форматом зображення віртуальної машини. Вона започаткувала OCSI та вивчає стандарти, які дозволять взаємодіяти між хмарними системами. CMWG (The Cloud Management Working Group – Робоча група управління хмарами), в якій VMware, Fujitsu та Oracle пропонують відповідний API. DMTF випустила «Білий документ» про сумісність між хмарними системами, а інший – щодо випадків використання управління хмарами та взаємодії. Членами Правління є VMware, Microsoft, IBM, Citrix, Cisco та Hitachi.

OGF (Open Grid Forum – Відкритий Грід форум). OGF створив робочу групу OCCI-WG та визначив і випустив специфікацію API [11], що дозволяє керувати комп'ютером та робочими навантаженнями через IaaS. Відкритий інтерфейс хмарних обчислень реалізується у Європі у проекті OpenNebula. Основними учасниками цього проекту є Fujitsu, EMC та Oracle [14].

SNIA (Storage Networking Industry Association – Асоціація виробників мереж зберігання даних). SNIA заснувала Технічну робочу групу хмарних сховищ (Cloud Storage Technical Working Group) і випустила CDMI, яка є специфікацією інтерфейсу для керування даними у хмарі. Асоціація створила підгрупу під назвою CSI (Cloud Storage Initiative – Ініціатива хмарних сховищ) для навчання користувачів та просування ринку хмарних сховищ за допомогою проекту Cloud BUR SIG (Cloud Backup and Recovery Special Interest Group – Група спеціальних інтересів по хмарному резервуванню та відновленню). Членами SNIA є EMC, IBM, Fujitsu та Hitachi [14].

OCC (Open Cloud Consortium – Відкритий хмарний консорціум). OCC - це некомерційна організація, що утворена під керівництвом університету штату Іллінойс у Чикаго. Він спрямований на розробку еталонних тестів за допомогою хмарного випробувального стенду та досягнення сумісності між хмарними системами.

CSA (Cloud Security Alliance – Альянс хмарної безпеки). CSA – це некомерційна організація, створена для вивчення найкращих практик

забезпечення безпеки хмари та сприяння їх використанню. Було опубліковано вказівки щодо забезпечення безпеки хмар.

GICTF (Global Inter-Cloud Technology Forum – Глобальний форум з хмарних технологій). GICTF - це японська організація, що займається вивченням стандартних інтерфейсів між хмарами з метою підвищення надійності хмар. В його склад входять понад 80 корпоративних членів і організацій з промисловості, уряду і наукових кіл, вона випустила офіційний документ щодо випадків використання міжхмарного об'єднання і функціональних вимог [14].

Державні органи в США та Європі також активно працюють у сфері стандартизації, пов’язаної з хмарами. Зокрема NIST та ENISA.

NIST (National Institute of Standards and Technology – Національний інститут стандартів та технологій) – це технічний відділ, який належить Торгово-промисловому департаменту США. Одним з перших документів, який розроблений NIST й який встановлює визначення зісфери хмарних технологій є «The NIST Definition of Cloud Computing». В той же час NIST здійснює стандартизацію хмарних технологій за п’ятьма робочими групами. Одна з них – SAJACC (Standards Acceleration to Jumpstart Adoption of Cloud Computing – Прискорення стандартів для швидкого впровадження хмарних обчислень), яка покликана сприяти розробці стандартів хмарних технологій на основі фактичних прикладів та випадків використання [27, с. 60].

ENISA (European Union Agency for Network and Information Security – Європейська агенція мереж та інформаційної безпеки). ENISA розробило наступні документи: «Cloud Computing: Benefits, Risks and Recommendations for Information Security», який надає рекомендації з організації безпеки інформації при хмарних обчисленнях, а також «Cloud Computing Information Assurance Framework», яка є основою для забезпечення безпеки інформації при хмарних обчисленнях.

Хоч багато організацій обговорюють питання стандартизації хмарних технологій, діяльність щодо консолідації обговорень і рішень нині є недостатньою. Такі заходи проводяться лише частково. Головним питанням є,

наскільки добре національні та міжнародні органи стандартизації, які почали повномасштабні дослідження хмарних технологій, можуть співпрацювати з робочими групами розвитку та підтримки хмарних технологій утвореними бізнесом, як новітні світові розробки впровадити до інформаційного простору нашої держави та закріпити в нормативних документах України [29, с. 232]. Розглянемо деякі основні стандарти забезпечення безпеки інформації в хмарних технологіях.

В даний час два технічних підкомітети Об'єднаного технічного комітету1 ISO (JTC 1) «Інформаційні технології» ведуть розробку міжнародних стандартів в області хмарних технологій. Ними були розроблені такі документи:

Стандарт ISO/IEC 17788 «Information technology. Distributed application platforms and services. Cloudcomputing. Overview and vocabulary» («Інформаційні технології. Розподілені прикладні платформи і сервіси. Хмарні обчислення. Загальні положення та словник»).

Стандарт описує концепцію хмарних обчислень і містить ряд термінів і визначень. Він став термінологічної основою для подальшої роботи зі стандартизації в сфері хмарних обчислень [9].

Стандарт ISO/IEC 17789 «Information technology. Cloud computing. Reference architecture» («Інформаційні технології. Хмарні обчислення. Еталонна архітектура»). Стандарт містить огляд загальних понять і характеристик хмарних обчислень, типів хмар, компонентів хмарних обчислень сторін-учасниць. У ньому зроблено наголос на вимоги до того, що повинні забезпечувати хмарні сервіси, а не на питаннях проектування і впровадження відповідних рішень [3].

Технічна специфікація ISO/IEC TS 27017 «Information technology - Security techniques - Information security management – Guidelines on information security controls for the use of cloud computing services based on ISO / IEC 27002» («Інформаційні технології. Методи захисту. Звід практик стосовно заходів інформаційної безпеки, що ґрунтуються на ISO/IEC 27002, для хмарних послуг») [14]. Стандарт містить рекомендації щодо забезпечення інформаційноїбезпеки хмарних обчислень. Він спирається на переглянуту версію ISO/IEC 27002 і

містить здебільшого рекомендації з реалізації описаних в цьому документі заходів інформаційної безпеки в контексті хмарних обчислень.

Стандарт ISO/IEC 27018 «Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors» («Інформаційні технології. Методи захисту. Кодекс усталеної практики для захисту персональної ідентифікаційної інформації (PII) у загальнодоступних хмарах, що діють як процесори PII») [15]. Стандарт призначений для постачальників послуг «публічної хмари», які ведуть обробку персональних даних (і є операторами персональних даних). Він містить рекомендації щодо різних аспектів і елементів захисту персональних даних і недоторканності особистої інформації в публічній хмарі. Стандарт не дублює або модифікує рекомендації стандарту ISO/IEC 27002. У ньому визначені додаткові цілі і заходи контролю і управління, пов’язані із захистом персональних даних в хмарному середовищі.

З прийняттям міжнародного стандарту ISO 17788 [9] регламентовано 7 репрезентативних категорій хмарних послуг: CaaS (Communications as a Service – Зв'язок як послуга), CompaaS (Compute as a Service – Обчислення як послуга), DSaaS (Data Storage as a Service – Зберігання даних як послуга), IaaS (Infrastructure as a Service – Інфраструктура як послуга), NaaS (Network as a Service – Мережа як послуга), PaaS (Platform as a Service – Платформа як послуга), SaaS (Software as a Service – Програмне забезпечення як послуга). А також додаткові категорії хмарних послуг: Database as a Service (База даних як послуга), Desktop as a Service (Робочий стіл як послуга), Email as a Service (Електрона пошта якпослуга), Identity as a Service (Ідентифікація як послуга), Management as a Service(Управління як послуга), Security as a Service (Безпека як послуга). Надамо пояснення основних типів послуг в сфері хмарних обчислень:

Програмне забезпечення як послуга. У цій моделі надання хмарних обчислень споживач використовує застосунки постачальника, що запущені в хмарній інфраструктурі та які доступні клієнту через веб браузер або інтерфейс

програми. Споживачі не можуть керувати і контролювати те, що лежить в основі інфраструктури хмари, включаючи мережу, сервери, операційні системи, сховища даних або навіть змінювати параметри налаштування конкретного застосунку.

Платформа як послуга. Модель надання хмарних обчислень, при якій споживач отримує доступ до використання програмної платформи: операційних систем, систем управління базами даних, прикладного програмного забезпечення, засобів розробки і тестування програмного забезпечення. Фактично споживач отримує в оренду комп'ютерну платформу зі встановленою операційною системою і спеціалізованими засобами для розробки, розміщення і управління веб застосунками. Споживач не управляє основною інфраструктурою хмари, включаючи мережу, сервери, операційні системи або сховища даних, але управляє розгорнутими застосунками і можливо параметрами налаштування конфігурації середовища оточення.

Інфраструктура як послуга. Модель надання хмарних обчислень, при якій споживач отримує можливість управляти засобами обробки і зберігання, а також і іншими фундаментальними обчислювальними ресурсами (віртуальними серверами і мережевою інфраструктурою), на яких він може самостійно встановлювати операційні системи та прикладні програми за власною потребою. Тобто споживач орендує абстрактні обчислювальні потужності (серверний час, дисковий простір і пропускну здатність мережевих каналів) або використовує послуги аутсорсингу інфраструктури. Споживач не управляє основною інфраструктурою хмари, але управляє операційними системами, сховищем і розгорнутими ним застосунками.

Виходячи з вищевикладеного визначення хмарних обчислень, хмарні сервіси можна представити у вигляді багатошарової моделі, що складається з трьох основних шарів: IaaS, PaaS, SaaS. Базисом або фундаментом хмарних сервісів є фізична інфраструктура (physical infrastructure), тобто сервери, сховища, мережі та системне програмне забезпечення хмарного дата-центру або мережі взаємопов'язаних хмарних дата-центрів.

У проекті стандарту [16], крім перерахованих, представлені також послуги: HaaS (Hardware as a service – Апаратне забезпечення як послуга), BPaaS (Business process as a service – Бізнес-процес як послуга), DaaS (Data as a service – Дані як послуга), TaaS (Trust as aservice – Довіра як послуга), SDPaaS (Service delivery platform as a service – Хмарне середовище розробки як послуга), TraaaS (Transparency as a service – Прозорість як послуга), WaaS (Workplace as a service – Робоче місце як послуга). Міжнародний стандарт ISO 17788 також не обмежує список нових хмарних послуг, так що в майбутньому варто очікувати розширення списку послуг і узгодження їх назв і позначень.

Приклад стандартної архітектури системи хмарних обчислень описано в стандарті Національного Інституту стандартів і технологій США (National Institute of Standards and Technology, NIST) NIST SP 500-299 [11]. Мета цього стандарту полягає у визначені орієнтованої на безпеку формальної архітектурної моделі хмарних обчислень, а також ідентифікації основних наборів компонентів безпеки, які можна реалізувати в хмарній екосистемі для захисту середовища, операцій та даних.

В свою чергу розроблене CSA Керівництво з безпеки для критично важливих областей хмарних обчислень (Security Guidance for Critical Areas of Focus in Cloud Computing) надає детальні рекомендації щодо зниження ризику при впроваджені хмарних обчислень, а також які комбінації розгортання й моделей обслуговування в хмарних обчисленнях є прийнятними[17].

Провівши аналіз нормативно-правових документів в сфері хмарних обчислень було визначено множину моделей послуг хмарних обчислень. На основі цього аналізу наведемо відображеність моделей послуг у нормативно-правових документах (табл. 2.2) [38].

Таблиця 2.2

Відображеність моделей послуг у нормативно-правових документах

Моделі послуг	NIST	ГОСТ	ISO	CSA
IaaS	+	+	+	+
PaaS	+	+	+	+
SaaS	+	+	+	+
NaaS		+	+	
WaaS/DaaS		+	+	
CaaS		+	+	
Haas/CompaaS		+	+	
SecaaS		+	+	
BPaaS		+		
DaaS/DSaaS		+	+	
TaaS		+		
SDPaaS		+		
TraaaS		+		
Database as aService			+	
Email as aService			+	
Identify as aService			+	
Management as aService			+	

Як висновок, можна стверджувати, що найбільш повно моделі послуг представлені в нормативних документах щодо хмарних обчислень ГОСТ та ISO.

Також під час аналізу нормативно-правових документів в сфері хмарних обчислень були виокремленні суб’єкти взаємодії (табл. 2.3) й визначено, що таким суб'єктам, як Cloud Auditor, Cloud Broker і Cloud Partner в кожному нормативному документі делегуються частково різні обов’язки, які описують функції посередника між Cloud Consumer і Cloud Provider. В свою чергу Cloud Consumer і Cloud Provider мають схожі ролі в моделі взаємодії в сфері хмарних обчислень в усіх представлених нормативних документах [38].

Таблиця 2.3

Суб'єкти взаємодії в сфері хмарних обчислень

Суб`єкти	NIST	ГОСТ	ISO	CSA
Cloud Consumer	+	+	+	+
Cloud Provider	+	+	+	+
Cloud Auditor	+			+
Cloud Broker	+			
Cloud Partner			+	

Ще одним напрямком аналізу зазначених стандартів було виділення та інтеграція методів захисту інформації в сфері хмарних обчислень. На основі цього можна зробити висновок, що найбільш цим методам відповідають стандарти ISO та проект ГОСТ [38]. Тобто для подальшого удосконалення та розвитку вітчизняної нормативно-правової бази у сфері захисту інформації в хмарних обчисленнях можна брати за основу стандарти ISO та проект ГОСТ, з врахуванням особливостей зазначених у інших стандартах.

Таблиця 2.4

Методи захисту інформації в сфері хмарних обчислень

Методи	NIST	ISO	ГОСТ	CSA
Криптографічні методи		+	+	
Управління кіберінцидентами	+	+	+	
Управління ідентифікацією	+	+	+	+
Системи управління інформаційною безпекою	+	+	+	
Оцінка інформаційної безпеки IT-систем		+		+
Мережева інформаційна безпека				
Автоматизований і неперервний моніторинг інформаційної безпеки				
Гарантований супровід програмного забезпечення				
Управління ризиками				
Система інженерії інформаційноїбезпеки				

Одним з напрямом вирішення завдання створення захищених дата-центрів є їх створення на основі використання хмарних технологій. Прогалини вітчизняної нормативно-правової бази у сфері захисту інформації в хмарних обчисленнях вимагають перегляду й аналізу національних й міжнародних інституцій й об’єднань, які займаються проблематикою стандартизації й розвитку хмарних технологій. Виявляється багато органів стандартизації й їх вплив на розвиток хмарних технологій взагалі, й на проблематику захисту хмарних обчислень зокрема. Наведені стандарти різняться щодо повноти опису моделі послуг хмарних обчислень, хоча можна виділити три основні моделі послуг (IaaS, PaaS, SaaS) які зазначені в кожному стандарті. Також наведені в стандартах суб'єкти взаємодії в сфері хмарних обчислень мають різні обов’язки посередництва між двома схожими за функціями в різних стандартах суб’єктами

(Cloud Consumer і Cloud Provider).

Отже, використання хмарних технологій значно розширює можливості е-документообігу, забезпечуючи мобільність, масштабованість та доступність. Однак хмарні сервіси вимагають особливої уваги до питань захисту даних через загрози витоку, уразливість хмарної інфраструктури та залежність від провайдерів. Важливим є вибір перевірених постачальників послуг і впровадження технологій шифрування та резервного копіювання.

РОЗДІЛ 3. ПРАКТИЧНЕ ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ БЕЗПЕКИ Е-ДОКУМЕНТООБІГУ НА ПІДПРИЄМСТВІ

3.1. Аналіз поточного стану безпеки е-документообігу на підприємстві

В умовах цифрової трансформації та зростання обсягу електронних документів, що циркулюють у підприємствах, забезпечення безпеки е-документообігу стає надзвичайно важливим завданням. Е-документообіг спрощує бізнес-процеси, зменшує час обробки інформації та підвищує ефективність роботи, проте разом з цим виникають нові загрози, які потребують відповідних заходів безпеки.

Сучасний стан електронного документообігу в Україні має важливе значення для ефективності державних та приватних установ. Підприємства, як суб’єкти економічної діяльності, стикаються з необхідністю надавати регулярні звіти до відповідних державних органів. Традиційна паперова форма звітності, крім значних затрат часу, також незручна в обігу, що підштовхує до пошуку більш ефективних рішень [40].

Наразі в Україні існують два альтернативні підходи до автоматизації завдань документообігу в державних органах: послідовна реалізація окремих програм, які автоматизують конкретні ділянки управління документообігу, та впровадження платформи для реалізації комплексної системи автоматизації документообігу та управління процесами. Перший підхід характеризується фіксованою функціональністю, такою як реєстрація документів та контроль за їх виконанням, і має відносно низьку вартість та швидкий ефект від впровадження. Другий підхід передбачає створення модулів, інтегрованих в єдиний комплекс, що дозволяє комплексно вирішувати завдання автоматизації [38, с. 10].

Стан електронного документообігу в Україні оцінюється через призму принципів побудови та функціонування, а також через критерії ефективності, що визначають успішність впровадження цих систем у державному секторі.

Принципи побудови «електронного документообігу» засновані на інтеграції сучасних інформаційно-технологічних рішень, що дозволяють ефективно управляти великими обсягами даних. Системи електронного документообігу мають бути спроектовані таким чином, щоб забезпечувати високий рівень контролю, гнучкість у зв'язках між різними відомствами, а також мінімізувати зміни в системі, що допомагає уникнути частих переконфігурацій і налаштувань.

Ключові критерії ефективності системи електронного документообігу можна розділити на кілька аспектів [37]:

1) організаційний аспект вимагає від системи забезпечення рівня контролю, який дозволяє відстежувати весь життєвий цикл документа від створення до архівування;

2) інформаційний аспект підкреслює важливість інтеграції даних між різними відомствами та забезпечення доступу до них у локальному режимі, що забезпечує високий рівень відповідності до сучасних IT-стандартів;

3) Алгоритмічний аспект ставить вимоги до систем, щоб їх алгоритми функціонування відповідали міжнародним стандартам і рекомендаціям, особливо в управлінні базами даних;

4) Техніко-технологічний аспект включає забезпечення системи необхідними технічними ресурсами для гарантування її взаємозамінності та резервування, а також розширення програмно-технічних засобів для підтримки всіх діловодних процесів.

Для електронних документів важливими є такі критерії, як правомірність, достовірність, лаконічність, оперативність, інформативність та доказовість. Вони допомагають гарантувати, що документи можуть слугувати надійною юридичною основою для рішень і процесів.

Основними викликами для розвитку електронного документообігу є забезпечення системного підходу, контрольованості, безперервності та безпеки обробки та зберігання даних. Важливо також врахувати потреби у раціональному та функціонально цільовому спрямуванні систем для забезпечення їхньої ефективності та відповідності потребам державного управління [25, с. 4].

Основними принципами, за якими працюють системи електронного документообігу, є однократна реєстрація документів для їх однозначної ідентифікації у будь-якій інсталяції системи, забезпечення паралельного виконання операцій для скорочення часу руху документів, безперервність руху документа, єдина або погоджено розподілена база документної інформації, що виключає дублювання документів, а також розвинута система пошуку і звітності по документах.

Ці принципи сприяють підвищенню оперативності та контрольованості документообігу в державних органах, дозволяючи приймати управлінські рішення на основі повної та достовірної документованої інформації. Наразі в Україні функціонують різноманітні пропрієтарні системи електронного документообігу, такі як АСКОД, Megapolis. Документообіг, Вчасно.ЕДО, OPTIMA-WorkFlow. Ці системи по-різному використовуються в державних органах та інших установах, що демонструє варіативність та адаптивність технологічних рішень у сфері електронного документообігу [49].

Ефективність управління державними органами в сучасних умовах суттєво залежить від якості та швидкості обробки документів, що забезпечується завдяки впровадженню електронного документообігу. Ці системи не тільки покращують культуру діловодства та сприяють економії коштів, але й забезпечують високу швидкість обробки та точність управлінських рішень, враховуючи сучасні вимоги до швидкості та безпеки інформаційних процесів [41].

В державних органах для роботи з електронними документами використовується програмне забезпечення, яке варіюється залежно від розмірів органу, структури, кількості працівників, обсягу документообігу та фінансових ресурсів. Організація документообігу в державних органах реалізується за допомогою системи електронного документообігу, яка інтегрується з системою взаємодії, дозволяючи передавати електронні документи та їх копії та взаємодіяти з іншими системами електронного документообігу. Впровадження електронного документообігу полегшує обробку документів та прискорює обмін інформацією. Однак це вимагає матеріальних витрат на комп’ютерне обладнання

та програмне забезпечення. Втрати можуть бути компенсовані зменшенням витрат на зберігання паперових документів і оптимізацією роботи з документами. Ключовим аспектом у цій сфері є розробка та впровадження системи інформаційної безпеки, яка забезпечує захист важливих даних і ресурсів від вторгнень, витоків та пошкоджень. Це включає використання сучасних методів шифрування, контролю доступу, систем аутентифікації та авторизації користувачів, а також здійснення резервного копіювання та відновлення даних [28, с. 89].

Система електронного документообігу АСКОД активно використовується в таких державних установах і організаціях України, як Міністерство фінансів України, Національний банк України, Міністерство оборони України, «Укренерго», територіальних громадах та ін [41]. Ця система допомагає цим організаціям в автоматизації обробки документів, забезпечуючи високий рівень безпеки та оперативності обігу інформації. Особливо цінним вона є для державних установ, де потреба в швидкому доступі до актуальної інформації та її збереження є критичною [1]. Так, Луцька міська рада у 2018 р. також розпочала реєстрацію документів в системі електронного документообігу «АСКОД» з одночасним опрацюванням їх в паперовому вигляді [41].

Система електронного документообігу FossDoc [10] , у свою чергу, знайшла застосування у таких фінансових установах, як «АКТАБАНК» та «Мегабанк», а також у таких відомствах як Служба зовнішньої розвідки України. Крім того, вона широко використовується в ряді обласних державних адміністрацій, включаючи Закарпатську, Чернігівську та Сумську, а також в освітніх і енергетичних організаціях, наприклад, Харківський національний автомобільно-дорожній університет та ТОВ «Прикарпатенерготрейд». Використання системи FossDoc дозволяє забезпечувати ефективний обмін інформацією та підвищувати рівень управлінської ефективності завдяки цифровій трансформації процесів [10].

Україна робить кроки у впровадженні електронного документообігу, виходячи з потреби оптимізувати обмін документами між державними

структурами та громадянами. Так, за допомогою Тимчасового регламенту обміну електронними документами, учасники цивільного процесу можуть ефективно ідентифікувати, стежити та отримувати інформацію про дату, час і місце розгляду справ, що значно спрощує комунікацію та знижує ризик втрати важливих повідомлень.

Значні кроки було зроблено з впровадженням проекту «Електронний суд», що включає автоматизацію судових процесів. Ця ініціатива дозволила значно зменшити часові та фінансові витрати на адміністративні процедури і забезпечила швидший перегляд та обробку судових документів, підвищивши тим самим загальну ефективність судової системи [45].

Процес впровадження електронного документообігу важливий для реалізації програми «Електронний уряд», який покращує якість надання державних послуг та забезпечує прозорість взаємовідносин між громадянами та державою. Введення в дію законодавства щодо електронного документообігу відповідає за розвиток та нормативно-правове забезпечення обігу, створення, передавання, та зберігання електронних документів [29, с. 231].

В умовах сучасного освітнього середовища, електронний документообіг виступає як ключовий елемент інформаційної системи управління, інтегруючи основні ділові процеси організації та перетворюючи їх у рамки комп’ютерних технологій. Завданням автоматизації електронного документообігу в таких установах є створення єдиної бази документальної інформації, що дозволяє уникнути дублювання документів та забезпечує ефективне управління документацією на всіх етапах її обігу. Важливо відзначити позитивні зміни в українських університетах, такі як збільшення прозорості адміністративних процесів та підвищення доступності інформації для студентів та викладачів завдяки цифровій трансформації. Застосування сучасних інформаційних систем сприяє не тільки швидшому і точнішому доступу до документів, але й значно підвищує ефективність виконавчих процесів, дозволяючи установам краще реагувати на зміни в освітньому та науковому середовищах [4].

Сучасний стан електронного документообігу в Україні демонструє значний прогрес у спрощенні та оптимізації управлінських процесів, зокрема у державних та приватних структурах, що виражається у зменшенні часу та ресурсів, витрачених на документообіг. Однак, не дивлячись на значні кроки уперед, існують певні виклики, що вимагають уваги і вирішення.

У контексті державного управління, альтернативні підходи до автоматизації документообігу – послідовне впровадження окремих програм та розвиток інтегрованих платформ – відіграють критичну роль у формуванні ефективної системи управління. Важливо підкреслити, що більш комплексний підхід, який включає створення модульних систем, може краще задовольнити потреби сучасного управління завдяки гнучкості і масштабованості, хоча й вимагає більших початкових інвестицій та зусиль для імплементації.

Принципи та критерії, що стоять за успішною реалізацією систем електронного документообігу, забезпечують не тільки технічне втілення, але й стратегічне розуміння потреб управління документами. Інтеграція даних, контроль за документацією від її створення до архівації, та впровадження алгоритмів, що відповідають міжнародним стандартам, важливі для підвищення загальної ефективності системи.

Неочевидним, але значущим аспектом в удосконаленні електронного документообігу є зосередження на культурі діловодства. Відходження від паперових процесів не лише спрощує обробку інформації, але й сприяє формуванню нових навичок і звичок серед співробітників, підвищуючи їхню продуктивність і залученість. Ця культурна трансформація також спонукає організації до переосмислення і оптимізації своїх внутрішніх процесів.

Окрему увагу варто приділити позитивним змінам в університетському середовищі, де електронний документообіг стає невід’ємною частиною академічного та адміністративного управління [8, с. 150]. Цифрова трансформація в освітніх інституціях не тільки спрощує обмін інформацією між студентами та викладачами, але й відкриває нові можливості для проведення досліджень, оцінювання та адміністрування [2].

Одним з ключових аспектів безпеки е-документообігу є інфраструктура, на якій він базується. Сучасні підприємства використовують потужні сервери, надійні мережеві пристрої та ефективні сховища даних. Застосування хмарних сервісів для зберігання та обробки документів надає гнучкість та масштабованість, проте вимагає додаткових заходів безпеки для захисту інформації в хмарі. Одним з таких заходів є шифрування даних як у стані спокою, так і під час передачі. Це забезпечує конфіденційність та цілісність інформації, а також використання цифрових підписів для автентифікації документів.

Ефективне управління доступом є критично важливим для захисту е-документообігу. На підприємстві повинні бути впроваджені політики доступу, що визначаються відповідно до ролей та обов'язків користувачів. Системи управління ідентифікацією та доступом (IAM) дозволяють контролювати доступ до документів і забезпечують багатофакторну аутентифікацію (МФА) для підвищення рівня безпеки. Регулярне оновлення паролів та контроль за їх складністю також є важливими заходами для запобігання несанкціонованому доступу [7].

Системи моніторингу та виявлення загроз дозволяють підприємству своєчасно виявляти та реагувати на потенційні загрози. Моніторинг мережевого трафіку та активності користувачів допомагає виявляти підозрілі дії та аномалії. Інструменти для аналізу логів та подій (SIEM-системи) дозволяють детально аналізувати безпекові інциденти. Системи виявлення та запобігання вторгнень (IDS/IPS) забезпечують додатковий рівень захисту, блокуючи неавторизовані спроби доступу та інші загрози.

На підприємстві повинні бути впроваджені засоби захисту від шкідливого програмного забезпечення. Це включає використання антивірусних програм, фільтрів електронної пошти для блокування фішингових та шкідливих листів, а також брандмауерів для захисту мережі. Запроваджені політики безпеки допомагають захиститися від внутрішніх загроз, включаючи контроль за діями співробітників.

Регулярна оцінка ризиків та вразливостей дозволяє підприємству ідентифікувати та мінімізувати потенційні загрози. Аналіз впливу загроз на бізнес-процеси допомагає розробити ефективні стратегії управління ризиками. Планування та тестування процедур реагування на інциденти забезпечують готовність до швидкого відновлення після збоїв.

Безпека е-документообігу залежить не тільки від технологій, але й від обізнаності співробітників. Регулярні тренінги з інформаційної безпеки допомагають підвищити рівень знань працівників про актуальні загрози та методи їх уникнення. Проведення симуляцій та тестів підвищує готовність співробітників до реальних інцидентів [11].

Отже, аналіз поточного стану безпеки е-документообігу на підприємстві показує, що впровадження сучасних технологій та методів захисту є необхідним для мінімізації ризиків та забезпечення надійного захисту інформації. Регулярні аудити безпеки, оновлення систем захисту, навчання співробітників та впровадження ефективних політик безпеки дозволять підприємству захистити свої електронні документи від загроз та забезпечити безперебійну роботу бізнес-процесів.

Отже, багато підприємств недооцінюють важливість регулярного тестування безпеки своїх систем, що створює ризики для конфіденційності даних та їх доступності.

3.2. Пропозиції щодо вдосконалення системи управління безпекою е-документообігу

Електронний документообіг відіграє ключову роль у цифровізації державних послуг. Він надає значні переваги у швидкості, доступності та зменшенні обсягу паперового обігу. Однак, ці системи також зустрічають виклики, які можуть стримувати їхнє використання та розвиток.

Переваги електронного документообігу електронний документообіг забезпечує значні переваги у швидкості пошуку та обробки документів, знижуючи витрати часу на обробку на 48%, та на пошук документів на 80- 85%.

Це також включає економію місця та вартості, оскільки створення та розсилка копій є майже безкоштовними, а електронні документи можуть бути доступні відразу в багатьох місцях.

Основною організаційною перешкодою у впровадженні електронного документообігу є недостатня готовність персоналу до змін і вивчення нових технологій. Будь-яка, навіть найдосконаліша, система залежить від людей, які її використовують. Співробітники часто негативно ставляться до нововведень через небажання освоювати нові технології. Критично важливим є проведення досліджень як внутрішніх факторів – швидкості пошуку та обробки документів, так і зовнішніх – соціального прийняття системи користувачами [7].

На ринку існує багато комерційних систем електронного документообігу, але більшість з них фокусуються на функціоналі, ігноруючи зручність користувачів. Інтуїтивно зрозумілий інтерфейс може значно спростити процес впровадження та щоденне використання системи, але сам по собі він не вирішує проблему страху перед прозорістю діяльності. Консервативність персоналу та небажання підвищення прозорості своєї діяльності можуть стати суттєвими бар'єрами для впровадження системи електронного документообігу.

Технічні перешкоди включають несумісність з застарілим обладнанням, що веде до технічних збоїв, помилок, і зниження продуктивності. Великі витрати на оновлення і підтримку, а також відсутність фінансування та кваліфікованих фахівців є серйозними викликами для удосконалення та підтримки електронних систем [43].

Зростання кіберзагроз, таких як несанкціонований доступ, вірусні атаки, і витоки даних, ставить під загрозу безпеку інформації в системах електронного документообігу. Необхідно розробляти безпечні системи, проводити регулярні аудити та застосовувати сучасні досягнення в криптографії для забезпечення безпеки [43].

Хакерські атаки на системи електронного документообігу стають все більш звичним явищем, особливо в умовах військових конфліктів, де інформаційна безпека має критичне значення. Одним з прикладів є кібератака

на урядові установи України на початку 2022 року, коли хакери застосували методики DDoS (Distributed Denial of Service) для того, щоб заблокувати доступ до електронних сервісів, в тому числі до систем електронного документообігу. Це призвело до тимчасової неможливості доступу до критично важливої документації та сповільнило роботу державних органів [41].

Ще один поширений приклад – атака за допомогою шкідливого програмного забезпечення, що цілить у мережу установи, яка використовує системи електронного документообігу. Хакер розповсюджує вірус через електронні листи, який шифрує дані на серверах, вимагаючи викуп за їхнє розшифрування. Це не тільки порушує нормальний документообіг, але й загрожує втратою важливих даних [46].

Ці приклади підкреслюють необхідність забезпечення посиленого захисту систем електронного документообігу, особливо в умовах війни.
Важливими кроками є впровадження багаторівневої системи захисту, яка включає застосування сучасних антивірусних рішень, регулярне оновлення програмного забезпечення та використання криптографічних методів для захисту даних. Також критично важливим є навчання персоналу методам розпізнавання фішингових атак та інших типів кіберзагроз. Впровадження комплексних стратегій кібербезпеки допоможе знизити ризики і забезпечити стабільність роботи установ, що використовують системи електронного документообігу в умовах збільшення кіберзагроз.

Системи електронного документообігу пропонують значні можливості для оптимізації діяльності установ. Однак, для повноцінного використання їх потенціалу необхідно вирішити існуючі організаційні, технічні, юридичні та безпекові виклики через комплексний підхід, який включає технологічне оновлення.

О. Лаба у своїй статті зазначає, що електронне діловодство сьогодення має певні недоліки. Серед основних проблем було виокремлено неузгодженість стандартів і технічних регламентів щодо електронних документів [28, с. 89].

Крім того, була відзначена відсутність автоматизованих засобів для

забезпечення уніфікованого виконання документаційних процесів, властивих документам в електронній формі, як-от технічна перевірка, конвертування, інкапсуляція. Також бракує нормативно-правового та нормативного забезпечення щодо співіснування паперового та електронного документообігу та передавання електронних документів до державних архівів на постійне зберігання [24, с. 89].

У своєму дослідженні В. Третяк виявляє, що перехід на автоматизовану форму обліку документів вимагає уважного розгляду існуючих недоліків та викликів, які можуть залишитися актуальними навіть після впровадження бухгалтерських комп'ютерних програм. На практиці часто виникає проблема з автоматичним оформленням первинних документів у електронній формі, що пов'язано з різницею у стандартах та програмному забезпеченні між учасниками документообігу. Така ситуація вимагає додаткових кроків для переведення паперових документів у електронний формат.

Ще однією істотною проблемою є оптичне введення та обробка документів, де важливо використовувати ефективні програми для обробки сканованих документів та розробляти оптимальні уніфіковані форми, які дозволять швидку обробку після сканування. Крім того, автор звертає увагу на необхідність контролю доступу та захисту документів, щоб запобігти несанкціонованим змінам та забезпечити належний рівень безпеки документації в електронному архіві [40, с. 161-163]

Удосконалення системи електронного документообігу є ключовим аспектом для оптимізації діяльності сучасних підприємств. Важливим є впровадження ефективних процесів створення, обробки та зберігання документів. У рамках удосконалення, важливо зменшити кількість інстанцій, через які проходить кожен документ, скоротити час на їх обіг та впровадити централізовану обробку схожих операцій.

Один із способів удосконалення – це впровадження комплексного електронного документообігу, який включає всі етапи від створення до зберігання документів які можуть істотно скоротити фізичний обсяг архівів,

забезпечуючи легкий доступ до інформації та її захист [31, с. 58].

Інноваційні технології для зберігання документів включають ряд рішень, які покращують ефективність та безпеку архівування документів. Ось декілька прикладів таких технологій:

1) хмарне зберігання: використання хмарних сервісів для зберігання документів дозволяє забезпечити гнучкий доступ до документації з будь-якого місця та пристрою, що підключений до інтернету. Це також забезпечує кращу масштабованість та стійкість системи;

2) розподілені файли системи: системи, такі як blockchain, дозволяють зберігати документи в розподіленому реєстрі, забезпечуючи високий рівень безпеки та цілісності даних завдяки криптографії [2];

3) електронні архіви з повним текстовим пошуком: ці системи дозволяють не тільки зберігати, але й швидко знаходити потрібні документи за допомогою пошуку за ключовими словами, що значно спрощує управління документами;

4) автоматизація метаданих: системи можуть автоматично генерувати метадані для документів, що полегшує їх класифікацію та управління;

5) системи управління документами: ці системи інтегрують різні аспекти управління документами, включаючи створення, зберігання, архівацію та знищення, забезпечуючи комплексне управління документацією на всіх етапах її життєвого циклу;

6) віртуальні кімнати даних: застосовуються переважно для забезпечення безпеки при обміні конфіденційною інформацією між підприємствами під час великих угод;

7) комплексна інтеграція з бізнес- процесами: забезпечення тісної інтеграції системи зберігання документів з іншими бізнес-процесами та системами підприємства для автоматизації та підвищення ефективності обробки документів.

Для подальшого удосконалення системи електронного документообігу, установам важливо зосередити увагу на інтеграції сучасних інформаційних технологій, які можуть значно поліпшити автоматизацію процесів і безпеку

даних. Використання хмарних рішень для зберігання документів дозволяє забезпечити легкий доступ до них з будь-якого місця та з будь-якого пристрою, що значно збільшує гнучкість робочих процесів і сприяє швидшому реагуванню на зміни умов роботи.

Сьогодні одним із ключових трендів є розвиток штучного інтелекту та машинного навчання. Системи штучного інтелекту можуть суттєво спростити та автоматизувати процес обробки електронних документів (класифікація документів, збір даних та їх аналіз за заданими параметрами, ухвалення рішень на основі великих обсягів даних тощо), допомогти виявляти та усувати помилки [44, с. 39].

Розвиток мобільних застосунків для систем електронного документообігу становить значущий прогресивний напрям. Використання мобільних технологій дозволяє співробітникам оперативно доступатися до документів та управляти ними з будь-якого місця та в будь-який час, сприяючи значному збереженню часу. Завдяки мобільним рішенням процеси оформлення, підпису, перегляду документів, а також термінова відправка іншим співробітникам та партнерам стають швидшими і не залежать від стаціонарного робочого місця. Це особливо важливо в умовах сучасних викликів, які ставить війна, забезпечуючи підвищену ефективність взаємодії та прийняття рішень [44, с. 40].

Крім того, застосування розширених функцій безпеки, таких як біометрична ідентифікація і двофакторна аутентифікація, може значно знизити ризики несанкціонованого доступу до важливої інформації, збільшуючи в цілому рівень довіри до системи електронного документообігу. Також, важливим аспектом удосконалення системи є забезпечення високої масштабованості та модульності системи, що дозволить легко адаптувати її до мінливих потреб організації і зростаючих обсягів даних без втрати продуктивності.

Зосередившись на цих напрямах, можна значно підвищити ефективність системи електронного документообігу та забезпечити більш ефективне і безпечне управління документацією в організації [19].

Для удосконалення системи електронного документообігу в контексті

розвитку цифрового урядування та електронної демократії в Україні, акцентується увага на ряд стратегічних завдань. Впорядкування адміністративних процедур та стандартизація розпорядчих документів є критичними для забезпечення однорідності та ефективності управління документацією. Важливо також встановити політику зберігання документів, яка визначає умови зберігання паперових та електронних документів, забезпечуючи їх довгострокове зберігання та доступність.

Організація інформаційної взаємодії на базі електронного документообігу з використанням кваліфікованого електронного підпису має важливе значення для функціональної інтеграції ресурсів державних органів. Це дозволяє ефективно координувати використання стандартів документообігу на всіх рівнях взаємодії та розвивати організаційно-адміністративні механізми для управління розвитком інфраструктури електронного документообігу.

Суттєвим аспектом є також забезпечення інформаційної безпеки системи електронного документообігу на всіх рівнях управління. Це передбачає розробку стратегій розвитку інфраструктури, включаючи технологічне, правове та організаційне забезпечення. Ключовими елементами є оцінка часових та ресурсних показників розвитку, вибір стандартів обміну інформацією та реалізація координованого підходу до використання цих стандартів.

Загалом, впровадження системи електронної обробки документів в управлінні сприяє скороченню термінів підготовки та виконання документів, автоматизації підтримки актуального стану нормативних баз, скороченню рутинних операцій і зосередженню на змістовних завданнях управління, а також підвищенню якості управлінських рішень та зменшенню числа втрачених документів [21].

Перехід до модернізації систем електронного документообігу можливий шляхом замовлення послуг у зовнішніх розробників або використанням внутрішніх ресурсів. Проте, замовлення зовнішніх розробок може призвести до залежності від третіх сторін та потенційного припинення співпраці, якщо фірма-розробник припинить своє існування. Також це може призвести до високих

витрат на обслуговування та модернізацію.

Установам доцільніше вести модернізацію власними силами, що дозволить повністю контролювати весь процес розроблення та економічно вигідніший в довгостроковій перспективі [30].

Удосконалення системи електронного документообігу є важливим елементом підвищення ефективності управління і оптимізації бізнес-процесів сучасних підприємств і державних установ. Впровадження комплексних рішень, які включають створення, обробку та зберігання документів із використанням сучасних технологій, таких як електронний підпис та хмарні рішення, може значно зменшити час на документообіг та підвищити юридичну значимість та цілісність документів. Інноваційні методи зберігання документів, такі як блокчейн та системи з повним текстовим пошуком, дозволяють забезпечити високий рівень безпеки та доступність інформації. Окрім того, інтеграція цих технологій із загальними бізнес-процесами компанії може поліпшити управління документацією та забезпечити комплексний контроль за всіма етапами її життєвого циклу.

Подальше удосконалення системи електронного документообігу має включати розвиток автоматизації процесів, впровадження штучного інтелекту для аналізу даних та використання передових функцій безпеки для захисту інформації. Зосередження зусиль на цих напрямках дозволить не тільки спростити робочі процеси, але й забезпечити їх прозорість і підвищити загальну продуктивність та ефективність діяльності організацій. Врахування змін у законодавстві та технічному прогресі є ключовим для забезпечення гнучкості та масштабованості системи, що в свою чергу сприятиме більш гладкому переходу до повністю автоматизованого документообігу в майбутньому.

Отже, необхідно впровадити багаторівневу модель безпеки, що буде включати оновлення програмного забезпечення, навчання персоналу з основ інформаційної безпеки, запровадити автоматизовані системи моніторингу та використання сучасних стандартів шифрування.

ВИСНОВКИ

У магістерській кваліфікаційній роботі на тему «Можливості інформаційних технологій в системі управління безпекою е-документообігу на підприємстві» було проведено комплексне дослідження актуальних аспектів впровадження та використання інформаційних технологій для забезпечення безпеки електронного документообігу. Отже, проведене дослідження дозволило дійти таких висновків:

1. У ході вивчення теоретичних основ електронного документообігу встановлено, що ця система є ключовим елементом сучасного підприємства, сприяючи автоматизації бізнес-процесів, підвищенню продуктивності праці та зменшенню витрат. Е-документообіг дозволяє підприємствам ефективніше організовувати обробку, зберігання та передачу інформації, що сприяє досягненню стратегічних цілей. Водночас було визначено основні вимоги до безпеки таких систем: конфіденційність, цілісність, доступність даних та їх захист від несанкціонованого доступу.

2. Проведений аналіз загроз показав, що електронний документообіг є вразливим до кіберзлочинів, які включають крадіжку даних, витоки інформації, несанкціонований доступ до системи, зловмисне втручання та атаки на інфраструктуру. Також важливим фактором є людський фактор, який може спричинити випадкові помилки чи ненавмисне розголошення інформації. Ці ризики вимагають комплексного підходу до їх виявлення та мінімізації.

3. Сучасні принципи забезпечення безпеки е-документообігу базуються на системності, багаторівневому захисті та дотриманні міжнародних стандартів інформаційної безпеки. Виявлено, що ефективна система безпеки повинна включати ідентифікацію користувачів, регулярний моніторинг, політику управління доступом, а також періодичну оцінку ризиків. Методології, які застосовуються, включають моделі загроз, системи управління ризиками та адаптацію до змінюваних умов.

4. Аналіз показав, що шифрування даних, цифрові підписи, технології аутентифікації та авторизації є основними інструментами для забезпечення

захисту е-документообігу. Зокрема, асиметричне шифрування дозволяє захистити інформацію під час передачі, а цифрові підписи забезпечують перевірку цілісності документів і їх автентичності. Інтеграція таких технологій значно знижує ризики втрати даних та несанкціонованого доступу.

5. Системи моніторингу та виявлення загроз забезпечують своєчасне виявлення спроб зловмисного впливу, несанкціонованих доступів чи інших загроз. Дослідження показало, що інтеграція IDS/IPS у системи е-документообігу дозволяє підвищити безпеку шляхом проактивного реагування на потенційні ризики. Такі системи ефективні для запобігання DDOS-атак, сканування вразливостей та фішингових загроз.

6. Використання хмарних технологій значно розширює можливості е-документообігу, забезпечуючи мобільність, масштабованість та доступність. Однак хмарні сервіси вимагають особливої уваги до питань захисту даних через загрози витоку, уразливість хмарної інфраструктури та залежність від провайдерів. Важливим є вибір перевірених постачальників послуг і впровадження технологій шифрування та резервного копіювання.

7. Проведений аналіз показав наявність слабких місць у системах управління доступом, недостатній рівень моніторингу та відсутність чітких процедур реагування на інциденти. Виявлено, що багато підприємств недооцінюють важливість регулярного тестування безпеки своїх систем, що створює ризики для конфіденційності даних та їх доступності.

8. На основі дослідження запропоновано впровадити багаторівневу модель безпеки, яка включає оновлення програмного забезпечення, навчання персоналу з основ інформаційної безпеки, впровадження автоматизованих систем моніторингу та використання сучасних стандартів шифрування.

9. Розроблено пропозиції щодо інтеграції інноваційних технологій, таких як блокчейн для збереження цілісності документів, машинне навчання для виявлення аномалій у поведінці користувачів та багатофакторна аутентифікація. Реалізація цих заходів сприятиме зниженню ризиків і підвищенню надійності системи.

ПЕРЕЛІК ПОСИЛАНЬ

1. Бєліх І.В. Повна функція публічного управління в аспекті прояву фундаментальних сил природи. *Держава та регіони. Серія «Державне управління»*. 2021. № 1 (71) С. 6–12.

2. Блокчейн як фактор цифрової трансформації економіки України. *Вісник СумДУ. Серія «Економіка».* 2021. № 2. С. 18–20.

3. Вернигора А. Як бізнесу обмінюватися документами швидше і зручніше: навіщо потрібен єдиний стандарт ЕДО. URL: https://blog.liga.net/user/avernyhora/article/40708 (дата звернення: 22.11.2024).

4. Виадук Телеком. Віадук-Телеком. Розробка документоорієнтованих баз даних. URL: https://www.viaduk.net/viaduk/web5ua.nsf/0/ACC6E5C6C0A30BD9C225726F0051E265 (дата звернення: 17.12.2024).

5. Гарбич-Мошора О. Електронний документообіг у закладах вищої освіти, тенденції та перспективи. *Молодь і ринок.* 2018. Т. 9, № 164. С. 82–83.

6. Герасим О. Р., Чирун Л. Б. Аналіз засобів управління корпоративною конфіденційною інформацією. *Інформаційні системи та мережі.* 2014. № 805. С. 122–123.

7. Деякі питання документування управлінської діяльності : Постанова Кабінету Міністрів України від 17.01.2018 р. № 55 . URL: https://zakon.rada.gov.ua/laws/show/55-2018-п#Text (дата звернення: 16.11.2024).

8. Діхтяренко О. В. Проблеми і перспективи стану сучасного документообігу та діловодства. *Управління розвитком складних систем.* 2013. № 13. С. 149–151.

9. Електронний документообіг в умовах війни: як роботодавцю організувати процес підписання кадрових документів на підприємстві. *Кадровик.ua. головний кадровий журнал України*. URL: http://surl.li/hsidt (дата звернення: 27.09.2024).

10. Електронний документообіг FossDoc. Foss-On-Line. *Інформаційні системи для автоматизації бізнесу*. URL: https://foss.ua/sed-fossdoc-uk/ (дата

звернення: 19.10.2024).

11. Електронний документообіг: види систем та їхні функції. Deals – майбутнє документообігу. URL: https://dealssign.com/blog/elektronnij-dokumentoobig-vidi-sistem-ta-yixni-funkciyi/ (дата звернення: 11.12.2024).

12. Електронний документообіг: можливості та переваги. URL: https://intelserv.net.ua/news/material/id/529 (дата звернення: 16.12.2024).

13. Електронний документообіг: що треба знати. Deals – майбутнє документообігу. URL: https://dealssign.com/blog/elektronnij-dokumentoobig- shho-treba-znati/ (дата звернення: 12.11.2024).

14. Етапи впровадження системи електронного документообігу. Wiki TNEU. URL: http://wiki.tneu.edu.ua/index.php/Етапи_впровадження_системи_електро нного_документообігу (дата звернення: 27.09.2024).

15. Етапи переходу до електронного документообігу в організаціях. URL: https://kvpubd.kiev.ua/wp-content/uploads/2024/09/urok-37.pdf (дата звернення: 09.10.2024).

16. Закон України «Про електронні документи та електронний документообіг». *Верховна Рада України.* URL: http://zakon0.rada.gov.ua/laws/show/851-15 (дата звернення: 21.10.2024).

17. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» *Верховна Рада України* URL:http://zakon3.rada.gov.ua/laws/show/852-15 (дата звернення: 21.10.2024) .

18. Закон України «Про інформацію». *Верховна Рада України.* URL: http://zakon2.rada.gov.ua/laws/show/2657-12 (дата звернення: 21.10.2024).

19. Зелена А. Щодо електронного документообігу. *Юрист&Закон.* 2022. № 31. URL: https://uz.ligazakon.ua/ua/magazine_article/EA015950 (дата звернення: 17.12.2024).

20. Золотухін-Голубка Є. О., Мірзоян Р. Ю., Стояцький М. М. Досвід країн заходу в сфері правового регулювання електронного документообігу. *Вісник Київського національного університету технологій та дизайну. Серія*

«Економічні науки» : міжнар. наук.-практ. конф, м. Київ, 21–22 берез. 2018 р. 2018. С. 177–179.

21. ІПС ЛІГА:ЗАКОН – система пошуку, аналізу та моніторингу нормативно-правової бази. LIGA 360. URL: https://ips.ligazakon.net/document/view/MU01283?ed=2001_01_01 (дата звернення: 22.10.2024).

22. Каланча І. Міжнародний досвід використання електронного сегмента в кримінальній процесуальній діяльності суду. *Національний юридичний журнал: теорія і практика.* 2015. № 1. С. 224–227.

23. Касаткін Д. Ю., Касаткіна О. М. Організація електронного документообігу шляхом вдосконалення інформаційного забезпечення у вищому навчальному закладі. *Науковий вісник Національного університету біоресурсів і природокористування України*. 2015. С. 57–59.

24. Коротко про процедуру обміну первинними документами з контрагентами. URL: https://fredo. com.ua/help/pdocs_reestr_funkc_edo_kontr.htm (дата звернення: 20.09.2024).

25. Копняк К. В., Покиньчереда В. В. Електронний документообіг в публічному управлінні: проблеми впровадження, переваги та перспективи. *Державне управління: удосконалення та розвиток*. 2020. № 10. С. 3–8.

26. Корнієнко А. Ю. Захист інформації у системах електронного документообігу в епоху глобальної цифровізації. *Україна у світовому просторі: минуле і сучасність :* зб. мат. III Всеукр. наук.-практ. конф. студентів та аспірантів, м. Луцьк, 22 трав. 2024 р. Луцьк, 2024. С. 251.

27. Королюк Т. М., Мазуренок О. Р. Діджиталізація діяльності підприємств: тенденції, цифровий облік, перспективи. *Галицький економічний вісник.* 2021. Том 70. № 3. С. 59-70.

28. Лаба О. До проблем організації електронного діловодства в Україні. *Документознавство: історія, теорія, практика.* 2015. С. 89.

29. Лиско Н. А. Державне регулювання у сфері електронного документообігу в Україні. *Вісник соціально-економічних досліджень.* 2013. №

1. С. 231–234.

30. Мазниченко Н. І. Захист інформації в системах електронного документообігу на основі систем ідентифікації. *Комп'ютерне моделювання в наукоємних технологіях (КМНТ-2014)* : практ міжнар. наук.-техн. конф., м. Харків, 28–31 трав. 2014 р. С. 1–2.

31. Майстренко А. А. Нормативно-правове забезпечення електронного документообігу в Україні: інформаційно-аналітичний огляд. *Архіви України*. 2016. № 3/4 (302/303). С. 58–82.

32. Мізіна О., Вощенко В., Вдовіна О. Законодавче регулювання електронного документообігу в україні. *Наукові перспективи*. 2021. № 4 (10). URL: https://doi.org/10.52058/2708-7530-2021-4(10)-138-147 (дата звернення: 17.11.2024).

33. Новицький А. М. Електронний документообіг як елемент забезпечення правового регулювання становлення інститутів інформаційного суспільства. *Науковий вісник Національного університету ДПС України (економіка, право)*. 2013. Т. 4, № 63. С. 18–19.

34. Овсієнко А. С., Дубовчук М. В. Впровадження електронного документообігу в системі управління підприємством. *Економіка. Менеджмент. Бізнес*. № 1(44), 2024. ДУІКТ. С. 87-93. URL: https://journals.dut.edu.ua/index.php/emb/article/view/2933/2829 (дата звернення: 07.12.2024).

35. Овсієнко А.С. Проблеми надання електронних послуг через портал Дія. *Передові технології реалізації освітніх ініціатив***:** зб. наук. праць / наук. ред. А. М. Зленко. Переяслав (Київ. обл.): Домбровська Я. М., 2024. С. 126-129. URL: https://drive.google.com/file/d/1oOu-Z1J5ZOxPR1qvUCdH6dy-EUYqSRrN/view (дата звернення: 07.12.2024).

36. Олійченко І. М., Дітковська М. Ю. Шляхи формування та удосконалення електронного урядування в системі органів державної влади. *Вісник Чернігівського державного технологічного університету*. 2013. № 4. С. 480–482.

37. Остапенко Ю. І., Шипілова О. А., Ткаченко Ю. А. Інноваційні методи удосконалення документообігу на підприємстві. *Вісник СНТ ННІ бізнесу і менеджменту ХНТУСГ.* 2020. № 2. С. 65–67.

38. Петрович В., Надольська В., Чарікова І. Запровадження системи електронного документообігу в Україні: особливості законодавчого регулювання. *Актуальні питання гуманітарних наук.* 2024. Т. 3. № 72. С. 10-16.

39. Писаренко В. П. Міжнародний досвід і зарубіжне законодавство у сфері регулювання електронного документообігу та можливості його впровадження в електронній комерції. *Науковий вісник Полтавського університету економіки і торгівлі*. 2013. № 6. С. 42–46.

40. Пронь Н.О. Вимоги до електронних документів: міжнародна практика та досвід України. URL:http://nbuv.gov.ua/UJRN/znpnudps_2012_1_36 (дата звернення: 24.10.2024).

41. Про проходження документів у системі електронного документообігу «АСКОД». Офіційний сайт Луцької міської ради. URL: https://www.lutskrada.gov.ua/documents/pro-prokhodzhennia-dokumentiv- u-systemi-elektronnoho-dokumentoobihu-askod (дата звернення: 23.10.2024).

42. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 р. № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 11.11.2024).

43. Про затвердження Положення про Національний реєстр електронних інформаційних ресурсів : Постанова Кабінету Міністрів України від 17.03.2004 р. № 326. URL: https://zakon.rada.gov.ua/laws/show/326-2004- п#Text (дата звернення: 07.12.2024).

44. Радченко С. В. Особливості систем електронного документообігу у державних органах України. *Архіви України.* 2013. № 4. С. 39–53.

45. Рекомендації та резолюції Комітету Міністрів Ради Європи. Вища кваліфікаційна комісія суддів України. URL: https://www.vkksu.gov.ua/page/rekomendaciyi-ta-rezolyuciyi-komitetu- ministriv-rady-yevropy (дата звернення: 09.12.2024).

46. Система електронного документообігу «АСКОД». URL: http://infoplus.ua/ (дата звернення: 23.11.2024).

47. Система електронного документообігу «Док Проф» URL:http://docprof.com.ua/index.php/products/elektroniy-dokymentoobig/sistema-elektronnogo-dokumentoobigu (дата звернення: 11.11.2024).

48. Система електронного документообігу «M.E.Doc» URL:http://www.me-doc.com.ua/ (дата звернення: 23.11.2024).

49. Система електронного документообігу Optima-Workflow. URL:http://www.optima-ukraine.com.ua/ (дата звернення: 23.11.2024).

50. Система електронної взаємодії органів виконавчої влади (СЕВ ОВВ). ДП «ДІЯ». Державне підприємство «ДІЯ». URL: https://se.diia.gov.ua/sev-ovv (дата звернення: 09.12.2024).

51. Системи електронного документообігу для бізнесу. URL: https://ain.business/2021/05/28/5-edo-systems/(дата звернення: 23.11.2024).

52. Ситник І. П., Мельниченко А. І. Системи електронного документообігу в електронному бізнесі. *Науковий вісник Ужгородського національного університету.* 2015. № 4. С. 175–177.

53. Стратегія і тактика захисту інформації від несанкціонованого доступу. URL: http://um.co.ua/3/3-8/3-89070.html (дата звернення: 07.12.2024).

54. Третяк В. О. Проблеми електронного документообігу та шляхи їх усунення. *Ринкова трансформація економіки: стан, проблеми, перспективи* : II Всеукр. науково-практ. Інтернет-конф., м. Харків, 20 трав. 2011 р. Харків, 2011. С. 181–183.

55. Трофімук-Кирилова Т. М. Електронний документообіг: інновації та перспективні напрями розвитку. *Культура та інформаційне суспільство XXI століття :* матеріали міжнар. науково-теорет. конф. молодих уч., м. Харків, 18 квіт. 2024 р. Харків, 2024. С. 196–197.

56. Угриновська О. Електронний документообіг у цивільному процесі України. *Вісник Львівського університету*. 2017. № 64. С. 147–148.

57. Україна у світовому просторі: минуле і сучасність: зб. мат. III Всеукр.

наук.-практ. конф. студентів та аспірантів (м. Луцьк, 22 травня 2024 р.). Луцьк, 2024. 313 с.

58. Шабанова Я. Швидше, зручніше, ефективніше: як запроваджується електронний документообіг у громадах. *Громадський Простір.* URL: https://www.prostir.ua/?library=shvydshe-zruchnishe- efektyvnishe-yak-zaprovadzhujetsya-elektronnyj-dokumentoobih-u-hromadah (дата звернення: 07.12.2024).

59. Шимченко Л. Електронний документообіг як інноваційний механізм організації публічного адміністрування в умовах удосконалення децентралізацій них процесів, 2021. № 12. С. 294-311.

60. BAS Документообіг КОРП. URL: https://cbt.ua/product/bas-dokumentoobig-korp/ (дата звернення: 13.11.2024).

61. ISpro: workflow – ваш сучасний та надійний помічник в електронному документообороті. URL: https://ispro.ua/mobile/ispro- workflow (дата звернення: 04.04.2024). Megapolis.DocNet. InBASE. URL: https://www.inbase.com.ua/ua/soft/megapolis-docnet.html (дата звернення: 27.11.2024).