

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ФІЛОЛОГІЇ ТА МАСОВИХ КОМУНІКАЦІЙ
КАФЕДРА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ**

До захисту допустити:
Завідувач кафедри

(підпис) (ПІБ завідувача кафедри)
«__» _____ 20__ р.

**«Захист інформаційних процесів у діловодстві засобами програмного
забезпечення»**

Кваліфікаційна робота
здобувача вищої освіти другого
(магістерського) рівня вищої освіти
освітньо-професійної програми
«Інформаційна, бібліотечна та архівна
справа»
Петрової Анни Валеріївни
Науковий керівник:
Сивак Оксана Анатоліївна,
кандидат педагогічних наук, доцент кафе-
дри інформаційної діяльності
Рецензент:
Сирмамійх Ірина Вікторівна,
кандидат економічних наук

Кваліфікаційна робота захищена
з оцінкою _____
Секретар ЕК _____
«__» _____ 20__ р.

ЗМІСТ

ВСТУП	3
РОЗДІЛ 1. СТАН УПРОВАДЖЕННЯ ПРОБЛЕМ ЗАХИСТУ ІНФОРМАЦІЙНИХ ПРОЦЕСІВ У ДІЛОВОДСТВІ	8
1.1. Історіографічне та термінологічне дослідження	8
1.2. Нормативно-правове забезпечення захисту інформаційних процесів у діловодстві	17
Висновки до розділу 1	21
РОЗДІЛ 2. ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ ПРОЦЕСІВ	23
2.1. Огляд дійсного програмного забезпечення захисту інформаційних процесів	23
2.2. Розвиток програмного забезпечення захисту інформаційних процесів у діловодстві	27
Висновки до розділу 2	33
РОЗДІЛ 3. ЗАХИСТ ІНФОРМАЦІЙНИХ ПРОЦЕСІВ У ДІЛОВОДСТВІ ЗАСОБАМИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ	34
3.1. Порівняльна характеристика програмного забезпечення захисту інформаційних процесів	34
3.2. Здійснення захисту інформаційних процесів у Маріупольському державному університеті	43
Висновки до розділу 3	57
ВИСНОВКИ	59
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	63

ВСТУП

Нещодавно вагомо ускладнилися функції управління та збільшився обсяг завдань, що покладаються на органи державної влади, змінилися вимоги до якості документів. При цьому активно впроваджуються інформаційні технології як засіб автоматизації процесів, пов'язаних з документацією. Розвиток суспільних відносин став загалом вимогою до розвитку, удосконалення та оновлення нормативно-правової бази України, створення спеціальних правових норм і правил регулювання інформаційних відносин, тому в законодавстві з'явилися нові юридичні об'єкти – електронний документ та електронний цифровий підпис. На основі електронного документообігу розвиваються нові форми відносин.

Розвиток інформаційних технологій змінило ставлення до інформації та уявлення про можливі способи та методи освіти. Все більше навчальних закладів намагаються відповідати очікуванням студентів та пропонують сучасні та зручні методи отримання знань.

Але за новими технологіями прийшли нові загрози та небезпеки. І сучасна освіта – це не лише зручність, інтерактивність та автоматизація, а й безпека.

Проблема побудови світової системи захисту інформації пов'язана з появою першого інтернет-хробака Моріса у 1988 році в США. Саме тоді провідні фахівці з комп'ютерної безпеки зрозуміли необхідність комплексного підходу до забезпечення інформаційної безпеки та оголосили 30 листопада 1988 року Міжнародним днем захисту інформації. Хробак Моріса вперше показав, наскільки небезпечно беззастережно довіряти комп'ютерним мережам, які потребують посилення та оновлення норм безпеки та захисту інформації.

При скануванні комп'ютера хробак визначав, чи вже інфікований комп'ютер чи ні, і випадково вибирав, чи перезаписувати існуючу копію, щоб убезпечитися від хитрощів з підробленою копією, внесеною системними адміністраторами. З певною періодичністю програма якимось чином

перезаписувала свою копію. Замало чисел, наведених Робертом для опису періодичності, спричинило першу в світі епідемію мережеских хробаків.

Незначна логічна помилка в програмному коді призвела до деструктивних наслідків. Комп'ютери неодноразово заражалися хробаками, і кожен додатковий екземпляр сповільнював роботу комп'ютера до стану відмови в обслуговуванні, повністю виснажуючи ресурси організаційної техніки.

Епідемія наочно показала, наскільки небезпечно безтурботно довіряти комп'ютерним мережам. Згодом були розроблені нові жорсткі правила комп'ютерної безпеки щодо безпеки програмного коду, адміністрування мережеских вузлів та вибору безпечних паролів.

Залежно від розміру навчального закладу, інформаційна система університету, що складається з сукупності всіх підсистем, що використовуються, може налічувати сотні тисяч користувачів. Користувачами будуть всі співробітники та студенти університету, а також абітурієнти, аспіранти, докторанти, випускники та, можливо, навіть школярі, які відвідують програми довузівської освіти, та їхні батьки.

Призначення програмного забезпечення захисту інформаційних процесів передбачає наявність у системі персональних даних всіх користувачів. Наприклад, для роботи бухгалтерії та відділу кадрів необхідні дані про співробітників, для роботи приймальної комісії – про абітурієнтів, для роботи гуртожитків та медичних центрів – дані про студентів.

Неприємним фактом є те, що захищати потрібно все та від усіх. Необхідно забезпечити захист компонентів інформаційної системи та даних від деструктивних та протиправних дій користувачів.

Ідеологія навчання передбачає відкритість та зручність доступу до інформації, при цьому кваліфікація та мотивація користувачів, яким надається доступ, не відомі та не можуть бути визначені. Кількість користувачів робить можливими багато сценаріїв злову системи, крадіжки або псування даних,

виведення з ладу обладнання або маніпуляції даними для досягнення будь-яких цілей.

Стан дослідження теми: Проблематика інформаційної безпеки складна і багатоаспектна, що зумовлює необхідність вивчення й узагальнення наукових праць представників різних галузей науки. Деякі аспекти регулювання інформаційної сфери стали об'єктом наукового дослідження в працях українських та зарубіжних науковців, зокрема І. Арістової [1], І. Бачило [3], Р. Калюжного [124], Т. Костецької [68], О. Кохановської [70], В. Цимбалюка [124], та ін. Ключовими для вивчення проблеми забезпечення інформаційної безпеки стали дослідження В. Гурковського [19], О. Золотар [47;48], Б. Кормича [65;66], В. Ліпкана [76;77], В. Настюка [83], М. Швеця [120], тощо.

Аналіз останніх досліджень і публікацій. Проблеми впровадження електронного документообігу в державних установах, установах і організаціях різних форм власності досліджували такі науковці, як О. Матвієнко [81;82], Г. Охріменко [84], М. Цивін [82]. Проблемних питань упровадження системи електронного документообігу в органах державної влади торкалися в своїх публікаціях І. Двойленко [20], І. Клименко [63], К. Линьов [2], В. Писаренко [88]. До питань електронного урядування та інформаційного суспільства в Україні, та в інших країнах світу зверталися в своїх працях такі вітчизняні дослідники, як К. Вознюк [13], Б. Дзюндзюк [21], Н. Драгомирецька [29], О. Загаєцька [40], О. Загвойська [119], І. Лопушинський [78], І. Рубан [102], А. Семенченко [106], С. Чукут [122] та ін.

Актуальність теми кваліфікаційної роботи. В сучасних умовах стрімкої комп'ютеризації забезпечення захисту інформаційних процесів займає особливе місце. Дослідження програмного забезпечення захисту інформації дозволяє убезпечити особисті відомості та інформаційний продукт від кібератак зловмисників.

У зв'язку з широким використанням інформаційних технологій у всіх сферах життя суспільства виникла проблема захисту інформації, що робить

захист користувачів, інформаційних ресурсів, каналів передачі даних від злочинних посягань зловмисників важливою темою дослідження.

Концентрація інформації в комп'ютерах спонукає одних активізувати пошук шляхів доступу до інформації, а інші відповідно посилити контроль за захистом щодо її використання.

Складність створення системи захисту визначається тим, що дані можуть бути вкрадені з комп'ютера навіть без видалення їх з носія. Цінність деяких даних полягає у володінні ними, а не у їх знищенні або заміні.

Забезпечення безпеки інформації – справа дорога, і це не тільки витрати на придбання або встановлення різного апаратного або програмного забезпечення, а й через те, що важко вміло взаємодіяти між розумовою безпекою та відповідною системою підтримки в робочому стані.

Об'єктами зазіхання можуть бути як матеріально-технічні засоби (комп'ютери та периферійні пристрої), так і програмне забезпечення, бази даних.

Кожен збій комп'ютерної мережі – це моральні та фінансові збитки для працівників підприємства, корпорацій та структур. У розвитку електронних платіжних технологій та документообігу вихід з ладу локальних мереж може паралізувати роботу цілих підприємств, що призведе до значних збитків. Невипадково захист даних у комп'ютерних мережах часто стає найбільш актуальною проблемою.

Об'єктом кваліфікаційної роботи є програмне забезпечення захисту інформаційних процесів.

Предмет кваліфікаційної роботи: особливості програмного забезпечення захисту інформаційних процесів у діловодстві.

Мета кваліфікаційної роботи полягає у дослідженні захисту інформаційних процесів у діловодстві засобами програмного забезпечення.

Завданнями кваліфікаційної роботи є:

1. Дослідити історіографію та термінологію;
2. Дослідити нормативно-правове забезпечення;

3. Розглянути дійсне програмне забезпечення захисту інформаційних процесів;
4. Проаналізувати розвиток програмного забезпечення захисту інформаційних процесів у діловодстві;
5. Порівняти характеристики програмного забезпечення захисту інформаційних процесів;
6. Розглянути здійснення захисту інформаційних процесів у Маріупольському державному університеті.

Апробація: участь у II-й Всеукраїнській науково-практичній конференції з міжнародною участю «Феномен бібліотек в сучасному світі» (30.09.2021 р.), участь у Декаді студентської науки (2021 р.), участь у Декаді студентської науки (2022 р.),

Публікація тез на тему: «Безпека інформаційних систем» (2021 р.) [89], «Програмні засоби захисту інформаційних процесів» (2021 р.) [87], «Програмне забезпечення захисту інформаційних процесів» (2022 р.) [88].

РОЗДІЛ 1. СТАН УПРОВАДЖЕННЯ ПРОБЛЕМ ЗАХИСТУ ІНФОРМАЦІЙНИХ ПРОЦЕСІВ У ДІЛОВОДСТВІ

1.1. Історіографічне та термінологічне дослідження

Сучасний світ характеризується такою тенденцією, як постійне підвищення ролі інформації. Як відомо, всі виробничі процеси мають в своєму складі матеріальну і нематеріальну складові.

Перша складова – це необхідне для виробництва обладнання, матеріали та енергія в потрібній формі, тобто, чим і з чого виготовляється предмет.

Друга складова – технологія виробництва, тобто, як він виготовляється. Згадавши в загальних рисах історію розвитку продуктивних сил на Землі, кожен бачить, що роль і, відповідно, вартість інформаційної компоненти в будь-якому виробництві з плином часу зростає. В останнє сторіччя з'явилося багато таких галузей виробництва, які майже на 100% складаються з однієї інформації, наприклад, дизайн, створення програмного забезпечення, реклама.

Настільки ж яскраво демонструє підвищення ролі інформації в виробничих процесах поява в ХХ столітті такого заняття, як промислове шпигунство. Чи не матеріальні цінності, а чиста інформація стає об'єктом викрадення. З підвищенням значущості і цінності інформації відповідно зростає і важливість її захисту.

Історію захисту інформаційних процесів у діловодстві умовно можна поділити на 14 етапів, з першого по сьомий етапи – це роки, коли Україна була у складі СРСР, а починаючи з восьмого етапу вже як незалежна держава:

I етап – до 1816 року, характеризується використанням природно сформованих засобів інформаційної комунікації. У цей період основним завданням інформаційної безпеки був захист інформації про події, факти, майно, та інші дані, що має особа або спільнота, до якої вона належить, життєво важливі цінності.

II етап – починаючи з 1816 року, пов'язаний з використанням штучно створених технічних засобів електрозв'язку та радіозв'язку. Для забезпечення секретності та завадостійкості радіозв'язку необхідно було використати досвід першого періоду інформаційної безпеки на найвищому технологічному рівні, а саме використання завадостійкого кодування комуніката від комуніканта до реципієнта з подальшим декодуванням отриманого повідомлення для зворотнього зв'язку.

III етап (1935 – 1946 рр.) на цьому етапі з'явилися засоби радіолокації і гідроакустики. Основним способом забезпечення інформаційної безпеки в цей період було поєднання організаційно-технічних заходів, спрямованих на покращення захисту засобів від впливу на приймальні пристрої шляхом активної підробки та пасивного моделювання електронних перешкод.

З 1946 року розпочався IV етап завдяки появі і впровадженню в практичну діяльність електронно-обчислювальних машин. Завдання інформаційної безпеки вирішувалися переважно методами та засобами обмеження фізичного доступу до обладнання засобів вилучення, обробки та передачі інформації.

Створення і розвиток локальних інформаційно-комунікаційних мереж в 1965 р. дали можливість новому V етапу. Завдання інформаційної безпеки також вирішувалися, в основному, методами та засобами фізичного захисту засобів вилучення, обробки та передачі інформації, об'єднаних в локальну мережу шляхом адміністрування та управління доступом до ресурсів мережі.

1973 рік, пов'язаний з використанням надмобільних комунікаційних пристроїв з широким спектром завдань, який відкрив VI етап. Загрози інформаційній безпеці стали набагато небезпечними. Необхідно було розробити нові критерії безпеки для забезпечення інформаційної безпеки в комп'ютерних системах з бездротовими мережами передачі даних. Спільноти хакерів були створені з метою завдати шкоди інформаційній безпеці окремих користувачів, організацій та цілих країн. Інформаційний ресурс став найвагомішим ресурсом держави, а забезпечення його безпеки – найважливішою та обов'язковою

складовою національної безпеки. З'являється інформаційне право – нова галузь міжнародно-правової системи.

VII етап – починаючи з 1985 року, пов'язаний зі створенням і розвитком глобальних інформаційно-комунікаційних мереж з використанням космічних засобів забезпечення.

Акт проголошення незалежності України, 24 серпня 1991 року, надав нову хвилю історії захисту інформаційних процесів у діловодстві – розпочався VIII етап, який тривав до жовтня 1992 року, а саме часу прийняття Закону України «Про інформацію» [112].

IX етап – розпочався з прийняттям Закону України «Про інформацію». Цей законодавчий акт став першим документом, який установив правові основи одержання, використання та зберігання інформації, закріпив право особи на інформацію, а також систему інформації, визначив статус учасників інформаційних відносин, урегулював доступ до інформації [112]. Регулювання суспільних правовідносин, пов'язаних з інформацією, обмеженням доступу до неї, її захистом, отримало новий вектор розвитку й імпульс до врегулювання відносин в інформаційній сфері за новими правилами незалежної України.

На цьому етапі розвиваються демократичні процеси в нашій державі, розпочинається творення зрозумілих правил поведінки в інформаційному просторі. У Законі України «Про державну таємницю» [103] зазначено такі терміни: державна таємниця, віднесення інформації до державної таємниці, засекречування матеріальних носіїв інформації, криптографічний захист секретної інформації. Надамо означення представленим термінам.

Державна таємниця – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим законом, державною таємницею і підлягають охороні державою [103].

Віднесення інформації до державної таємниці – процедура прийняття рішення про віднесення категорії відомостей або окремих відомостей до

державної таємниці з установленням ступеня їх секретності шляхом обґрунтування та визначення можливої шкоди національній безпеці України у разі розголошення цих відомостей, включенням цієї інформації до Зводу відомостей, що становлять державну таємницю, та з опублікуванням цього Зводу, змін до нього [103].

Засекречування матеріальних носіїв інформації – введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації [103].

Криптографічний захист секретної інформації – вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних з метою приховування змісту інформації, підтвердження її справжності [103].

Х етап. Без сумніву, державна таємниця є особливим видом інформації з обмеженим доступом правовідносини, пов'язані з нею, та компетенції суб'єктів таких правовідносин визначалися законом України, а не відомчою інструкцією СРСР чи постановою ЦК КПРС. [3].

Цей етап розпочався у 1996 році, з прийняттям Конституції України. У подальшому всі правовідносини, пов'язані із захистом інформації, регулювалися її нормами або актами законодавства, виданими в її розвиток. Закон України «Про захист інформації в автоматизованих системах», на підставі Закону України від 31.05.2005 № 2594-IV отримав назву «Про захист інформації в інформаційно-телекомунікаційних системах» [110], унормував правовідносини із захисту інформації в автоматизованих системах

До цього етапу також варто зарахувати прийняття важливих для системи Закону України «Про національну програму інформатизації», Указів Президента України «Про Положення про порядок здійснення криптографічного захисту інформації в Україні» від 22.05.1998 № 505 і «Про Положення про технічний захист інформації в Україні» від 27.09.1999 № 1229.

Цей етап видався дуже продуктивним для системи загалом, під час його дії прийнято багато актів законодавства, стандартів і нормативів, які врегульовували захист інформації з обмеженим доступом.

XI етап – (2002-2006 рр.) розпочався із прийняттям Закону України «Про Національну систему конфіденційного зв'язку» – етап початку функціонування спеціальних телекомунікаційних систем, які за допомогою криптографічних або технічних засобів забезпечують обмін інформацією з обмеженим доступом в інтересах органів державної влади й органів місцевого самоврядування, створюють належні умови для їх взаємодії в мирний час і в разі введення надзвичайного й воєнного стану [10].

Указаний законодавчий акт відіграв вагому роль для розвитку системи обміну та захисту службової інформації в Україні. Також приймаються важливі для системи акти – Закони України «Про основи національної безпеки», «Про телекомунікації», та інші підзаконні акти, які в сукупності дали змогу підняти систему захисту інформації з обмеженим доступом на новий рівень.

XII етап – (2006-2011 рр.) розвитку системи захисту інформації з обмеженим доступом розпочався прийняттям Закону України «Про Державну службу спеціального зв'язку та захисту інформації України». Указаний законодавчий акт не тільки вплинув на суб'єктний склад системи, передбачаючи формування окремого державного органу – Державної служби спеціального зв'язку та захисту інформації України, призначеної для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, захисту державних інформаційних ресурсів криптографічного та технічного захисту інформації [2], а й дав визначення тим процесам, явищам, які на той час потребували законодавчого розуміння.

XIII етап – (2011-2014 рр.) розпочався з набранням чинності Законом України «Про захист персональних даних» і прийняттям Закону України «Про доступ до публічної інформації». Починається етап захисту персональних даних і відмежування публічної інформації від такої, що публічною не є. Цей

період характеризується створенням і реєстрацією баз персональних даних, вирішенням питань про їх захист, а також запитами на публічну інформацію й пошуком їх відмінностей від звернень громадян. Ці акти законодавства мали значний вплив на аналізовану систему, адже давали розуміння видів інформації з обмеженим доступом.

XIV етап – (2014 рік – по теперішній час). Виокремлюємо його як особливий, адже старт йому дав Указ Президента України «Про часткову мобілізацію» від 17.03.2014 № 303. Першопричиною для початку вказаного етапу стали зовнішня агресія щодо нашої держави, тимчасова окупація частини території України. Цей етап є етапом загартування досліджуваної системи в умовах особливого періоду й воєнного стану. Ще цей етап характеризується як етап кібербезпеки, яка на рівні закону започаткована у травні 2018 року.

У цей період державні інституції та інститути громадянського суспільства об'єднали зусилля для опору противнику, в тому числі й в інформаційній сфері, і в кіберпросторі. Приймається багато суттєвих змін до законодавства України. Відбувається парад доктрин і стратегій, зокрема затверджуються Стратегія Національної безпеки України, Стратегія кібербезпеки України, Доктрина інформаційної безпеки, нова редакція Воєнної доктрини України.

У липні 2018 року законодавство нашої держави перестало визначати основи національної безпеки, а перейшло до визначення безпосередньо національної безпеки з набранням чинності Законом України «Про національну безпеку України». І на всі ці події впливають інтеграційні процеси, зумовлені виконанням нашою державою зобов'язань відповідно до Угоди про асоціацію між Україною та Європейським Союзом, Європейським співтовариством з атомної енергії.

Категорія «інформаційна безпека» виникла з появою інформаційних комунікацій між людьми, а також з усвідомленням людиною інтересів їх співтовариств, яким може бути завдано збитків через дії на засоби

інформаційних комунікацій, наявність і розвиток, які забезпечує інформаційний обмін між усіма наявними елементами соціуму.

Відповідно до різноманітності поняття інформації, словосполучення «інформаційна безпека» в різних контекстах може мати різний сенс. Так, у Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [113] наводиться таке поняття інформаційної безпеки:

Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [113].

Поняття інформаційної безпеки значно поширилося у світлі розвитку нових ІТ-технологій. Деякі науковці зазначають, що доцільніше користуватися поняттям «Кібербезпека», ніж «Інформаційна безпека». Це обумовлено тим, що сьогодні захист процесів, інформації та діяльності у кіберпросторі – це не тільки втрата інформації. Втрата інформації завжди тягне за собою ряд інших ускладнень.

Кібербезпека – це захист від вірусів, хакерських атак і підробки даних. Тому що віруси можуть не тільки видаляти чи красти дані, а й впливати на роботу та продуктивність працівників або навіть зупиняти весь робочий процес. Інформація також може бути використана проти особи чи структури. Що може спричинити непоправну шкоду. Кібербезпека сьогодні відповідає за три фактори: системи, процеси, люди. Окрім цього, через широку інтеграцію цифрових технологій у життя людини, питання інформаційної безпеки іноді стає питанням безпеки життя. Таким чином, стара концепція інформаційної безпеки не включає до себе весь обсяг широкого кола проблем, які виникають у кіберпросторі XXI століття. Натомість інформаційна безпека має місце як частина кібербезпеки.

У галузі інформаційних систем, згідно Закону України «Про інформацію» [112], рекомендується таке означення інформації та її захисту:

Інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [112].

Захист інформації – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї [112].

Як відомо, інформація може мати різноманітні форми, зокрема комп'ютерні дані, листи, записи, файли, формули, креслення, діаграми, моделі виробів, дисертації тощо.

Як і будь-який товар, інформація має споживачів, які її потребують, а отже, має певні споживчі якості, а також має своїх власників чи виробників.

Термін «Інформація» багаторазово змінювався, межі інформації розширювались і звужувалися. Спочатку це слово означало «представництво», «поняття», потім – «відомості», «передача повідомлень». Вперше термін «інформація» знайшов відображення в математичній теорії інформатики та теорії передачі даних по каналах зв'язку Клода Шеннона (1948), в якій він розумів під «інформацією» всі види повідомлень. К. Шеннон і В. Вівер запропонували ймовірні методи визначення обсягу переданої інформації. Однак такі методи описують лише символічну структуру інформації, не впливаючи на її зміст.

Науковцями термін «інформаційна безпека» розуміється по-різному, причому найчастіше мається на увазі якийсь один аспект цієї проблеми. Так О. Литвиненко зазначає, що під інформаційною безпекою варто розуміти одну зі сторін розгляду інформаційних відносин у межах інформаційного законодавства з позицій захисту життєво важливих інтересів особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами [77].

У свою чергу О. Горбатюк у своїй праці вказує, що інформаційна безпека являє собою стан захищеності потреб в інформації особистості,

суспільства і держави, за якого забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз [16].

В. Богуш вважає, що інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави [5].

Згідно праці О. Сороківської під інформаційною безпекою підприємства пропонуємо розуміти суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності [119].

Л. Дж. Хоффман зазначив, що інформаційна безпека – це стан інформації, у якому забезпечується збереження визначених політикою безпеки властивостей інформації [130].

У свою чергу, у працях В. Бурячок ототожнює інформаційну безпеку із кібербезпекою та зазначає, що кібербезпеку можна визначити як стан захищеності кіберпростору держави загалом або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання і нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам [7].

Розуміння складових системи забезпечення інформаційної безпеки виразили О. Довгань і Т. Ткачук. Формуючи власне розуміння поняття «система захисту інформації» органам, які здійснюються правозастосовну функцію, слід враховувати законодавчі визначення суміжних понять та не ігнорувати об'єкти щодо яких здійснюються заходи захисту [24].

Отже, поняття «інформаційна безпека» неодноразово змінювалось та поширювалось. Це пов'язано із різним трактуванням науковцями цього терміну. Коли ми говоримо про інформаційну безпеку, ми часто маємо на увазі інформаційну безпеку в загальному сенсі, як набір заходів, спрямованих на зменшення кількості можливих шкідливих сценаріїв або розмір збитків, які мо-

же зазнати компанія у разі втечі конфіденційної інформації. Маючи на увазі цю точку зору можна зазначити, що інформаційна безпека – це економічний параметр, який необхідно враховувати в роботі підприємства, а інформація може розглядатися як конкретний продукт, що підлягає захисту, тому вона має бути доступна лише авторизованим користувачам чи програмам.

1.2. Нормативно-правове забезпечення захисту інформаційних процесів у діловодстві.

Вимоги інформаційної безпеки повинні органічно включатися в усі рівні законодавства, у тому числі й у конституційне законодавство, основні загальні закони, закони з організації державної системи управління, спеціальні закони та відомчі правові акти.

Законами щодо регулювання в сфері захисту інформаційних процесів виступають: Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [110], Закон України «Про електронні документи та електронний документообіг» [104].

Також існує перелік не менш важливих документів. Розглянемо їх.

Закон України «Про інформацію» [112], який регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

Закон України «Про захист персональних даних» [84] котрий регулює правовідносини пов'язані із охороною та обробкою особистих даних і має на меті захист основних прав людини і громадянина, зокрема право на приватність, у випадку з обробкою та збереженням персональних даних.

Цей Закон поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів.

Закон України «Про електронну комерцію», який визначає організаційно-правові засади діяльності у сфері електронної комерції в Україні, встановлює порядок вчинення електронних правочинів із застосуванням інформаційно-телекомунікаційних систем та визначає права і обов'язки учасників відносин у сфері електронної комерції [105].

Закон України «Про державну таємницю» регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України [103].

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, встановлено інші правила, ніж ті, що передбачені цим законом, застосовуються правила міжнародного договору [80].

Закон України «Про електронні документи та електронний документообіг» що встановлює основні організаційно-правові засади електронного документообігу та використання електронних документів [104].

Положення про порядок здійснення криптографічного захисту інформації в Україні визначає порядок здійснення криптографічного захисту інформації з обмеженим доступом, розголошення якої завдає шкоди державі, суспільству або особі [113].

Перелік постанов Кабінету Міністрів України щодо врегулювання відносин у сфері електронного документообігу та ведення електронної документації.

Постанова Кабінету Міністрів України «Про перелік відомостей, що не становлять комерційної таємниці» від 9 серпня 1993 року № 611 [114].

Постанова Кабінету Міністрів України «Про затвердження Інструкції з діловодства за зверненнями громадян в органах державної влади і місцевого самоврядування, об'єднаннях громадян, на підприємствах, в установах, організаціях незалежно від форм власності, в засобах масової інформації» від

14 квітня 1997 року № 348 має рекомендаційний характер для об'єднань громадян, а також підприємств, установ та організацій приватної форми власності [106].

Постанова Кабінету Міністрів України «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію» від 27 листопада 1998 року № 1893 визначає обов'язковий для всіх центральних органів виконавчої влади, Ради міністрів Автономної Республіки Крим, місцевих органів виконавчої влади, органів місцевого самоврядування, підприємств, установ і організацій незалежно від форм власності порядок обліку, зберігання, використання та знищення документів, справ, видань, магнітних та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави [107].

Постанова Кабінету Міністрів України «Про проведення експертизи цінності документів» від 8 серпня 2007 року № 1004 визначає процедуру утворення комісій з проведення експертизи цінності документів та організацію їх діяльності [116].

Постанова Кабінету Міністрів України «Про внесення змін до Порядку утворення та діяльності комісій з проведення експертизи цінності документів і порядку віднесення документів Національного архівного фонду до унікальних, їх обліку та зберігання» від 28 листопада 2012 року № 1103 визначає зміни до порядку утворення та діяльності комісій з проведення експертизи цінності документів і порядку віднесення документів Національного архівного фонду до унікальних, їх обліку та зберігання [102].

Наказ Міністерства юстиції України «Про затвердження Переліку типових документів, що створюються під час діяльності органів державної влади та місцевого самоврядування, інших установ, підприємств та організацій, із зазначенням строків зберігання документів» від 12 квітня 2012 року № 578/5 [108].

Наказ Державного комітету архівів України «Про затвердження Примірного положення про експертну комісію об'єднання громадян, релігійної організації, а також підприємства, установи та організації, заснованої на приватній формі власності» від 6 травня 2008 року № 83 [109].

Національний стандарт України «Діловодство й архівна справа. Терміни та визначення понять» (ДСТУ 2732:2004); поширюється на організаційно-розпорядчі документи – постанови, розпорядження, накази, положення, рішення, протоколи, акти, листи тощо [22].

Національний стандарт України «Інформація та документація. Керування документаційними процесами. Частина 1. Основні положення (ISO 15489 1:2001, MOD)» (ДСТУ 4423 1:2005); є перекладом ISO 15489-1:2001(E) Information and documentation – Records management – Part 1: General (Інформація та документація. Керування документаційними процесами. Частина 1. Основні положення) з окремими технічними змінами [64].

Збірник уніфікованих форм організаційно розпорядчих документів, схвалений Методичною комісією Державного комітету архівів України (протокол від 20 червня 2006 року № 3) найпоширеніші види організаційно-розпорядчих документів, що створюються у державних органах, органах місцевого самоврядування, на підприємствах, в установах, організаціях, будь-яких інших юридичних особах незалежно від форм власності, розроблено згідно з вимогами чинного національного стандарту та нормативно-правових актів, що встановлюють єдині вимоги до створення управлінських документів.

Методичні рекомендації з розроблення галузевих переліків документів та типових (примірних) номенклатур справ, схвалені Нормативно методичною комісією Державної архівної служби України (протокол від 18 грудня 2012 року № 5). підготовлено з метою надання допомоги міністерствам, іншим центральним і місцевим органам виконавчої влади та іншим центральним установам у розробленні галузевих переліків документів та типових номенклатур справ.

Нормативні документи в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України (ДСТУ) стосовно створення і функціонування КСЗІ направлені на нормування АСДО: НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі, НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу, НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

Державну політику у сфері захисту інформації реалізує Державна служба спеціального зв'язку та захисту інформації України.

На сьогодні існує велика кількість нормативно-правових актів, які регламентують захист інформаційних процесів у діловодстві. Будь-яка сфера діяльності держави регулюється відповідною нормативно-правовою базою, тобто законодавством. Саме юридичне регулювання дозволяє якісно реалізовувати захист інформації та та спиратися у сумнівних питаннях.

Висновки до розділу 1

Актуальність правового захисту інформації зумовлена об'єктивним зростанням кількості інформаційних загроз та шляхів протидії їм і процесі побудови інформаційного суспільства.

У зв'язку з розвитком процесів інформатизації та комп'ютеризації суспільства захист інформації є проблемою, яка потребує нормативно-правового забезпечення.

Сьогодні в Україні розроблена основна нормативно-правова база, та створена інфраструктура, яка має забезпечити надійний захист інформаційних процесів у діловодстві.

Однак слід мати на увазі, що програмні засоби для несанкціонованого видалення та викрадення інформації та засоби протидії їм постійно оновлюються.

Враховуючи цей безперервний розвиток та постійну інформаційну боротьбу, Україні необхідно вдосконалювати та розвивати як законодавчу базу, так і структурно-технічну складову інформаційної безпеки для забезпечення своєї незалежності.

РОЗДІЛ 2. ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ ПРОЦЕСІВ

2.1. Огляд дійсного програмного забезпечення захисту інформаційних процесів

Безпека інформаційних систем – це, перш за все, захист системи від випадкового або навмисного втручання у стандартний процес її функціонування, від спроби крадіжки, а саме від несанкціонованого вилучення інформації, модифікації або фізичного знищення її компонентів, тобто здатність перешкоджати провокаційні дії та впливи на інформаційні системи.

Загроза інформаційній безпеці – це події або дії, які можуть призвести до спотворення, несанкціонованого використання або навіть знищення інформаційних ресурсів керованої системи, а також програмного та технічного забезпечення.

Загрози інформаційній безпеці можуть бути двох видів: навмисними або ненавмисними. Нині захист інформації потребує реалізації системного підходу, що включає комплекс пов'язаних між собою заходів, а також використання спеціальних програмно-технічних засобів, організаційних заходів, нормативно-правових актів, морально-етичних контрзаходів стосовно захисту. Характер захисту спирається на складені дії зловмисників, які прагнуть будь-яким способом отримати важливу для них інформацію.

Впровадження технології захисту інформаційної безпеки в комп'ютерні інформаційні системи та мережі передачі даних вимагає збільшення витрат і сил. Проте все це дозволяє уникнути значних непосильних втрат і збитків, які можуть виникнути при реалізації загроз інформаційним системам та інформаційним технологіям.

До основних загроз безпеки інформації і нормального функціонування інформаційних систем відносяться: витік конфіденційної інформації,

компрометація інформації, несанкціоноване використання інформаційних ресурсів, помилкове використання інформаційних ресурсів, несанкціонований обмін інформацією між абонентами, відмова від інформації, порушення інформаційного обслуговування, незаконне використання привілеїв.

Витік конфіденційної інформації – це безконтрольний вихід конфіденційної інформації за межі інформаційних систем або кола осіб, яким вона була довірена по службі або стала відома в процесі роботи. Цей витік може бути наслідком розголошення конфіденційної інформації, виходу інформації з різних, головним чином, технічних каналів, несанкціонованого доступу до конфіденційної інформації різними способами [87].

Програмні засоби захисту інформаційних процесів – системні та прикладні програми, призначені для захисту інформації, що передається по телекомунікаційним каналам, зберігається в базах даних і на інформаційних носіях [86].

Найчастіше програмні засоби безпеки використовуються для виконання таких процесів, як ідентифікація та аутентифікація користувачів, обмеження доступу користувачів до інформаційної мережі, захист паролем та аутентифікація, шифрування інформації, а також її захист від несанкціонованих змін, читання, копіювання.

Для домашнього використання часіше використовуються лише антивірусні програми. Цей вид програмного забезпечення надійно захищає особисті дання від кібератак та вірусного значення інформації.

Відомі нині антивірусні програми можна розділити на кілька типів:

1. Детектори. Їх мета – лише знайти вірус. Детектори вірусів можуть порівнювати завантажувальні сектори дискети з відомими завантажувальними секторами, створеними різними версіями операційних систем, і таким чином виявляти завантажувальні віруси або сканувати файли на магнітних носіях для

виявлення відомих вірусних сигнатур. Подібні програми в чистому вигляді зараз рідкість.

2.Доктора (Фагі. Фаг) – це програма, яка здатна не тільки виявити, а й знищити вірус, тобто видалити його код із заражених програм і відновити їх працездатність (якщо можливо). Найвідомішим фагом є Aidstest, створений Д. М. Лозинським. Одна з останніх версій виявляє більше 8000 вірусів. Aidstest для нормальної роботи він вимагає, щоб у пам'яті не було антивірусу, який блокує записи в програмних файлах, тому їх слід завантажити, вказавши опцію завантаження самої резидентної програми, або скориставшись відповідною утилітою.

3. Ревізори. Програма-ревізор відстежує можливі шляхи поширення і зараження комп'ютерів вірусами. Програми-ревізори є одними з найнадійніших засобів захисту від вірусів і мають бути частиною арсеналу кожного користувача. Ревізори — єдиний інструмент, який дозволяє контролювати цілісність і зміни у файлах і системних областях магнітних дисків.

4.Вакцини. Це так звані антивірусні програми, які поведуться як віруси, але не завдають шкоди. Вакцини захищають файли від змін і можуть не тільки виявити зараження, але в деяких випадках «вилікувати» файли, заражені вірусом. Програми противірусних вакцин наразі не є широко доступними, оскільки деякі несправні вакцини завдали шкоди багатьом користувачам останніми роками.

Сьогодні найбільшу увагу розробники та користувачі приділяють програмному забезпеченню для захисту від несанкціонованого доступу до інформаційних ресурсів та особливо до Інтернету. Організаційні, технологічні та апаратні методи захисту, як правило, не можуть бути реалізовані без програмної складової. При цьому слід враховувати, що вартість багатьох програмно-системних рішень для захисту значно перевищує вартість обладнання, технологій та організаційних рішень. Іншими недоліками програмного захисту є використання ресурсів системи, що призводить до зниження її ефективності,

принципова можливість обходу такого захисту або її кримінальна зміна під час роботи.

Але для забезпечення гарантованого захисту інформаційних процесів в діловодстві лише антивірусних програм не буде вистачати. Антивірусні програми захищають інформацію лише від шкідливих файлів, у той час як для захисту інформаційних процесів у діловодстві необхідний захист також і від кібератак зловмисників.

На ринці програмного забезпечення захисту інформаційних процесів України існує безліч програм, які використовуються у різних аспектах діяльності.

Згідно офіційному сайту Міністерства цифрової трансформації України [85] зазначається перелік протестованих систем електронного документообігу (Таблиця 2.1).

Таблиця 2.1

Системи електронного документообігу

Розробник	Назва та версія платформи
ТОВ «Софтлайн-ІТ»	Мегаполіс v.2.57
ТОВ «Софтлайн-ІТ»	«Megapolis. DocNet» v.1.x
ТОВ «Інтекресі Бейз»	«Megapolis. DocNet» v.1.x
ТОВ «Айкюжн ІТ»	«Megapolis. DocNet» v.1.x
АТ «ІнфоПлюс»	АСКОД II v 10.3.8.141
АТ «ІнфоПлюс»	АСКОД Корпоративний v.10
ТОВ «Транс Лінк Консалтинг»	ДОК ПРОФ™ СТЕП 2.0
ТОВ «Транс Лінк Консалтинг»	«Автоматизована система управління документами «ДОК ПРОФ 3»
ТОВ «Інтерактивні системи»	InterDoc v 4.2
ТОВ НВП «Інформаційні технології»	«IT-Enterprise»(ІТ Підприємство)
ТОВ «Алтерсайд»	Документаріум
ТОВ «Софт Експаншен Україна»	«SX-Government» v 3
ТОВ «ФОСС-ОН-ЛАЙН»	FossDoc Enterprize v 6.42
ТОВ «Новатум»	«ДОК ПРОФ ВЕБ»
ТОВ «СМАРТ БІЗНЕС»	«Система електронного документообігу Міністерства освіти і науки України Версія 4.0»
Укрпатент	АС «Загальне діловодство»
ТОВ "Е-ДОКС"	e-Docs.Platform
ТОВ «Адвертайзінг Експрес»	Комп'ютерна програма «CleverForms

	Document» 2.4
ТОВ «ІРБЕКС СОЛЮШНС»	«БД ДОКУМЕНТООБІГ V.1.2.x»
ТОВ «ІРІС»	Стратег.Смарт («Стратег.Смарт») версія 4.0
ТОВ «МАСТЕР:ГЛОБАЛ»	Система електронного документообігу «MASTER:Документообіг» версія 2019
ДП «ІНФОТЕХ»	СЕД системи МВС, версія 2019.x.x

Продовження таблиці 2.1

ТОВ «НЕВДА»	СЕД Deka office
ТОВ «АйКор Технолоджі»	СЕД «Айдок»
ДП Адміністрація морських портів України	СЕД «АМПУ» версія 1.0
ДП «ІНФОТЕХ»	СЕД «МІА:Документообіг» версія 1.0
ТОВ "МЕДИРЕНТ"	АСЕДО версія 2
ТОВ «СОФТ ПРОДАКШН»	Комп'ютерна програма «Альфа.Про»
ТОВ «МІАЦ»	СЕД «Електронне самоврядування 3.0»
ПАТ «ВФ Україна»	СЕД «Lotus Notes Domino»
ПП «КАІ»	«КАІ-Документообіг»
ТОВ науково - виробнича фірма «ГРІС»	«Інтранет - портал електронного документообігу Верховної Ради України» версія 1.0
ТОВ «М.Е.Д.О.К»	СЕД «М.Е.Doc», 11.XX.XXX
ТОВ «Інформаційно-аналітичний центр»	Комп'ютерна програма «TDocs» версії 3.x
Приватне акціонерне товариство «ВФ Україна»	Система електронного документообігу «OpenText» Приватного акціонерного товариства «ВФ Україна»

Запорукою результативної роботи органів влади завжди є продуктивна діяльність державних службовців та посадових осіб органів місцевого самоврядування. Однак для високоякісного задоволення запитів громадян звичні методи роботи з інформацією стають менш ефективними. Виникла необхідність впровадження оновленої системи документообігу, побудованої на основі електронного документообігу. Проте така система поки що не впроваджена на практиці.

2.2. Розвиток програмного забезпечення захисту інформаційних процесів у діловодстві

Питання інформаційної безпеки для сучасного світу є вкрай актуальним, важко визначити пріоритетні напрями для реагування на загрози кібербезпеки, але питання захисту інформації у корпораціях, які є основою сучасної економіки, завжди залишаються на перших місцях у розробників безпечних інформаційних технологій. Це, безумовно, пов'язано з великим обсягом залучених людських та грошових ресурсів. Метою цього посібника є дати уявлення про деякі важливі аспекти систем захисту інформації для корпорацій та їх складових частин – систем моніторингу трафіку та аналізу мережевої активності.

Поява вірусів спонукала до появи перші антивірусні програми. Зараз розробкою антивірусів займаються великі компанії. Зараз виробництвом антивірусних програм займаються провідні компанії світу. Як і у виробників вірусних програм у цих компаній починаються формуватися свої, оригінальні, засоби, але вже для виявлення та знищення файлів, які несуть загрозу для цінної інформації. Сучасні антивірусні програми можуть знаходити велику кількість вірусів.

2 листопада 1988-го перший масштабний комп'ютерний вірус «хробак» призвів до серйозних ушкоджень комп'ютерних мереж Пентагону та кількості закладів вищої освіти Сполучених Штатів Америки.

Вірус «Хробак Морріса» був написаний студентом Корнельського Університету Робертом Моррісом. У липні 1989-го року він був першим кого звинуватили у комп'ютерному шахрайстві. Йому присудили до 3 років позбавлення волі та нарахували штраф у розмірі \$10 тис.

Вірус ушкодив 6,2 тис. пристроїв. Це 10% усіх комп'ютерів, які мали доступ до інтернету. Наслідки дії вірусу оцінили у \$96,5 млн.

«Хробак Морріса» автоматично підбирав паролі до облікових записів. Для цього він користувався ім'ям користувача та списком із 400 найбільш поширених слів. «Хробак» користувався маскуванню, щоб приховати свою наявність у операційній системі. Він видаляв файл, який виконував та перейменовував свій процес.

Хронологічно можна поділити розвиток антивірусного програмного забезпечення на сім етапів.

Перший етап розпочався у 1981 із появою першого вірусу «Elk Cloner». Вірус був створений в 1981 році 15-річним школярем Річардом Скрента для комп'ютерів Apple II.

У 1984 році став початком для другого етапу. Була створена «Утиліта СНК4ВОМВ». Програма для виявлення і видалення шкідливого ПЗ, розробив її зимою 1984 року американський програміст Енді Хопкінс.

Третій етап, 1985 рік, розробка «G Data Software AG». Німецька компанія, виробник програмного забезпечення, що спеціалізується на ІТ-безпеці.

DPROTECT. Резидентний монітор DPROTECT дозволяв убезпечити комп'ютер від деструктивних дій програм, які могли, наприклад, відформатувати диск або зіпсувати завантажувальний запис.

1988 рік був переломний та став початком четвертого етапу. Створення хробака Морріса призвело до чисельних фінансових збитків, та саме у цьому році розпочались масштабні роботи над створенням потужних антивірусних програм, а саме «McAfee Virus Scan». Автор – програміст з Lockheed Corporation Джон Макафі, на честь якого і названий антивірус. Та «Aidstest». Дмитро Миколайович Лозинський, який розробив антивірус, практично одночасно з Макафі.

П'ятий етап розпочався у травні 1989 року. Американська компанія Symantec випустила перший антивірусний пакет для комп'ютерів Macintosh (SAM).

У період шостого етапу (1990 – 2015 рр.) була створена низка антивірусних програм. «Panda Software». Ці антивірусні продукти містять тільки інформацію про зразки шкідливих програм, які є причиною більшості заражень у сучасності, в той час як інша інформація зберігається в базі даних Panda. «Tadpole». Перші дослідження Ігоря Данилова з лікування вірусів за допомогою Aidstest. Створено перший повноцінний антивірус — резидентний сторож Tad-

pole. «Spider's Web» випущена антивірусна система Spider's Web, що з'єднала сторож Spider (наступник Tadpole) і доктор Web (наступник Tornado). Саме з цього моменту ведеться відлік історії розвитку Dr.Web. «Lie Detector» Євгена Суслікова, який став першим антивірусом, який міг виявляти невідомі віруси, такі антивіруси отримали назву «Евристичні аналізатори». «Norton Internet Security 2000». Файрвол Norton Internet Security був заснований на міжмережевому екрані AtGuard, який був спочатку розроблений WRQ Inc. і придбаний компанією Symantec. «Alwil Software» Заснована 21 квітня 1991 року. У Україні найбільш відома як розробник антивіруса Avast.

Сьомий етап розпочався у 2016 році та триває до теперішнього часу. Це впровадження сучасних антивірусних програм, які захищають інформацію на електронних носіях більшості населення. «Dr.Web» це загальна назва сімейства програмного антивірусного програмного забезпечення для різних платформ і лінійки програмно-апаратних рішень (Dr.Web Office Shield), а також рішень для забезпечення безпеки всіх вузлів корпоративної мережі (Dr.Web Enterprise Suite).

«Panda Security SL». Продукти Panda містять засоби безпеки для домашніх і корпоративних користувачів, включаючи захист від кіберзлочинців і різних видів шкідливих програм, які здатні завдати шкоди ІТ-системам.

«AVG Free». Безкоштовний антивірус AVG Free збільшує обсяг зібраних на комп'ютері даних. Компанії AVG Technologies може відсилатися інформація про використовувані додатки, про хакерські програми, імена підозрілих файлів, історія пошуку та відвідувань сайтів в інтернеті.

«Лабораторія Касперського». Міжнародна група компаній з центральним офісом в Москві, що спеціалізується на розробці програмного забезпечення.

«Norton Internet Securit». Пакет безпеки, розроблений компанією Symantec. Включає в себе антивірус, брандмауер, сканер електронної пошти, фільтр спаму, захист від фішингу.

Розробка антивірусних пакетів безпеки триває постійно. Це пов'язано із постійним оновленням шкідливих вірусів, які загрожують безпеці інформаційних процесів усього населення. Перелік дійсного та актуального програмного забезпечення постійно оновлюється, та та буде оновлюватися і у майбутньому. Необхідно постійно слідкувати за сучасними тенденціями на ринці для якісного захисту особистих даних на електронних носіях.

Існує безліч систем SIEM, які розробляються різними фірмами-розробниками систем обробки даних та комп'ютерної безпеки [3]. У певному сенсі SIEM є поліпшеною системою виявлення шкідливої активності та різних системних аномалій. Робота SIEM дає можливість побачити більш повну картину активності мережі і подій безпеки. Коли звичайні засоби виявлення, взяті окремо, не бачать атаки, вона може бути виявлена за умови ретельного аналізу та кореляції інформації з різних джерел. Тому багато корпорацій розглядають використання SIEM-систем як додатковий і дуже важливий елемент захисту від цілеспрямованих атак.

SIEM-системи продовжують розвиватися і з часом можуть стати частиною чогось більш досконалого, але зараз без використання SIEM неможливо побудувати такі системи і центри моніторингу і реагування як SOC (Security Operation Centre) і під'єднатися до FinCert або подібних організацій, тому що SIEM дає можливість вирішити цілу низку ключових завдань: збирати та зберігати лог-файли в єдиному централізованому сховищі, надавати спеціалізовані звіти аудиторам для перевірки відповідності вимогам законодавства та відомчим стандартам, досліджувати кореляцію між різними джерелами даних.

Особливо потрібно звернути увагу на налаштування SIEM під вимоги користувача, його інфраструктури та системи безпеки. Добре налаштовані правила кореляції дають змогу оператору аналізувати справді важливі повідомлення про інциденти, відсіюючи зайве. Важливо, щоб система брала на себе максимум рутинних операцій.

Треба розуміти, що SIEM-системи не призначені та і не можуть попереджати інциденти порушення інформаційної безпеки. Їх сутність закладе

у назві: аналіз інформації, яка надходить із різних джерел (DPL, IDS, антивіруси, міжмережеві екрани та інше), та подальше виявлення різних відхилень від норм за призначеними критеріями.

Перед системою SIEM ставлять такі завдання: консолідація та зберігання журналів з різних джерел, надання інструментів для аналізу подій та розборки інцидентів, виконання кореляційного аналізу та обробки подій за правилами, автоматичне сповіщення та інцидент-менеджмент.

Зараз поняття SIEM стало ширше. Від SIEM-системи вимагаються нові функції та механізми, здатні більш швидше та точно не тільки виявляти, але і попереджати інциденти інформаційної безпеки, водночас не обмежуючись аналізом лише журналів подій. SIEM рішення нового покоління прагне поєднувати у собі «традиційні» функціональні якості SIEM, а також функції аналізу мережевого трафіку та управління ризиками.

Класифікацію програмних засобів захисту за функціональним призначенням наведено на рис. 2.1.

До програмних засобів зовнішнього захисту належать програмні засоби забезпечення функціонування фізичних засобів, захисту території, приміщень, окремих каналів зв'язку й пристроїв ІС. У цей час випускається безліч систем охоронної сигналізації, що містять мікропроцесори та комп'ютери. Програмні засоби використовуються також у пристроях біометричного розпізнавання особистості.



Рис. 2.1 Класифікація програмних засобів захисту

Важливо керувати інформаційними системами в цілому і механізмами безпеки особливо ретельно. Ці заходи безпеки повинні ґрунтуватися на загальноприйнятих стандартах, бути стійкими до мережевих загроз, враховувати особливості окремих систем.

Висновки до розділу 2

Через недоліки операційного програмного забезпечення, пов'язані з безпекою даних в Інтернеті, зловмисники можуть захоплювати закриті ключі шифрів користувача і діяти від їх імені.

До навмисних загроз належать: несанкціонований доступ до інформації та мережевих ресурсів; розкриття та зміна даних та програм, їх копіювання; розкриття, зміна чи заміна трафіку комп'ютерної мережі; розробка та розповсюдження комп'ютерних вірусів; крадіжка магнітних носіїв та розрахункових документів; знищення архівної інформації або її умисне

знищення; фальшування повідомлення, відмова від факту отримання інформації або зміна часу її отримання; перехоплення та ознайомлення з інформацією, що передається по каналах зв'язку та ін.

Найпоширенішими прикладами програмних засобів захисту інформації є такі: система контролю і управління доступом; антивірусні програми; шифрувальне програмне забезпечення; мережевий екран; система виявлення вторгнень; керування записами; пісочниця; система управління інформаційною безпекою; SIEM.

У повсякденні достатньо застосовувати лише антивірусні програми, але для надійного захисту інформаційних процесів у діловодстві необхідно застосовувати, у першу чергу, SIEM.

РОЗДІЛ 3. ЗАХИСТ ІНФОРМАЦІЙНИХ ПРОЦЕСІВ У ДІЛОВОДСТВІ ЗАСОБАМИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

3.1. Порівняльна характеристика програмного забезпечення захисту інформаційних процесів

Програмні засоби захисту інформації – системні та прикладні програми, призначені для захисту інформації, що передається по телекомунікаційним каналам, зберігається в базах даних і на інформаційних носіях [19].

Програмні засоби захисту інформаційних процесів, частіше за все, використовуються для автентифікації та ідентифікації користувачів для їх подальшого доступу до мережі, паролі та чисельні перевірки повноважень. Шифрування зберігаємої інформації а також її захист від усіх видів зловмисних зазіхань шахраїв.

Найбільшу увагу розробники й користувачі сьогодні приділяють програмним засобам захисту від несанкціонованого доступу до інформаційних ресурсів і особливо до мережі Інтернет. Організаційні, технологічні й апаратні методи захисту, як правило, не можуть бути здійснені без програмної складової. При цьому слід мати на увазі, що вартість здійснення багатьох програмних системних рішень із захисту інформації суттєво перевищує за затратами апаратні, технологічні й організаційні рішення. Іншими недоліками програмних засобів захисту інформації є використання ресурсів системи, що призводить до зниження її ефективності, принципова можливість обходу такого захисту або його злочинної зміни в процесі експлуатації [19].

Кабінет Міністрів України кожен рік звітує про стан інформатизації та розвиток інформаційного суспільства в Україні. На ринку України існує багата чисельність програмного забезпечення захисту інформаційних процесів у діловодстві, саме тому, при наявності великої конкуренції, державні органи віддають перевагу провідним системам електронного документообігу.

Найпоширенішими прикладами програмних засобів захисту інформації є Megapolis, OPTIMA-WorkFlow, Док Проф, ДЕЛО, MasterDOC, Атлас ДОК, Летограф, АСКОД, El-Doc.

Megapolis. Документообіг це базовий вибір. Це програмне забезпечення дозволяє організувати електронний документообіг на будь-якому обраному рівні та галузі діяльності.

Програмний продукт Megapolis.DocNet відповідає концепції ECM (Enterprise Content Management) і підтримує повний життєвий цикл управління документами та автоматизації бізнес-процесів (рис. 3.1).

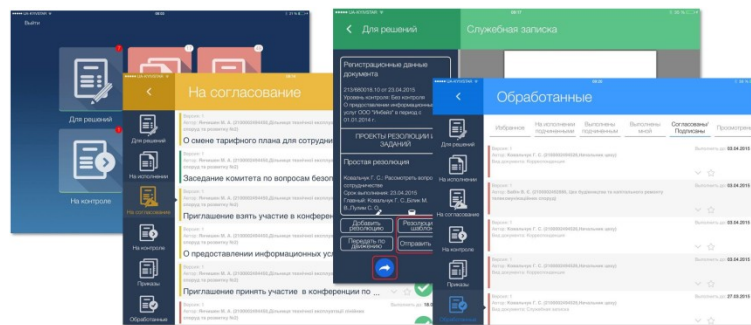


Рис. 3.1 Програмне забезпечення Megapolis. Документообіг

OPTIMA-WorkFlow це комплексна платформа для створення автоматизованих систем керування документами Система Optima Workflow призначена для керування процесами створення, обробки, тиражування та зберігання документів або інших інформаційних об'єктів, а також автоматизації основних процедур сучасного діловодства та організації документообігу (рис. 3.2).

Док Проф автоматизує весь комплекс документообігів: введення в систему документів, їх реєстрацію, розповсюдження та редагування, оперативне-зберігання, пошук і перегляд, відтворення, контроль виконання, розмежування доступу до документів, прискорення роботи над документами, покращення зберігання та оформлення документів тощо. СЕДО «Док Проф» підтримує використання електронного цифрового підпису, що забезпечує організацію якісно нового юридично значущого документообігу (рис. 3.3).

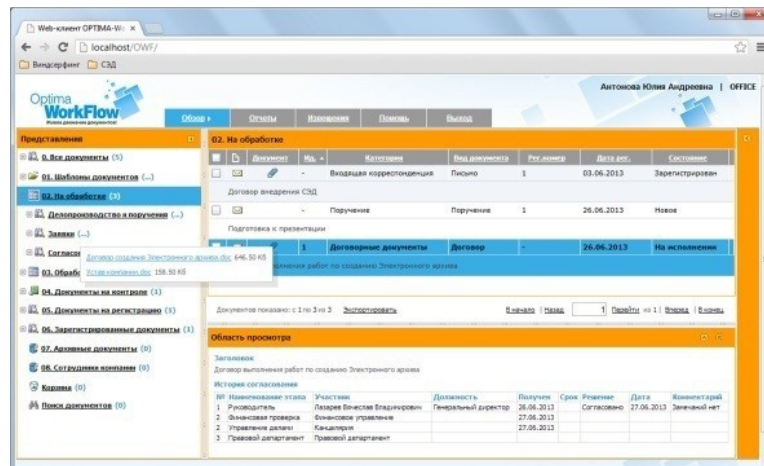


Рис. 3.2 Програмне забезпечення OPTIMA-WorkFlow

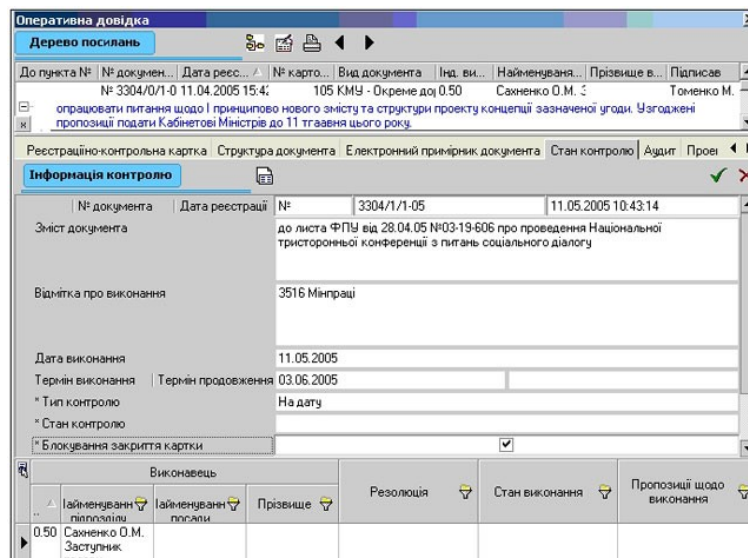


Рис. 3.3 Програмне забезпечення Док Проф

ДЕЛО це система з повним набором інструментів для управління документообігом та діловодством, розрахована на максимальні навантаження. Надійне та безвідмовне рішення (рис. 3.4).

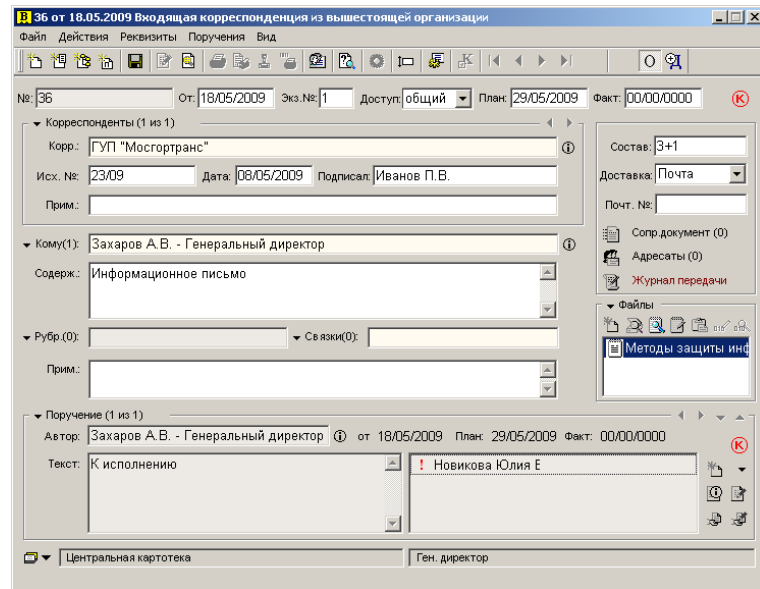


Рис. 3.4 Програмне забезпечення ДЕЛО

MasterDOC являє собою програмний комплекс на платформі IBM Lotus Notes/Domino для автоматизації управлінського документообігу та діловодства підприємств та організацій різних форм власності, масштабів та структур (рис. 3.5).

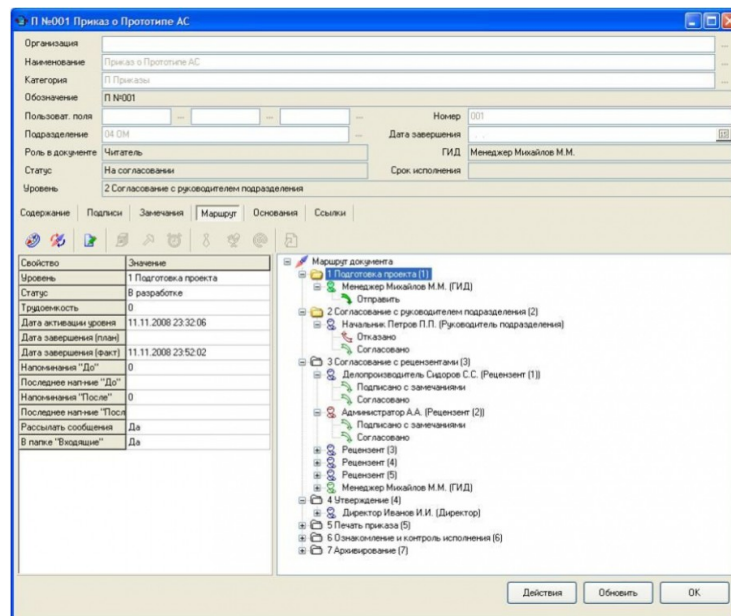


Рис. 3.5 Програмне забезпечення MasterDOC

Атлас ДОК являє собою модульне рішення в галузі організації електронного діловодства та документообігу. Система підходить для

використання як у державних організаціях, так і у комерційних структурах будь-якого масштабу (рис. 3.6).

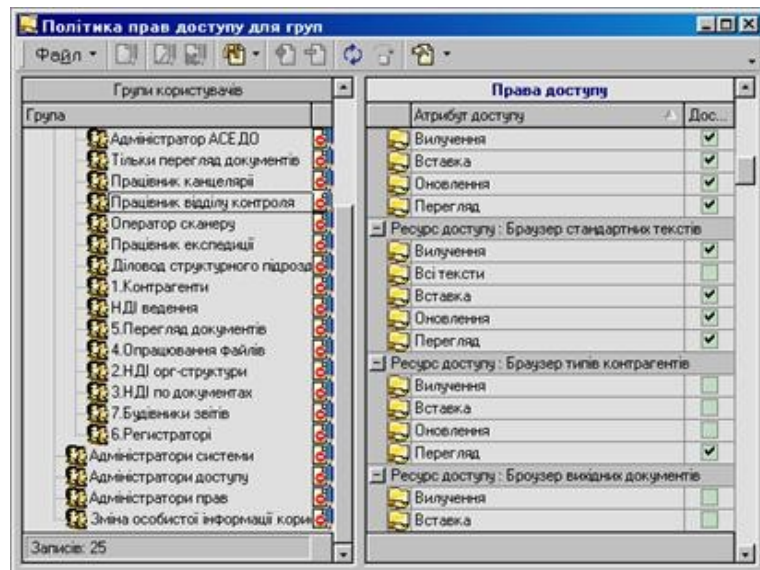


Рис. 3.6 Програмне забезпечення Атлас ДОК

Летограф готове централізоване розширюване рішення для автоматизації документообігу та архіву територіально-розподілених організацій.

Система включає унікальний набір функціональних можливостей для комфортної щоденної роботи. У системі реалізовано інноваційний підхід до автоматизації, що знижує терміни та витрати на впровадження та розвиток. В основі ЛЕТОГРАФ застосовується потужна технологічна платформа, що забезпечує швидку та надійну роботу. Замовник, який ухвалив рішення про впровадження системи, платить лише за те, що використовує (рис. 3.7).

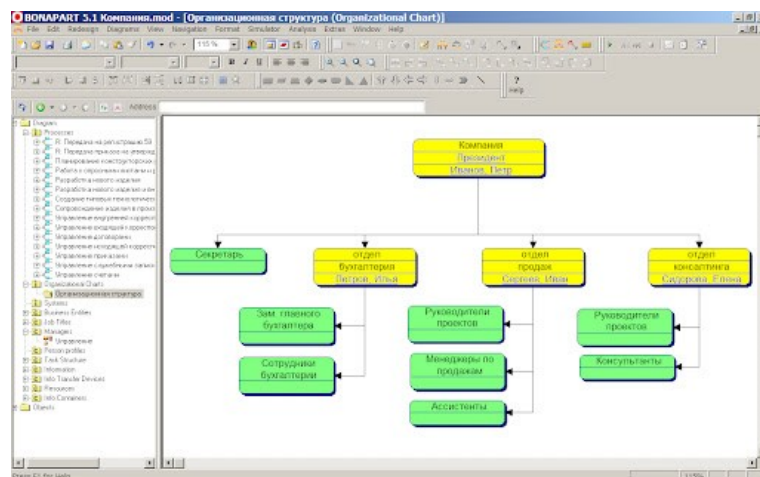


Рис. 3.7 Програмне забезпечення Летограф

АСКОД це сервіс (програмне забезпечення) для зовнішнього юридично значимого документообігу, який дозволяє виконувати погодження, підписання та обмін електронними документами між суб'єктами правовідносин (рис. 3.8).

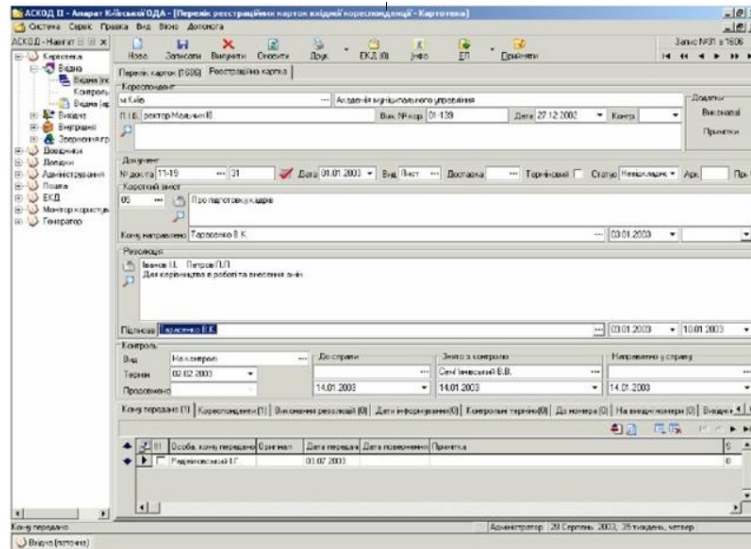


Рис. 3.8 Програмне забезпечення АСКОД

El-Doc інтегрована інтелектуальна платформа яка автоматизує документообіг та процеси обробки документованої інформації, що має у собі:

ElDoc IDP (Intelligent Document Processing) – високотехнологічне рішення для високоінтелектуальної обробки документів, це рішення базується на використанні когнітивних технологій для класифікації, нормалізації («image clearance & enhancement»), розпізнавання інформації зі сканованих та цифрових документів;

ElDoc BPM (Business Process Management) – високотехнологічне рішення для управління бізнес-процесами, яке дозволяє налаштувати документообіг і формати документів відповідно до різних бізнес-сценаріїв і вимог, використовуючи можливості «No Code» (рис.3.9).

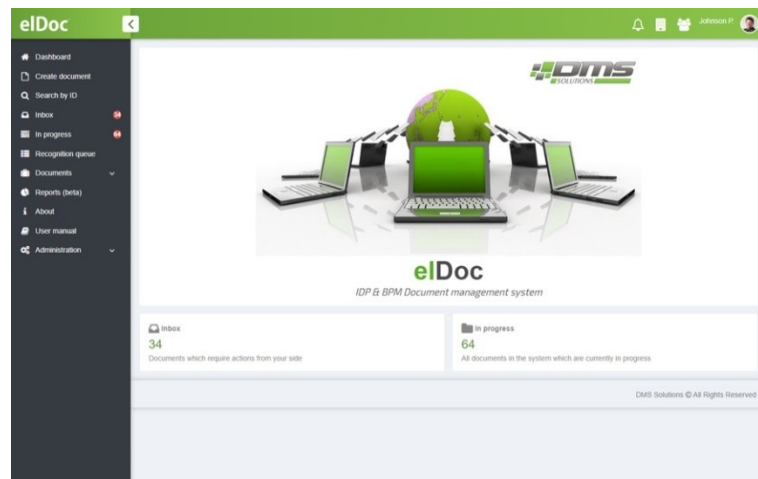


Рис. 3.9 Програмне забезпечення ElDoc

Для проведення порівняльного аналізу характеристик програмного забезпечення захисту інформаційних процесів у діловодстві були обрані такі системи, як: Megapolis. Документообіг, OPTIMA-WorkFlow, АСКОД, Док Проф та El-Dok. Вибір був обумовлений результатами дослідження Центрального державного електронного архіву України щодо використання органами влади систем електронного документообігу. Згідно з ним, у 39,5% державних органів влади функціонує система електронного документообігу Megapolis. Документообіг, у 13,2% – система OPTIMA-WorkFlow, у 10,5% – АСКОД та у 5,3% – Док Проф [2].

Порівняння здійснювалось за такими характеристиками: робота з документами (реєстрація, накладання резолюцій, контроль за виконання, відстеження документів, наявність централізованого сховища документів, розповищення та прийом документів, пошук документів), налаштування (підтримка ПЗ, сповіщення, поєднання з іншими ПЗ), захищеність (контроль за цілісністю документів, підтримка ЕЦП), додатковий функціонал (автоматизація архівування документації, український правопис, функції електронної пошти).

Порівняння програмного забезпечення електронного документообігу представлено у таблиці 3.1. Для характеристики було використано таку систему оцінювання:

- «-» можливість не реалізована;
- «+» можливість повністю реалізована

Таблиця 3.1

Порівняння систем електронного документообігу

Вид характеристик	Характеристика	Megapolis	OPTIMA-WorkFlow	АСКОД	Док Проф	el-Dok
Робота з документами	Реєстрація документації	+	+	+	+	+
	Накладання резолюції	+	+	+	+	+
	Контроль за виконанням	+	+	+	+	+
	Відстеження документів	—	+	+	—	+
	ЦСД	+	+	—	—	+
	Розпоширення та прийом документів	+	+	+	+	+
	Пошук документів	+	+	+	+	+
Налаштування	Підтримка ПЗ	+	+	+	+	+
	Сповіщення	—	—	—	—	+
	Поєднання з іншими ПЗ	+	+	+	—	—
Захищеність	Контроль за цілісністю документів	+	+	+	+	+
	Підтримка ЕЦП	+	+	+	—	+
Додатковий функціонал	Автоматизація архівування документів	+	+	+	+	+
	Український правопису	+	+	+	+	+
	Функції електронної пошти	+	+	+	+	+

Програмне забезпечення захисту інформаційних процесів яке порівнювалось, належить до класу систем електронного управління документами. В усіх системах присутні можливості реєстрації документів, накладання резолюції та контролю за виконанням документів. Також усі системи мають у собі функції накладання резолюції, контроль за виконанням, розпоширення та прийом документів, пошук документів у системі, підтримку іншого використовуваного програмного забезпечення, контроль за цілісністю

документації, автоматизацію архівування документів, підтримку українського правопису та функцію електронної пошти.

Функцію відстеження документів у системі мають у собі три програмних забезпечення із представлених. А саме: OPTIMA-WorkFlow, АСКОД та el-Dok. Централізоване сховище документів, також, наявне не в усіх Програмних забезпеченнях, а тільки у Megapolis, OPTIMA-WorkFlow та el-Dok. Функція сповіщень доступна лише у системі el-Dok. Поєднання з іншим програмним забезпеченням реалізована у трьох системах, таких як: Megapolis, OPTIMA-WorkFlow та АСКОД. Підтримка електронного цифрового підпису є в усіх системах, окрім Док Проф.

Проблему з електронним цифровим підписом можна вирішити завдяки створенню внутрішнього атестаційного центру, це дасть змогу усім працівникам отримати електронний цифровий підпис. Також важливо створення в тих, які не мають цієї функції, електронних системах централізованого сховища документів так як це вагомо поіпшить процес пошуку та зберігання документів.

Проаналізувавши виконане порівняння систем електронного документообігу можна зробити висновок, що жодна із представлених програм не має у собі повний спектр функції по яким проводився аналіз. Усі системи мають спільні риси та відмінності. У кожній із систем електронного документообігу присутні як вади так і переваги над іншими.

Для вибору необхідного програмного забезпечення потрібно перш за все розуміти, який функціонал вимагається від системи електронного документообігу. Відмінності в характеристиках програмного забезпечення дозволяє вибрати той продукт, який буде необхідний в індивідуальному випадку.

Після аналізу систем Megapolis, Документообіг та OPTIMA-WorkFlow можна зробити висновок, що саме ці системи здатні реалізувати більше функцій на відмінність від інших систем, які було порівняно.

Але слід зазначити, що програмне забезпечення обирається згідно завданням, які необхідно виконувати у структурі. На базі МДУ використовується ПЗ АСКОД. Ця програма має весь необхідний функціонал для використання у закладах вищої освіти.

3.2. Здійснення захисту інформаційних процесів у Маріупольському державному університеті

Наразі, в умовах широкої доступності Інтернету та швидкого розвитку комунікацій, залишається помітний розрив між очікуваннями студентів та можливостями, які їм може запропонувати вища освіта (ЗВО).

Форми та методи роботи в ЗВО мають постійно формуватися залежно від інформаційних потреб та технологічного розвитку суспільства. При цьому не останнє місце займає забезпечення інформаційної безпеки як навчальних матеріалів, так і іншої інформації обмеженого доступу, а також самої ІТ-інфраструктури від випадкових або цілеспрямованих атак.

Заклади вищої освіти в Україні переживають період адаптації не лише до об'єктивних процесів інформаційного суспільства, а й до нових суспільно-політичних умов із різноманітними проявами конкуренції. Створення ефективних механізмів управління інформаційними ресурсами системи вищої освіти в сучасних умовах неможливе без наукового обґрунтування та практичної реалізації збалансованої політики інформаційної безпеки ЗВО, яка може формуватися на основі вирішення наступних завдань: аналіз процесів інформаційної взаємодії в усіх сферах основної діяльності ЗВО: інформаційні потоки, їх масштаби та якість, суперечності, конкуренція з виявленням власників і суперників; визначення ролі та місця політики інформаційної безпеки в управлінні інформаційними ресурсами ЗВО та вироблення гармонізуючих принципів і підходів; формулювання основних складових політики інформаційної безпеки: цілей, завдань, принципів та основних напрямів забезпечення інформаційної безпеки в ЗВО; розробка основних

методів управління процесом забезпечення політики інформаційної безпеки; підготовка проектів нормативних документів.

Під час вибору систем електронного документування звертають увагу на наступні критерії: безпека; простота у використанні; інтеграція; ціна. Найбільш використовуваною системою є АСКОД, яка призначена для автоматизації процесів діловодства та документообігу, накопичення та надійного зберігання документів, забезпечення оперативного доступу до документів, контроль виконавчої дисципліни, надання статистичної та аналітичної інформації, забезпечення конфіденційності, застосування електронного цифрового підпису, інтеграції процесів документообігу в територіально-розподілених підрозділах, забезпечення внутрішніх комунікацій структурних підрозділів. Вона підтримує технології Workflow, автоматизує процес документообігу чисельних процесів, включаючи розробку маршрутів, контроль за виконанням, розсилання повідомлень засобами самої системи, електронної пошти, SMS-повідомлень, можливість виконання автоматичних операцій системою електронного документообігу та іншими системами при досягненні певного етапу або стану документу тощо.

WEB-додаток системи АСКОД забезпечує повноцінну автоматизацію електронного документообігу для тих підрозділів, які територіально знаходяться у віддаленні від центрального підрозділу.

До основних загроз безпеки інформації відносяться розкриття конфіденційної інформації: компрометація інформації; несанкціоноване використання ресурсів локальної обчислювальної мережі; помилкове використання її ресурсів; несанкціонований обмін інформацією; відмова від інформації; відмова в обслуговуванні.

На базі мариупольського державного університету використовується система АСКОД.

Автоматизована система електронного документообігу АСКОД™ призначена для автоматизації процесів опрацювання документів шляхом використання сучасних комп'ютерних технологій, впровадження єдиної

технології роботи з різноманітними службовими документами, кореспонденцією, зверненнями громадян та іншими фінансово-господарськими документами

Система АСКОД має три види (рис.3.10):



Рис. 3.10 Види системи АСКОД

АСКОД™ Корпоративний створює загальний інформаційний простір та загальне централізоване сховище документів підприємства, автоматизує процеси діловодства та контролю за виконанням. Система значно скорочує термін проходження документації та підвищує ефективність роботи робітників (рис.3.11).

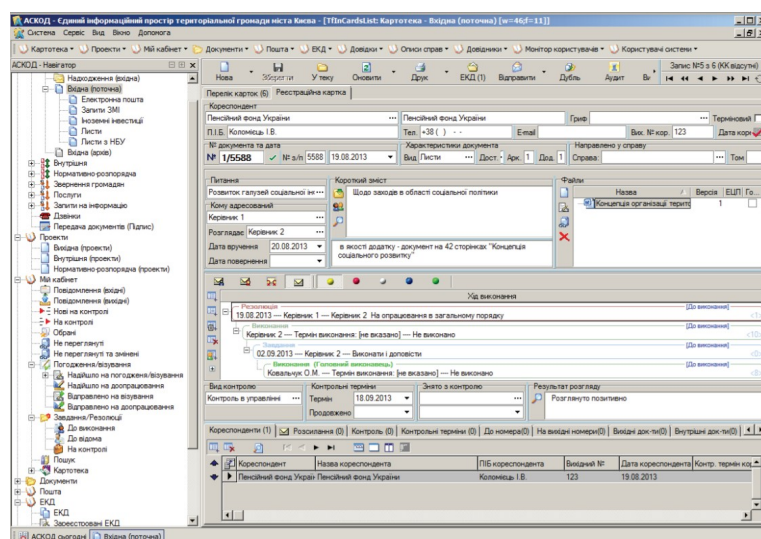


Рис. 3.11 АСКОД Корпоративний

АСКОД™-WEB забезпечує доступ до функцій системи АСКОД™ через вебінтерфейс з використанням найпопулярніших браузерів Google Chrome, Mozilla Firefox, Opera, Internet Explorer, Safari тощо, та охоплює практично усі аспекти електронного документообігу щодо опрацювання вхідної, вихідної, внутрішньо-розпорядчої кореспонденції, фінансово-господарських документів, звернень громадян та контроль за проходженням і виконанням документів, доручень і завдань (рис.3.12).

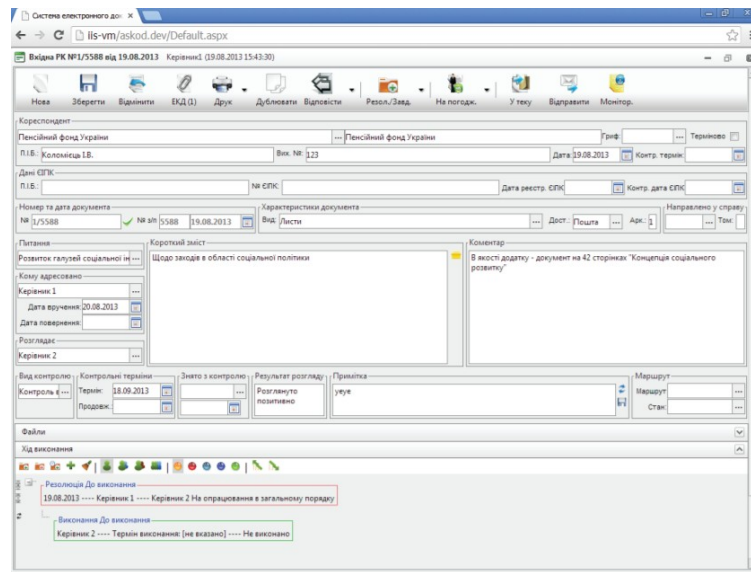


Рис. 3.12 АСКОД WEB

АСКОД™ Мобільний призначений для автоматизації управлінських функцій, що складають перелік службових обов'язків керівника. Встановлюється на мобільних комп'ютерних пристроях (планшетних ПК і смартфонах), що працюють під управлінням операційних систем Android, Windows, iOS (рис.3.13).

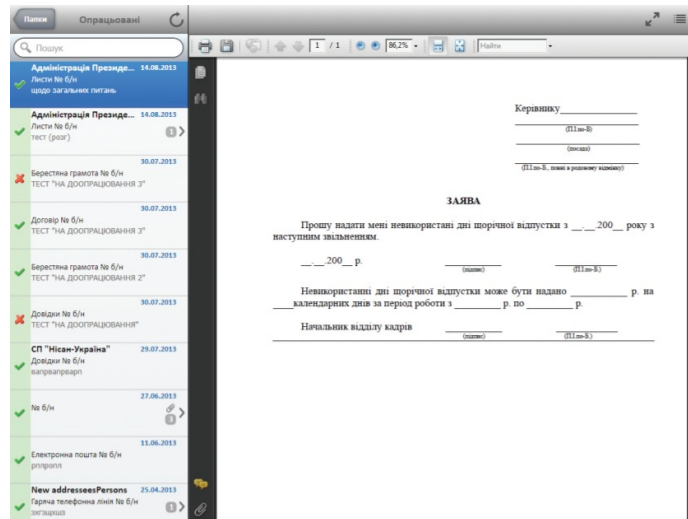


Рис. 3.13 АСКОД Мобільний

Система АСКОД™ призначена для автоматизації ділових процесів щодо обліку та опрацювання проектів документів, вхідної, вихідної, внутрішньорозпорядчої службової кореспонденції, нормативних документів та звернень громадян, запитів на інформацію, заявок, договорів, комерційних та інших документів, забезпечення контролю за виконанням документів, завдань та доручень. Система АСКОД™ дозволяє швидко і прозоро організувати усі процеси документообігу будь-якої установи, організації або підприємства як в умовах зосередженої, так і територіально-розподіленої оргструктури.

Доступ користувачів до системи АСКОД за допомогою WEB-додатку здійснюється згідно з встановленим регламентом виконання робіт, відповідно до наданих прав і повноважень щодо застосування функцій системи та доступу до даних і документів. Використання АСКОД-WEB розширює гнучкість, масштабованість системи та надає ряд переваг з розгортання та супроводження системи.

Відзнаками мобільної версії АСКОД™ є більш лаконічний графічний дизайн та узагальнений набір функцій, які дозволяють: відбирати документи із загального переліку за їх статусом та за значеннями їх реквізитів, читати електронну копію та вміст реєстраційної картки вибирати документ, розглядати та аналізувати документ, формувати документні постанови та завдання,

підписувати документ електронним цифровим підписом, затверджувати та візувати документ, здійснювати контроль за виконавчою дисципліною.

Робота з документами АСКОД™ автоматизує процеси роботи з вхідною, вихідною, розпорядчою, службовою кореспонденцією, зверненнями громадян та юридичних осіб, проектами документів, фінансовими документами, договорами, законами. На усіх етапах проходження та опрацювання документів система забезпечує підтримку взаємних посилань документів (рис.3.14).

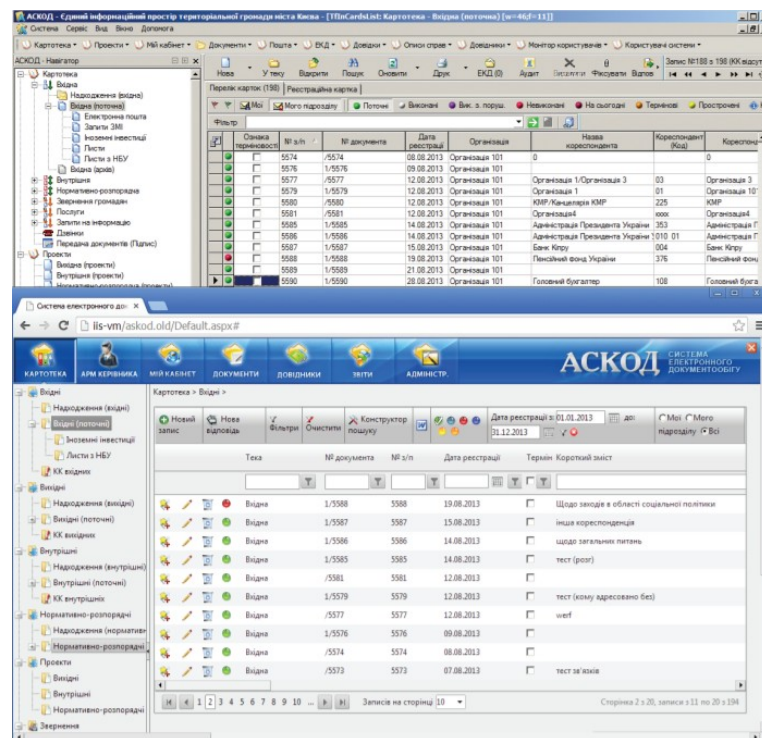


Рис. 3.14 Робота з документами АСКОД

Хід виконання документів АСКОД™ забезпечує зручний інтерфейс для накладання та виконання резолюції, формування доручень як на увесь документ загалом так і на окремі його частини. Контроль виконання документів забезпечується автоматичним формуванням нагадувань (всередині системи, засобами електронної пошти або SMS) (рис.3.15).

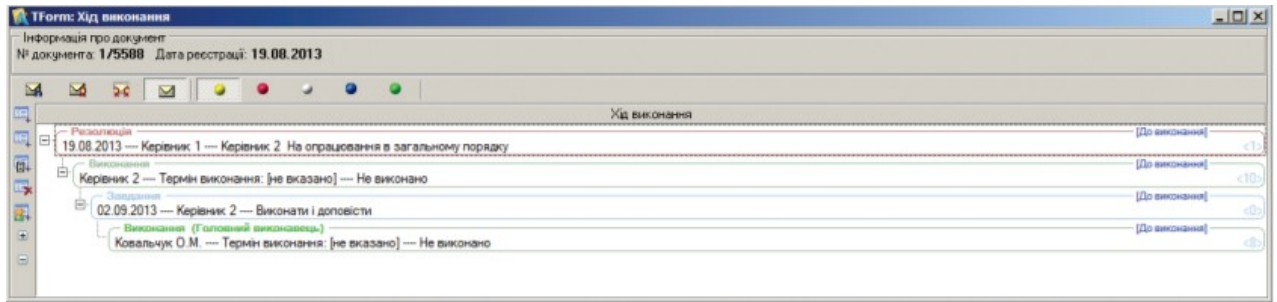


Рис. 3.15 Хід виконання документів АСКОД

Штрих-кодування В АСКОД™ підтримується функціонал нанесення штрих-коду та QR-коду (двовимірного матричного штрих-коду) на документи і швидкий індексований пошук документів за штрих-кодом і QR-кодом.

ЕЦП АСКОД™ надає можливість використання електронного цифрового підпису. Використання ЕЦП також надає можливість направленої (адресної) шифрування документів.

Робота з файлами Модуль використовується для створення та опрацювання електронних копій документів та електронних документів, що зберігаються в системі: отримання інформації у графічному вигляді про зв'язки між документами; повнотекстовий пошук документів (усі текстові формати, документи MS Office, PDF); створення та супровід реєстру електронних копій документів; сканування документів; перегляд та друкування електронної копії документа; застосування електронного цифрового підпису (ЕЦП); забезпечення конфіденційності шляхом шифрування; надання вичерпної інформації про документ.

Колективна робота (КР) АСКОД™ надає можливість групі фахівців спільно розробляти проекти документів, автоматизуючи всі стадії колективної роботи. Підсистема КР має такі особливості: інтегрований характер її функціоналу, коли в екранній формі зосереджений набір функцій, достатній для реалізації всіх етапів колективної роботи; оптимізована діаграма станів колективно розроблюваних проектів документів, орієнтована на управлінську специфіку; спеціалізована панель фільтрів, що забезпечує зручний відбір інформаційних об'єктів із загального переліку; ситуаційно-орієнтована

командна панель, склад кнопок якої визначається поточною ситуацією (станом і режимом) опрацювання інформаційного об'єкту. Ця панель забезпечує швидке виконання відповідних команд колективної роботи; підтримка паралельної та послідовної технології ведення версій проекту документу і його складових частин (рис.3.16).

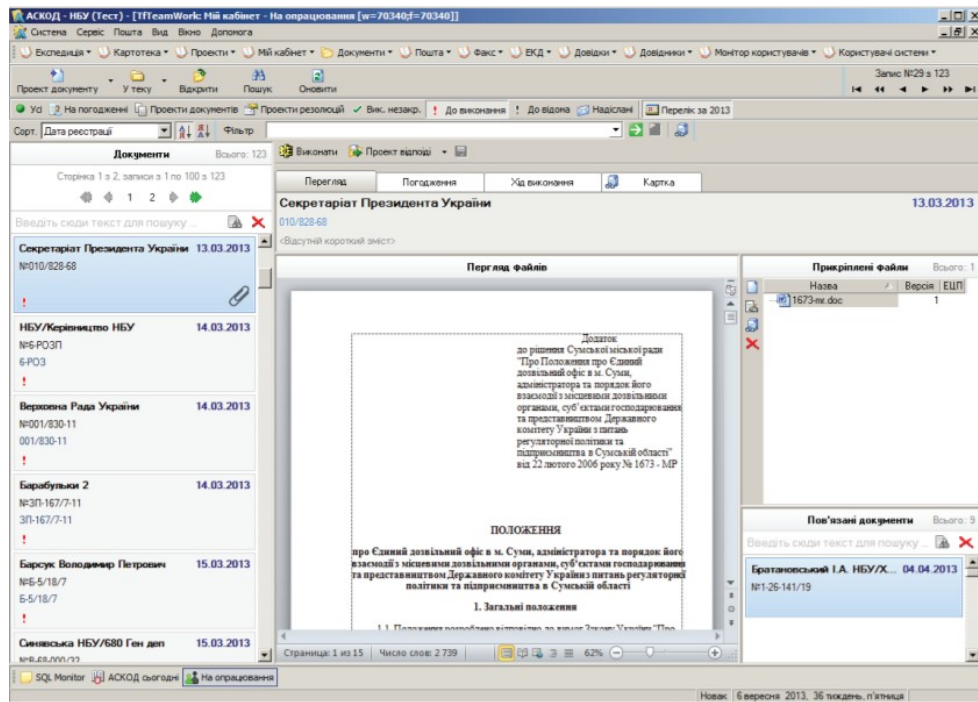


Рис. 3.16 Колективна робота АСКОД

Маршрутизація бізнес-процесів Модуль «Маршрутизація» системи АСКОД™ дозволяє автоматизувати довільні бізнес-процеси, що використовують різноманітні документи, створювати жорсткі та гнучкі маршрути документів, що забезпечуватимуть паралельне та послідовне погодження документів, автоматичні операції над документами, контрольоване проходження документа.

Панель «АСКОД™ Сьогодні». АСКОД™ містить узагальнену інформаційну панель, яка відображує ключові показники роботи поточного користувача. Структура панелі включає групи показників (Документи, Резолюції/Завдання, Повідомлення), всередині яких показники додатково групуються згідно станам інформаційних об'єктів. Кожен показник представляє

дані як у вигляді згорнутої кількості, так і у вигляді розгорнутого переліку інформаційних об'єктів відповідного типу (рис.3.17).

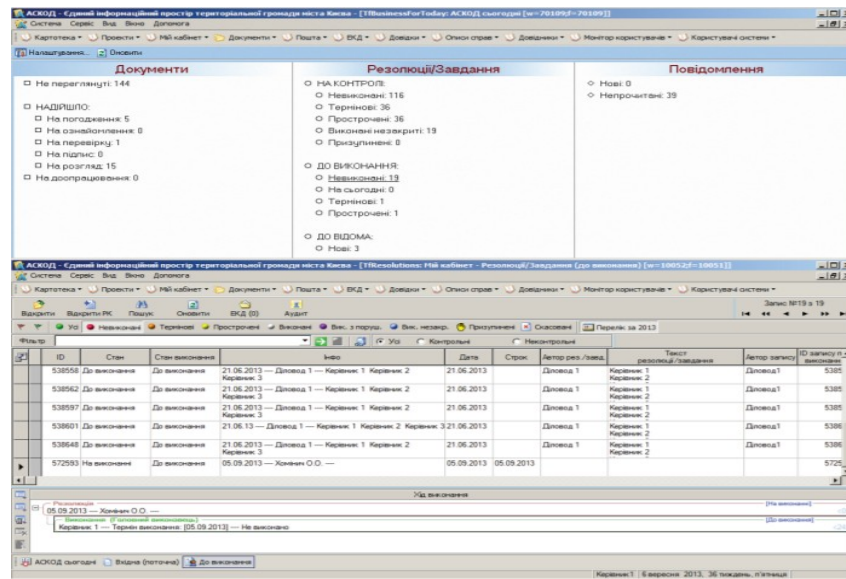


Рис. 3.17 Панель «АСКОД Сьогодні»

Адміністративні послуги АСКОД™ автоматизує всі етапи процесу надання адміністративних послуг: прийом документів від заявника, реєстрацію заяви на надання послуги, передачу заяви та вхідного пакету документів органу з надання послуг, отримання дозвільних документів від органу надання послуг, попередження заявника про готовність дозвільних документів, видача заявнику дозвільних документів, формування відповідних описів документів, що прийняті і передані адміністративного органу, видані заявнику. Штрих-код на опису дозволяє заявнику контролювати стан виконання його заяви на надання послуги.

Електронна черга Система «Електронна черга» є автономним програмним продуктом, який виступає розширенням функціоналу системи АСКОД™ в рамках процесу надання адміністративних послуг. До складу СЕЧ входять окремі модулі, що автоматизують відповідні етапи процесу керування чергою відвідувачів: Конфігуратор – налаштування параметрів системи «Електронна черга»; Інформаційний КІОСК – самостійне виконання відвідувачем операцій: вибір послуги, постановка в чергу, друк талона з

номером в черзі, представлення стану опрацювання заявки на надання послуги; АРМ Рецепсiонiста – виконання операцiй Інформацiйного кiоску рецепсiонiстом замість відвідувача; Інформацiйне ТАБЛО – відображення динаміки проходження номерів в черзі, призначення відвідувачу вікна обслуговування; АРМ фахівця центру надання послуг – проведення сеансів обслуговування відвідувачів; АРМ адміністратора – керування електронною чергою в «ручному» режимі. Система «Електронна черга» інтегрована з системою АСКОД™ на рівні спільних довідників.

Шаблони документів. АСКОД забезпечує можливість створення документів на підставі створених користувачем шаблонів з автоматичним заповнення визначених полів шаблону (рис.3.18).

The screenshot displays the ASKOD system's document template management interface. The top window, titled 'Шаблони документів', contains a table with columns for 'Назва (рус.)', 'Назва (укр.)', and 'Правка'. It lists various templates such as 'Шаблон наказів по трудовим відносинам', 'Про особовому складу', 'Про забезпечення прав кермачів', 'Про звільнення', 'Про надання відпустки', 'Про надання відпустки по догляд за дитиною', 'Про переведення на роботу з/з', 'Про прийняття на роботу за контрактом', 'Про прийом на роботу (П.1)', and 'Про призначення працівника до роботи (П.2)'. Below this, a larger window shows a preview of a selected template, 'Типова форма № П-8 Затверджена наказом Міністерства України від 09.10.95 р. № 253'. The preview form includes fields for 'підприємство, організація', 'Ідентифікаційний код ЄДРПОУ', 'Код за УКУД', 'НАКАЗ (РОЗПОРЯДЖЕННЯ) ПРО ПРИПІНЕННЯ ТРУДОВОГО ДОГОВОРУ (КОНТРАКТУ)', 'Номер документа #FulIndex#', and 'Дата складання #RegDate#'. The bottom status bar indicates 'Керівник: 6 вересня 2013, 36 годин, гітхаус'.

Рис. 3.18 Шаблони документів

Електронна пошта АСКОД™ містить вбудований поштовий клієнт, що забезпечує усі можливості з опрацювання електронної пошти, у тому числі автоматичну реєстрацію, розсилання документів за постійними та тимчасовими переліками адресатів.

Статистичні довідки і звіти Система АСКОД™ надає можливість автоматизованого формування визначеного переліку статистичних довідок щодо документообігу та стану виконавчої дисципліни за певний період часу. За допомогою операції експорту та налаштування довільних фільтрів користувачі

мають можливість на основі системних переліків формувати довільні звіти. Нескладні лінійні звіти користувач може будувати у модулі «Генератор звітів».

Датовані довідники з підтримкою спадковості Інформаційна сумісність усіх компонентів системи АСКОД™ базується на єдиній нормативно-довідковій інформації. Модулі ведення довідників АСКОД™ побудовані за принципами підтримки часу дії та спадковості елементів.

Підсистема безпеки Підсистема безпеки АСКОД™ забезпечує шифроване збереження даних облікових записів у базі даних, налаштування термінів дії паролів, складності паролів, захист від несанкціонованого доступу до системи, часом «холодного» простою системи, керування доступом до даних та інше. Окремо виконується налаштування захищених протоколів зв'язку. Забезпечується можливість використання засобів шифрування документів третіх розробників за допомогою відповідного API.

Моніторинг. Усі дії користувачів у системі АСКОД™ фіксуються у відповідному журналі. Дані журналу історії дій користувачів завжди доступні у різноманітних зрізах – за датами, по модулям, по користувачам або по конкретному документу (рис.3.19).

Пошук і фільтри За допомогою зручних механізмів пошуку і фільтрів АСКОД™ надає можливість здійснювати локальну та глобальну вибірку накопиченої інформації як в рамках певної категорії документів, так і в межах усієї бази даних. Система забезпечує: оперативний пошук документів за реквізитами та їх комбінаціями; швидкий індексований пошук за ключовими словами; зберігання умов пошуку в іменованих шаблонах; застосування як тимчасових, так і постійних фільтрів зі зберіганням умов фільтрації в шаблонах для повторного використання; комбінування фільтрів; повнотекстовий пошук у файлах.

Адміністрування. Модулі підсистеми адміністрування системи АСКОД™ дозволяють гнучко налаштувати систему для кожного користувача, або групи користувачів, керувати обліковими записами користувачів, налаштовувати ролі та різноманітні дозволи користувачам, налаштовувати

глибину моніторингу дій користувачів, формувати друкувальні форми реєстраційних та контрольних карток, виконувати сервісні операції з базою даних тощо (рис.3.20).

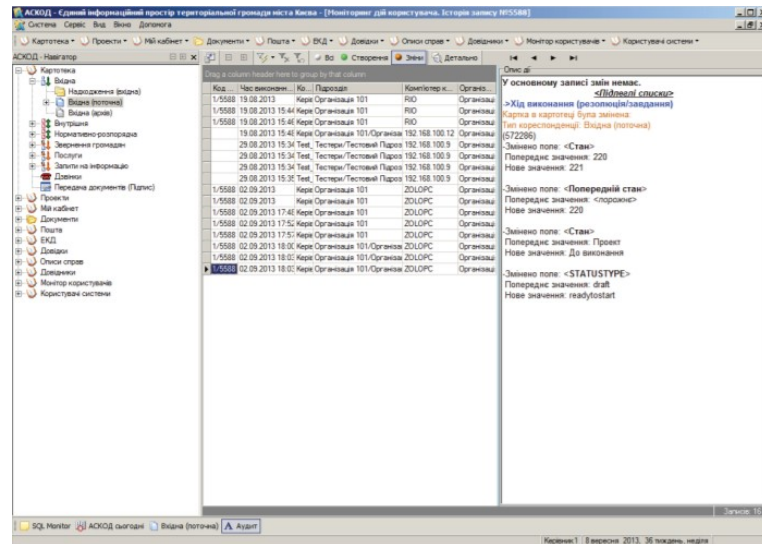


Рис. 3.19 Моніторинг

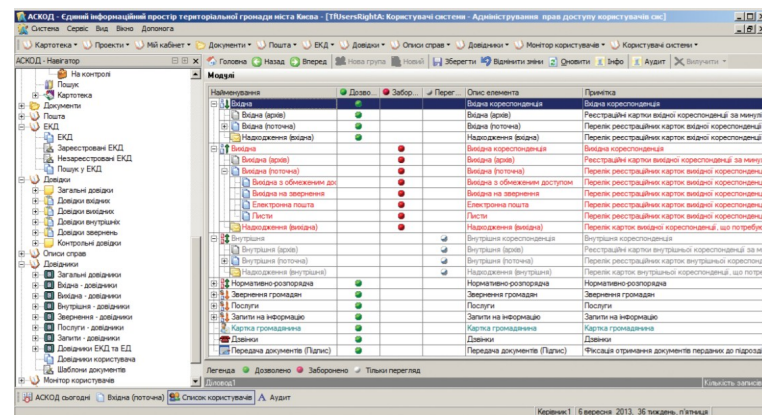


Рис. 3.20 Адміністрування

АСКОД™ Конструктор АСКОД™ надає великий обсяг можливостей щодо налаштування та доробки базового функціоналу Системи відповідно до змін в предметній області та побажань користувачів, згідно з потребами розробки додаткових модулів для автоматизації необхідних процесів. За допомогою Конструктора користувач може самостійно створювати додаткові класифікатори і довідники, розробляти нові або редагувати існуючі форми

реєстраційних карток, журналів інформаційних об'єктів та змінювати дизайн шаблонів друку.

Функціональне ядро системи «АСКОД™» містить бізнес-логіку, що властива широкому спектру предметних областей і відображує специфіку та проблематику ділових процесів у таких галузях, як: банківська сфера (документообіг в державних і комерційних банківських установах), державні центральні, обласні, місцеві, районні органи законодавчої та виконавчої влади, єдині дозвільні центри надання адміністративних послуг, керування чергою відвідувачів в центрах надання адміністративних послуг, міністерства і відомства, промислові і комунальні підприємства.

Кожне галузеве рішення є окремим програмним продуктом і реалізоване як автономний набір функцій системи «АСКОД™».

Oracle Database (Oracle) – об'єктно-реляційна система керування базами даних від Oracle Corporation. Система електронного документообігу АСКОД™ застосовується тривалий час у багатьох державних установах та органах місцевого самоврядування, а також в банківських установах, промислових, енергетичних та комунальних підприємствах.

Система АСКОД підтримує обмін даними і документами з системою електронної взаємодії центральних органів виконавчої влади. Система АСКОД забезпечує можливість формування переліку публічної інформації (даних та електронних копій документів) для публікації на WEB-сайтах.

Відповідно до статті 9 Закону України «Про електронні документи та електронний документообіг» електронний документообіг – це сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів. Електронний документообіг здійснюється шляхом використання систем електронного документообігу. Система електронного документообігу – це організаційно-технологічний комплекс методичних, технічних, програмних та інформаційних засобів, який забезпечує комплекс фу-

нкції для роботи з електронними документами: перетворення паперових документів у електронні, організація захисту і розподілу доступу до електронних документів, їх маршрутизація, механізми узгодження документів [104].

Система електронного документообігу АСКОД призначена для автоматизації діловодства, діловодства, господарського та управлінського документообігу, організації колективної роботи над документами за безпаперовими технологіями та забезпечення електронного документообігу за допомогою електронного цифрового підпису. Сучасна версія системи електронного документообігу АСКОД™ працює на платформі системи управління базами даних ORACLE [98].

Oracle Database (Oracle) – це об'єктно-реляційна система управління базами даних від корпорації Oracle. Система електронного документообігу АСКОД™ вже давно використовується в багатьох державних установах та органах місцевого самоврядування, а також у банківських установах, промислових, енергетичних та комунальних підприємствах.

Наразі на базі системи електронного документообігу АСКОД реалізується декілька проектів з електронного управління, а саме: створення та впровадження систем електронного документообігу, систем електронної взаємодії структурних підрозділів державних підприємств та установ, автоматизованих систем центри надання адміністративних послуг та інші проекти.

Система АСКОД підтримує обмін даними та документами із системою електронної взаємодії центральних органів виконавчої влади. Система АСКОД забезпечує можливість формування списку загальнодоступної інформації для публікації на WEB-сайтах.

Система АСКОД дозволяє реалізувати технологію централізованого документообігу для підприємств з територіально розподіленою організаційною структурою та забезпечує повноцінну роботу територіально віддалених користувачів системи через WEB-доступ. WEB-інтерфейс системи АСКОД дозволяє географічно віддаленим і мобільним користувачам отримати доступ до центральної бази даних системи для виконання всіх необхідних дій у процесах

робочого процесу, в тому числі ведення власного локального робочого процесу відповідно до наданих прав і повноважень. Робота користувачів у системі АСКОД через WEB-доступ може здійснюватися за допомогою таких браузерів: Mozilla FireFox 3.5+, Google Chrome 5+, Internet Explorer 8+, Safari 5+, Opera 12.0. Система АСКОД має інтерфейс програмування (API) для інтеграції з іншими додатками, а також підтримує можливість експорту даних в інші формати (наприклад, XML, MS Office).

Висновки до розділу 3

Правильно обране програмне забезпечення – це запорука електронного документообігу. Системи можуть значно полегшити роботу персоналу, якщо буде автоматизація робочого процесу. Маріупольський державний університет у своїй роботі використовує таке програмне забезпечення як АСКОД. Ця система відповідає вимогам, які встановлює заклад вищої освіти.

На серверах центрального офісу підприємства встановлюється програмне забезпечення та база даних системи електронного документообігу АСКОД. Користувачі системи АСКОД у територіально віддалених підрозділах та мобільні користувачі можуть працювати в системі АСКОД через WEB-доступ або за допомогою планшетних пристроїв.

WEB-додаток системи АСКОД забезпечує повноцінну автоматизацію процесів документообігу на територіально віддалених підрозділах. Використання WEB-додатку системи АСКОД не вимагає установки на робочих місцях користувача.

Недоліками системи АСКОД є відсутність централізованого сховища документів та нагадувань користувачам, а також неповне впровадження електронного цифрового підпису всіх працівників органів місцевого самоврядування та інтеграції з іншим програмним забезпеченням.

Проблему з електронним цифровим підписом можна вирішити, створивши внутрішній центр сертифікації, тоді кожен працівник місцевого самоврядування матиме свій цифровий підпис. Також важливо створити централізоване

зберігання документів, оскільки це значно полегшить процедури пошуку та зберігання документів. Крім того, необхідно вдосконалити процеси інтеграції СЕД з іншим програмним забезпеченням, що зробить його більш ефективним.

Тому, враховуючи сучасний розвиток інформаційних технологій та розвиток економічних процесів на державному рівні, слід зазначити необхідність удосконалення системи електронного документообігу АСКОД. Покращення системних недоліків може значно спростити використання продукту та нормалізувати виконання проектів електронного урядування.

ВИСНОВКИ

За час свого існування людство пережило багато інформаційних революцій, вони стали причиною перетворень суспільних відношень через значні зміни у сфері обробки інформації. Наслідком подібних перетворень, зазвичай ставало надбання людством нової якості в процесі своєї еволюції. З кожним роком інформаційні системи ускладнюються, інформаційна безпека й політика набувають усе більш глобальний характер, виходячи на перший план. У ХХІ ст. виникло багато проблем, пов'язаних з інформаційною безпекою.

Роки паперового діловодства створили систему в структурах нашої держави. Одним з багатьох недоліків цієї системи є необхідність роботи із матеріальними об'єктами, що значно уповільнює більшість робочих процесів. Побудова кращої системи в інформаційному суспільстві, має базуватися на найкращих здобутках «паперового світу» при мінімізації його недоліків. Цей підхід спростить і прискорить перехід на новий етап розвитку електронного документообігу – електронного діловодства. Впровадження електронних систем обміну даними в усіх галузях країни, відкриває можливість застосування великої гнучкості в обробці і зберігання інформації та примушує організації чи структури до роботи швидше та ефективніше приймати рішення відповідно до швидкої зміни ситуації в реальному часі.

Процеси глобалізації дуже гостро дали про себе знати й, крім позитивних елементів, виникли серйозні негативні явища, до яких світова спільнота виявилася неготовою. Головною умовою роботи державного службовця повинні бути знання про інформаційну безпеку, її структурні складові та критерії. З кожним роком стає нагальною роль інформаційної безпеки, оскільки суспільство вступає в епоху інформаційних війн, при яких цінність інформації зростає в багато разів. При цьому інформація – це не тільки товар, а й інструмент маніпуляції суспільством, думкою громадян, створенню конфліктів.

Отже, як людина потребує захисту від інформації, так і інформація потребує захисту від людини. Особливо зростає роль інформаційної безпеки у сфері високих технологій, бо саме цифрова інформація стає одночасно і сировиною, і продуктом, яку виробляють, обробляють, продають та, на жаль, частіше крадуть. Здебільшого нині визначають інформаційну безпеку через комп'ютерну безпеку. Дійсно, величезні обсяги інформації, що містяться на електронних носіях дедалі відіграють усе більшу роль у сучасному світі. Але ця інформація дуже вразлива, що зумовлене її великими обсягами, багатозначністю, можливістю «інформаційних диверсій», анонімністю доступу. Захист інформації, що розміщена в середовищі комп'ютера – це набагато складніше, ніж збереження таємниці звичайного поштового листування. Враховуючи це, можна зробити висновок, що проблеми інформаційної безпеки надзвичайно актуальні й потребують поглибленого вивчення.

Впровадження оновлених інформаційних технологій та загальна комп'ютеризація призвели до того, що інформаційна безпека стала абсолютно необхідною та однією з характеристик інформаційних систем.

Неефективність державного управління привели до того, що інформаційна безпека України знаходиться на низькому рівні. Недостатня спрямованість управління на захист інтересів, а також непослідовність та неефективність реформ, нестача нормативно-правової бази про інформаційну безпеку, недостатній рівень кваліфікації державних службовців із питань інформаційної безпеки, корупція у структурах управління – усе це негативно впливає на розвиток інформаційної безпеки суспільства.

Щоб інформаційна безпека України відповідала рівню провідних держав, потрібні послідовні дії держави для підвищення ефективності та розвитку інформаційних систем.

З огляду на цей безперервний розвиток та постійну інформаційну боротьбу, яка є одним із важливих елементів сучасної світової політики, для забезпечення своєї незалежності Україні необхідно й надалі удосконалювати та

розвивати як правову базу, у тому числі міжнародну, так і структурну та технічну складову інформаційної безпеки.

Тому актуальність кваліфікаційної роботи обумовлена широким використанням комп'ютерних технологій у всіх сферах діяльності людини, що створює проблему захисту інформаційних процесів від кіберзловмисників.

У рамках кваліфікаційної роботи було розглянуто історіографію та термінологію у ланці захисту інформаційних процесів у діловодстві засобами програмного забезпечення. Також було проаналізовано стан нормативно-правової бази теми та зроблено огляд та порівняльну характеристику дійсного програмного забезпечення захисту інформаційних процесів у діловодстві.

Діяльність усіх сфер життя людини тісно пов'язано із комп'ютерними технологіями. Доцільним буде ставитися серйозно до електронних носіїв інформації. Викрадення або знищення особистих даних може торкнутися кожного у будь-який час. Завадити цьому можна, саме для цього і розробляється програмне забезпечення для захисту інформації

Широке використання інформаційних технологій у всіх сферах життя суспільства робить досить актуальною проблему захисту інформації, її користувачів, інформаційних ресурсів, каналів передачі даних злочинних посягань зловмисників.

Складність створення системи захисту визначається тим, які дані можуть бути вкрадені залишаючись на місці. Цінність деяких даних полягає в тому, щоб володіти ними, а не руйнувати чи змінювати їх.

Забезпечення інформаційної безпеки – дороге задоволення, і не стільки через вартість закупівель або встановлення різного обладнання або програмного забезпечення, скільки через те, що важко кваліфіковано визначити межі розумної безпеки і відповідної підтримки системи в працездатному стані.

Кожен збій комп'ютерної мережі – це не лише моральні збитки для співробітників, підприємств, корпорацій та мережевих адміністраторів. У процесі розвитку електронних технологій та «безпаперового» документообігу, серйозний збій локальних мереж може сповільнити або і зовсім зупинити

роботу цілих підприємств, що призведе до значних збитків. Тому не випадково захист даних у комп'ютерній мережі є однією з найгостріших проблем.

Таким чином, можна зазначити, що захист інформаційних процесів у діловодстві – це не забаганка, а гостра необхідність для кожної людини. Усі данні, які знаходяться на електронній носія знаходяться у можливій небезпеці. Саме тому програмне забезпечення для захисту будь-якої інформації абсолютно необхідне.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Арістова А. Наука «інформаційне право» на новому етапі розвитку інформаційного суспільства. Київ, 2011. № 1. С. 3-11.
2. Баглай Р.О. Загрози безпеки хмарних технологій для банків. Системи обробки інформації, 2018. № 1 (152). С. 127-135.
3. Бачило І., Соснін О. Інформаційне право як запорука інноваційного розвитку нації. Київ, 2012. № 1. С. 12-14.
4. Белай С.В., Корнієнко Д.М. Інформаційна безпека сьогодення – невід’ємна складова воєнної безпеки. Актуальні проблеми управління інформаційною безпекою держави. Київ: Національна академія Служби безпеки України, 2018. 408 с.
5. Богуш В., Юдін О. Інформаційна безпека держави. К.: «МК-Прес», 2005. 432 с.
6. Бурячок В., Богуш В., Борсуковський Ю., Складанний П. Модель підготовки фахівців у сфері інформаційної та кібернетичної безпеки в закладах вищої освіти України. Інформаційні технології та засоби навчання, 2018. Т. 67, № 5. С. 277–291.
7. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. К.: СІК ГРУП УКРАЇНА, 2015. 449 с.
8. Василюк В. Об’єкти захисту інформації. Методи та засоби захисту інформації. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2006. № 2 (13). С. 88-102.
9. визначених політикою безпеки властивостей інформації (конфіденційності, цілісності та
10. визначених політикою безпеки властивостей інформації (конфіденційності, цілісності та
11. визначених політикою безпеки властивостей інформації (конфіденційності, цілісності та

12. визначених політикою безпеки властивостей інформації (конфіденційності, цілісності та

13. Вознюк К.О. Стан та перспективи впровадження електронного урядування на місцевому рівні. Київ: Електронне урядування, 2016. 228 с.

14. Войнаренко М. П., Кузьміна О. М., Янчук Т. В. Інформаційні системи і технології в управлінні організацією. Вінниця: Едельвейс і К, 2015. 496 с.

15. Войціховський А.В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. Журнал східноєвропейського права. 2018. № 53. С. 26–37.

16. Горбатюк О.М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть. Вісник Київського університету імені Т. Шевченка, 1999. № 14: Міжнародні відносини. С. 46–48.

17. Горбулін В.П., Литвиненко О.В. Національна безпека: український вимір. К. : ПП «Інтертехнологія», 2008. 104 с.

18. Гуржій Т. Інформаційне право: виклики гібридної війни. Зовнішня торгівля: економіка, фінанси, право, 2018. № 4. С. 16–26.

19. Гурковський В. І. Сутність і феноменологія глобалізації в контексті формування глобального інформаційного суспільства. Київ: Державне управління: удосконалення та розвиток, 2010. № 3.

20. Двойленко І.В. Вирішення типових проблем впровадження систем електронного документообігу із застосуванням електронного цифрового підпису в органах державної влади. Державне управління: теорія і практика, 2008. № 1 (7).

21. Дзюндзюк Б.В. Зарубіжний досвід взаємодії органів влади з громадянами в умовах розвитку інформаційного суспільства. Вісник Національного університету цивільного захисту України. Серія: Державне управління, 2016. № 2. С. 94–101.

22. Діловодство й архівна справа. Терміни та визначення понять (ДСТУ 2732:2004): Національний стандарт України від 28.05.2004 № 29.

23. Дмитренко М.А. Проблемні питання інформаційної безпеки України. Міжнародні відносини. Серія Політичні науки, 2017. № 17. С. 236–243.

24. Довгань О., Ткачук Т. Система інформаційної безпеки України: онтологічні виміри: «Інформація і право», 2018, № 1 (24). С. 89–103.

25. Доктрина інформаційної безпеки України: затверджено Указом Президента України від 25 лютого 2017 р. № 47/2017.

26. доступності) під час створення та експлуатації інформаційної мережі; регламентує порядок

27. доступності) під час створення та експлуатації інформаційної мережі; регламентує порядок

28. доступності) під час створення та експлуатації інформаційної мережі; регламентує порядок

29. доступності) під час створення та експлуатації інформаційної мережі; регламентує порядок

30. Драгомирецька Н.М., Фоменко Т.М. Проект «школа електронного урядування» як технологія модернізації управлінської діяльності на регіональному рівні. Київ: Електронне урядування, 2016. 228 с.

31. ДСТУ 3843-99. Державна уніфікована система документації. Основні положення [Чинний від 2000-07-01]. Вид. офіц. Київ : Держспоживстандарт України, 2000. 8 с.

32. ефективного знешкодження і попередження загроз для ресурсів шляхом побудови

33. ефективного знешкодження і попередження загроз для ресурсів шляхом побудови

34. ефективного знешкодження і попередження загроз для ресурсів шляхом побудови

35. ефективного знешкодження і попередження загроз для ресурсів шляхом побудови

36. Єсін В. І., Кузнецов Л.С., Сорока Л.С. Безпека інформаційних систем і технологій. Х. : ХНУ імені В. Н. Каразіна, 2013. 632 с.

37. з інформаційною безпекою; правові положення окремих видів процесу керування та

38. з інформаційною безпекою; правові положення окремих видів процесу керування та

39. з інформаційною безпекою; правові положення окремих видів процесу керування та

40. з інформаційною безпекою; правові положення окремих видів процесу керування та

41. Загаєцька О.А. Проблеми та перспективи надання електронних послуг в Україні. Київ: Електронне урядування, 2016. 228 с.

42. Задірака В.К. Сучасні методи розв'язання задач інформаційної безпеки. Вісник НАН України, 2014. № 5. С. 65–69.

43. захищених ІКСМ, регламентують порядок одержання, перетворення та використання

44. захищених ІКСМ, регламентують порядок одержання, перетворення та використання

45. захищених ІКСМ, регламентують порядок одержання, перетворення та використання

46. захищених ІКСМ, регламентують порядок одержання, перетворення та використання

47. Зінюк А., Змій Л. Особливості забезпечення інформаційної безпеки в електронному навчанні. Вісник Одеського національного університету. Соціологія і політичні науки, 2016. Т. 21. Вип. 3. С. 33–40.

48. Золотар О. О. Класифікація інформаційної безпеки. Київ: Інформація і право, 2011. № 2. С. 109-113.

49. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.

50. ІКСМ; етапи побудови КСЗІ [9].

51. ІКСМ; етапи побудови КСЗІ [9].

52. ІКСМ; етапи побудови КСЗІ [9].

53. ІКСМ; етапи побудови КСЗІ [9].

54. Ільїн О., Серих С. Когнітивна модель управління інформаційною безпекою вищого навчального закладу. Сучасний захист інформації, 2017. № 2(30). С. 24–29.

55. інформації і інформаційних ресурсів.

56. інформації і інформаційних ресурсів.

57. інформації і інформаційних ресурсів.

58. інформації і інформаційних ресурсів.

59. Інформаційна безпека /Ю.Я. Бобало та ін. ; за заг. ред. Ю.Я. Бобало та І.В. Горбатого. Львів: Видавництво Львівської політехніки, 2019. 580 с.

60. інформаційної безпеки; права, обов'язки й відповідальність персоналу роботи яких пов'язані

61. інформаційної безпеки; права, обов'язки й відповідальність персоналу роботи яких пов'язані
62. інформаційної безпеки; права, обов'язки й відповідальність персоналу роботи яких пов'язані
63. інформаційної безпеки; права, обов'язки й відповідальність персоналу роботи яких пов'язані
64. Інформація та документація. Керування документаційними процесами: Національний стандарт України від 02.12.2005 № 345.
65. Клименко І.В., Линьов К.О. Система електронного документообігу в державному правлінні. Київ: НАДУ, 2006. 32с.
66. Конституція України: офіц. текст. Київ : КМ, 2013. 96 с.
67. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: Одеська національна юридична академія. О.: Юридична література, 2003. 471 с.
68. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України. автореф. дис. канд. юрид. наук, Харків: НУВС, 2004.
69. Косошов О.М., Сірик А.О. Завдання захисту національного інформаційного простору за досвідом ведення гібридної війни РФ на Сході України. Системи озброєння і військова техніка, 2017. С. 38–41.
70. Костецька Т. А. Конституційно-правове регулювання інформаційних прав: деякі термінологічні аспекти. Київ: Часопис Київського університету права, 2013. № 2. С. 114-117.
71. Котлієва Я. І. Документообіг: організація та ведення. Харків: Фактді, 2002. 63 с.
72. Кохановська О. Основні теорії у сфері інформаційних правовідносин: концепція інформаційних прав як приватноправового інституту і теорія інформаційного права як галузі права у сучасній правовій доктрині України. Київ: Приватне право, 2013. № 1. С. 186-200.
73. Кочарян А. Б. Виховання культури користувача Інтернету. Безпека у всесвітній мережі. Київ, 2011. 100 с.

74. Крижановський В. Г., Сергієнко С. П. Апаратно-програмні засоби захисту інформації у корпораціях. Вінниця: ДонНУ імені Василя Стуса, 2019. 36 с.
75. Кукарін О.Б. Електронний документообіг та захист інформації. К.: НАДУ. 2015. 84 с.
76. Левченко Ю.О. Проблеми протидії інформаційній окупації в умовах гібридної війни. Інформаційна безпека в умовах гібридної війни: Міжнародна науково-практична конференція (м. Хмельницький, 16–17 листопада 2017 р.). Хмельницький: МВС УКРАЇНИ, 2017. 50 с.
77. Литвиненко О. Інформація і безпека: Нова політика, 1998, № 1. С. 47–49.
78. Ліпкан В. А. Правові засади розвитку інформаційного суспільства в Україні: монографія. К.: ФОП О. С. Ліпкан, 2015. 664 с.
79. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. Київ: КНТ, 2006. 280 с.
80. Лопушинський І. Електронна демократія та електронне урядування: досвід США для України: Публічне управління: теорія та практика, 2011, № 2 (6). С. 60–68.
81. Лужецький В.А. Кожухівський А.Д., Войтович О.П. Основи інформаційної безпеки. Вінниця: ВНТУ, 2013. 221 с.
82. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України. автореф. дис. канд. юрид. наук, К., 2007. 20 с.
83. Матвієнко О., Дубова С. Професіоналізація інформаційної діяльності у сфері державного управління. Київ: Вісник Національної академії державного управління при Президентові України, 2007. №1. С.52-60.
84. Матвієнко О., Цивін М. Основи організації електронного документообігу. Київ: Центр учбової літератури, 2008. 112с.
85. Міністерство цифрової трансформації України [Електронний ресурс]. – Режим доступу: <https://thedigital.gov.ua/>

86. Настюк В., Бєлєвцева В. Адміністративно-правовий захист інформації: проблеми та шляхи вирішення: монографія. Київ: Право України, 2013.

87. Охріменко, Г. В. Основні принципи та проблеми впровадження електронного документообігу в організації: Наукові записки. Серія «Культура та соціальні комунікації». Острог: Видавництво національного університету «Острозька академія», 2009. № 1. С. 300-307.

88. Петрова А. В. Програмні засоби захисту інформаційних процесів: Декада студентської науки. Маріуполь: Маріупольський державний університет, 2021. С. 207-209.

89. Петрова А. В. Програмне забезпечення захисту інформаційних процесів: Декада студентської науки Маріуполь: Маріупольський державний університет, 2022.

90. Петрова А.В. Безпека інформаційних систем: Феномен бібліотек в сучасному світі. Маріуполь: Маріупольський державний університет, 2021. С. 149-151.

91. Писаренко В. організаційно-правові засади електронного документування в органах влади: монографія. Полтава: ПУЕТ, 2012. 250 с.

92. Під поняттям нормативно-правового забезпечення слід розуміти сукупність

93. Під поняттям нормативно-правового забезпечення слід розуміти сукупність

94. Під поняттям нормативно-правового забезпечення слід розуміти сукупність

95. Під поняттям нормативно-правового забезпечення слід розуміти сукупність

96. Почепцов Г. Г., Чукут С. А. Інформаційна політика. К.: Знання, 2008. 665с.

97. правових норм, що визначають порядок створення, правовий статус і функціонування

98. правових норм, що визначають порядок створення, правовий статус і функціонування

99. правових норм, що визначають порядок створення, правовий статус і функціонування

100. правових норм, що визначають порядок створення, правовий статус і функціонування

101. Прилипко Н.О. Вдосконалення системи електронного документообігу в органах державної влади: Збірник наукових праць Донецького державного університету управління. Серія: Державне управління, 2014, №. 286. С. 155-164.

102. Про внесення змін до порядків, затверджених постановою Кабінету Міністрів України: Постанова від 08.09.2007, № 1004.

103. Про державну таємницю: Закон України від 21.01.1994, № 3855-ХІІ.

104. Про електронні документи та електронний документообіг: Закон України від 22.05.2003, № 851-IV.

105. Про електронну комерцію: Закон України від 03.09.2015, № 675-VIII.

106. Про затвердження Інструкції з діловодства за зверненнями громадян в органах державної влади і місцевого самоврядування, об'єднаннях громадян, на підприємствах, в установах, організаціях незалежно від форм власності, в засобах масової інформації: Постанова від 14.04.1997 № 348.

107. Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію: Постанова від 27.11.1998 № 1893.

108. Про затвердження Переліку типових документів, що створюються під час діяльності державних органів та органів місцевого самоврядування, інших установ, підприємств та організацій, із зазначенням строків зберігання документів: Наказ від 12.04.2012 № 578/5.

109. Про затвердження Примірного положення про експертну комісію об'єднання громадян, релігійної організації, а також підприємства, установи та організації, заснованої на приватній формі власності: Наказ від 30.04.2003 № 64.

110. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994, № 80/94-ВР.

111. Про захист пресоональних даних: Закон України від 01.06.2010, № 2297-VI.

112. Про інформацію: Закон України від 02.10.1999, № 2657-XII.

113. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 № 537-V

114. Про перелік відомостей, що не становлять комерційної таємниці: Постанова від 09.08.1993 № 611.

115. Про порядок здійснення криптографічного захисту інформації в Україні: Положення від 22.05.1998 № 505/98.

116. Про проведення експертизи цінності документів: Постанова від 08.08.2007 № 1004.

117. Рубан І.А. Сучасна модель державного управління розвитком інформаційного суспільства та шляхи її удосконалення. Київ: Електронне урядування, 2016. 228 с.

118. Семенченко А.І. Електронне урядування в Україні: проблеми та шляхи вирішення. Київ: Електронне урядування, 2016. 228 с.

119. Сороківська О.А., Гевко В.Л. Інформаційна безпека підприємства: нові загрози та перспективи: Економічні науки: Вісник Хмельницького національного університету, 2010, № 2. Т. 2. С. 32–35.

120. Тарнавський Ю.А. Технології захисту інформації: КПІ ім. Ігоря Сікорського. Київ, 2018. 162 с.

121. Тобто нормативно-правове забезпечення регламентує та визначає порядок захисту

122. Тобто нормативно-правове забезпечення регламентує та визначає порядок захисту

123. Тобто нормативно-правове забезпечення регламентує та визначає порядок захисту

124. Тобто нормативно-правове забезпечення регламентує та визначає порядок захисту

125. управління доступом в захищених ІКСМ; порядок створення й використання захищених

126. управління доступом в захищених ІКСМ; порядок створення й використання захищених
127. управління доступом в захищених ІКСМ; порядок створення й використання захищених
128. управління доступом в захищених ІКСМ; порядок створення й використання захищених
129. Хом'як І. Порівняльний аналіз систем електронного документообігу в органах місцевого самоврядування України, 2015. 3 с.
130. Хоффман Л. Дж. Современные методы защиты информации / Л. Дж. Хоффман [пер. с англ.]. М: Советское радио, 1980. 57 с.
131. Центр комп'ютерних технологій «ІнфоПлюс». Стислий опис системи електронного документообігу АСКОД [Електронний ресурс]. – Режим доступу: <http://www.docflow.ua/products/ackod.pdf>.
132. Чмерук Г.Г., Краліч В.Р. Цифрова нерівність в Україні: аналіз та шляхи подолання: Молодий вчений, 2018. № 7 (1). С. 289-293.
133. Чукут С.А., Загвойська О.В. Магістерська програма з електронного урядування як сучасний інституційний механізм реформування державного управління. Київ: Електронне урядування, 2016. 228 с.
134. Швець М. Правова інформатика. Київ, № 4(16), 2006.
135. Швець М., Калюжний Р., Гавловський В., Цимбалюк В. Інформаційне законодавство України: концептуальні основи формування. Київ: Право України, 2001. С. 88-91.
136. Шепета О.В. Адміністративно-правові засади технічного захисту інформації: монографія. Київ: ФОП О.С. Ліпкан, 2012. 296 с.
137. Юдін О., Матвійчук-Юдіна О., Яковенко О. Методи розробки та впровадження комплексної інформаційно-довідкової системи підтримки навчального процесу. Київ: ІПМЕ НАН України, 2007. С. 123-124.
138. Яковів, І. Базова модель інформаційних процесів та поведінки системи кіберзахисту: Information Technology and Security, 2019. С. 183-196.