МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Сумська філія

Кафедра соціально-економічних дисциплін

ТЕКСТ ЛЕКЦІЇ

з навчальної дисципліни «Інформаційне забезпечення професійної діяльності»
обов'язкових компонент
освітньої програми першого (бакалаврського) рівня вищої освіти

081 Право (право)

за темою – «Основи інформаційної безпеки»

Суми 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 30.08.2023 р № 7

СХВАЛЕНО
Вченою радою Сумської філії
Харківського національного
університету внутрішніх справ
Протокол від 29.08.2023 р № 8

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 29.08.2023 р № 7

Розглянуто на засіданні кафедри соціально-економічних дисциплін Протокол від 29.08.2023 р № 2

Розробники:
Доцент кафедри соціально-економічних дисциплін Сумської філії ХНУВС, канд.екон.наук, доцент Виганяйло Світлана Миколаївна

Рецензенти:
1. Доцент кафедри протидії кіберзлочинності, факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ, канд.пед.наук, доцент Тетяна Петрівна Колісник
2. Доцент кафедри кібернетики та інформатики СНАУ, канд.екон.наук, доцент Олександр Борисович В'юненко

План лекції

1. Інформаційна безпека та захист даних.
2. Складові інформаційної безпеки. Шляхи вирішення питань інформаційної безпеки. Критерії інформаційної безпеки та її складові частини.
3. Об’єкти захисту інформації. Законодавство про інформаційну безпеку. Основні терміни у сфері інформаційної безпеки. Вимоги до забезпечення захисту інформації в системі. Організаційні засади забезпечення захисту інформації.

Рекомендована література:

Нормативні документи

1. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII // Відомості Верховної Ради України. – 2015. – № 40-41. – ст. 379 URL: **https://zakon.rada.gov.ua/laws/show/580-19**
2. Закон України “Про захист персональних даних” від 01.06.2010 за 2297-VI. URL: **https://zakon.rada.gov.ua/laws/show/2297-17**
3. Про захист інформації в інформаційно-телекомунікаційних системах.

   Закон України URL: **https://zakon2.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80**
4. Про затвердження Положення про інформаційно-телекомунікаційну систему “Інформаційний портал Національної поліції України”: Наказ МВС України від 03.08.2017 № 676 URL: **https://zakon.rada.gov.ua/laws/show/z1059-17**
5. Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів: Постанова КМУ від 14 листопада 2018 р. № 1024 URL: **https://zakon.rada.gov.ua/laws/show/1024-2018-%D0%BF**

Основна

1. Виганяйло С. М. Інформаційне забезпечення професійної діяльності: навч. посіб. Харків: ХНУВС, 2021. 110 с. URL: **http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/11258/Informatsiine%20zabezpechennia%20profesiinoi%20diialnosti_Vyhaniailo_2021.pdf?sequence=1&isAllowed=y**
2. Клімушин, П. С. Інформаційні системи та технології в економіці : навчальний посібник / П. С. Клімушин, О. В. Орлов, А. О. Серенок; Нац. акад. держ. управління при Президентові України, Харк. регіон. ін-т держ. управління. - Харків : Вид-во ХарРІ НАДУ "Магістр", 2011. - 448 с. URL: http://dspace.univd.edu.ua/xmlui/handle/123456789/4730
3. Сезонова, І. К. Інформатика для правоохоронців: навч. посіб. / І. К. Сезонова; МВС України, Харк. нац. ун-т внутр. справ. - Харків, 2015. – 182 с. URL: **http://dspace.univd.edu.ua/xmlui/handle/123456789/1311**

Допоміжна

1. Вишня В. Б. Основи інформаційної безпеки: навч. посіб. / В.Б. Вишня, О.С. Гавриш, Е.В. Рижков. Дніпро: ДДУВС, 2020. 128 с. URL: **http://er.dduvs.in.ua/handle/123456789/4206**
2. Заплотинський Б.А. Інформаційні технології в юридичній діяльності.

Посібник. Київський інститут інтелектуальної власності та права НУ “Одеська юридична академія”, кафедра інформаційно-аналітичної та інноваційної діяльності, 2018.–108с.

3. Застосування інформаційних технологій у діяльності правоохоронних органів : зб. матеріалів кругл. столу (м. Харків, 9 груд. 2020 р.) / МВС України, Харків. нац. ун-т внутр. справ. – Харків : ХНУВС, 2020. – 132 с. URL: **http://dspace.univd.edu.ua/xmlui/handle/123456789/9984 http://dspace.onua.edu.ua/bitstream/handle/11300/11095/%D0%86%D0%A2%20%D0%B2%20%D0%AE%D0%94%20%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA.pdf?sequence=1&isAllowed=y**
4. Інформаційне забезпечення юридичної діяльності : підручник / В.Б. Вишня, Л.В. Рибальченко, О.О. Косиченко та ін.; за заг. ред. В.Б. Вишні; МВС України, Дніпропетр. держ. ун-т внутр. справ.- Дніпро : ДДУВС, 2019.- 227 с. URL:**http://er.dduvs.in.ua/handle/123456789/3718**
5. Інформаційне забезпечення діяльності Національної поліції України: зб. законодавчих та нормативних документів / уклад.:В.Б. Вишня та ін. Дніпро: ДДУВС, 2016. 476 с. URL: **http://er.dduvs.in.ua/handle/123456789/2043**
6. Кормич Б.А., Федотов О.П., Аверочкіна Т.В. Правове регулювання інформаційної діяльності: навчально-методичний. Одеська юридична академія. 2018. 150 с. URL:https://pidruchniki.com/15931106/politologiya/pravove_regulyuvannya_informatsiynoyi_sferi_ukrayini
7. Краснобрижий І.В. Інформаційне забезпечення професійної діяльності : навч. посіб. Уклад: І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков. Дніпро : ДДУВС, 2018. 220 с. URL: http://er.dduvs.in.ua/handle/123456789/2046
8. Методичні рекомендації щодо використання комп’ютерної програми «Навчальний ЄРДР» (для ролі «курсант») / [Розроб. Коршенко В. А., Демидов З. Г., Колмик О. О., Абламський С. Є.]; МВС України, Харків. нац. ун-т внутр. справ, Наук.-досл. лаб. з проблем розвитку інформац. технологій, Каф. крим. процесу та організації досуд. слідства ф-ту № 1. - Харків: ХНУВС, 2019. - 30 с. URL: **http://dspace.univd.edu.ua/xmlui/handle/123456789/6675**
9. Мордвинцев М. В. Використання автоматизованих систем відеодокументування переміщень об'єкта для протидії торгівлі людьми / М. В. Мордвинцев, О. В. Хлєстков, С. П. Ницюк // Використання сучасних інформаційних технологій в діяльності Національної поліції України: матеріали Всеукр. наук.-практ. семінару (м. Дніпро, 23 листоп. 2018 р.). – Дніпро: Дніпропетр. держ. ун-т внутріш. справ, 2018. – С. 52-54. URL: http://dspace.univd.edu.ua/xmlui/handle/123456789/3953
10. Наказ МВС “Про затвердження Положення про Інтегровану інформаційно-пошукову систему ОВС України” від 12.10.2009 за № 436. URL: **http://tranzit.ltd.ua/nakaz/**
11. Наказ МВС “Про затвердження Положення про систему Інтернет у телекомунікаційній мережі Національної поліції України” від 22.02.2017 № 141. URL: **http://tranzit.ltd.ua/nakaz/**

12. Нелюбов В.О., Куруца О.С. Основи інформатики. Microsoft Word 2016: електронний навчальний посібник. Ужгород: ДВНЗ УжНУ, 2018. 96 с. URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/18659
13. Про електронні довірчі послуги: Закон України від 5 жовтня 2017 р. № 2155-VIII. URL: **http://zakon2.rada.gov.ua/laws/show/2155-19/page**
14. Проведення оперативно-тактичних навчань на основі інформаційного моделювання дій нарядів та інших підрозділів Національної поліції : методичні рекомендації / О.О. Акімова, О.С. Гавриш, О.В. Махницький, С.О. Прокопов, Е.В. Рижков, Ю.І. Тюря. Дніпро: Дніпроп. держ. ун-т. внутр. справ, 2017. 37 с.
URL:**https://dduvs.in.ua/wp-content/uploads/files/Structure/library/student/eib2.pdf**

Інформаційні ресурси в Інтернеті

1. **http://www.nau.kiev.ua**
2. **http://www.liga.kiev.ua**
3. **http://www.informjustr.kiev.ua**
4. http://www.rada.gov.ua
5. https://zakon.rada.gov.ua
6. http://www.president.gov.ua

Текст лекції

1. Інформаційна безпека та захист даних.

Об'єктом автоматизації може бути діловодство або документообіг. Діловодство − це діяльність зі створення документів та Організації роботи з ними. Під організацією роботи з документами розуміють створення умов, що забезпечують рух, пошук і збереження документів. Рух документів в організації з моменту їх одержання або створення до завершення виконання або відправлення позначається як документообіг. Документообіг становить близько 15−20 % діловодства.

Діловодство і документообіг є окремими випадками більш загального поняття управління документами, яке, окрім них, включає ведення великих архівів документів, їх перетворення з однієї форми в іншу (наприклад, сканування і розпізнавання або публікація в Інтернет), розмежування і контроль доступу, координацію дій співробітників, а також тісну інтеграцію з офісними і прикладними програмами, що є інструментами обробки документів.

Сучасне українське діловодство здебільшого є спадком радянської системи. Залежно від виконуваних функцій розрізняють організаційно-розпорядницьке, бухгалтерське, нотаріальне, кадрове, технічне, медичне, військове та інші види діловодства. Кожний з них має свої відмітні риси, але спільним для будь-якої галузі та функції управління є організаційно-розпорядницьке (адміністративне) діловодство. Тому в разі впровадження системи автоматизації найчастіше йдеться про цей вид. Організаційно-розпорядницькі документи такі:

•організаційні − положення, статути, інструкції, правила;

•розпорядницькі − постанови, розпорядження, накази, вказівки, рішення;

•довідково-інформаційні − листи, доповідні і пояснювальні записки, протоколи, акти, огляди, звіти, стенограми, списки, переліки, реєстраційно-контрольні картки, графіки і т. ін.

Щодо системи управління розрізняють потоки вхідних (тих, що надходять), вихідних (тих, що відправляються) та внутрішніх документів.

За реалізованою концепцією розрізняють автоматизовані системи, зорієнтовані на вітчизняне і західне діловодство. Вітчизняне діловодство характеризується вертикальною спрямованістю − документ, що надходить в організацію, після реєстрації передається керівникові, який після розгляду документа накладає резолюцію із зазначенням відповідального виконавця. Далі документ надходить до відповідального виконавця, який або виконує документ, або направляє його на виконання своїм підлеглим. Після виконання документ передається у зворотному напрямку з нижнього рівня ієрархії до верхнього, де приймається звіт про виконання. На Заході звичною є горизонтальна схема − документи відразу направляються виконавцям без доповіді вищим керівникам. Ще однією важливою відмінністю нашої практики є наявність органу, що контролює виконання документа − перед відправленням документа відповідальному виконавцеві він ставиться на контроль. Таким чином, третя особа − діловод − завжди знає, у кого перебуває документ на виконанні і коли він має бути виконаний. Такі відмінності у веденні діловодства спричиняють суттєву різницю між системами західних і вітчизняних та російських розробників.

Стосовно завдань управління документами і застосування ІТ чіткої

класифікації систем не існує. Можна навести такий загальний розподіл.

Засоби автоматизації офісної діяльності − текстові редактори для підготовки і коригування документів, процесори електронних таблиць, програми генерації запитів за зразком з різних БД, мережні планувальники для призначення робочих зустрічей і нарад, засоби розробки і демонстрації презентацій, словники і системи порядкового перекладу, програми посилки і прийому факсів, електронна пошта для обміну повідомленнями і пересилання файлів. Це можуть бути окремі пакети (Word. WordPerfect. Excel. Lotus1-2-3 тощо), інтегрований пакет програм (MS Works) або узгоджений набір пакетів (Microsoft Office або Corel Perfect Office). Для створення додатків на основі цих пакетів використовують макромови чи діалекти Basic (Word Basic, Basic Excel та ін.) або єдину мову для розширення додатків. Для багатьох пакетів характерне використання так званих «майстрів» Wizard), які в режимі діалогу допомагають користувачеві виконати складну процедуру.

Автоматизовані системи контролю виконання документів (АСКВД) призначені для обліку всієї документації установи, поставлення на контроль і контролю за виконанням документів (нагадування про наближення строків закінчення виконання документа, повідомлення про прострочені документи тощо). З цією метою у системах передбачається ведення журналу реєстрації і контролю або реєстраційно-контрольних карток документів. Такі системи побудовані на основі персональних СКБД і використовуються персоналом з діловодства і групами контролю.

Електронні архіви − системи автоматизації, призначені, насамперед, для фізичного збереження електронних копій документів та їх пошуку. Основою таких систем є персональна або клієнт-серверна СКБД. Документи зберігаються або у базі даних, або у файловій системі. Недоліком першого варіанта є прив'язка до конкретної СКБД і складність відновлення після збоїв, а другого − низький рівень захищеності інформації. Електронні архіви забезпечують пошук як за атрибутами, так і за змістом документів і можуть включати функції з контролю за виконанням документів.

Якщо в АСКВД реалізується традиційний облік документів із заміною паперових журналів обліку на електронні, то електронні архіви передбачають принципово новий погляд на документообіг − у системі зберігаються не тільки реєстраційні та контрольні картки, а й повний текст документа і його зображення. При цьому полегшується пошук і відновлення документа, його тиражування і розсилання, заповнення полів карток і посилання на документ (дані автоматично розпізнаються з образу документа і переносяться в картку або новий документ). Водночас такий підхід вимагає більше ресурсів (насамперед, пам'яті ЕОМ) і додаткового обладнання (сканер, лазерний принтер), система працює ефективно лише в умовах комп'ютерної мережі, її експлуатація ускладнюється, що підвищує вимоги до користувачів та обслуговуючого персоналу.

Системи організації групової роботи (групове забезпечення, groupware) зорієнтовані на автоматизацію роботи невеликих колективів і підтримують коректне спільне використання інформації групою користувачів. Основним призначенням цих систем є автоматизація офісної діяльності, документообігу, координації користувачів під час виконання поточних проектів і відстеження їх здійснення. В основу покладено електронну пошту, яка «знає» належність

користувача до тієї чи іншої групи, структуру проекту та склад робочих груп і «вміє» розсилати повідомлення належним чином згідно з їхнім призначенням. При цьому відсутня структуризація проведення робіт − правила їх виконання у системі не визначаються.

Системи автоматизації ділових процесів (САДП, системи автоматизації управління потоками робіт, workflow-системи) застосовуються, насамперед, для автоматизації документообігу і рутинних багатокрокових офісних операцій. Серед найбільш відомих розробок можна назвати системи Staffware, ActionWorkflow System, “OPTiMA-WorkFlow”. Будь-яка САДП грунтується на комбінації таких технологій, як електронна пошта, управління проектами, робота з базами даних, об'єктно-орієнтоване програмування, CASE-технології.

САДП є складовою цієї групи додатків. Із суто технічного погляду work-системи одночасно обслуговують множину працівників і множину задач, тоді як groupware -додатки паралельно обслуговують множину користувачів і тільки одну задачу. Інші відмінності САДП такі:

• специфічність систем, зумовлена специфікою ділових процесів. Наприклад, на відміну від додатків календарного групового планування, які є стандартними для будь-якої організації, автоматизація ділових процесів − це технологія, яка допомагає користувачеві створювати додатки, необхідні саме йому;

• докладне визначення маршрутів, правил і ролей. Додаток колективного використання інформації стає додатком автоматизації управління потоками робіт тоді, коли визначений специфічний маршрут (наприклад, від А до В, від В до С), встановлені ролі (наприклад, А − організатор, В − юрист, С − ОПР) і зазначені певні правила («Контракт дійсний, якщо його схвалив С; якщо С його відхилив, контракт повертається до А, який вносить необхідні зміни»).

Системи керування (електронними) документами вважаються універсальними і мають забезпечувати:

• ведення довідника користувачів на основі організаційно-штатної структури організації;

• ведення журналів реєстрації і контролю виконання документів;

• контроль термінів виконання документів, оповіщення виконавця і діловода про наближення термінів контролю та про документи, не виконані вчасно;

• збереження документів у системі;

• підтримку шаблонів документів, складених документів, версій і підверсій, перехресних посилань між документами;

• відстеження документів поза системою, виписування документів із системи;

• пошук документів за атрибутами, повнотекстовий та нечіткий пошук;

• розробку документів, включаючи колективну розробку;

• візування, узгодження та затвердження документів;

• документообіг − усі види маршрутизації, автоматичне розсилання повідомлень, обмін повідомленнями і дорученнями усередині системи, формування реєстрів відправлення до зовнішніх організацій;

• ведення класифікаторів документів (за типом, видом тощо), довідників зовнішніх і внутрішніх організацій та ін.;

• суворе розмежування повноважень у системі, підтримку ролей,

протоколювання та аудит дій користувачів;

• шифрування, цифровий підпис;

• ведення справ документів, списання документів у справу, передачу справ на збереження в архів;

• формування необхідних звітів, зокрема статистичних звітів з діловодства організації.

Системи керування документами ґрунтуються на промислових СКБД (Oracle, Informix, MS SQL, Server, Sybase). Документи можуть зберігатись як у БД, так і у файловій системі. Загальні вимоги до системи автоматизації діловодства/документообігу з будь-якої названої категорії такі:

• зручність і простота в адмініструванні та користуванні;

• масштабовуваність − система має підтримувати будь-яку кількість користувачів, її здатність нарощувати свою потужність має визначатись тільки потужністю відповідного апаратного забезпечення;

• розподіленість − система має підтримувати роботу з документами у територіально-розподілених організаціях, а також взаємодію з віддаленими користувачами;

• модульність − система має складатись з окремих модулів, інтегрованих між собою, що дає можливість замовникові вибирати й упроваджувати компоненти згідно зі своїми потребами;

• відкритість − система повинна мати відкриті інтерфейси для можливої доробки та інтеграції з іншими системами;

•переносимість − можливість використання на різних апаратних платформах у середовищі різного системного програмного забезпечення.

Автоматизація завжди розглядалась як засіб підвищення ефективності управління. Але позитивного результату неможливо досягти в разі використання комп'ютерів як друкарських машинок, а ЛОМ − для тривіального обміну файлами. Водночас варто враховувати, що вигоди від автоматизованого виконання операцій (прискорення, спрощення і т. ін.) далеко не завжди компенсують необхідні витрати. Розуміння такої ситуації призвело до появи в 1990 році принципово нової концепції підвищення ефективності функціонування компаній − бізнес-процес реінжинірингу. За визначенням, ВРК − це фундаментальне переосмислення і радикальне перепроектування бізнес-процесів для досягнення докорінного покращення основних показників діяльності − вартості, якості, послуг, швидкості. При цьому новітні ІТ розглядаються як інструмент реконструкції існуючих бізнес-процесів.

ІТ за своєю сутністю створюють умови для вдосконалення бізнес-процесів. Так, електронні комунікації дали змогу перебороти обмеження в розподілі та оновленні інформації, притаманні «паперовій» технології, а технології «клієнт-сервер» створили передумови для децентралізації прийняття рішень, залишивши проте практично без змін процеси комунікацій і координації. У цьому контексті особливого значення набувають workflow-системи, які слід розглядати не як окремі додатки, а як засоби інтеграції ділових процесів підприємства.

Діловий процес − це логічно завершений набір операцій (ділових процедур), що підтримують структуру підприємства і реалізують його політику, спрямовану на досягнення поставленої мети. Ідеологія САДП ґрунтується на твердженні, що здебільшого ділові процеси мають такі

характеристики:

• складаються зі скінченного набору завдань, що виконуються заданим чином;

• до їх виконання залучено численних працівників з різним ступенем відповідальності;

• вони полягають у вивченні, створенні, обробленні та передаванні інформації у різних формах (не тільки у формі документів);

• мають деяку мету, можливо, не очевидну всім учасникам.

Ділова процедура − це логічний етап ділового процесу, який необхідно реалізувати для його завершення. Наприклад, діловий процес «Обробка вхідного документа» складається з процедур реєстрації документа, видачі резолюції, постановки на контроль, виконання резолюції, контролю виконання, перевірки результатів.

Для відокремлення понять «виконання документа» і «виконання доручення» використовується термін «робота», який позначає конкретне доручення, що виконується в рамках ділового процесу і складається з певних процедур.

Конкретні процедури виконуються за правилами. Правило оброблення процедури − це деяка умова, дотримання або недотримання якої викликає визначені дії. Такі правила можна поділити на правила оброблення даних і правила маршрутизації. Правила маршрутизації визначають сценарій реалізації ділового процесу, послідовність виконання його процедур. Прикладом різної маршрутизації одного об'єкта може бути правило розгляду вхідних документів і накладання резолюцій на них: «Документи, що належать до групи особливо важливих, розглядає і розписує керівник, а решту − його заступники, відповідно до кола питань, якими вони відають».

Залежно від *визначеності порядку виконання процедур* розрізняють жорстку і вільну маршрутизацію. Жорстка маршрутизація задається у випадку, коли порядок виконання процедур відомий заздалегідь і не залежить від результату виконання попередньої процедури. Іншими словами, завершення однієї процедури приводить до автоматичного запуску іншої. Вільна маршрутизація (умовна або ad hoc-маршрутизація) визначається умовами, виконання або невиконання яких з'ясовується тільки після завершення попередньої ділової процедури. У цьому разі не можна сказати заздалегідь, яку процедуру буде запущено після виконання поточної, це визначає учасник ділового процесу з відповідними правами.

Залежно від порядку проходження процедур розрізняють послідовну і паралельну маршрутизацію. Послідовна маршрутизація передбачає виконання ділових процедур одну за іншою. Чергова процедура розпочинається тільки після завершення попередньої. Таким чином, у певний момент часу може виконуватись тільки одна процедура. За паралельної маршрутизації відбувається кілька ділових процедур одночасно. Це можливо, якщо такі процедури незалежні і їх виконання не вимагає результатів виконання інших.

Маршрути можуть бути складнішими, ніж прості послідовні чи паралельні. У деяких випадках задаються комбіновані маршрути з послідовних і паралельних елементів, а в деяких − умовні, з переходами залежно від стану тих чи інших змінних. Маршрутизація також може передбачати контроль виконання. Це поняття охоплює контроль доставки завдання, контроль

ознайомлення із завданням, власне контроль виконання, моніторинг завдання, повідомлення про порушення термінів виконання, історію виконання завдань, контроль якості виконання.

Ще одним важливим компонентом опису ділового процесу є розподіл ролей між його учасниками. Роль визначає набір дій у рамках ділового процесу, який учасник має виконати для досягнення мети процесу. Під час визначення ролі закріплюються місце її розташування, функції, права доступу. Учасник може бути членом певної робочої групи, тоді на нього поширюються всі характеристики цієї групи. Існують три типи ролей:

• ініціатор роботи − це учасник ділового процесу, який формулює зміст роботи, описує її, запускає на виконання, здійснює контроль і приймає результати;

• виконавець роботи − це учасник ділового процесу, який виконує роботу, а також звітує і несе відповідальність за її результати. За наявності відповідних прав виконавець може створювати нову роботу як частину тієї, що доручена йому, і призначати нових виконавців. Таким чином він сам стає ініціатором робіт, − створюється традиційна ієрархічна структура управління з кількома рівнями підпорядкованості;

• спостерігач − це учасник ділового процесу, який відстежує виконання роботи.

Формалізований опис ділового процесу та ділових процедур. що входять до його складу, правил їх виконання і ролей учасників процесу називають моделлю процесу. Модель процесу є результатом ретельного обстеження та аналізу об'єкта автоматизації на предмет оптимізації його діяльності. Із цією метою застосовуються традиційні методології системного аналізу, такі як SADT чи DFD. Існують і спеціалізовані методології, що підтримуються окремими САДП.

У процесі використання САДП керівник або його секретар оформляє розпорядження у вигляді роботи, для якої описуються строки її початку, завершення та інші характеристики. Якщо виконання роботи вимагає ознайомлення з тим чи іншим документом, представленим в електронній формі, він може бути прикріплений до опису роботи для передавання користувачеві.

При переході роботи від одного учасника до іншого до неї можуть додаватися нові дані − «дані про виконання роботи». Вони або вводяться виконавцем у спеціальну екранну форму, яка описує роботу, або генеруються системою самостійно. Зокрема, система генерує дані про час проходження роботою чергового етапу, поточний статус роботи (ініційована, завершена, відкладена), її місцезнаходження і т. ін. Саме ця інформація потрібна ініціаторові роботи для координації процесу і контролю за його виконанням. САДП забезпечує передавання такої інформації в режимі реального часу, усуваючи можливість втрати даних і скорочуючи час їхньої передачі. Одержана інформація є основою для вироблення рішень, які теж оформляються у вигляді робіт. Використання САДП дає змогу значно підвищити рівень обґрунтованості рішень завдяки своєчасному інформуванню керівництва про стан справ.

Таким чином, функціонування САДП дозволяє створити і підтримувати чітку технологію життєдіяльності всього апарата управління. Воно сприяє належній організації робіт, удосконалює зворотні інформаційні зв'язки, зміцнює трудову дисципліну і підвищує організаційну культуру. Поєднання технологій

workflow з Web-технологіями дає змогу розширити комунікації та координацію у середовищі розподіленого прийняття рішень за межі окремої установи у рамках систем електронної комерції та віртуальних підприємств.

2. Складові інформаційної безпеки. Шляхи вирішення питань інформаційної безпеки. Критерії інформаційної безпеки та її складові частини.

Статтею 32 Конституції України проголошено право людини на невтручання в її особисте життя. Крім того, не допускається збирання, зберігання, використання поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

З метою конкретизації права людини, гарантованого ст. 32 Конституції України, та визначення механізмів його реалізації 1 червня 2010 р. Верховною Радою України було прийнято Закон України «Про захист персональних даних» (далі – Закон), який набрав чинності з 1 січня 2011 р. Предметом правового регулювання Закону є правовідносини, пов'язані із захистом персональних даних під час їх обробки.

Закон декілька разів коригувався. Визначення поняття персональні дані наводиться в ст. 2 Закону України, відповідно до якого персональними даними є відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Але законодавством України не встановлено і не може бути встановлено чіткого переліку відомостей про фізичну особу, які є персональними даними, задля можливості застосування положень Закону до різноманітних ситуацій. В тому числі, при обробці персональних даних в інформаційних (автоматизованих) базах та картотеках персональних даних, що можуть виникнути у майбутньому. Це пов'язано зі зміною в технологічній, соціальній, економічній та інших сферах суспільного життя. Наприклад, відповідно до ст. 24 Кодексу законів про працю України громадянин при укладенні трудового договору зобов'язаний надати паспорт або інший документ, що посвідчує особу, трудову книжку, а у випадках, передбачених законодавством, – також документ про освіту (спеціальність, кваліфікацію), про стан здоров'я та інші документи.

У зв'язку з цим персональні дані працівника, які містяться в паспорті або документі, що посвідчує особу, в трудовій книжці, документі про освіту, документі про стан здоров'я та інших документах, які він подав при укладенні трудового договору, обробляються володільцем бази персональних даних на підставі ст. 24 Кодексу законів про працю України виключно для здійснення повноважень володільця бази персональних даних у сфері правовідносин, які виникли в нього з працівником на підставі трудового договору.

Таким чином, інформація про найманих працівників є базою персональних даних, оскільки особові справи, трудові книжки, копії паспортів, документів про освіту зберігаються та обробляються роботодавцем.

Поняття база персональних даних визначене в ст. 2 Закону, відповідно до якого база персональних даних – це іменована сукупність упорядкованих персональних даних в електронній формі або у формі картотеки персональних даних.

З огляду на це база персональних даних є упорядкованою сукупністю

логічно пов’язаних даних про фізичних осіб:

1) що зберігаються та обробляються відповідним програмним забезпеченням, є базою персональних даних в електронній формі;

2) що зберігаються та обробляються на паперових носіях інформації, є базою персональних даних у формі картотек.

Таким чином картотекою персональних даних є будьякий структурований масив персональних даних, що є доступним за визначеними критеріями незалежно від того, чи є такий масив централізованим, децентралізованим або розділеним на функціональних або географічних засадах.

Такі дані мають бути структуровані за визначеними критеріями, що стосуються фізичних осіб, щоб забезпечити легкий доступ до відповідних персональних даних.

Варто зазначити, що, виходячи з положень ст. 2 Закону, персональні дані одночасно можуть бути упорядковані і в електронній формі, і в формі картотек.

Наведемо приклади того, що не є базою персональних даних. Фізичні особи самостійно визначають: чи володіють вони базами персональних даних у сенсі Закону. Законодавець поширив дію Закону на всі види діяльності, пов’язані зі створенням баз персональних даних та обробкою персональних даних у цих базах за винятком такої діяльності, яка здійснюється:

1) фізичною особою – виключно для непрофесійних особистих чи побутових потреб,

2) журналістом – у зв’язку з виконанням ним службових чи професійних обов’язків,

3) професійним творчим працівником – для здійснення творчої діяльності.

Так, під час здійснення своєї професійної діяльності на адвокатів законодавством не покладено обов’язок ведення баз персональних даних клієнтів. Але, якщо адвокати формують справи на своїх клієнтів, які вони постійно оновлюють та підтримують в актуальному стані, такі справи є базою персональних даних та підлягають державній реєстрації.

Нотаріуси можуть обробляти персональні дані своїх найманих працівників, клієнтів у базах персональних даних, однак документи нотаріального діловодства та архів нотаріуса, визначені у ст. 14 Закону України «Про нотаріат», не є базою персональних даних у сенсі Закону України «Про захист персональних даних» та не підлягають державній реєстрації.

Крім того, у випадку, якщо фізичні особипідприємці укладають договори виконання робіт або надання послуг з фізичними особами, такі договори також не є базою персональних даних та не підлягають державній реєстрації.

Володільцем бази персональних даних згідно зі ст. 2 Закону є фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом.

Так, якщо персональні дані обробляються юридичною особою, то володільцем бази персональних даних є юридична особа.

Розпорядником бази персональних даних згідно зі ст. 2 Закону може бути фізична чи юридична особа, якій володільцем бази персональних даних або законом надано право обробляти ці дані.

Практичним прикладом можуть бути відносини між юридичними особами та їх представництвами, філіями, відділеннями тощо. Так, у сенсі

Закону ці представництва, філії, відділення виступатимуть розпорядниками баз персональних даних, володільцем яких є юридична особа.

Згідно зі ст. 4 Закону володільцем чи розпорядником бази персональних даних можуть бути підприємства, установи і організації усіх форм власності, органи держави влади чи органи місцевого самоврядування, які обробляють персональні дані відповідно до Закону.

Але якщо володільцем бази персональних даних є орган державної влади чи орган місцевого самоврядування, то розпорядником бази персональних даних, крім цих органів, може бути лише підприємство державної або комунальної форми власності, що належить до сфери управління цього органу.

Закон не передбачає обов'язкової реєстрації баз персональних даних і натомість запроваджує обов'язок для володільців персональних даних повідомляти уповноважений державний орган про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних. До таких даних відносяться національність, приналежність тій чи іншій конфесії, генетичні, біометричні дані тощо.

Функції державного органу з питань захисту персональних даних Закон покладає на Уповноваженого Верховної Ради України з прав людини (далі – Уповноважений).

Уповноважений наділений правом затверджувати нормативно-правові акти у сфері захисту персональних даних. Також Уповноважений наділений повноваженнями взаємодіяти із структурними підрозділами або відповідальними особами володільців персональних даних, які відповідно до Закону організовують роботу, пов'язану із захистом персональних даних при їх обробці, та оприлюднювати інформацію про такі структурні підрозділи та відповідальних осіб. З цією метою Уповноважений здійснює контроль за додержанням законодавства про захист персональних даних шляхом проведення виїзних та безвиїзних перевірок володільців та (або) розпорядників баз персональних даних. Складає адміністративні протоколи про виявлені порушення законодавства у сфері захисту персональних даних.

Реєстрація бази персональних даних здійснюється за заявочним принципом шляхом повідомлення. Суть заявочного принципу полягає в тому, що основним є подання володільцем бази персональних даних заяви про реєстрацію бази персональних даних, а не отримання свідоцтва про державну реєстрацію бази персональних даних.

Сайт Державного реєстру баз персональних даних https://rbpd.informjust.ua, на якому є можливість слідкувати за ходом державної реєстрації заяви в режимі он-лайн.

Однією зі складових процесу обробки персональних даних є їх збирання, що передбачає дії з підбору чи впорядкування відомостей про фізичну особу та внесення їх до бази персональних даних. Згідно зі ст. 12 Закону володілець бази зобов'язаний повідомити суб'єкта персональних даних виключно в письмовій формі про його права, що визначені ст. 8 Закону, мету збору даних, яка визначається володільцем бази персональних даних, та осіб, яким будуть передаватися персональні дані. На це Закон надає термін у десять робочих днів з дня включення персональних даних до бази персональних даних.

Володілець бази звільняється від виконання вказаного обов'язку лише у разі, якщо персональні дані збираються ним із загальнодоступних джерел. Під

визначенням «загальнодоступні джерела інформації», зокрема, розуміються друковані засоби масової інформації, засоби телерадіомовлення, інтернет-портали, публічні виступи та інші джерела інформації, до яких фізичні та юридичні особи мають вільний, необмежений чинним законодавством, доступ.

Власники, розпорядники персональних даних та треті особи зобов'язані забезпечити захист особистих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі, незаконного знищення чи доступу до персональних даних.

В органах державної влади, органах місцевого самоврядування, а також у володільців чи розпорядників персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього Закону, створюється структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці.

Інформація про структурний підрозділ або відповідальну особу повідомляється Уповноваженому, який забезпечує її оприлюднення.

Структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці:

1) інформує та консультує володільця або розпорядника персональних даних з питань додержання законодавства про захист персональних даних;

2) взаємодіє з Уповноваженим та визначеними ним посадовими особами його секретаріату з питань запобігання та усунення порушень законодавства про захист персональних даних від 28 січня 1981 р.

3. Об'єкти захисту інформації. Законодавство про інформаційну безпеку. Основні терміни у сфері інформаційної безпеки. Вимоги до забезпечення захисту інформації в системі. Організаційні засади забезпечення захисту інформації.

Захист даних, захист інформації (data protection) – сукупність заходів і відповідних засобів, які забезпечують захист прав власності володільців інформаційної продукції, у першу чергу – програм, баз і банків даних від несанкціонованого доступу, використання, руйнування або завдання шкоди в будь- якій іншій формі.

У галузі знань із захисту інформації сформульовано три основні постулати.

Перший постулат: абсолютно надійний захист створити не можна. Система захисту інформації може бути в кращому разі адекватною потенційним загрозам.

Другий постулат: система захисту інформації повинна бути комплексною: слід використовувати не тільки технічні засоби захисту, а й адміністративні та правові.

Третій постулат: система захисту інформації повинна бути гнучкою, здатною адаптуватися до умов, що змінюються. Головна роль у цьому належить адміністративним (або організаційним) заходам, таким, наприклад, як регулярна зміна паролів і ключів, додержання строгого порядку їх зберігання, аналіз журналів реєстрації подій у системі, правильний розподіл повноважень користувачів. Залежно від способів захисту всі заходи, спрямовані на запобігання злочинам, можна класифікувати на технічні, правові та організаційні.

Технічні заходи:

1) захист від несанкціонованого доступу до системи, резервування особливо важливих комп'ютерних підсистем;

2) організація обчислювальних мереж з можливістю перерозподілу ресурсів у разі порушення працездатності окремих ланок;

3) вживання конструкційних заходів захисту від розкрадань, саботажу, диверсій, вибухів;

4) установка резервних систем електроживлення, оснащення приміщень замками, сигналізацією і багато що інше.

Правові заходи:

1) розробка норм, що встановлюють відповідальність за комп'ютерні злочини;

2) захист авторських прав;

3) удосконалення кримінального й цивільного законодавства, а також судочинства.

Організаційні заходи:

1) охорона обчислювального центру;

2) підбір персоналу, виключення випадків ведення особливо важливих робіт тільки однією людиною;

3) наявність плану відновлення працездатності інформаційного центру після виходу його з ладу;

4) організація обслуговування обчислювального центру сторонньою організацією або особами, не зацікавленими в приховуванні фактів порушення роботи центру;

5) універсальність засобів захисту від усіх користувачів (у тому числі й вищого керівництва);

6) покладання відповідальності на осіб, які повинні забезпечити безпеку центру, вибір місця розташування центру тощо.

До основних видів порушень інформаційної безпеки можна віднести дані про типи атак.

4. Аналіз погроз інформаційній безпеці. Практичні напрямки захисту.

Необхідність в інформаційній безпеці випливає із самої природи мережних служб, сервісів і послуг.

Потрібно чітко дотримуватися прийнятих протоколів обміну в мережі. Будь-яке розширення клієнтської програми може супроводжуватися певною загрозою. Рівень безпеки на кожному комп'ютері свій. Забезпеченням режиму безпеки займається системний адміністратор.

Загроза віддаленого адміністрування. Під віддаленим адмініструванням слід розуміти несанкціоноване управління віддаленим комп'ютером. Віддалене адміністрування дозволяє брати чужий комп'ютер під своє управління. Це може дозволити копіювати і модифікувати наявні на ньому дані, установлювати довільні програми, у тому числі й шкідливі, використовувати чужий комп'ютер для вчинення злочинних дій у мережі від імені його власника.

Загроза активного змісту. Активний зміст – це активні об'єкти, вбудовані у веб-сторінки. На відміну від пасивного змісту (текстів, малюнків, аудіокліпів тощо) активні об'єкти містять у собі не тільки дані, а й програмний код, що одержує клієнт веб-сторінки, яка завантажується. Агресивний програмний код, що потрапив у комп'ютер, здатний поводитися як комп'ютерний вірус чи як агентська програма.

Загроза постачання даних неприйнятного змісту. Не вся інформація, яка публікується в Інтернеті, може вважатися суспільно корисною, і досить часто люди хочуть від неї захиститися.

У більшості країн світу Інтернет поки не вважається засобом масової інформації. Це пов'язано з тим, що постачальник інформації не займається її копіюванням, тиражуванням і поширенням, тобто він не виконує функції ЗМІ. Усе це робить сам клієнт у момент використання гіперпосилання. Тому звичайні закони про засоби масової інформації, які регламентують, що можна поширювати, а що ні, в Інтернеті поки не працюють.

Функції фільтрації інформації, що надходить, її змісту покладаються на браузер чи на спеціально встановлену для цієї мети програму.

Класифікація комп'ютерних злочинів базується на класифікації способів скоєння таких злочинів. Спосіб скоєння злочину є системою взаємообумовлених, рухомих детермінованих дій, направлених на підготовку, здійснення і приховування злочину, зв'язаних з використанням відповідних знарядь і засобів, а також часу, місця і інших сприяючих обставин об'єктивної обстановки скоєння злочину.

Розділення комп'ютерних злочинів за способом їх здійснення на:

1. методи перехоплення;
2. методи несанкціонованого доступу;
3. методи маніпуляції.

1) Комп'ютер є об'єктом правопорушення, коли мета злочинця – викрасти інформацію або завдати шкоди системі, що цікавить його:

a) вилучення засобів комп'ютерної техніки. До цієї групи відносяться традиційні способи здійснення звичайних видів злочинів, в яких дії злочинця направлені на вилучення чужого майна;

b) розкрадання інформації;

c) розкрадання послуг (діставання несанкціонованого доступу до якоїсь системи з метою безвідплатного користування послугами, що надаються нею);

d) пошкодження системи. Дана група об'єднує злочини, здійснені з метою зруйнувати або змінити дані, що є важливими для власника одного або багатьох користувачів системи – об'єкта несанкціонованого доступу;

e) уівинг (заплутування слідів, коли метою атаки є прагнення приховати своє ім'я і місцезнаходження).

Тут слід зазначити, що об'єктом правопорушення може бути пристрій, що не є комп'ютером в загальноприйнятому розумінні цього слова, – мобільний телефон, касовий апарат і тому подібне.

2) Комп'ютери використовуються як засоби, що сприяють скоєнню злочину:

a) як засіб скоєння традиційних злочинів (як правило, шахрайство);

b) як засіб атаки на інший комп'ютер, засіб скоєння іншого комп'ютерного злочину.

3) Комп'ютер використовується як пристрій, що запам'ятовує (наприклад, після злому системи створюється спеціальна директорія для зберігання файлів, що містять програмні засоби злочинця, паролі для інших вузлів, списки вкрадених номерів кредитних карток і тому подібне).

Зарубіжними фахівцями розроблені різні класифікації способів скоєння

комп'ютерних злочинів. Нижче приведені назви способів скоєння подібних злочинів, відповідних кодифікатору Генерального Секретаріату Інтерполу. Всі коди, які характеризують комп'ютерні злочини, мають ідентифікатор, що починається з букви Q. Для характеристики злочинів можуть використовуватися до п'яти кодів, розташованих в порядку убу вання значущості.

QA – Несанкціонований доступ і перехоплення

QAH – комп'ютерний абордаж; QAI – перехоплення; QAT – крадіжка часу; QAZ – інші види несанкціонованого доступу і перехоплення.

QD – Зміна комп'ютерних даних

QDL – логічна бомба; QDT – троянський кінь; QDV – комп'ютерний вірус; QDW – комп'ютерний черв'як; QDZ – інші види зміни даних.

QF – Комп'ютерне шахрайство

QFC – шахрайство з банкоматами; QFF – комп'ютерна підробка; QFG – шахрайство з ігровими автоматами; QFM – маніпуляції з програмами введення-виводу; QFP – шахрайства з платіжними засобами; QFT – телефонне шахрайство; QFZ – інші комп'ютерні шахрайства.

QR – Незаконне копіювання

QRG – комп'ютерні ігри; QRS – інше програмне забезпечення; QRT – топографія напівпровідникових виробів; QRZ – інше незаконне копіювання.

QS – Комп'ютерний саботаж

QSH – з апаратним забезпеченням; QSS – з програмним забезпеченням; QSZ – інші види саботажу.

QZ – Інші комп'ютерні злочини

QZB – з використанням комп'ютерних дошок оголошень; QZE – розкрадання інформації, складовій комерційної таємниці; QZS – передача інформації конфіденційного характеру; QZZ – інші комп'ютерні злочини.

Несанкціонований доступ і перехоплення інформації

(QA) включає наступні види комп'ютерних злочинів:

Комп'ютерні шахрайства (QF) об'єднують у своєму складі різноманітні способи скоювання комп'ютерних злочинів:

QFC – комп'ютерні шахрайства, пов'язані з розкраданням готівки з банкоматів.

QFF – комп'ютерні підробки: шахрайства і розкрадання з комп'ютерних систем шляхом створення підроблених пристроїв (карток і ін.).

QFG – шахрайства і розкрадання, пов'язані з ігровими автоматами.

QFM – маніпуляції з програмами введення-виводу: шахрайства і розкрадання за допомогою невірного введення або виводу в комп'ютерні системи або з них шляхом маніпуляції програмами. У цей вид комп'ютерних злочинів входить метод підміни даних кода (data diddling code change), що зазвичай здійснюється при введенні-виводі даних. Це простий і тому дуже часто використовуваний спосіб.

QFP – комп'ютерні шахрайства і розкрадання, пов'язані з платіжними засобами. До цього виду відносяться найпоширеніші комп'ютерні злочини, пов'язані з крадіжкою грошових коштів, які складають близько 45% всіх злочинів, зв'язаних з використанням ЕОМ.

QFT – телефонне шахрайство: доступ до телекомунікаційних послуг шляхом посягання на протоколи і процедури комп'ютерів, обслуговуючих

телефонні системи.

Незаконне копіювання інформації (QR) складають наступні види комп'ютерних злочинів:

QRG/QRS – незаконне копіювання, розповсюдження або публікація комп'ютерних ігор і іншого програмного забезпечення, захищеного законом.

QRT – незаконне копіювання топографії напівпровідникових виробів: копіювання без права на те захищеній законом топографії напівпровідникових виробів, комерційна експлуатація або імпорт з цією метою без права на те топографії або самого напівпровідникового вироба.

Комп'ютерний саботаж (QS) складають наступні ви ди злочинів:

QSH – саботаж з використанням апаратного забезпечення: введення, зміна, стирання комп'ютерних даних або програм; втручання у роботу комп'ютерних систем з наміром перешкодити функціонуванню комп'ютерної або телекомунікаційної системи.

QSS – комп'ютерний саботаж з програмним забезпеченням: стирання, пошкодження, погіршення або знешкодження комп'ютерних даних або програм без права на те.

До інших видів комп'ютерних злочинів (QZ) відносяться:

QZB – використання електронних дошок оголошень (BBS) для зберігання, обміну і розповсюдження матеріалів, що мають відношення до злочинної діяльності;

QZE – розкрадання інформації, складовій комерційної таємниці: придбання незаконними засобами або передача інформації, що представляє комерційну таємницю без права на те, або іншого законного обґрунтування з наміром заподіяти економічний збиток або отримати незаконні економічні переваги;

QZS – використання комп'ютерних систем або мереж для зберігання, обміну, розповсюдження або переміщення інформації конфіденційного характеру.

Контрольні запитання

1. Назвіть класи систем автоматизації роботи з документами залежно від задач та технологій, що застосовуються.

2. Порівняйте концепції організації автоматизованих систем контролю виконання документів та електронних архівів.

3. Назвіть завдання, що їх автоматизують системи керуван¬ня електронними документами.

4. Чим відрізняються системи groupware від workflow систем?

5. Що таке модель ділового процесу і як вона використовується у workflow -системах?

6. Як розвиток електронної комерції впливає на економіку, управління, повсякденне життя пересічного громадянина?

7. Назвіть учасників електронної комерції і визначте роль кожного з них.

8. Як у системах електронної комерції використовуються методи криптографії?

9. Визначте напрямки участі держави в електронній комерції.

10. Визначте підходи до організації роботи юристів у режимі віртуального офісу.