*МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ*
*Харківський національний університет внутрішніх справ*
*Факультет № 4*
*Кафедра протидії кіберзлочинності*
*Факультет №6*
*Кафедри кібербезпеки та DATA-технологій*

**ЗАТВЕРДЖЕНО**
Спільне засідання кафедри протидії кіберзлочинності факультету №4 та кафедри кібербезпеки та DATA-технологій факультету №6
Протокол № 2 від 22.06.2023 (бакалаври).
Завідувач кафедри

**_____Олександр МАНЖАЙ**

Завідувач кафедри

**_____Юрій ГНУСОВ**

# ІНФОРМАЦІЙНІ ТА КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ (ОК.11)

# ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

| | |
|---|---|
| **Кафедра** | Кафедра протидії кіберзлочинності (univd.edu.ua/uk/dir/1740/kafedra-informatsiynykh-tekhnologiy-ta-kiberbezpeky) |
| **Контактний телефон** | +38 057 73-98-385 (роб.) |
| **E-mail** | klimushyn@ukr.net |
| **ЛЕКТОР (ЛЕКТОРИ)** | |
|  | **Клімушин Петро Сергійович,**<br>доцент кафедри протидії кіберзлочинності факультету № 4,<br>к.т.н., доцент<br>klimushyn@ukr.net<br>**Лекційний потік:** факультет № 4,<br>шифр навчальних груп Ф4-102 |
| **Назва освітньо-професійної** | Кібербезпека та захист інформації (безпека |

| | |
|---|---|
| **програми** | інформаційних та комунікаційних систем)<br>Cybersecurity and information protection (security of information and communication systems) |
| **Рівень вищої освіти** | Перший (бакалаврський) (НРК України – 7 рівень та другий цикл вищої освіти Рамки кваліфікацій Європейського простору вищої освіти) |
| **Галузь знань** | 12 Інформаційні технології |
| **Спеціальність** | 125 Кібербезпека та захист інформації |
| **Статус дисципліни** | Обов'язкова компонента освітньої програми, вивчається в 1, 2 семестрах І курсі навчання. |
| **Мета вивчення дисципліни** | Метою навчальної дисципліни є вивчення курсантами теоретичних основ інформаційно-аналітичного забезпечення діяльності підрозділів національної поліції (ПНП), формування знань, умінь та навичок, необхідних для використання сучасних інформаційних технологій в професійної роботи з електронними документами, електронними таблицями, інформаційними базами даних, інформаційними представництвами ПНП, сервісами ідентифікації, надання довірчих послуг та засобами захисту інформації в кіберсфері. |
| **Завдання вивчення дисципліни** | − панування сутністю новітніх інформаційних технологій, які використовуються в діяльності поліції;<br>− удосконалення практичних навичок щодо використання комп'ютерних програм та систем в діяльності правоохоронця;<br>− вивчення питань щодо напрямів, тенденцій та перспектив розвитку інформаційних технологій професійної діяльності. |
| **Обсяг дисципліни в кредитах ECTS/годинах** | Кількість кредитів ECTS (загальний обсяг – 120 год.)<br>З них (денна/заочна):<br>- аудиторна робота: 60/12 год.<br>- самостійна робота: 60/108 год. |
| **Форми та види проведення навчальних занять** | Форма навчання – денна<br>Види навчальних занять:<br>- лекції: 26 год.;<br>- семінарські заняття: 0 год.;<br>- практичні заняття:14 год.;<br>- лабораторні заняття:20 год.<br><br>Форма навчання – заочна<br>Види навчальних занять: |

| | |
|---|---|
| | - лекції: 4 год.;<br>- семінарські заняття:0 год.;<br>- практичні заняття: 4 год.;<br>- лабораторні заняття: 4 год. |
| **Індивідуальні завдання** | Наукові доповіді, індивідуальні завдання до лабораторних занять. |
| **Необхідне обладнання** | Мультимедійне обладнання (ноутбук та проектор), комп'ютерне забезпечення з виходом у мережу Інтернет. |
| **Мова викладання** | Українська |
| **Контроль** | Поточний та підсумковий контроль Форми поточного контролю: захист індивідуальних завдань на лабораторних заняттях, тестування, перевірка аудиторних контрольних робіт, перевірка виконання самостійних робіт.<br>Критерії оцінки поточного контролю викладач повідомляє на першому занятті та перед кожними оцінюванням.<br>Форми підсумкового контролю: **залік.** |
| **Інтегральна компетентність, загальні компетентності (ЗК)** | Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та\або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.<br>ЗК 1. Здатність застосовувати знання у практичних ситуаціях.<br>ЗК 5. Здатність до пошуку, оброблення та аналізу інформації. |
| **Спеціальні (фахові) компетентності (ФК)** | ФК 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.<br>ФК 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки. |
| **ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ЗА ТЕМАМИ** | |
| **Тема № 1. Інформаційно-аналітичне забезпечення НПУ**<br>Міжнародно-правові та конституційні засади прав людини в галузі інформації. Доступ до публічної інформації. Захист персональних даних. Особливості правового режиму інформаційних систем з обробки персональних даних. Інформаційна система для обробки персональних даних.<br>Нормативно-правове регулювання у сфері інформаційних відносин у поліцейській | |

діяльності. Повноваження поліції у сфері інформаційно-аналітичного забезпечення. Формування інформаційних ресурсів поліцією. Використання поліцією інформаційних ресурсів. Відповідальність за протиправне використання інформаційних ресурсів.
Організація інформаційно-аналітичного забезпечення НПУ. Основні завдання системи «Інформаційний портал Національної поліції України» Складові системи. Організація роботи підрозділів ГУНП та їх посадових осіб, уповноважених на приймання і реєстрацію заяв і повідомлень про правопорушення або події та реагування на них. Розділ «категорія повідомлення». Автоматизоване робоче місце «Оператор», «Диспетчер» підрозділу "102".

**Тема № 2. Безпека роботи з інформацією**

Політика інформаційної безпеки (ПІБ) при роботі з інформацією. Основні напрями розробки ПІБ. Основні правила забезпечення політики безпеки в інформаційній системі. Ідентифікація активів та загроз.
Базові принципи застосування ідентифікації громадян та установ: адекватність вимог, децентралізація та диверсифікація, індивідуальний вибір, роз'яснення наслідків, контроль розповсюдження. Основні технології ідентифікації: інфраструктура відкритих ключів (PKI), банківська ідентифікація (BankID), мобільна ідентифікація (mobileID), Ідентифікація з допомогою електронних карт.
Основи криптографічного захисту інформації. Інфраструктура сертифікації ключів. Державні та міжнародні стандарти алгоритмів криптографічного захисту інформації. Дослідження процедур шифрування, дешифрування та підпису електронних документів.

**Тема № 3. Використання радіозв'язку та відеофіксації у роботі патрульного поліцейського. Робота патруля з базами даних**

Правила ведення радіоефіру під час патрулювання. Особливості використання радіозв’язку. Приклади радіообміну. Правила проведення сеансів радіозв’язку. Перелік повідомлень, дозволених для відкритої передачі. Заходи безпеки під час роботи з радіостанцією.
Відеофіксація з допомогою персонального відеореєстратора під час патрулювання. Целі використання персональних відеореєстраторів. Події які вимагають відеозйомки та події при яких не повинні використовуватись відеокамера. Дії з реєстратором після закінчення патрулювання.
Робота патруля з базами даних. Спрощена схема роботи патруля з базами даних. Панель задач після реєстрації. Форма для пошуку особи. Форма для пошуку номерних речей. Форма запиту для пошуку викраденого автотранспорту. Оформлення адміністративного протоколу.

**Тема № 4. Автоматизація підготовки юридичних документів в текстовому процесорі**

Архітектура Microsoft Word. Власне додаток. Шаблони. Документи. Вимоги та рекомендацій щодо оформлення юридичних документів. Форматування документа. Основні типи стилів. Операцій редагування таблиць. Графічні об'єкти. Малюнки.
Створення виносок, автоматичних назв об'єктів, перехресних посилань, списку ілюстрацій, списку-літератури та посилань на джерела, автозмісту документу. Використання текстового процесору для створення шаблонів юридичних

документів. Злиття юридичних документів в текстовому процесорі.
Нові можливості Microsoft Word. Надання спільного доступу до документа. Спільне редагування документа.

**Тема № 5. Обробка і аналіз інформації у табличному процесорі**

Характеристика комірки електронної таблиці. Поняття книги, аркуша, комірки. Основні операції з комірками, рядками і стовпцями. Введення, редагування та опрацювання даних. Поняття функцій і формул. Типи посилань у формулах. Обробка числових та текстових даних.
Обробка табличних даних у MS Excel. Ділова графіка. Створення звіту з аналізом стану злочинності. Створення бази даних у середовищі MS Excel. Можливості програми для створення структури бази даних. Установка перевірки введення початкових даних. Введення початкових даних. Пошук інформації за критеріями.
Нові можливості Excel. Діаграми з картами. Воронкоподібні діаграми. Вставка тривимірних моделей і їх перегляд. Цифровий олівець. Рукописна формула. Покращення зведених таблиць. Персоналізація стандартного макета зведеної таблиці. Інтелектуальне перейменування.

**Тема № 6. Організація та проектування реляційних баз даних**

Основні поняття реляційних баз даних (БД). Етапи проектування реляційної бази даних. Типи ключів в реляційних базах даних. Нормалізація даних в реляційній моделі. Типи відношень між таблицями БД. Індексація сучасних баз даних.
Основні об’єкти СУБД Access. Створення таблиць та форм. Типи даних Access. Створення запитів. Створення зв'язків. Забезпечення цілісності даних. Створення зв'язку з використанням майстра підстановок. Використання фільтрів. Запити для проведення статистичних розрахунків. Створення розрахункових полів. Оформлення звітів.

**Тема №7. Функціонування комп’ютерних мережі та пошук інформації в Інтернеті**

Основні поняття та класифікація комп'ютерних мереж. Принципи функціонування і ресурси мережі Інтернет. Провайдери. Інформаційні ресурси Інтернету. IP-адреси. Доменні імена DNS. Система World Wide Web. Web-сторінки, браузери. Електронна пошта. Інформаційно-пошукові системи. Ключові слова. WEB-каталоги. Файлові ресурси Інтернету (FTP-вузли). Використання метапошукових серверів глобальної мережі Інтернет та спеціалізованих метапошукових програмних комплексів. Пошук людей в глобальної мережі за допомогою онлайн сервісів. Використання довідково-інформаційних баз даних вільного доступу (державних реєстрів).

**Тема № 8. Проектування інформаційних представництв органів поліції**

Етапи розробки веб-сайту. Створення технічного завдання. Дизайн основний і типових сторінок сайту. HTML-верстка. Тестування сайту. Розміщення сайту в Інтернет. Наповнення контентом і публікація. Внутрішня та зовнішня SEO-оптимізація. Розкрутка і просування сайтів в топ рейтингах.

**Тема № 9. Використання систем управління контентом**

Дослідження систем управління контентом. Встановлення системи управління контентом. Елементи та режими роботи системи управління контентом. Система розмежування доступу користувачів сайта. Управління шаблонами та розширеннями сайта. Управління матеріалами сайта. Розробка інформаційного

| | |
|---|---|
| представництва органу поліції. Проблеми побудови інтелектуальних систем управління контентом сайтів. Системи управління контентом і безпека web-сайтів. Концепція захищеної системи управління. | |
| **Тема № 10. Організація систем електронного документообігу**<br>Документаційне забезпечення управлінської діяльності. Маршрут документа. Механізми автоматичного розподілу документів по картотеках, кабінетах, папках та посадових осіб. Схема документообігу. Обов'язкові типові компоненти СЕД.<br>Дослідження можливостей системи електронного документообігу. Адміністрування системи. Робота із загальними папками. Ролі співробітників. Виконання документів. Узгодження документів. Робота з вхідною та вихідною кореспонденцією. Створення документів. Тенденції та перспективи розвитку систем е-документообігу. Механізми управління правами суб'єктів. Технологія атрибутивних сертифікатів. | |
| **Тема № 11. Інформаційні реєстри та системи надання електронних довірчих послуг**<br>Адміністративно-правові, інституційні, інтеграційні та сервісні механізму розвитку електронного урядування. Базові сервіси надання е-адмінпослуг. Реінжиніринг адміністративно-управлінських процесів за допомогою електронних регламентів. Реєстрова модель надання послуг. Типовий алгоритм впровадження е-адмінрегламенту. Розвиток єдиного веб-порталу адміністративних послуг. Завдання сервісних центрів адміністративних послуг МВС. Реалізація процедур обліку кримінальних правопорушень в єдиному реєстрі досудових розслідувань. Реєстрація правопорушення. Відкриття та перегляд незареєстрованих кримінальних правопорушень. Відкриття и перегляд реєстру кримінальних проваджень. Внесення змін у кримінальному правопорушенні. | |
| **Програмні результати навчання (ПРН)** | ПРН 11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах. |
| | ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. |
| | ПРН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів. |
| | ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. |
| | ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів у інформаційно-телекомунікаційних системах. |
| | ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. |
| | ПРН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних |

| | |
|---|---|
| | (автоматизованих) системах. |
| | ПРН 52. Використовувати інструментарій щодо моніторингу процесів в інформаційно-телекомунікаційних системах |
| | ПРН 55. Брати участь у попередженні, розкритті та розслідуванні правопорушень, здійснених з використанням можливостей кіберсфери. |
| **Критерії оцінювання** | Оцінювання навчальної дисципліни проводиться за результатами поточного та підсумкового контролю:<br>• поточний контроль - 50 балів;<br>• підсумковий контроль - 50 балів.<br>Оцінка за поточний контроль складається з оцінювання аудиторної та самостійної роботи здобувача вищої освіти. Оцінка за аудиторну роботу визначається як середнє арифметичне балів, які ним отримані на семінарських заняттях (здобувач має отримати не менш 5 позитивних оцінок) з коефіцієнтом 5. Оцінка за самостійну роботу визначається як середнє арифметичне балів, які отримані здобувачем за: реферати, програми (здобувач має підготувати не менш 2 проектів) з коефіцієнтом 5.<br>Підсумкові бали з навчальної дисципліни визначаються як сума балів, які отримані здобувачем протягом семестру, та балів, які набрані на підсумковому контролі (заліку). |

**ШКАЛА ОЦІНЮВАННЯ: НАЦІОНАЛЬНА ТА ECTS**

| **Оцінка в балах** | **Оцінка за національною шкалою** | **Оцінка за шкалою ECTS** | |
|---|---|---|---|
| | | **Оцінка** | **Пояснення** |
| **97-100**<br>**94-96**<br>**90-93** | Відмінно (“зараховано”) | A | **„Відмінно”** – теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом сформовані, всі навчальні завдання, які передбачені програмою навчання виконані в повному обсязі, відмінна робота без помилок або з однією незначною помилкою. |
| **85-89**<br>**80-84** | Добре (“зараховано”) | B | **„Дуже добре”** – теоретичний зміст курсу освоєний цілком, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконані, якість виконання більшості з них оцінено числом балів, близьким до максимального, робота з двома – трьома незначними помилками. |

| | | | |
|---|---|---|---|
| **75-79** | | C | **„Добре”** – теоретичний зміст курсу освоєний цілком, практичні навички роботи з освоєним матеріалом в основному сформовані, всі навчальні завдання, які передбачені програмою навчання виконані, якість виконання жодного з них не оцінено мінімальним числом балів, деякі види завдань виконані з помилками, робота з декількома незначними помилками, або з однією – двома значними помилками. |
| **70-74** | Задовільно (“зараховано”) | D | **„Задовільно”** – теоретичний зміст курсу освоєний не повністю, але прогалинине носять істотного характеру, необхідні практичні навички роботи з освоєним матеріалом в основному сформовані, більшість передбачених програмою навчання навчальних завдань виконано, деякі з виконаних завдань, містять помилки, робота з трьома значними помилками. |
| **65-69** | | | |
| **60-64** | | E | **„Достатньо”** – теоретичний зміст курсу освоєний частково, деякі практичні навички роботи не сформовані, частина передбачених програмою навчання навчальних завдань не виконані, або якість виконання деяких з них оцінено числом балів, близьким до мінімального,робота, що задовольняє мінімуму критеріїв оцінки. |
| **40-59** | Незадовільно („не зараховано”) | FX | **„Умовно незадовільно”** – теоретичний зміст курсу освоєний частково, необхідні практичні навички роботи не сформовані, більшість передбачених програм навчання, навчальних завдань не виконано, або якість їхнього виконання оцінено числом балів, близьким до мінімального; при додатковій самостійній роботі над матеріалом курсу можливе підвищення якості виконання навчальних завдань (з можливістю повторного складання), робота, що потребує доробки |
| **21-40** | | | |
| **1-20** | | F | **„Безумовно незадовільно”** – теоретичний зміст курсу не освоєно, необхідні практичні навички роботи не сформовані, всі виконані навчальні завдання містять грубі помилки, додаткова самостійна робота над матеріалом курсу не приведе до значимого підвищення якості виконання |

| | | | |
|---|---|---|---|
| | | | навчальних завдань, робота, що потребує повної переробки |

**Перелік питань, що виносяться на підсумковий контроль**

1. Яка інформація відноситься до службової?
2. Яка інформація відноситься до персональних даних?
3. Принципи побудови та склад системи інформаційного забезпечення
4. Основні завдання та призначення системи ІПНП?
5. Структура системи ІПНП.
6. Що таке «інформація». Основні властивості інформації.
7. Основні види інформації за змістом
8. Основні види інформаційної діяльності
9. Види інформації, що використовуються в органах Національної поліції
10. Загрози інформації: сутність, види.
11. Поясніть сутність ідентифікації користувача в системі.
12. Які вимоги до завдання паролів на доступ до інформації?
13. Що таке криптографічне шифрування?
14. Складові частини системи інформаційного забезпечення.
15. Назвіть призначення Інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України».
16. Назвіть основні завдання Інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України».
17. Охарактеризуйте обов'язки користувачів системи «Інформаційний портал Національної поліції України».
18. Назвіть складові системи «Інформаційний портал Національної поліції».
19. Охарактеризуйте комплексну систему захисту інформації системи «Інформаційний портал Національної поліції України».
20. Назвіть які системи входять до складу Єдиної інформаційної системи МВС.
21. Структура системи централізованого управління нарядами поліції.
22. Загальні вимоги до обробки персональних даних.
24. Організація простого та розширеного пошуку інформації у пошукових серверах глобальної мережі Інтернет.
25. Прийоми та засоби автоматизації розробки юридичних документів текстового процесора
26. Обробка табличних даних у MS Excel.
27. Основні поняття баз даних, метаданих, структур даних і систем управління базами даних
28. Основні об'єкти баз даних: таблиці, форми, запити, звіти, сторінки.
29. Класифікація спеціальних засобів поліції.
30. Технічні засоби захисту інформації з обмеженим доступом.
31. Засоби зв'язку поліції.
32. Завдання та типи система управління контентом.
33. Загальні аспекти розроблення сайта.
34. Система розмежування доступу користувачів сайта.
35. Принципи застосування ідентифікації громадян та установ.
36. Національна інфраструктура відкритих ключів (PKI).

37. Банківська ідентифікація (BankID).
38. Мобільна ідентифікація (mobileID).
39. Організаційне, правове та технічне забезпечення електронного підпису.
40. Управління потоками робіт і організація захищеного документообігу.
41. Базові сервіси надання електронних послуг.
42. Реєстрова модель надання послуг.

## ОСНОВНА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

**Навчальна та наукова література:**


1. Гнусов Ю. В.,. Світличний В. А, Онищенко Ю. М. Спеціальна техніка Національної поліції України : навч. посіб. з дис. «Тактико-спеціальна підготовка» Харк. нац. ун-т внутр. справ, факультет № 4, каф. кібербезпеки. Харків : ХНУВС, 2017. 175 с.
2. Дрінь Б.М. Конспект лекцій з дисципліни «Сучасні інформаційні технології» для студентів спеціальності «Політологія». Івано-Франківськ, ДВЗН «Прикарпатський національний університет». 2016. 211 с.
3. Електронна комерція: навч. посіб. / Ю. Г. Машкаров, І. В. Кобзев, О. В. Орлов, М. В. Мордвинцев. Харків : Вид-во ХарРІ НАДУ “Магістр”, 2014. 192 с.
4. Клімушин П. С. Стратегії та механізми електронного урядування в інформаційному суспільстві : монографія. Харків. Вид-во ХарРІ НАДУ “Магістр”, 2016. 524 с.
5. Клімушин П. С., Орлов О. В., Серенок А. О. Інформаційні системи та інформаційні технології в економіці. Навч. посіб. Харків. Вид-во ХарРІ НАДУ “Магістр”, 2011. 448 с.
6. Кормич Б.А., Федотов О.П., Аверочкіна Т.В. Правове регулювання інформаційної діяльності: навчально-методичний. Одеська юридична академія. 2018. 150 с.
7. Косиченко О.О., Махницький О.В. Захист службової інформації під час використання електронної Web-пошти на основі асиметричного шифрування з відкритим ключем за допомогою програми Mailvelope. Методичні рекомендації. Дніпропетровський державний університет внутрішніх справ. Дніпро, 2018.36 с.
8. Краснобрижий І.В., Прокопов С.О., Рижков Е.В. Інформаційне забезпечення професійної діяльності: навч. посіб. Дніпро : ДДУВС, 2018. 218 с.
9. Методичні рекомендації проведення оперативно-тактичних навчань на основі інформаційного моделювання дій нарядів та інших підрозділів Національної поліції/ О.О. Акімова, О.С. Гавриш, О.В. Махницький, С.О. Прокопов, Е.В. Рижков, Ю.І. Тюря. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2017. 37 с.
10. Нелюбов В.О., Куруца О.С. Основи інформатики. Microsoft Word 2016: електронний навчальний посібник. Ужгород: ДВНЗ УжНУ, 2018. 96 с.
11. Прикладний кримінальний аналіз на базі інформаційно-аналітичної системи «Ricas»: Методичні рекомендації щодо аналітичної діяльності та кримінального аналізу на базі інформаційно-аналітичної системи «Ricas». Харків: «Юрайт», 2018. 92 с.
12. Трофименко О.Г., Буката Л.М. СУБД ACCESS створення та опрацювання баз даних. Методичні вказівки до лабораторних, практичних занять та самостійної

роботи студентів. Одеська національна академія зв'язку ім. О. С. Попова. Одеса: Одеська національна академія зв'язку ім. О. С. Попова. 2016. 96с.

## ДОДАТКОВА ЛІТЕРАТУРА З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

**Навчальна та наукова література:**

1. Андрєєв О., Каменчук О., Семеніхін В., Шамрай Н. Єдині вимоги (стандарт) до якості обслуговування відвідувачів центрів надання адміністративних послуг. Київ : Міністерство економічного розвитку і торгівлі України, 2017. 40с.
2. Бригілевич І. Діяльність ЦНАП та оцінка якості надання адміністративних послуг: практичний посібник. Київ. 2017. 40 с.
3. Буханевич О. М. Проблеми впровадження електронних адміністративних послуг в Україні. Науковий вісник Херсонського державного університету. Серія «Юридичні науки». 2015. Вип. 3. Том 2. С. 57–60.
4. Величкевич М. Б, Мітрофан Н. В., Кунанець Н. Е. Електронний документообіг, тенденції та перспективи. Вісник Нац. ун-ту "Львів. політехніка". 2010. № 689. С. 44–53.
5. Домінова І. В. Форми електронного банкінгу: еволюція, переваги та недоліки. Облік і фінанси. 2016. № 2. С. 104 109.
6. Інструкція з організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України. Наказ Міністерства внутрішніх справ України 27 квітня 2020 року N 357. URL: https://zakon.rada.gov.ua/laws/show/z0443-20#Text
7. Положення про Єдину Інформаційну Систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів : постанова КМУ від 14.11.2018 № 1024 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1024-2018-%D0%BF
8. Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України» : наказ МВС України від 03.08.2017 № 676 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/z1059-17
9. Порядок функціонування центральної підсистеми Єдиної інформаційної системи Міністерства внутрішніх справ України: Наказ МВС України від 16.09.2020 № 655. // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/z1092-20#Text
10. Практичні аспекти організації припинення роботи інтернет-ресурсів національного та закордонного сегментів, що використовуються для вчинення злочинів: методичні рекомендації / [В.О. Мирошниченко, І.В. Краснобрижий, В.Д. Поливанюк, С.В. Бабанін, І.О. Кисельов, Д.Ю. Чередниченко, Ю.В. Заскока]. – Дніпропетровськ: Дніпроп. держ. ун-т. внутр. справ, 2015. – 50 с.
11. Про електронні довірчі послуги : Закон України від 5 жовтня 2017 р. № 2155-VIII. URL: http://zakon2.rada.gov.ua/laws/show/2155-19/page
12. Про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку і скасування Директиви 1999/93/ЄС: Регламент ЄС №910/2014 Європейського парламенту та Ради від 23 липня 2014. URL:http://eur-lex.europa.eu/legal-

content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG .
13. 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.

**Нормативно-правові акти:**

1. Про інформацію. Закон України від 02.10.1992, № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.
2. Про Державну службу спеціального зв'язку та захисту інформації України. Закон України: від 23.02.2006, № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text.
3. Про захист інформації в інформаційно-комунікаційних системах. Закон України: від 05.07.1994, № 1170-VII. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
4. Про електронні комунікації: Закон України від 16.12.2020 : [із змінами і доповненнями]. Офіційний вісник України. 2021. № 6 (21.01.2021). Ст. 306.
5. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
6. Про захист персональних даних. Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
7. Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 10.05.2023).
8. Стратегія інформаційної безпеки України, затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 10.05.2023).
9. Про створення Центру протидії дезінформації: Рішення Ради національної безпеки і оборони України від 11 березня 2021 року, введено в дію Указом Президента України від 19 березня 2021 року № 106/2021. URL: https://zakon.rada.gov.ua/laws/show/106/2021#Text.
10. ДСТУ ISO/IEC 27000:2019 (ISO/IEC 27000:2018, IDT) Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів - На заміну ДСТУ ISO/IEC 27000:2017 (ISO/IEC 27000:2016, IDT).
11. ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013; Cor 1:2014, IDT) / Поправка № 2:2019.
12. (ISO/IEC 27001:2013/Cor 2:2015, IDT) Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги.
13. ДСТУ ISO/IEC 27002:2015 (ISO/IEC 27002:2013; Cor 1:2014, IDT) / Поправка № 2:2019 (ISO/IEC 27002:2013/Cor 2:2015, IDT). Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.
14. ДСТУ ISO/IEC 27003:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова (ISO/IEC 27003:2017, IDT).
15. ДСТУ ISO/IEC 27004:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання (ISO/IEC 27004:2016, IDT).

16. ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT) Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки - На заміну ДСТУ ISO/IEC 27005:2015 (ISO/IEC 27005:2011, IDT).

**Інформаційні ресурси в Інтернеті:**

1. http://docprof.com.ua/
2. http://geekhub.ck.ua/
3. http://sed.reforms.in.ua/basic-page/prezentaciya
4. http://www.basic.com.ua/
5. http://www.optima-ukraine.com.ua/
6. https://acskidd.gov.ua/
7. https://ca.informjust.ua/
8. https://ca.mvs.gov.ua/certificates-searc
9. https://czo.gov.ua/ca-registry
10. https://danco.com.ua/
11. https://e-docs.ua/
12. https://fossdoc.com/
13. https://garant-school.com.ua
14. https://id.bank.gov.ua/
15. https://inbase.com.ua/ua/
16. https://itea.ua/
17. https://it-rating.in.ua/rating-cms-2018
18. https://itstep.kh.ua/
19. https://kharkov-it-courses.blogspot.com
20. https://kursor.kiev.ua
21. https://support.office.com/uk-ua
22. https://ukrzvit.ua/
23. https://www.hostinger.ru/rukovodstva/luchshie-cms-platformy-2019/