МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
КАФЕДРА КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ
ФАКУЛЬТЕТУ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ

ФОРОС Г.В., БАЛТОВСЬКИЙ О.А.

Навчально-методичні рекомендації до вивчення навчальної дисципліни

«ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ»

Для здобувачів вищої освіти освітнього ступеня «магістр » у галузі знань 26 «Цивільна безпека» спеціальність 262 «Правоохоронна діяльність»

ФАКУЛЬТЕТ № 2 НАВЧАЛЬНО-НАУКОВОГО ІНСТИТУТУ ПРАВА ТА КІБЕРБЕЗПЕКИ

2022 рік

Схвалено та рекомендовано до друку Навчально-методичною радою ОДУВС

Рецензенти:
Тетерятник Г.К. – доктор юридичних наук, доцент, завідувачка кафедри кримінального процесу факультету підготовки фахівців для органів досудового слідства ОДУВС
Кобозєва А.А. – доктор технічних наук, професор, завідувачка кафедри кібербезпеки та програмного забезпечення Інституту інформаційної безпеки, радіоелектроніки та телекомунікацій Національного університете «Одеська політехніка»

Інформаційно-аналітичне забезпечення правоохоронної діяльності: навчально-методичні матеріали /уклад. Г.В. Форос, О.А. Балтовський. Одеса: ОДУВС, 2022. 26 с.

ЗМІСТ

1. ПОЯСНЮВАЛЬНА ЗАПИСКА

Програма вивчення навчальної дисципліни «Інформаційно-аналітичне забезпечення правоохоронної діяльності» складена відповідно до освітньо-професійної програми підготовки магістрів в галузі знань 26 «Цивільна безпека», спеціальності 262 «Правоохоронна діяльність».

«Інформаційно-аналітичне забезпечення правоохоронної діяльності» є навчальною дисципліною, яка надає базові теоретичні знання та практичні навички з питань застосування сучасних інформаційних технологій в діяльності Національної поліції.

Зміст навчальної дисципліни «Інформаційно-аналітичне забезпечення правоохоронної діяльності» містить теоретичні питання інформаційного забезпечення Національної поліції, базові знання про аспекти застосування інформаційних систем та підсистем в діяльності Національної поліції, про єдиний облік злочинів та осіб, які їх вчинили, розглядає методи та засоби інформаційної безпеки, а також систему інформаційної безпеки Національної поліції.

Метою викладання навчальної дисципліни “Інформаційно-аналітичне забезпечення правоохоронної діяльності» є: оволодіння здобувачами вищої освіти основними положеннями теорії, методології інформації та управління інформаційно-аналітичними процесами для досягнення ефективності в управлінської діяльності, а також навичок, необхідних для використання сучасних інформаційних технологій в практичній діяльності правоохоронних органів для вирішення практичних задач.

Предметом вивчення навчальної дисципліни є основні поняття інформаційно-аналітичного забезпечення, інформаційних процесів та технологій, що використовуються в роботі правоохоронних органів та навички їх використання в практичній діяльності.

Основними завданнями вивчення дисципліни “Інформаційно-аналітичне забезпечення правоохоронної діяльності» є ознайомлення з теоретичними засадами інформатизації правоохоронних органів України; опанування інформаційними технологіями та системами, які використовуються в професійній діяльності; вивчення проблемних питань щодо основних тенденцій, напрямів та шляхів розвитку системи інформаційно-аналітичного забезпечення правоохоронних органів України. Відповідно до інформаційної політики ці завдання нерозривно пов'язані з формуванням інформаційного середовища підрозділів Національної поліції України, що складається з відомчих інформаційних ресурсів і всієї інформаційної інфраструктури МВС. Ефективність інформаційного середовища правоохоронних органів забезпечується за рахунок комплексного, системного підходу до рішення проблем техніко-технологічного й соціально-політичного характеру. Рішення останніх проблем пов'язано, у першу чергу, з відкритістю інформаційного середовища для суспільства, що дає можливість реалізувати погоджені інтереси громадян, суспільства й держави на системній основі.

Теоретичні знання та практичні навички одержані протягом вивчення навчальної дисципліни «Інформаційно-аналітичне забезпечення правоохоронної діяльності" дадуть змогу майбутнім фахівцям на кваліфікованому рівні застосовувати інформаційні системи та підсистеми в практичній діяльності. Поважне місце у вивченні курсу займають питання забезпечення управління, а саме такі його аспекти як інформаційне, документаційне, правове, кадрове, матеріально-технічне та фінансове.

Міждисциплінарні зв’язки: дана навчальна дисципліна тісно пов'язана і логічне доповнює такі навчальні дисципліни, як «Інформаційні технології», «Інформаційне забезпечення професійної діяльності», «Криміналістика», «Кримінальний процес», «Оперативно-розшукова діяльність». Успішне її вивчення вимагає від здобувачів знання різних законодавчих і нормативних актів, а також цілого комплексу спеціальних знань, які були придбані в перелічених навчальних дисциплінах.

2. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин			
	заочна форма			
	усього	у тому числі		
		л	с	с.р
Тема 1. Теоретичні та методологічні засади інформаційно-аналітичного забезпечення	21	2		19
Тема 2. Теоретичні основи інформаційно - аналітичної діяльності. Методи аналітики, їхня універсальність у процесі пізнання.	25	2	2	21
Тема 3. Правове регулювання інформаційної сфери в Україні. Суб'єкти інформаційної діяльності, та їх потреби в інформації	23		2	21
Тема 4. Інформаційний процес. Інформаційні посередники як функціональні складники системи інформаційно-аналітичної діяльності	21	2		19
Усього годин	90	6	4	80

3. ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ТЕМА 1. ТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ ЗАСАДИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ

Поняття про інформаційно-аналітичне забезпечення. Мета та завдання аналітичного забезпечення (оперативне отримання інформації; збір, обробка та узагальнення інформації; забезпечення захисту інформації). Нормативно-правова база інформаційно-аналітичного забезпечення Національної поліції України. Підготовка, навчання та перепідготовка кадрів для інформаційно-технічних служб Національної поліції України.

Історія виникнення та розвитку системи інформаційно-аналітичного забезпечення правоохоронних органів. Тенденції розвитку систем аналітичного забезпечення правоохоронних органів.

Інформація як основна категорія системи інформаційно-аналітичного забезпечення. Якісні та кількісні характеристики інформації. Вимоги, що ставляться до інформації в діяльності правоохоронних органів.

Теоретичні знання: у наслідку вивчення даної теми здобувачі вищої освіти повинні знати роль і місце інформації в діяльності правоохоронних органів, поняття про інформаційно-аналітичне забезпечення, його мету та завдання, генезис системи інформаційно-аналітичного забезпечення, нормативно-правове забезпечення діяльності інформаційних служб та підрозділів, визначення інформації як основної категорії системи інформаційно-аналітичного забезпечення.

Практичні навички: при вивченні даної теми здобувачі вищої освіти повинні вміти отримувати необхідну інформацію з веб-сайтів правоохоронних органів.

Методичні рекомендації

При вивченні цієї теми здобувачі вищої освіти повинені засвоїти, що поняття

аналітичне забезпечення немає однозначного визначення. Для певного виду діяльності надається певне визначення цього поняття, але аналітичне забезпечення слід розглядати як управлінську функцію будь-якої діяльності, якій властиві певні принципи та ознаки, і яка направлена на ефективне вирішення певних управлінських задач.

Так, інформаційно-аналітичне забезпечення це – сукупність дій та заходів … для збору, нагромадження, обробки та аналізу даних на основі інформаційних технологій, у процесі реалізації якого особливої ваги набуває систематичність визначення кола питань, що виникають у процесі базової діяльності споживача інформації, їх аналіз та прогнозування тенденцій розвитку. До поняття інформаційно-аналітичного забезпечення віднесений організаційний аспект, який вказує на головні напрямки правового регулювання інформаційно-аналітичного забезпечення. Таке значення зазначеного терміну може бути співвіднесене з діяльністю, що пов’язана із збиранням, реєстрацією, передачею, зберіганням і опрацюванням інформації.

Інформаційно-аналітичне забезпечення організації управління є однією з функцій створення умов (організовування) ефективності здійснення управлінської діяльності на всіх її рівнях від окремої посадової особи до вищих органів державної влади. Саме від інформаційно-аналітичного забезпечення залежить ефективність управління певною системою.

Також при вивченні цієї теми зазначити, що відповідно до Закону України "Про інформацію" (ст. 1), інформація - це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Доступність інформації обумовлена не лише її юридичним статусом, а й фактичними умовами її використання для різних суб'єктів. Для задоволення своїх інформаційних потреб суб'єкти інформаційної діяльності використовують певні джерела інформації. А оскільки поняття "джерело інформації" вживається надзвичайно широко, то, щоб уникнути ускладнень у роботі, аналітику треба добре розуміти, яке змістове навантаження несе цей термін у кожному конкретному випадку. У загальному розумінні під джерелами інформації розуміють документи та інші носії інформації, які являють собою матеріальні об'єкти, що зберігають інформацію, а також повідомлення засобів масової інформації, публічні виступи.

При розгляданні питання про інформаційно-аналітичне забезпечення правоохоронної діяльності потрібно основну увагу приділяти інформаційно-технічному забезпеченню (бази даних, використання персональних комп'ютерів, при обробці інформації).

Самостійна робота. При самостійній підготовці слід визначити основі тенденції та проблеми розвитку системи аналітичного забезпечення НП. Також визначити шляхи ефективного вирішення завдань сучасного аналітичного забезпечення НП по розкриттю та розслідуванню злочинів.

З даної теми передбачено читання лекції та проведення семінарського заняття, формою контролю є усне опитування здобувачів вищої освіти під час проведення занять.

Питання для самоконтролю

1. Вкажіть мету та завдання вивчення навчальної дисципліни «Інформаційно-аналітичне забезпечення професійної діяльності».
2. Надайте визначення поняття інформаційно-аналітичне забезпечення та охарактеризуйте його специфіку.
3. Охарактеризуйте місце та роль навчальної дисципліни в системі навчальних дисциплін.
4. Охарактеризуйте основні етапи розвитку інформаційно-аналітичної діяльності в історичному аспекті.
5. Що таке інформація та які види інформації Вам відомі?
6. Вкажіть основні характеристики інформації.
7. Перелічіть основні завдання системи інформаційно-аналітичного забезпечення правоохоронних органів.

ТЕМА 2. ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ. МЕТОДИ АНАЛІТИКИ, ЇХНЯ УНІВЕРСАЛЬНІСТЬ У ПРОЦЕСІ ПІЗНАННЯ

Поняття про інформаційно-аналітичну діяльність. Актуальність, суть, основні принципи інформаційно-аналітичної діяльності. Поняття про цілі, об'єкт, предмет, суб'єкти інформаційно-аналітичної діяльності.

Визначення поняття «аналітика». Загальні професійні вимоги до рівня фахової підготовки аналітика. Основні методи аналітики. Характеристика основних різновидів інформаційно-аналітичної діяльності.

Методи організації інформаційно-аналітичної діяльності. Методи збору аналітичної інформації. Поняття та методи аналітичних прогнозів. Моделі та типи прогнозів.

Теоретичні знання: у наслідок вивчення даної теми здобувачі вищої освіти повинно знати визначення понять «інформаційно-аналітична діяльність», «аналітика», знати цілі та основні принципи інформаційно-аналітичної діяльності, загальні професійні вимоги до рівня фахової підготовки аналітика, основні методи організації інформаційно-аналітичної діяльності, а також методи збору аналітичної інформації.

Практичні навички: при вивченні даної теми здобувачі вищої освіти повинні вміти методи аналітики в практичній діяльності.

Методичні рекомендації

При вивченні цієї теми здобувачам вищої освіти слід засвоїти, що інформаційно-аналітична діяльність – це специфічний різновид інтелектуальної, розумової діяльності людини, в процесі якої внаслідок певного алгоритму послідовних дій з пошуку, накопичення, зберігання, обробки, аналізу первинної інформації утворюється нова, вторинна аналітична інформація у формі аналітичної довідки, звіту, огляду, прогнозу тощо.

Обов'язково звернути увагу на той факт, що в сучасних умовах специфіка інформаційно-аналітичної роботи полягає в забезпеченні особи, яка приймає рішення (управлінця), необхідною і достатньою кількістю аналітичної інформації для прийняття єдино правильного, ефективного в умовах непередбаченості і кризових явищ управлінського рішення.

При визначенні цілій інформаційно-аналітичної діяльності слід поділити їх на дві групи: стратегічні і тактичні. При цьому необхідно вказати на їх відмінності та сфери застосування. Стратегічні спрямовані на збір та обробку інформації, для надання споживачеві (замовнику) якомога більш якісний і повний інформаційний продукт, а тактичні спрямовані на визначення конкретно в кожному випадку окремо, залежно від завдання, яке ставить перед аналітиком споживач (замовник).

При встановленні особливостей інформаційно-аналітичної діяльності необхідно вказати, що аналі́тик це - фахівець, який займається аналізом даних в конкретній галузі або дослідженнями та узагальненнями в певній сфері діяльності. Серед позитивних рис професії аналітика слід вказати, що це творча робота - кожен проект унікальний і вимагає свого підходу до розробки, видима і відчутна користь діяльності, коли робочий процес в організації має чіткий стиль і послідовність; придбання навичок комунікативного спілкування, а також розширення кола корисних знайомств за рахунок проектів у різних організаціях.

Самостійна робота. При самостійній підготовці до заняття здобувачам вищої освіти необхідно закріпити загальне поняття про методи організації інформаційно-аналітичної діяльності методи збору аналітичної інформації. Більш детальніше розглянути поняття аналітичних прогнозів та дослідити методи, моделі аналітичних прогнозів.

З даної теми передбачено читання лекції, проведення семінарського заняття, формою контролю є усне опитування здобувачів вищої освіти під час проведення семінарського заняття.

Семінарське заняття № 1 – 2 години

Учбові питання:

1. Інформаційно-аналітична діяльність: поняття, актуальність, суть, основні принципи інформаційно-аналітичної діяльності.
2. Загальні професійні вимоги до рівня фахової підготовки аналітика. Основні методи аналітики.
3. Методи організації інформаційно-аналітичної діяльності та збору аналітичної інформації.
4. Поняття та методи аналітичних прогнозів. Моделі та типи прогнозів.

Питання для самоконтролю

1. Дайте характеристику основним методам організації інформаційно-аналітичної діяльності.
2. Окресліть загальноприйнятий алгоритм діагностики інформаційних подій і процесів.
3. Назвіть найпоширеніші види аналізів інформаційних процесів і явищ.
4. Охарактеризуйте основні методи збору інформації.
5. Дайте обґрунтування використання основних логічних законів.
6. Назвіть типові помилки при написанні та оформленні аналітичної роботи.
7. Дайте визначення поняттям «прогноз» та «прогнозування».
8. Окресліть загальне правило прогнозу.
9. Коротко охарактеризуйте методи прогнозу інформаційних подій і явищ.
10. Назвіть основні етапи прогнозування.

ТЕМА 3. ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ СФЕРИ В УКРАЇНІ. СУБ'ЄКТИ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, ТА ЇХ ПОТРЕБИ В ІНФОРМАЦІЇ

Система законодавчого забезпечення інформаційно-аналітичної діяльності в Україні. Закон України «Про інформацію» як базовий акт у системі регулювання інформаційних відносин. Класифікація нормативних актів стосовно інформаційно-аналітичної діяльності.

Поняття «суб'єкт інформаційних відносин». Учасники (суб'єкти) інформаційних правовідносин та їх класифікація. Види суб'єктів інформаційних правовідносин щодо суспільної організації та за правовим статусом. Інформаційні потреби споживачів. Сутність і структура інформаційного циклу. Характеристики інформаційних потреб. Методи вивчення інформаційних потреб.

Теоретичні знання: у наслідок вивчення даної теми здобувачі вищої освіти повинні знати систему законодавчого забезпечення інформаційно-аналітичної діяльності в Україні, основні поняття, що визначенні в Законі України «Про інформацію», класифікацію нормативних актів стосовно інформаційно-аналітичної діяльності. Окрім цього дослідити учасників (суб'єкти) інформаційних правовідносин та їх класифікація.

Практичні навички: при вивченні даної теми здобувачі вищої освіти повинні вміти встановлювати інформаційні потреби споживачів та надавати . характеристику інформаційних потреб.

Методичні рекомендації

При підготовці до семінарського заняття слід детальніше зупинитися на основних положеннях теорії інформації щодо розуміння суспільних відносин та соціальних аспектах інформаційних відносин (правовий, психологічний, економічний, управлінський і т.ін.). Ефективна організація інформаційної діяльності в суспільстві можлива тільки за умов її адекватного правового забезпечення. Інформаційні правовідносини виникають, змінюються та припиняються в інформаційній сфері та регулюються інформаційно-правовими нормами. Особливість інформаційно-правових норм полягає в тому, що вони регулюють відособлені групи суспільних відносин, що застосовуються до особливостей інформаційної сфери.

Обов’язково слід зазначити, що інформаційні правовідносини - це відносини, що виникають при: формуванні і використанні інформаційних ресурсів на основі створення, збору, опрацювання, накопичення, збереження, пошуку, поширення і надання споживачу документованої інформації; створенні і використанні інформаційних технологій і засобів їхнього забезпечення; захисту інформації, прав суб'єктів, що беруть участь в інформаційних процесах та інформатизації. Слід також вказати основні принципи інформаційних відносин: гарантованість права на інформацію; відкритість, доступність інформації та свобода її обміну; об'єктивність, вірогідність інформації; повнота і точність інформації; законність одержання, використання, поширення та зберігання інформації.

Окремо слід підкреслити, що в українському національному праві системоутворюючим фактором в системі інформаційно-аналітичного забезпечення можна вважати прийнятий 2 жовтня 1992 р. Закон України "Про інформацію". Подальший розвиток регулювання інформаційних відносин у публічному (державному) праві набув відображення в прийнятих нових законах України.

При самостійні підготовці до семінарського заняття слід більш детальніше розкрити систему правового регулювання соціальних інформаційних відносин. Особливу увагу приділити сучасній нормативній базі, що регламентує визначення інформаційно-аналітичного забезпечення, принципи організації інформаційного-аналітичного процесу, вимоги до інформаційно-аналітичного забезпечення діяльності правоохоронних органів.

З даної теми передбачено проведення семінарського заняття, формою контролю є усне опитування здобувачів вищої освіти під час проведення занять.

Семінарське заняття № 2- 2 години

Учбові питання:

1. Інформаційно-правові норми: поняття, зміст та класифікація.
2. Система законодавчого забезпечення інформаційно-аналітичної діяльності в Україні.
3. Учасники (суб’єкти) інформаційних правовідносин та їх класифікація. Види суб’єктів інформаційних правовідносин щодо суспільної організації та за правовим статусом.
4. Інформаційні потреби споживачів. Характеристики інформаційних потреб. Методи вивчення інформаційних потреб.

Питання для самоконтролю

1. Охарактеризуйте систему законодавчого забезпечення інформаційно-аналітичної діяльності в Україні.
2. Чому Закон України «Про інформацію» фахівці визначають як базовий?
3. Надайте класифікацію Законів України та підзаконних актів, що регламентують інформаційно-аналітичну діяльність.
4. Охарактеризуйте поняття «суб’єкт інформаційних відносин».
5. Дайте визначення поняттям «потреба», «інформаційна потреба».
6. Розкрийте поняття «інформаційний цикл».
7. Вкажіть види інформаційних потреб.
8. Охарактеризуйте методи вивчення інформаційних потреб.

ТЕМА 4. ІНФОРМАЦІЙНИЙ ПРОЦЕС. ІНФОРМАЦІЙНІ ПОСЕРЕДНИКИ ЯК ФУНКЦІОНАЛЬНІ СКЛАДНИКИ СИСТЕМИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ

Поняття та сутність інформаційного процесу. Складники (етапи) інформаційно-аналітичного процесу. Причини викривлення інформації.

Інформаційні шуми, бар’єри та їх вплив на якісні та кількісні показники інформації. Загальна характеристика поняття «інформаційні посередники».

Бібліотеки як універсальна форма інформаційного посередництва. ЗМІ як потужний

ресурс інформаційного посередництва. Суспільно-інформаційна роль реклами.

Теоретичні знання: у наслідок вивчення даної теми здобувачі вищої освіти повинні знати поняття та сутність інформаційного процесу, причини викривлення інформації, поняття інформаційний шум, бар'єри та їх вплив на якісні та кількісні показники інформації, «інформаційні посередники».

Практичні навички: при вивченні даної теми слухачі повинні вміти інтерпретувати факті та типові помилки в аналітичних висновках та мати поняття та методи аналітичних прогнозів.

Методичні рекомендації

При вивченні цієї теми здобувачі вищої освіти повинні засвоїти, що інформаційні процеси - це послідовна зміна стану та уявлення про інформацію в результаті дій, які з нею можна виконувати. До таких дій можна віднести створення, збирання, зберігання, обробка(аналіз), відтворення, передавання, розповсюдження, використання і захист інформації. Під час інформаційного процесу дані перетворюються з одного виду в інший за допомогою певних методів.

При підготовці до семінарського заняття слід особливу увагу приділити визначенню поняття «інформаційні посередники» та встановити їх специфічні особливості. Так, інформаційний посередник – це особа чи організація, яка від імені іншої особи відправляє, одержує або зберігає електронні документи, повідомлення або надає інші послуги із використанням інформаційно-телекомунікаційних технологій. До особливостей слід віднести, що інформаційний посередник не несе юридичної відповідальності за збереження електронних документів при автоматичному і короткочасному збереженні даних документів з метою їхньої передачі, здійснюваної за доручення учасника електронної торгівлі. Інформаційний посередник не зобов'язаний контролювати і перевіряти законність переданих і збережених електронних документів, за винятком випадків, передбачених законодавством України.

Матеріали даної теми пов'язані з практичною діяльністю різних підрозділів НП. Також слід засвоїти, що інформаційно-аналітична робота – це постійна дослідна діяльність (функція процесу управління), що охоплює своїм змістом широкий комплекс організаційних заходів і методичних прийомів дія вивчення і оцінки інформації про зовнішні та внутрішні фактори функціонування системи управління щодо виконання визначених для неї мети і завдань. На практиці аналітичне забезпечення охоплює систему руху і перетворення інформації.

Самостійна робота. Під час самостійної підготовки до даного заняття здобувачі повинні приділити увагу наданню характеристики бібліотек як універсальної форми інформаційного посередництва, а також визначенню засобів масової інформації як потужного ресурсу інформаційного посередництва.

З даної теми передбачено читання лекції, проведення семінарського заняття, формою контролю є усне опитування здобувачів вищої освіти під час проведення занять.

Питання для самоконтролю

1. Дайте характеристику поняття «інформаційний процес».
2. Визначте основні етапи інформаційно-аналітичного процесу.
3. Обґрунтуйте необхідність «пастки часу».
4. Які основні причини викривлення інформації?
5. Що таке інформаційний шум?
6. Охарактеризуйте поняття «інформаційного бар'єру».
7. Дайте визначення поняття «інформаційні посередники».
8. Чому саме бібліотеки є потужним ресурсом інформаційного посередництва?
9. Як відбувається політичне маніпулювання?
10. Коротко охарактеризувати PR (паблік рилейшинз).

ПЕРЕЛІК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ:

Нормативні акти:

1. Конституція України від 28. 06. 1996 р. № 254к/96-ВР. URL: http://zakon.rada.gov.ua/laws/show/254к/96-вр
2. Про Національну поліцію : Закон України від 05 жовтня 2016 р. № 580-VIII // Відомості Верховної Ради України. – 2015. № 40-41. ст. 379. https://zakon.rada.gov.ua/laws/show/580-19
3. Про оперативно-розшукову діяльність : Закон України від 08 жовтня 2016 р. № 2135-XII // Відомості Верховної Ради України. – 1992. №22. ст. 303. https://zakon.rada.gov.ua/laws/show/2135-12
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР. URL: http://zakon.rada.gov.ua/laws/show/80/94-вр
5. Закон України «Про інформацію» від 02.10.1992 № 2657-12. URL: http://zakon.rada.gov.ua/laws/show/2657-12
6. Закон України «Про Національну програму інформатизації» від 04.02.1998 № 74/98-ВР. URL: http://zakon.rada.gov.ua/laws/show/74/98-вр
7. Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України», затверджене наказом МВС України від 03 серпня 2017 р. № 676, зареєстрованого в Міністерстві юстиції України 28 серпня 2017 р. № 1059/30927. https://zakon.rada.gov.ua/laws/show/z1059-17
8. Положення про інформаційно-телекомунікаційну систему прикордонного контролю "Гарт-1" Державної прикордонної служби України, затверджене наказом Адміністрації Державної прикордонної служби України 30.09.2008 N 810 https://zakon.rada.gov.ua/laws/show/z1086-08
9. Інструкція з формування та ведення інформаційної підсистеми «СЛІД» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України», затверджена наказом МВС України від 16 березня 2020 р. № 257 https://zakon.rada.gov.ua/laws/show/z0319-20
10. Інструкція з формування та ведення інформаційної підсистеми «Дорожньо-транспортна пригода» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України», затверджена наказом МВС України від 15 липня 2020 року № 533 https://zakon.rada.gov.ua/laws/show/z0726-20
11. Інструкція з формування та ведення інформаційної підсистеми "Гарпун" інформаційно-телекомунікаційної системи "Інформаційний портал Національної поліції України", затверджена наказом МВС України від 13 червня 2018 року № 497 https://zakon.rada.gov.ua/laws/show/z0787-18
12. Інструкція з формування та ведення інформаційної підсистеми «Атріум» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України», затверджена наказом МВС України від 11 грудня 2019 року № 1032 https://zakon.rada.gov.ua/laws/show/z0217-20
13. Інструкція з формування та ведення інформаційної підсистеми "Єдиний облік" інформаційно-телекомунікаційної системи "Інформаційний портал Національної поліції України", затверджена наказом МВС України від 14 червня 2019 року № 508 https://zakon.rada.gov.ua/laws/show/z0739-19#Text

Допоміжна

14. Балтовський О.А., Ісмайлов К.Ю., Сіфоров О.І., Форос Г.В., Заєць О.М. Теорія систем і системний аналіз: навч. посібник. Одеський держ. унів-т внутр. справ, 2020. 156 с.
15. Вировий С.В. Інформаційно-аналітичне забезпечення діяльності органів державної влади та місцевого самоврядування. Ефективність державного управління. 2014. № 39. С. 201–206
16. Грохольський В.Л., Ісмайлов К.Ю., Форос Г.В. Науково-практичний коментар до Закону України «Про основні засади забезпечення кібербезпеки України» / за заг. ред. д. ю. н., проф. В. Л. Грохольського. Одеса. ОДУВС, 2020. 134 с.

17. Державне управління : підручник: у 2 т. /ред. кол. : Ю. В. Ковбасюк (голова), К. О. Ващенко (заст. голови), Ю. П. Сурмін (заст. голови) та ін. К. Дніпропетровськ : НАДУ, 2012. Т. 1. 564 с.
18. Дорошко М.С., Шпакова Н.В. Соціально-правові основи інформаційної безпеки. Навчальні матеріали он-лайн. URL: https://pidruchniki.com/ gosguu. narod.ru/gos/96.html.
19. Дяченко Н.П. Інформаційно-аналітичне забезпечення діяльності органів державної влади та місцевого самоврядування. Теорія та практика державного управління. 2011. № 1(118).
20. Інформаційне забезпечення професійної діяльності: навч. посібник / І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков. Дніпро : ДДУВС, 2018. 220 с.
21. Ісмайлов К. Ю., О.І. Лефтеров, В.С. Жогов Навчально-методичні рекомендації щодо пошуку оперативнозначущої інформації в мережі Інтернет. Одеса: Одеський державний університет внутрішніх справ, 2019. 26 с.
22. Катеринчук І.П. Інформаційне забезпечення діяльності правоохоронних органів України: проблеми теорії і практики : монографія. Одеса : ОДУВС, 2015. 392.
23. Коваленко Ю.О. Інформаційне забезпечення протидії корупції в правоохоронних органах України: визначення та сутність. Науковий вісник Ужгородського національного університету. 2016. Вип. 41. С. 204-207.
24. Короткий тлумачний словник керівника підрозділу кримінального аналізу: словник / Ісмайлов К.Ю., Кіреєва О.С., Половніков В.В., Постол О.І., Фаріон О.Б. Одеса: Одеський державний університет внутрішніх справ, 2018. 110 с.
25. Марущак А.І. Інформаційне право: регулювання інформаційної діяльності: Навчальний посібник. К.: Дакор, 2011. 344 с.
26. Методичні рекомендації щодо використання інформаційних ресурсів Інтегрованої інформаційно-пошукової системи ОВС України / О.О. Мельнікова, К.Ю. Ісмайлов. Одеса: Одеський державний університет внутрішніх справ, 2018. 39 с.
27. Методичні рекомендації щодо виявлення, фіксації та вилучення криміналістично значущої інформації з мобільних пристроїв під час розслідування кримінальних правопорушень / Д.С. Афонін, К.Ю. Ісмайлов, Д.В. Лісніченко, О.І. Постол. Одеса: Одеський державний університет внутрішніх справ, 2018. 38 с.
28. Нормативно правове забезпечення системи аналітичного забезпечення НП України. http://www.pravo.vuzlib.net/book_n046_page_40.html
29. Основи кримінального аналізу: підручник / Бабенко А.М., Заєць О.М., Некрасов В.А., Ісмайлов К.Ю., Пефтієв Д.О. та ін.; за заг. ред. Користіна О.Є., 2019. 270 с.
30. Тактичний кримінальний аналіз: теорія і практика: Навчальний посібник /Н.П. Свиридюк, О.М. Цильмак, Заєць О.М., Ісмайлов К.Ю., Некрасов В.А. за заг. ред. Користіна О.Є.; МВС України, ДНДІ, ОДУВС. Одеса: РВВ ОДУВС, 2019. 298 с.
31. Теорія систем та системний аналіз: навчальний посібник / О.А. Балтовський, К.Ю. Ісмайлов, О.І. Сіфоров, Г.В. Форос, О.МЗаєць. Одеса: РВВ ОДУВС, 156 с.
32. Форос Г.В., Кірей Д.В. Інформаційно-аналітичний документ як результат інформаційно-аналітичної діяльності. Матеріали Міжнародної НПК «Кібербезпека в Україні: правові та організаційні питання». Одеса. 2019.
33. Форос Г.В., Колпакова В. Окремі аспекти інформаційно-аналітичного забезпечення правоохоронної діяльності. Матеріали ІІІ Всеукраїнська НПК «Кібербезпека в Україні: правові та організаційні питання». Одеса. 2018. С. 23

5. ФОРМА ПОТОЧНОГО ТА ПІДСУМКОВОГО КОНТРОЛЮ УСПІШНОСТІ НАВЧАННЯ, КРИТЕРІЇ ОЦІНЮВАННЯ ЗНАНЬ

Система оцінювання передбачає накопичення 100 балів з кожної навчальної дисципліни, які перераховуються в національну шкалу та шкалу оцінювання ЄКТС.

Встановлюються: максимальні суми балів за виконання завдань у рамках аудиторної, самостійної роботи та модульної контрольної роботи - 60 балів; 40 балів - за

виконання завдань, винесених на підсумковий контроль.

Поточний контроль			Підсумковий контроль
Аудиторна робота	**Самостійна робота**	**Модульна контрольна робота**	**ЗАЛІК (З)/ ЕКЗАМЕН (Е)**
≤ 30	**≤ 20**	**≤ 10**	
≤ 60			**≤ 40**
Підсумкова оцінка у випадку заліку (П) = ПК+ З ≤ 100			
Підсумкова оцінка у випадку складання екзамену (П) = ПК+Е ≤100			
ДЛЯ ЗАОЧНОЇ ФОРМИ НАВЧАННЯ			
Поточний контроль			**Підсумковий контроль**
Аудиторна робота	**Самостійна робота**		**ЗАЛІК (З)/ ЕКЗАМЕН (Е)**
≤ 20	**≤ 40**		
≤ 60			**≤ 40**
Підсумкова оцінка у випадку заліку (П) = ПК+ З ≤ 100			
Підсумкова оцінка у випадку складання екзамену (П) = ПК+Е ≤100			

Здобувач вищої освіти, як додатковий здобуток за наукову роботу в межах навчальної дисципліни може отримати до 10 балів, при цьому загальна сума накопичувальних балів не повинна перевищувати 100.

Оцінювання компетентностей здобувача вищої освіти з навчальної дисципліни та виставлення підсумкової кількості балів за аудиторну роботу здійснюється шляхом встановлення відповідного рівня знань за кожне навчальне заняття та виставлення балів від 3 до 5. Підсумкова кількість балів визначається, як сума всіх отриманих під час проведення навчальних занять балів розділена на кількість семінарських/практичних занять, передбачених тематичним планом у семестрі та помножена на коефіцієнт відповідності максимально можливого балу:

$$= \frac{ПК}{КЗ} \times \frac{\sum ПК}{КВ},$$

де: ПК – підсумкова кількість балів за аудиторну роботу; ∑пк – сума всіх отриманих балів за семінарські/практичні заняття; КЗ – кількість семінарських/практичних занять, передбачених тематичним планом за семестр; КВ – коефіцієнт відповідності максимально можливого балу (6 – для денної форми навчання; 4 – для заочної форми навчання).

Здобувач вищої освіти може отримати «5» балів за умови, що він дуже добре орієнтується в матеріалі, приймав активну участь у занятті та надав повну відповідь на питання семінарського заняття, або на додаткове питання науково-педагогічного працівника, навів приклади, висловив та аргументував власну точку зору, або суттєво доповнював більше трьох разів відповіді колег, не допустивши помилок. Також у «5» балів може бути оцінено виступ з доповіддю або рефератом, які було підготовлено з використанням декількох джерел інформації, а під час виступу тему розкрито повно.

Здобувач вищої освіти може отримати «4» бали за умови, що він достатньо добре орієнтується в матеріалі, приймає активну участь у занятті, доповнюючи колег, знає основні визначення та факти з теми семінарського заняття, надав правильну, але не зовсім повну відповідь, висловлює власну думку, але не може змістовно її аргументувати, йому складно навести приклади. Також у «4» балів може бути оцінено виступ здобувача з доповіддю або рефератом, які було підготовлено з використанням одного джерела інформації, а під час виступу тему розкрито не повно.

Здобувач вищої освіти може отримати «3» бали за умови, якщо не приймає активної участі в семінарському занятті та не висловлює цікавості до матеріалу, йому складно дати визначення понять, відповідає фрагментарно та спутано, допускає помилки, не орієнтується

у темі, власної думки не має, або висловлюючи її відмовляється аргументувати. Також у «3» балів може бути оцінено виступ здобувача з доповіддю або рефератом, які містять мізерний обсяг інформації, або застарілі данні.

Під час навчальних занять на денній формі навчання науково-педагогічний працівник може поставити оцінку «2» (незадовільно). Незадовільна оцінка «2» ставиться за умови незнання здобувачем вищої освіти значної частини навчального матеріалу за змістом відповідної теми навчальної дисципліни, що міститься в основних рекомендованих нормативних та базових джерелах, допустив істотні помилки у відповідях на поставлені питання, виявив невміння застосовувати теоретичні положення під час розв'язання практичних задач, відмовився від відповіді та/або не вирішив практичне завдання. Незадовільна оцінка «2» потребує перескладання та в загальну суму накопичення балів не враховується.

Підсумкова кількість балів за самостійну роботу з навчальної дисципліни визначається науково-педагогічним працівником, як сума отриманих здобувачем вищої освіти балів за всі види виконаних завдань, які передбачені відповідними методичними матеріалами із зазначенням балів за виконання кожної самостійної роботи відповідно до тематичного плану.

Умови допуску здобувача вищої освіти до складання підсумкового контролю:

Для денної форми навчання:

1. сума балів поточного контролю не менше ніж 36;
2. має не більше трьох невідпрацьованих пропусків;
3. має не більше трьох невідпрацьованих незадовільних оцінок за поточний контроль.

Для заочної форми навчання:

- сума балів поточного контролю не менше ніж 36.

З метою підвищення поточного рейтингу успішності здобувач вищої освіти має право перескладати аудиторну та самостійну роботу відповідно до графіку, встановленого науково-педагогічним працівником до підсумкового контролю і не більше двох пропусків та/або незадовільних оцінок у один робочий день.

Здобувач вищої освіти, який за результатами поточного контролю накопичив менше 60 балів, зобов'язаний складати підсумковий контроль.

Здобувач вищої освіти, який за результатами поточного контролю протягом семестру накопичив 60 балів, має можливість:

1. не складати підсумковий контроль і отримати накопичену кількість балів як підсумкову оцінку;
2. складати підсумковий контроль відповідно до розкладу.

Недопущення здобувача вищої освіти до підсумкового контролю прирівнюється до незадовільної оцінки. Питання про недопущення здобувача вищої освіти до підсумкового контролю вирішує науково-педагогічний працівник та здійснює відповідний запис «не допущено» в заліково-екзаменаційної відомості.

Здобувач вищої освіти, який недопущенний до складання підсумкового контролю, має право скласти його під час визначеного окремим графіком для ліквідації академічної заборгованості, попередньо досягнувши всіх умов допуску.

Відсутність здобувача вищої освіти, який накопичив менше 60 балів за поточний контроль на підсумковому контролі без поважної причини прирівнюється до незадовільної оцінки. Такий здобувач вищої освіти має право скласти підсумковий контроль під час ліквідації академічної заборгованості визначеним окремим графіком.

Здобувач вищої освіти зобов'язаний попередити деканат/інститут про свою можливу відсутність на підсумковому контролі до його початку. Здобувач вищої освіти, який був відсутній на підсумковому контролі з поважних причин, які підтверджені відповідними документами, за рішенням декана факультету (директора інституту) може скласти пропущений підсумковий контроль у визначений деканатом час.

Здобувач вищої освіти, який за результатами поточного та підсумкового контролю

сумарно накопичив менше 60-ти балів, допускається до повторного перескладання підсумкового контролю після закінчення екзаменаційної сесії, але до початку наступного семестру чи атестації.

КРИТЕРІЇ ОЦІНЮВАННЯ ЗНАНЬ

Оцінка "відмінно"/ A – виставляється, якщо здобувач вищої освіти має глибокі і системні знання, вміє узагальнювати теоретичний матеріал, співвідносити загальні знання з конкретними ситуаціями; оволодів навиками аналізу, моделювання та адекватного оцінювання ситуації; обізнаний з науковими працями вітчизняних та зарубіжних фахівців в даній галузі; матеріал викладає логічно, послідовно, переконливо і аргументовано.

Оцінка "добре"/ B, C – виставляється, якщо здобувач вищої освіти показав достатній рівень знання курсу; надав правильні, але не зовсім повні визначення термінів; засвоїв основи аналітичного методу; допускає незначні неточності в розкритті окремих теоретичних положень.

Оцінка "задовільно"/ D, E – виставляється, якщо здобувач вищої освіти в цілому засвоїв теоретичний матеріал курсу навчальної дисципліни, але декламує із деякими упущеннями при визначенні основних явищ та процесів; намагається висловити своє ставлення до проблемних питань, хоча і не зовсім аргументовано; вміє аналізувати набуті теоретичні знання і співвідносити їх з конкретними ситуаціями; викладає матеріал непослідовно, неточно, з наявними помилками.

Оцінка "незадовільно"/ FX, F – виставляється, якщо здобувач вищої освіти виявив слабкі (відсутні) знання теоретичного матеріалу навчальної дисципліни; не зміг дати визначення основних категорій та явищ; відсутні знання основних норм і визначень; матеріал викладається непослідовно, нелогічно, фрагментарно та з допущенням помилок.

Оцінка A, B, C, D, E / "зараховано" – виставляється, якщо здобувач вищої освіти виявив достатньо повні знання матеріалу навчальної дисципліни; вміє узагальнювати теоретичний матеріал, співвідносити загальні знання з конкретними ситуаціями, дає правильні, хоча і не завжди повні відповіді на поставлені запитання; допускає неточності у розкритті окремих теоретичних положень, норм та визначень.

Оцінка FX, F / "не зараховано" – виставляється, якщо здобувач вищої освіти виявив слабкі знання або повну неготовність щодо вивчення ним матеріалу навчальної дисципліни; не зміг дати визначення основних термінів та визначень; викладає матеріал непослідовно, нелогічно, фрагментарно, неточно, стисло; відсутня переконливість у викладенні матеріалу.

Шкала оцінювання: національна та ECTS

<table>
<tr><th>За внутрішньою шкалою закладу вищої освіти в балах</th><th colspan="2">За шкалою ECTS /За національною шкалою</th></tr>
<tr><td></td><td colspan="2">Вноситься до відомості</td></tr>
<tr><td></td><td>Екзамен</td><td>залік</td></tr>
<tr><td>90 – 100</td><td>A/Відмінно</td><td rowspan="5">A,B,C,D,E/Зараховано</td></tr>
<tr><td>82-89</td><td>B/Добре</td></tr>
<tr><td>74-81</td><td>C/Добре</td></tr>
<tr><td>64-73</td><td>D/Задовільно</td></tr>
<tr><td>60-63</td><td>E/Задовільно</td></tr>
<tr><td rowspan="2">35-59</td><td>FX/Незадовільно</td><td>FX/Не зараховано</td></tr>
<tr><td colspan="2">з можливістю повторного складання</td></tr>
<tr><td rowspan="2">0-34</td><td>F/Незадовільно</td><td>F/Не зараховано</td></tr>
<tr><td colspan="2">з обов'язковим повторним курсом</td></tr>
</table>

6. ПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ

1. Поняття про інформаційно-аналітичне забезпечення професійної діяльності.
2. Мета та завдання аналітичного забезпечення (оперативне отримання інформації; збір, обробка та узагальнення інформації; забезпечення захисту інформації).
3. .Історія виникнення та розвитку інформаційно-аналітичної діяльності.
4. Тенденції розвитку систем аналітичного забезпечення правоохоронних органів.
5. Інформація як основна категорія системи інформаційно-аналітичного забезпечення
6. Якісні та кількісні характеристики інформації. Вимоги, що ставляться до інформації в діяльності правоохоронних органів.
7. Суть та основні принципи інформаційно-аналітичної діяльності.
8. Поняття про цілі, об'єкт, предмет, суб'єкти інформаційно-аналітичної діяльності.
9. Методи аналітики, їх універсальність в процесі пізнання.
10. Визначення поняття «аналітика» та основні методи аналітики
11. Загальні професійні вимоги до рівня фахової підготовки аналітика.
12. Специфіка аналітики в системі сучасних наук: проблеми і перспективи.
13. Методи організації інформаційно-аналітичної діяльності.
14. Методи збору аналітичної інформації.
15. Поняття та методи аналітичних прогнозів.
16. Моделі та типи прогнозів.
17. Етапи і порядок підготовки інформаційно-аналітичних документів.
18. Проблема «пастки часу» і засоби її подолання.
19. Прогностична діяльність в інформаційно-аналітичному процесі.
20. Специфіка інформаційних систем аналітичної обробки інформації.
21. Система законодавчого забезпечення інформаційно-аналітичної діяльності в Україні.
22. Закон України «Про інформацію» як базовий акт у системі регулювання інформаційних відносин.
23. Класифікація нормативних актів стосовно інформаційно-аналітичної діяльності.
24. Поняття «суб'єкт інформаційних відносин».
25. Учасники (суб'єкти) інформаційних правовідносин та їх класифікація.
26. Види суб'єктів інформаційних правовідносин щодо суспільної організації та за правовим статусом.
27. Інформаційні потреби споживачів.
28. Сутність і структура інформаційного циклу.
29. Характеристики інформаційних потреб. Методи вивчення інформаційних потреб.
30. Становлення і розвиток інформаційного суспільства: проблеми і перспективи.
31. Особливості національної моделі розвитку інформаційного суспільства.
32. Сучасні концепції розвитку цивілізацій: перспективи і загрози.
33. Поняття та сутність інформаційного процесу.
34. Складники (етапи) інформаційно-аналітичного процесу.
35. Причини викривлення інформації.
36. Інформаційні шуми, бар'єри та їх вплив на якісні та кількісні показники інформації.
37. Загальна характеристика поняття «інформаційні посередники».
38. Бібліотеки як універсальна форма інформаційного посередництва. ЗМІ як потужний ресурс інформаційного посередництва.
39. Суспільно-інформаційна роль реклами.
40. Інформаційні війни в структурі сучасних світових процесів: виклики та загрози.

8. ГЛОСАРІЙ

Автоматизована інформаційна система оперативного призначення (АІС ОП)- сукупністю програмно-технічних і телекомунікаційних засобів та призначена для накопичення й обробки відомостей, що утворюються в процесі оперативно-розшукової діяльності Національної поліції Україні.

Автоматизовані інформаційно-пошукові системи – сукупність методів і засобів, призначених для зберігання та пошуку документів, відомостей про них чи певних фактів.

Автоматизовані комп'ютерні системи (АКС) – сукупність взаємопов'язаних АЕОМ, периферійного обладнання та програмного забезпечення, призначених для автоматизації прийому, зберігання, обробки, пошуку і видачі інформації споживачам.

Аналіз - поділ об'єкта (подумки чи реально) на складові частини з метою їх окремого вивчення. Такими частинами можуть бути якісь матеріальні елементи об'єкта або ж його властивості, ознаки, зв'язки й т.п.

Аналітичний документ - вторинний документ, що містить узагальнену інформацію, отриману в результаті всебічного, глибокого та критичного аналізу первинних документів, аргументовану оцінку стану і тенденцій розвитку проблеми, що розвивається.

Блокування інформації в системі - дії, внаслідок яких унеможливлюється доступ до інформації в системі.

Виток інформації - результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї.

Віртуальний простір - простір, що моделюється за допомогою комп'ютера, у якому перебувають відомості про особи, предмети, факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому виді й рухи, що перебувають у процесі, по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального устрою, а також іншого носія, спеціально призначеного для їхнього зберігання, обробки й передачі.

Документ - матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі.

Доступ до інформації в системі - отримання користувачем можливості обробляти інформацію в системі.

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

Захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі.

Знищення інформації в системі - дії, внаслідок яких інформація в системі зникає.

Інтегрована інформаційно-пошукова система органів внутрішніх справ України – це сукупність організаційно-розпорядчих заходів, програмно-технічних та інформаційно-телекомунікаційних засобів, що забезпечують формування та ведення довідково-інформаційних, оперативно-розшукових обліків, авторизований доступ до інформаційних ресурсів ІІПС.

Інтегрована інформаційно-телекомунікаційна система «Аркан» - це сукупність організаційно-розпорядчих заходів, програмно-технічних та телекомунікаційних засобів, що забезпечують обробку інформації (уведення, приймання, отримання, передавання, реєстрація, зберігання) щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон України, та автоматизований доступ до інформаційних ресурсів (баз даних) суб'єктів системи «Аркан».

Інтегрована інформаційно-телекомунікаційна система «Гарт-1» - це сукупність організаційно-розпорядчих заходів, програмно-технічних та телекомунікаційних засобів, що забезпечують обробку інформації (уведення, записування, зчитування, зберігання, знищення, приймання, передавання) щодо прикордонного контролю осі і транспортних

засобів, які перетинають державний кордон України, та автоматизований доступ до інформації, що зберігається в базах даних системи "Гарт-1".

Інформаційна система - сукупність організаційних і технічних засобів для збереження та обробки інформації з метою забезпечення інформаційних потреб користувачів.

Інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

Інформаційна безпека - складова національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України;

Інформаційна безпека – це стан захищеності інформаційного простору, що забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави

Інформаційна війна: 1) дії з метою досягнення інформаційної переваги шляхом застосування заходів для експлуатування, підриву, знищення, дестабілізації і руйнування інформаційного потенціалу противника і його функцій; 2) міри з метою захисту власних інформаційних ресурсів і телекомунікаційних систем; 3) дії з метою використання інформаційних ресурсів і телекомунікаційних систем іншої сторони для досягнення цілей і інтересів, наприклад електронна війна (інформаційна війна в оборонному і військовому контексті), війна в Інтернеті (інформаційна війна в більш широкому суспільному контексті).

Інформаційна мережа – мережа, призначена для обробки, зберігання та передачі даних.

Інформаційна послуга - це отримання і надання в розпорядження користувача інформаційних продуктів.

Інформаційна продукція - матеріалізований результат інформаційної діяльності, призначений для задоволення потреб суб'єктів інформаційних відносин.

Інформаційне забезпечення - це: 1) комплекс організаційних, правових, технічних і технологічних заходів, засобів та методів, котрі забезпечують в процесі управління і функціонування системи інформаційні зв'язки та елементів (суб'єктів і об'єктів) шляхом оптимальної організації інформаційних масивів баз даних і знань; 2) діяльність, що організується в рамках управління, спрямована на проектування, функціонування та вдосконалення інформаційних систем, що забезпечують ефективне виконання задач управління; 3)органічна єдність роботи щодо визначення змісту, обсягів, якості інформації, необхідної для здійснення управління, а також заходів щодо раціональної організації процесів для здійснення управління, а також заходів щодо раціональної організації процесів збирання, систематизації, накопичення та обробки цієї інформації шляхом.

Інформаційне суспільство - суспільство, в якому більшість робітників займаються створенням, збиранням, відображенням, реєстрацією, накопиченням, збереженням і поширенням інформації, особливо її вищої форми - знань.

Інформаційний продукт (продукція) - створена виробником сукупність документованої інформації, відомостей, даних і знань, яка призначена для забезпечення інформаційних потреб користувача.

Інформаційний простір (національний) - інформаційне середовище, в якому здійснюються інформаційні процеси та інформаційні відносини щодо створення, збирання, відображення, реєстрації, накопичення, збереження, захисту і поширення інформації, інформаційних продуктів та інформаційних ресурсів, на яке розповсюджується юрисдикція держави.

Інформаційний ресурс – це сукупність документів в інформаційних системах.

Інформаційний суверенітет - здатність держави контролювати і регулювати потоки інформації поза межами держави з метою додержання законів України, прав і свобод громадян, забезпечення національної безпеки держави.

Інформаційні відносини - відносини, які виникають у всіх сферах життя і діяльності людини, суспільства і держави при одержанні, використанні, поширенні та зберіганні інформації.

Інформаційні ресурси - це весь обсяг знань, відчужених від їх творців, зафіксованих на матеріальних носіях і призначених для суспільного використання.

Інформаційні ресурси єдиної інформаційної системи МВС - визначені групи взаємозв'язаних задокументованих одиниць інформації, які формуються і об'єднуються в автоматизованих інформаційних системах суб'єктів єдиної інформаційної системи МВС за певними ознаками.

Інформаційні технології - цілеспрямована організована сукупність інформаційних процесів з використанням засобів електронної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування.

Інформаційно-аналітична діяльність: 1) сукупність дій на основі концепцій, методів, засобів, нормативно-методичних матеріалів для збору, накопичення, обробки та аналізу даних з метою обґрунтування та прийняття рішень. 2) специфічний різновид інтелектуальної, розумової діяльності людини, в процесі якої внаслідок певного алгоритму послідовних дій з пошуку, накопичення, зберігання, обробки, аналізу первинної інформації утворюється нова, вторинна аналітична інформація у формі аналітичної довідки, звіту, огляду, прогнозу тощо.

Інформаційно-аналітичне забезпечення це – сукупність дій та заходів … для збору, нагромадження, обробки та аналізу даних на основі інформаційних технологій, у процесі реалізації якого особливої ваги набуває систематичність визначення кола питань, що виникають у процесі базової діяльності споживача інформації, їх аналіз та прогнозування тенденцій розвитку.

Інформаційно-аналітичні документи містять інформацію, що є підставою для прийняття певних рішень, тобто ініціюють управлінські рішення, дозволяють обирати той або інший спосіб управлінського впливу.

Інформаційно-телекомунікаційна система - сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

Інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України» - сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності Національної поліції України та її інформаційно-аналітичного забезпечення.

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

Інформація моніторингова - інформація, що надходить у систему управління по каналам зворотного зв'язку і відображає реакцію керованої системи на управляючі впливи.

Кібербезпека - безпека інформації та інфраструктури в цифровому середовищі, що її забезпечує. Кібербезпека передбачає досягнення і збереження властивостей безпеки в ресурсах організації або користувачів, що спрямовані на запобігання відповідним кіберзагрозам.

Комплексна система захисту інформації - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

Комп'ютерна інформація – це текстова, цифрова, графічна чи інша інформація (дані, відомості) про осіб, предмети, події, яка існує в електронному вигляді, зберігається на відповідних електронних носіях і може використовуватися, оброблятися або змінюватися при допомозі ЕОМ (комп'ютерів).

Комп'ютерні мережі (мережа ЕОМ) – це об'єднання декількох комп'ютерів (ЕОМ) та комп'ютерних систем, що взаємопов'язані і розташовані на фіксованій території та орієнтовані на колективне використання загальномережевих ресурсів.

Криптографічний захист інформації - вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Міжнародні злочини – суспільно небезпечні умисні посягання на життєвоважливі інтереси міжнародного співтовариства, основи існування держав і народів – міжнародний мир і міжнародну безпеку.

Моделювання – це метод дослідження різних явищ і процесів, вироблення варіантів управлінських рішень.

Моніторинг – комплекс наукових, технічних, технологічних, організаційних та інших засобів, які забезпечують систематичний контроль (стеження) за станом та тенденціями розвитку природних, техногенних та суспільних процесів.

Національна безпека – здатність країни своєчасно виявляти, запобігати і нейтралізувати реальні та потенційні загрози національним інтересам.

Несанкціоновані дії щодо інформації в системі - дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства.

Обробка інформації в системі - виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів.

Програмне забезпечення «Акорд» - сучасний програмний продукт, який забезпечує фіксування запису аудіо та відео судового процесу на базі якого можливе проведення відеоконференцій між сторонами та учасниками процесу.

Режим доступу до інформації – це передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації.

Ринок інформаційних послуг - сукупність економічних, правових і організаційних відносин по продажу і купівлі інформаційних продуктів та послуг (*ІПП)*, які складаються між їхніми постачальниками і споживачами.

Сервіс єдиної інформаційної системи МВС - спеціальний програмний засіб, що забезпечує доступ користувачів єдиної інформаційної системи МВС до інформаційних ресурсів єдиної інформаційної системи МВС.

Система інформаційного забезпечення - це сукупність інформаційних підсистем певних обліків, побудованих з урахуванням дотримання таких вимог: наявності нормативно-правової бази; організаційно-кадрового забезпечення інформаційних підрозділів; організації підготовки та перепідготовки кадрів; наявності відповідних технічних, програмних та телекомунікаційних технологій; матеріально-технічного та фінансового забезпечення.

Суб'єкти єдиної інформаційної системи МВС - апарат МВС та його територіальні органи з надання сервісних послуг МВС, Національна гвардія, заклади, установи і підприємства, що належать до сфери управління МВС, центральні органи виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ, інші державні органи, які обробляють інформацію в єдиній інформаційній системі МВС для реалізації своїх повноважень;

Телекомунікаційна система - сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Технічний захист інформації - вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Додатки

ПОЛОЖЕННЯ
про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України»

І. Загальні положення

1. Це Положення визначає основні завдання, призначення, суб'єктів та структуру інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України», а також умови її функціонування.
2. Інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України» (далі - система ІПНП) - сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності Національної поліції України та її інформаційно-аналітичного забезпечення. Система ІПНП є складовою частиною єдиної інформаційної системи МВС (далі - ЄІС МВС).
3. У цьому Положенні терміни вживаються у значеннях, наведених у Законах України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про телекомунікації», «Про електронні документи та електронний документообіг», «Про електронний цифровий підпис».

ІІ. Основні завдання та призначення системи ІПНП

1. Основними завданнями системи ІПНП є:
інформаційно-аналітичне забезпечення діяльності Національної поліції України;
забезпечення наповнення та підтримки в актуальному стані інформаційних ресурсів баз (банків) даних, що входять до ЄІС МВС;
забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу;
забезпечення електронної взаємодії з МВС та іншими органами державної влади.
2. Система ІПНП призначена для:
формування інформаційних ресурсів ЄІС МВС;
обробки інформації, яка утворена в процесі діяльності поліції;
надання безпосереднього оперативного доступу до інформаційних ресурсів ЄІС МВС;
генерації інтерфейсів та оброблення тимчасових наборів даних для здійснення інформаційної взаємодії органів (підрозділів) поліції з іншими органами державної влади, органами правопорядку іноземних держав, міжнародними організаціями;
здійснення пошукових та аналітичних функцій для використання інформації з інформаційних ресурсів (баз даних) поліції, МВС та інших органів державної влади в межах службової діяльності відповідно до рівня доступу і повноважень за запитом або регламентом;
використання програмних компонентів геоінформаційних підсистем для візуалізації інформації у вигляді електронних карт, автоматичної зміни зображеного образу об'єкта в залежності від зміни його характеристик, зміни масштабу та деталізації картографічної інформації в інформаційних ресурсах;
забезпечення автоматизації процесів управління силами та засобами поліції;
забезпечення електронного документообігу в органах (підрозділах) поліції, обміну електронними документами з МВС;
комплексного захисту інформації та розмежування доступу до інформації, що зберігається в базах даних системи ІПНП.

ІІІ. Інформаційні ресурси системи ІПНП

1. Інформаційними ресурсами системи ІПНП є інформація, що утворена в процесі діяльності поліції та використовується для формування:
тимчасових наборів даних, що створюються в процесі діяльності поліції та використовуються для наповнення та підтримки в актуальному стані баз (банків) даних, які входять до ЄІС МВС та визначені статтею 26 Закону України «Про Національну поліцію»;

баз даних у сфері управлінських відносин, необхідних для виконання покладених на поліцію повноважень;
баз даних, необхідних для забезпечення щоденної діяльності поліції, у сфері трудових відносин, фінансового забезпечення, документообігу.
2. В інформаційних ресурсах системи ІПНП обробляється інформація, яка належить до державних інформаційних ресурсів. Така інформація не підлягає поширенню та передачі іншим особам, крім випадків, передбачених законодавством.
3. Бази даних поліції, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції, містять відомості, зокрема, стосовно:
повідомлень про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події, що надійшли технічними каналами зв'язку;
щодобових переліків та складу нарядів поліції та слідчо-оперативних груп, що заступають на чергування;
завдань та орієнтувань, що доводились до нарядів поліції для реагування на повідомлення про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події;
звітування нарядів поліції за результатами реагування на повідомлення про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події, виявлення додаткових обставин на місці пригоди;
пересувань нарядів поліції, які отримані із планшетних комп'ютерів (мобільних терміналів) та засобами GPS.
Поліція може створювати інші бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції, відповідно до статті 25 Закону України «Про Національну поліцію».
4. Порядок формування та використання інформаційних ресурсів системи ІПНП регулюється окремими нормативно-правовими актами із дотриманням вимог Закону України «Про захист персональних даних» та інших актів законодавства у сфері захисту персональних даних.

IV. Суб'єкти системи ІПНП

1. Розпорядником системи ІПНП є Національна поліція України.
Розпорядник системи ІПНП вживає заходів із організації матеріально-технічного та кадрового забезпечення, що необхідні для ефективного функціонування системи.
2. Адміністратором системи ІПНП є уповноважений структурний підрозділ апарату центрального органу управління Національної поліції України.
Адміністратор системи ІПНП забезпечує
вирішення організаційних питань щодо забезпечення функціонування системи;
ведення обліку користувачів та надання їм доступу до інформації, що в ній обробляється;
захист інформації від несанкціонованого доступу, знищення, модифікації та блокування доступу до неї шляхом здійснення організаційних і технічних заходів, впровадження засобів та методів технічного захисту інформації;
вжиття заходів стосовно розвитку і вдосконалення системи;
координацію функціонування складових системи.
3. Користувачами системи ІПНП є посадові особи органів (підрозділів) поліції, яким в установленому порядку надано право доступу до інформації в цій системі.
4. Ідентифікація користувача та підтвердження цілісності даних, що обробляються в системі ІПНП, забезпечуються застосуванням електронного цифрового підпису або інших програмно-технічних засобів авторизації користувачів та забезпечення цілісності даних.
5. Кожна дія користувача щодо отримання інформації з інформаційних ресурсів системи ІПНП фіксується у спеціальному електронному архіві.
6. Користувачі системи ІПНП зобов'язані не розголошувати у будь-який спосіб інформацію, яка їм стала відома у зв'язку з виконанням посадових обов'язків, крім випадків, передбачених законом, відповідають за достовірність інформації, що вводиться ними до

відповідних інформаційних ресурсів системи ІПНП, та зобов'язані дотримуватися законодавства у сфері захисту інформації.

V. Структура системи ІПНП

1. Складовими системи ІПНП є:
центральний програмно-технічний комплекс;
автоматизовані робочі місця користувачів;
телекомунікаційна мережа доступу;
комплексна система захисту інформації.
2. Центральний програмно-технічний комплекс системи ІПНП - це сукупність технічних і програмних засобів, призначених для обробки інформації, які забезпечують:
введення, записування, зберігання, видалення, знищення, приймання та передавання інформації та формування баз даних у системи ІПНП;
формування тимчасових наборів даних для наповнення та підтримки в актуальному стані інформаційних ресурсів баз (банків) даних ЄІС МВС;
моніторинг стану інформаційного обміну між складовими системи ІПНП, а також системних журналів аудиту роботи користувачів, технічних і програмних засобів;
захист інформації під час її обробки.
3. До складу центрального програмно-технічного комплексу системи ІПНП входять:
центральне сховище даних - програмно-технічний комплекс, який складається із серверів, систем керування базами даних та іншого програмного забезпечення, призначених для безперервного виконання операцій, записування, зберігання, знищення, приймання та передавання інформації, зберігання системних журналів аудиту роботи користувачів та системних журналів реєстрації роботи програмних засобів;
сервери додатків - програмно-технічний комплекс, який складається із серверів та програмного забезпечення, призначених для безперервного виконання операцій з інформаційного обміну між складовими системи ІПНП, функціонування програмних засобів генерації інтерфейсів користувачів для оброблення інформації, записування та зберігання системних журналів аудиту приймання та передавання інформації, реєстрації роботи програмних засобів;
шлюзові сервери - програмно-технічний комплекс, який складається із серверів, призначених для забезпечення захисту інформації під час здійснення обміну інформацією між підсистемами, взаємодії з інформаційними системами МВС та інших центральних органів виконавчої влади;
автоматизоване робоче місце адміністратора безпеки - складова комплексної системи захисту інформації в системі ІПНП, обладнана технічними засобами та програмним забезпеченням, призначеними для моніторингу системних журналів реєстрації роботи програмних та технічних засобів, аналізу порушень в роботі системи ІПНП, налагодження параметрів, необхідних для забезпечення стабільної роботи програмних та технічних засобів, визначення повноважень користувачів системи ІПНП.
4. Центральний програмно-технічний комплекс системи ІПНП розміщується в спеціалізованих службових приміщеннях Національної поліції України.
5. Автоматизовані робочі місця користувачів - це робочі місця поліцейських та інших працівників поліції, обладнані комп’ютерною технікою, у тому числі планшетними комп’ютерами, що підключені до телекомунікаційної мережі доступу системи ІПНП і призначені для автоматизації службової діяльності, реалізації повноважень обробляти інформацію відповідно до наданого рівня доступу в системі ІПНП.
6. Телекомунікаційна мережа доступу системи ІПНП - сукупність технічних і програмних засобів, призначених для обміну інформацією між складовими системи. Для захисту інформації, що обробляється органами (підрозділами) поліції в системі ІПНП, використовуються канали Єдиної цифрової відомчої телекомунікаційної мережі Міністерства внутрішніх справ України, а при використанні відкритих каналів - засоби

захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації.

7. Комплексна система захисту інформації з підтвердженою відповідністю - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

8. Завданням комплексної системи захисту інформації є забезпечення конфіденційності (у разі обробки інформації з обмеженим доступом), цілісності, доступності інформації в системі ІПНП шляхом здійснення заходів, спрямованих на захист інформації від несанкціонованих дій (у тому числі з використанням комп'ютерних вірусів), які можуть призвести до її випадкової або умисної модифікації чи знищення.

9. Контроль за дотриманням вимог законодавства України в сфері захисту інформації під час використання ІПНП здійснює керівник підрозділу, де експлуатується центральний програмно-технічний комплекс системи.

Директор Департаменту формування
політики щодо підконтрольних
Міністрові органів влади та моніторингу МВС В.Є. Боднар

ЗАКОН УКРАЇНИ
Про захист інформації в інформаційно-телекомунікаційних системах

Цей Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі - система).

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

блокування інформації в системі - дії, внаслідок яких унеможливлюється доступ до інформації в системі;

виток інформації - результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

володілець інформації - фізична або юридична особа, якій належать права на інформацію;

власник системи - фізична або юридична особа, якій належить право власності на систему;

доступ до інформації в системі - отримання користувачем можливості обробляти інформацію в системі;

захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

знищення інформації в системі - дії, внаслідок яких інформація в системі зникає;

інформаційна (автоматизована) система - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

інформаційно-телекомунікаційна система - сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

комплексна система захисту інформації - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

користувач інформації в системі (далі - користувач) - фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;

криптографічний захист інформації - вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

несанкціоновані дії щодо інформації в системі - дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;

обробка інформації в системі - виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації,

приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

порушення цілісності інформації в системі - несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;

порядок доступу до інформації в системі - умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації;

телекомунікаційна система - сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

технічний захист інформації - вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Стаття 2. Об'єкти захисту в системі

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Стаття 3. Суб'єкти відносин

Суб'єктами відносин, пов'язаних із захистом інформації в системах, є: володільці інформації; власники системи; користувачі; спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи.

На підставі укладеного договору або за дорученням власник системи може надати право розпоряджатися системою іншій фізичній або юридичній особі - розпоряднику системи.

Стаття 4. Доступ до інформації в системі

Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються володільцем інформації.

Порядок доступу до державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством.

У випадках, передбачених законом, доступ до інформації в системі може здійснюватися без дозволу її володільця в порядку, встановленому законом.

Стаття 5. Відносини між володільцем інформації та власником системи

Власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із володільцем інформації, якщо інше не передбачено законом.

Власник системи на вимогу володільця інформації надає відомості щодо захисту інформації в системі.

Стаття 6. Відносини між власником системи та користувачем

Власник системи надає користувачеві відомості про правила і режим роботи системи та забезпечує йому доступ до інформації в системі відповідно до визначеного порядку доступу.

Стаття 7. Відносини між власниками систем

Власник системи, яка використовується для обробки інформації з іншої системи, забезпечує захист такої інформації в порядку та на умовах, що визначаються договором, який укладається між власниками систем, якщо інше не встановлено законодавством.

Власник системи, яка використовується для обробки інформації з іншої системи, повідомляє власника зазначеної системи про виявлені факти несанкціонованих дій щодо інформації в системі.

Стаття 8. Умови обробки інформації в системі

Умови обробки інформації в системі визначаються власником системи відповідно до договору з володільцем інформації, якщо інше не передбачено законодавством.

Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

Стаття 9. Забезпечення захисту інформації в системі

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Про спроби та/або факти несанкціонованих дій у системі щодо державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган.

Стаття 10. Повноваження державних органів у сфері захисту інформації в системах

Вимоги до забезпечення захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України.

Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації:

розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;

визначає вимоги та порядок створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;

здійснює контроль за забезпеченням захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дає рекомендації з питань запобігання такій загрозі.

Державні органи в межах своїх повноважень за погодженням відповідно із спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкованим йому регіональним органом встановлюють особливості захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Особливості захисту інформації в системах, які забезпечують банківську діяльність, встановлюються Національним банком України.

Стаття 11. Відповідальність за порушення законодавства про захист інформації в системах

Особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно із законом.

Стаття 12. Міжнародні договори

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, визначено інші правила, ніж ті, що передбачені цим Законом, застосовуються норми міжнародного договору.

Стаття 13. Прикінцеві положення

1. Цей Закон набирає чинності з 1 січня 2006 року.

2. Нормативно-правові акти до приведення їх у відповідність із цим Законом діють у частині, що не суперечить цьому Закону.

3. Кабінету Міністрів України та Національному банку України в межах своїх повноважень протягом шести місяців з дня набрання чинності цим Законом:

привести свої нормативно-правові акти у відповідність із цим Законом;

забезпечити приведення міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів у відповідність із цим Законом.

Президент України Л.КУЧМА

м. Ки їв, 5 липня 1994 року N 80/94-ВР