ДОНЕЦЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ФАКУЛЬТЕТ № 3

КАФЕДРА ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ

Галузь знань 26 Цивільна безпека
Спеціальність 262 «Правоохоронна діяльність»
Освітній рівень другий (магістерський)
Освітньо-професійна програма Правоохоронна діяльність
Шифр за ОПП: ОК 15

Мова навчання: українська

Кропивницький – 2024

Розробник:

ГАБОРЕЦЬ Ольга, доцент кафедри
оперативно-розшукової діяльності та
інформаційної безпеки факультету № 3
ДонДУВС, доктор філософії, доцент

Робочу програму розглянуто та затверджено на засіданні кафедри оперативно-розшукової діяльності та інформаційної безпеки факультету № 3 ДонДУВС
Протокол № 15 від «24» липня 2024 року

Завідувач кафедри  **Артур ВОЛОБОЄВ**

Робочу програму погоджено з гарантом освітньо-професійної програми Правоохоронна діяльність

Гарант ОПП  **Артем САХНО**

Лист оновлення та перезатвердження

робочої програми навчальної дисципліни

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача

1. ВСТУП

1.1. Опис навчальної дисципліни

Найменування показників	Характеристика навчальної дисципліни	
	денна форма навчання	**заочна форма навчання**
Статус навчальної дисципліни:	обов'язкова	
Мова викладання, навчання та оцінювання	українська	
Рік підготовки:	1-й	1-й
Семестр:	2-й	2-й
Кількість кредитів ЄКТС / годин	3 / 90	
Модулів:	1	
Змістових модулів:	1	
Лекції:	20 годин	2 години
Семінарські:	4 годин	2 години
Практичні:	16 годин	6 години
Самостійна робота:	50 годин	80 години
Індивідуальні завдання (курсова робота):	не передбачено	
Підсумковий семестровий контроль:	залік	
Співвідношення кількості годин аудиторних занять до самостійної роботи становить:	1:1,25	1:8

1.2. Мета та завдання навчальної дисципліни

Мета дисципліни: підготовка висококваліфікованих професіоналів та професіоналок правоохоронної діяльності для реалізації завдань правоохоронних органів України, здатних володіти системою знань, умінь і практичних навичок щодо застосування сучасних інформаційних технологій, цифрових інструментів, спеціалізованих баз даних, засобів технічної та криптографічної інформаційної безпеки, а також технологій збирання та оброблення даних в умовах оперативно-розшукової діяльності правоохоронних органів; ідентифікувати та розв'язувати складні інформаційно-аналітичні, технічні й кібероперативні задачі, що виникають у процесі забезпечення національної безпеки, протидії злочинності, інформаційного супроводу

оперативно-розшукових заходів, зокрема в умовах воєнного стану та високого рівня кіберзагроз.

Завдання дисципліни: формування теоретичних знань щодо інформаційно-аналітичної роботи в оперативно-розшуковій діяльності, її видів, форм, основних процесів (ідентифікація, діагностика, прогнозування), ролі в умовах воєнного стану; опанування сучасних технологій захисту інформації та основ кібербезпеки, включаючи загрози інформаційній безпеці, анонімність в Інтернеті, шифрування, автентифікацію, менеджери паролів, цифровий відбиток браузера; розвиток навичок роботи з оперативно-розшуковою інформацією, включаючи збір, систематизацію, оцінку, аналіз даних, а також взаємодію з інформаційними джерелами різного типу; опанування сучасних засобів комп'ютерної та кіберрозвідки, включаючи роботу з електронними системами, біометричними технологіями, розпізнаванням облич, особливостями оперативно-розшукової ідентифікації та кібероперативної розвідки; формування навичок використання OSINT-технологій для збору, перевірки та інтерпретації відкритої інформації з інтернет-ресурсів, соціальних мереж, вебплатформ, форумів та державних реєстрів; розвиток компетентностей щодо застосування державних довідково-інформаційних систем, Єдиної інформаційної системи МВС, міжвідомчих реєстрів та інструментів електронної взаємодії державних органів.

1.3. Передумови для вивчення навчальної дисципліни

Навчальна дисципліна є вихідною. Компетентності, сформовані під час її вивчення в подальшому будуть використовуватися під час опанування окремих вибіркових освітніх компонентів та під час здобуття освіти на третьому (освітньо-науковому) рівні вищої освіти.

2. РЕЗУЛЬТАТИ НАВЧАННЯ ЗА ДИСЦИПЛІНОЮ

	ПРН 9	**ПРН 10**	**ПРН 13**	**ПРН 16**	**ПРН 17**	**ПРН 21**
Знати зміст, форми та принципи інформаційно-аналітичної роботи в оперативно-розшуковій діяльності, включаючи отримання, систематизацію, ідентифікацію та прогнозування оперативної інформації			+		+	
Знати інструменти комп'ютерної розвідки, оперативно-розшукової ідентифікації, використання біометричних даних, кіберрозвідки та технологій роботи в кібернетичному просторі	+				+	+

Вміти ідентифікувати інформаційні ризики та загрози, застосовувати технології кіберзахисту, шифрування, автентифікації, анонімності в Інтернеті та інструменти захисту даних		+			+	
Вміти збирати, перевіряти, структурувати та аналізувати оперативно-розшукову інформацію з різних джерел, у тому числі цифрових, відкритих і закритих інформаційних ресурсів	+		+	+		
Вміти застосовувати OSINT-технології: збирати, аналізувати та верифікувати інформацію з відкритих джерел, використовувати спеціалізовані інтернет-ресурси, соціальні мережі, форуми та інші платформи			+	+		+
Вміти ефективно працювати з державними довідково-інформаційними базами, реєстрами, Єдиною інформаційною системою МВС та міжвідомчими ресурсами, застосовувати цифрові технології для забезпечення правопорядку	+	+			+	

3. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістовних модулів та тем	**Кількість годин**									
	денна форма					**заочна форма**				
	Усього	**кількість аудиторних годин**			**Самостійна робота**	**Усього**	**кількість аудиторних годин**			**Самостійна робота**
		лекції	**семінарські**	**практичні**			**лекції**	**семінарські**	**практичні**	
Модуль 1										
Змістовий модуль 1. ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ										
Тема 1. Характеристика основних форм інформаційно-аналітичної роботи в оперативно-розшуковій діяльності Національної поліції.	14	2		2	10	14	2			12
Тема 2. Аналіз ризиків та загроз у сфері інформаційного забезпечення.	18	4	2	4	8	14		2		12

Тема 3. Особливості інформаційного забезпечення оперативно-розшукової діяльності.	14	4		2	8	14				14
Тема 4. Комп'ютерна розвідка та комп'ютерні засоби оперативно-розшукової ідентифікації.	16	4	2	2	8	16			2	14
Тема 5. Оптимізація збору та використання інформації з відкритих джерел (OSINT) у системі забезпечення правопорядку.	16	4		4	8	16			2	14
Тема 6. Використання довідково-інформаційних баз даних вільного доступу (державних реєстрів) у професійній діяльності.	12	2		2	8	16			2	14
Усього годин	**90**	**20**	**4**	**16**	**50**	**90**	**2**	**2**	**6**	**80**

4. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Модуль 1.

Змістовий модуль 1. ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ

Тема 1. Характеристика основних форм інформаційно-аналітичної роботи в оперативно-розшуковій діяльності Національної поліції. Поняття та сутність інформаційно-аналітичної роботи в оперативно-розшуковій діяльності Національної поліції в умовах воєнного стану. Основні форми інформаційно-аналітичної роботи в оперативно-розшуковій діяльності. Отримання оперативно-розшукової інформації. Систематизація оперативно-розшукової інформації. Оперативно-розшукова ідентифікація. Оперативно-розшукова діагностика. Оперативно-розшукове прогнозування.

Тема 2. Аналіз ризиків та загроз у сфері інформаційного забезпечення. Загрози інформаційної безпеки. Захист інформації в автоматизованих системах. Анонімність в Інтернеті: псевдоніми, IP-адреса, проксі, VPN, Cookie, блокування реклами. Цифровий відбиток браузера. Браузер Tor для підвищення анонімності. Парольний захист комп'ютерного обладнання. Двофакторна автентифікація. Паролі по замовчуванню на різних пристроях. Злом та крадіжка паролів. Виток паролів. Брутофорс паролів. Шифр та хеш паролів. Менеджери паролів. Цифрові цінності.

Тема 3. Особливості інформаційного забезпечення оперативно-розшукової діяльності. Загальна характеристика оперативно-розшукової інформації. Джерела інформації в оперативно-розшуковій діяльності. Використання оперативної інформації. Ознайомлення з документами та даними, що характеризують діяльність підприємств, установ та організацій.

Тема 4. Комп'ютерна розвідка та комп'ютерні засоби оперативно-розшукової ідентифікації. Поняття, мета та сутність комп'ютерної розвідки. Зняття інформації з електронних інформаційних систем. Біометричні дані. Біометрична ідентифікація. Автентифікація. Розпізнавання за зображенням обличчя. Особливості оперативно-розшукової ідентифікації. Кіберрозвідка як новітній напрям оперативно-розшукової діяльності. Основні характеристики розвідки інформації у кібернетичному просторі, особливо в умовах воєнного стану. Кібервійна як феномен асиметричних загроз.

Тема 5. Оптимізація збору та використання інформації з відкритих джерел (OSINT) у системі забезпечення правопорядку. Визначення терміну OSINT та його основні концепції. Роль OSINT у сучасному інформаційному суспільстві. Збір відкритої інформації та використання її для різноманітних цілей. Різновиди джерел та типи інформації, доступної через OSINT. Огляд методів використання пошукових систем та спеціальних інтернет-ресурсів для збору інформації. Пошук відкритої інформації через веб-сторінки, форуми, блоги та інші джерела.

Тема 6. Використання довідково-інформаційних баз даних вільного доступу (державних реєстрів) у професійній діяльності. Поняття і класифікація інформаційних ресурсів. Основні можливості відкритих реєстрів та баз даних державних органів. Єдина інформаційна система МВС. Електронна взаємодія між МВС, НП України та Державною прикордонною службою України з державними, приватними виконавцями. Дата-центр рівня TIER III.

5. ПОРЯДОК ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

5.1. Методи навчання

Під час проведення навчальних занять можуть застосовуватися такі методи:

– словесні методи навчання (пояснення, лекція, інструктаж, дискусія, бесіда, коментування алгоритмів роботи з інформаційними системами);

– наочні методи навчання (демонстрація інтерфейсів спеціалізованого програмного забезпечення, візуалізація кіберзагроз, презентація схем OSINT-збору, показ роботи з державними базами даних);

– практичні методи навчання (виконання індивідуальних та групових завдань із застосування сучасних IT-технологій, робота в реальних цифрових середовищах, моделювання операцій зі збору та обробки інформації);

– проблемно-пошукові методи навчання (аналіз кіберінцидентів, розв'язання практичних задач, пов'язаних із загрозами інформаційній безпеці, верифікація даних із відкритих джерел, пошук рішень у ситуаціях оперативно-розшукового характеру);

– активні методи навчання (тренінги, практикуми з кіберрозвідки, виконання вправ з OSINT-інструментами, симуляції кіберзагроз, робота в цифрових платформах).

5.2. Порядок оцінювання результатів навчання

Оцінювання роботи здобувачів/здобувачок вищої освіти здійснюється відповідно до загальноуніверситетської системи оцінювання знань.

Система передбачає:

для денної форми навчання

	Поточний контроль		**Підсумковий контроль**
	Семінарські та практичні заняття	Самостійна робота	Залік/екзамен
	40	20	40
Всього за навчальну дисципліну	**100**		

Для переводу оцінок у бали необхідно користуватися формулою:

$$АР = \frac{\text{сума всіх отриманих оцінок за аудиторну роботу}}{\text{кількість аудиторних занять за семестр за аудиторну роботу}} * 8 =$$

для заочної форми навчання

	Поточний контроль		**Підсумковий контроль**
	Семінарські та практичні заняття	Самостійна робота	Залік/екзамен
	20	40	40
Всього за навчальну дисципліну	**100**		

Для переводу оцінок у бали необхідно користуватися формулою:

$$АР = \frac{\text{сума всіх отриманих оцінок за аудиторну роботу}}{\text{кількість аудиторних занять за семестр за аудиторну роботу}} * 4 =$$

При оцінюванні заліку/екзамену застосовуються такі критерії:

- 36-40 балів – здобувач/здобувачка вищої освіти вільно володіє навчальним матеріалом, надав/надала повну, вичерпну відповідь на поставлене запитання, з посиланням на чинні нормативно-правові акти (або правильно відповів/відповіла на 90-100% тестових завдань). Максимальна кількість балів може бути знижена, якщо під час відповіді здобувач/здобувачка вищої освіти не зробив/зробила посилання на чинні нормативно-правові акти чи допустив/допустила незначні помилки.

- 28-35 балів – здобувач/здобувачка вищої освіти володіє достатнім обсягом навчального матеріалу, надав/надала відповідь на питання але допустив/допустила помилки, що впливають на загальний висновок (або правильно відповів/відповіла на 70-89% тестових завдань);

- 20-27 балів – здобувач/здобувачка вищої освіти володіє навчальним матеріалом поверхово і фрагментарно на репродуктивному рівні або володіє частиною навчального матеріалу чи допускає значні помилки, які приводять до викривлення інформації (або правильно відповів/відповіла на 50-69% тестових завдань);

- 0-19 балів – здобувач/здобувачка вищої освіти не може виконати завдання, не володіє навчальним матеріалом, відмовляється відповідати на запитання або робить принципові помилки, які викривлюють усе рішення (або правильно відповів/відповіла менше ніж на 50% тестових завдань).

Для визначення ступеня засвоєння навчального матеріалу та подальшого його оцінювання на семінарському чи практичному занятті слід врахувати певні рівні знань:

1. **Теоретична відповідь**

– оцінка «5» високий рівень – здобувач/здобувачка вищої освіти вільно володіє навчальним матеріалом, опрацювавши основну та додаткову літературу, аргументовано висловлює свої думки, проявляє творчий підхід до виконання індивідуальних та колективних завдань у самостійній роботі;

– оцінка «4» добрий рівень – здобувач/здобувачка вищої освіти володіє певним обсягом навчального матеріалу, здатний/здатна його аналізувати, але не має достатніх знань для формулювання висновків, поєднання теоретичних знань із практичними прикладами;

– оцінка «3» задовільний рівень – здобувач/здобувачка вищої освіти володіє навчальним матеріалом поверхово і фрагментарно на репродуктивному рівні або володіє частиною навчального матеріалу;

– оцінка «0» незадовільний рівень – здобувач/здобувачка вищої освіти не володіє навчальним матеріалом, відмовляється відповідати на запитання.

2. **Тест:** правильне вирішення тесту оцінюється в 1 бал.
3. **Задача:** вважається вирішеною і оцінюється:

– оцінка «5» високий рівень – здобувач/здобувачка вищої освіти повністю правильно вирішив/вирішила задачу, надав/надала відповіді на всі поставлені в умовах питання, з посиланням на чинні нормативно-правові акти;

– оцінка «4» добрий рівень – здобувач/здобувачка вищої освіти повністю правильно вирішив/вирішила задачу, надав/надала відповіді на всі поставлені в умовах питання, але не зробив посиланням на чинні нормативно-правові акти чи допустив незначні помилки;

– оцінка «3» задовільний рівень – здобувач/здобувачка вищої освіти надав/надала відповіді не на всі поставлені в умовах питання, чи не зробив посиланням на чинні нормативно-правові акти, чи допустив значні помилки;

– оцінка «0» незадовільний рівень – здобувач/здобувачка вищої освіти не правильно вирішив/вирішила задачу.

4. Реферативне повідомлення – оцінюється в 5 балів:

1 бал – належне оформлення реферативного повідомлення;

1 бал – глибока проробка теми (наявність достатньої кількості літературних джерел, наявність ґрунтовних висновків);

1 бал – теоретична обґрунтованість теми, визначення її актуальності, мети, завдань, чітко розроблений науковий апарат;

2 бали – грамотна і аргументована презентація реферату.

Кожну оцінку викладач/викладачка має аргументовано мотивувати.

Шкала оцінювання: національна та ECTS

Сума балів	Оцінка за національною шкалою	Оцінка за шкалою ECTS	Пояснення
90-100	Відмінно	A	Кредит зараховано. Контрольні заходи виконані лише з незначною кількістю помилок
82–89	Добре	B	Кредит зараховано. Контрольні заходи виконані вище середнього рівня з кількома помилками
75–81		C	Кредит зараховано. Контрольні заходи виконані вірно з певною кількістю суттєвих помилок
67–74	Задовільно	D	Кредит зараховано. Контрольні заходи виконані непогано, але зі значною кількістю недоліків
60–66		E	Кредит зараховано. Виконання контрольних заходів задовольняє мінімальним критеріям
35–59	Незадовільно	FX	Кредит не зараховано. Здобувачу/здобувачці вищої освіти надається можливість скласти

			оговорені контрольні заходи для поліпшення підсумкової оцінки
1-34		F	Кредит не зараховано. Здобувач/здобувачка вищої освіти повинен/повинна повторно освоювати навчальний матеріал дисципліни (модуля)

6. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Базові

1. Благута Р.І., Мовчан А.В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: ЛьвДУВС, 2020. 256 с.
2. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій: навчальний курс / [А. Вінаков, В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков, В. Носов, О. Соловйов]. К., 2017. 148 с.
3. Мовчан А. В. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції: навч. посібник / А. В. Мовчан. Львів: ЛьвДУВС, 2017. 244 с.
4. Організація розкриття шахрайств, учинених в кіберпросторі : монографія / Шевчишен А. В., Романов М. Ю., Волобоєв А. О., Лунгол О. М., Габорець О. А., Головкін С. В.; за заг. ред. С. С. Вітвіцького. Київ : ВД «Дакор», 2023. 200 с.

Додаткові

1. Tsurkan O., Haborets O., Lunhol O. Innovative development of technologies in training future law enforcement specialists. *Science and technology today*. 2022. Issue 12(12). P. 96-106.
2. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій: навчальний курс / А. Вінаков, В. Гузій, Д. Девіс, В Дубина, М. Каліжевський, О. Манжай, В. Марков, В. Носов, О. Соловйов. К. 2017. 148 с.
3. Габорець О.А. Значення біометричної автентифікації в сучасних системах безпеки. *Електронний журнал «Наука і техніка сьогодні»*. Серія «Техніка». Київ : Наукові перспективи. 2024. Вип. № 6 (34). С. 799-806.
4. Габорець О.А., Лунгол О.М. Основи кібербезпеки: методичні рекомендації до практичних занять. Мультимедійне видання. Кропивницький: Book Creator, 2023. 76 с.
5. Ковальова О. В., Лунгол О. М., Габорець О. А. Використання сучасних цифрових технологій для проведення OSINT-розвідки правоохоронними органами. *Науково-практичний журнал «Бюлетень з обміну досвідом»* [таємно]. Кропивницький, 2024.
6. Лунгол О.М., Габорець О.А. OSINT-технології в правоохоронній діяльності: навчальний посібник. Мультимедійне видання. Кропивницький: Book Creator, 2023. 107 с.

7. Лунгол О.М., Габорець О.А. Інноваційні методи та цифрові технології в оперативно-розшуковій діяльності. *Актуальні питання у сучасній науці*. 2023. № 11(17). С. 602-615.

8. 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.

9. Навчально-методичні рекомендації щодо застосування програми Proton VPN для анонімного пошуку оперативнозначущої інформації в Інтернеті / К.Ю. Ісмайлов, Сіфоров, В.С. Жогов, О.І. Одеса: Одеський державний університет внутрішніх справ, 2019. 14 с.

10. Навчально-методичні рекомендації щодо пошуку оперативнозначущої інформації в мережі Інтернет К.Ю. Ісмайлов, В.С. Жогов, Л.В. Лефтеров. Одеса: Одеський державний університет внутрішніх справ, 2019. 28 с.

11. Навчально-методичні рекомендації щодо пошуку оперативнозначущої інформації на електронних носіях / К.Ю. Ісмайлов, В.О. Русавський, Л.В. Лефтеров. Одеса: Одеський державний університет внутрішніх справ, 2019. 14 с.

12. Основи оперативно-розшукової діяльності в Україні : посіб. / В. В. Аброськін, С. В. Албул, С. О. Єгоров, та ін.; за заг. ред. В .В. Аброськіна. Одеса : Видавець Букаєв Вадим Вікторович, 2020. 198 с.

13. Пекарський С. П., Габорець О. А. Розробка механізму підбору позаштатного негласного співробітництва із застосуванням OSINT. *Науково-практичний журнал «Бюлетень з обміну досвідом»* [таємно]. Кропивницький, 2024.

Нормативно-правові акти

1. Конституція України. Закон України від 28.06.1996 № 254к/96-ВР. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

2. Кримінальний кодекс України. Закон України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

3. Кримінальний процесуальний кодекс України. Закон України від 13.04.2012 № 4651-VI. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/4651-17#n5329.

4. Про прокуратуру. Закон України від 02.07.2015 № 578-VIII. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/1697-18#Text.

5. Про судоустрій і статус суддів. Закон України від 02.06.2016 № 1402-VIII. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/1402-19#Text.

6. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні:

Наказ МВС України від 07.07.2017 № 575. URL: https://zakon.rada.gov.ua/laws/show/z0937-17#Text

Інформаційні ресурси

1. Освітня платформа «МІА: Освіта». URL: https://osvita.dnuvs.ukr.education/md/course/view.php?id=749
2. Офіційний сайт Міністерства внутрішніх справ України. URL: https://mvs.gov.ua/
3. Офіційний сайт Національної поліції України. URL: https://www.npu.gov.ua/
4. Офіційний сайт Кіберполіції НПУ. URL: https://cyberpolice.gov.ua/
5. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua.