МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра Права (№ 702)

ЗАТВЕРДЖУЮ

Гарант освітньої
програми

_____Н. Є. Філіпенко
(підпис) (ініціали та прізвище)

«30» серпня 2022 р.

СИЛАБУС ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Сучасні доктрини кримінального права

Галузь знань: 08 «Право»

Спеціальність: 081 «Право»

Освітня програма: Право

Рівень вищої освіти: **третій (доктор філософії права з галузі знань право)**

Силабус введено в дію
з 01.09.2022 року

Харків – 2022 р.

Розробник:

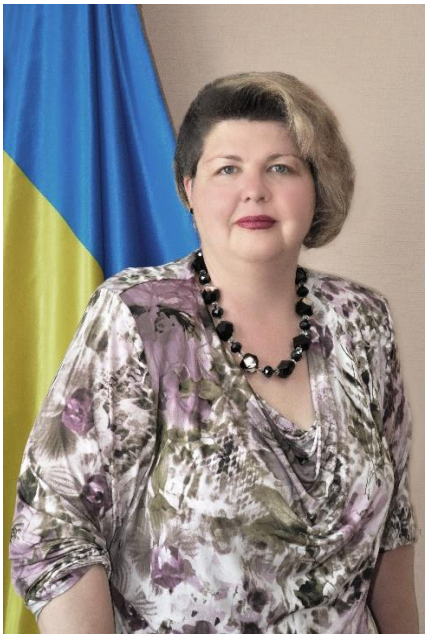
професор закладу вищої освіти кафедри права,
доктор юридичних наук, доцент **Н. Є. Філіпенко**

Силабус навчальної дисципліни розглянуто на засіданні кафедри Права гуманітарно-правового факультету
(назва кафедри)

протокол № 1 від 25. 08. 2022 року

Завідувач кафедри доктор юридичних наук, професор **Г.О. Спіцина**

1. Загальна інформація про викладачів



ПІБ: Філіпенко Наталія Євгенівна
Посада: професор
Наукова ступінь: доктор юридичних наук
Вчене звання: професор
Перелік дисциплін, які викладає:
– «Теорія держави та права»;
– «Кримінологія»;
– «Правове регулювання інформаційної безпеки в Україні»;
– «Актуальні проблеми правового регулювання та організації безпеки суб'єктів господарювання критичної інфраструктури та повітряного транспорту»
«Актуальні проблеми запобігання корупції»;

– «Судові експертизи кримінальному та адміністративному провадженнях за фактами втручань у діяльність об'єктів критичної інфраструктури та повітряного транспорту».

Напрями наукових досліджень:

- сучасні напрями протидії кримінальній кіберпротиправності;
- актуальні напрями забезпечення безпека критичної інфраструктури;
- права людини та їх забезпечення під час здійснення слідчих (розшукових) дій та оперативно-розшукових заходів;
- теоретичні проблеми організації проведення судових експертиз за фактами вчинення кримінальних правопорушень у сфері використання комп'ютерів, автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку;
- стратегія розвитку міжнародного співробітництва судово-експертних установ України із закордонними спеціалістами у попередженні терористичних атак на об'єкти авіакосмічної галузі та критичної інфраструктури;
- юридична відповідальність за порушення законодавства у сфері використання інформаційно-комунікаційних технологій;
- теоретико-правові та організаційно-тактичні питання забезпечення державної політики протидії злочинності на об'єктах аерокосмічної галузі як складової критичної інфраструктури України.

Профайл викладача: Тел.: (066) -305-20-64
E-mail: n.filipenko@khai.edu
https://orcid.org/0000-0001-5524-2259;
https://education.khai.edu/lecturer/filipenko-nataliia-evhensvna
Актуальні оголошення на сторінці дисципліни в системі Mentor

2. Опис навчальної дисципліни

Семестр, в якому викладається дисципліна – 3

Обсяг дисципліни:

Денна: 5 кредитів ЄКТС /150 годин, у тому числі аудиторних – 64 год. (лекції 32 год., семінарські / практичні 32 год.), самостійної роботи здобувачів – 86 год.

Заочна: 5 кредитів ЄКТС /150 годин, у тому числі аудиторних – 12 год. (лекції 06 год., семінарські / практичні 06 год.), самостійної роботи здобувачів – 138 год.

Форма здобуття освіти – *денна/заочна*

Дисципліна – *вибіркова*

Види навчальної діяльності – *лекції, семінарські / практичні заняття*

Види контролю – *іспит*

Мова викладання – *українська*

Пререквізити: Теорія держави і права; Філософія права; Кримінологія; Кримінальне право; Кримінально процесуальне право; Актуальні питання адміністративного права та адміністративного судочинства.

Кореквізити навчальної дисципліни: Сучасні проблеми доказування у кримінальному провадженні; Використання кримінального аналізу щодо протидії кримінальним правопорушенням на об’єктах критичної інфраструктури та повітряного транспорту; Актуальні проблеми правового регулювання та організації безпеки суб’єктів господарювання критичної інфраструктури та повітряного транспорту; Актуальні проблеми запобігання та протидії корупції; Актуальні питання забезпечення прав і свобод людини у кримінальному судочинстві; Судові експертизи у кримінальному та адміністративному провадженнях за фактами втручань у діяльність об’єктів критичної інфраструктури та повітряного транспорту; Військове право.

3. Мета та завдання навчальної дисципліни

Дисципліна «Сучасні доктрини кримінального права» будується на базовій програмі «Кримінальне право» і розрахована на подальше вивчення найбільш актуальних проблем кримінального законодавства України.

Мета дисципліни «Сучасні доктрини кримінального права» полягає у формуванні у майбутніх фахівців умінь та компетентності для забезпечення ефективного управління в сфері кримінальної юстиції з урахуванням останніх досягнень правової науки та міжнародного досвіду, а також в усвідомленні нерозривної єдності успішної професійної діяльності з глибокими теоретичними і практичними знаннями щодо кваліфікації злочинів, здійснення розслідування і правосуддя у кримінальних справах та сучасних тенденцій розвитку кримінального права України.

Дана дисципліна має своїм завданням розгляд новел кримінального законодавства, які відображають особливості кримінального законодавства під час воєнного стану у зв'язку з військовою агресією Російської Федерації проти України, а також інтегрувати необхідні знання та розв’язувати складні

задачі правозастосування у різних сферах професійної діяльності щодо убезпечення об'єктів підприємництва, критичної інфраструктури, повітряного транспорту тощо.

Перелік компетентностей

Інтегральна компетентність: здатність розв'язувати комплексні проблеми в галузі професійної та дослідницько-інноваційної діяльності у галузі права.

Загальні компетентності (ЗК)

Після закінчення цієї програми аспірант буде здатен:

ЗК01. Здатність до абстрактного мислення, аналізу та синтезу

ЗК02. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК03. Здатність працювати в міжнародному контексті.

ЗК04. Здатність розв'язувати комплексні проблеми у сфері Права на основі системного наукового світогляду та загального культурного кругозору із дотриманням принципів професійної етики та академічної доброчесності.

Фахові компетентності спеціальності (СК):

Після закінчення цієї програми аспірант буде здатен:

СК01. Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у галузі права та дотичних до неї (нього, них) міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з галузі права та суміжних галузей.

СК02. Здатність усно і письмово презентувати та обговорювати результати наукових досліджень та/або інноваційних розробок українською та іноземною мовами, глибоке розуміння іншомовних наукових текстів за напрямом досліджень.

СК03. Здатність застосовувати сучасні інформаційні технології, бази даних та інші електронні ресурси, спеціалізоване програмне забезпечення у науковій та навчальній діяльності.

СК04. Здатність здійснювати науково-педагогічну діяльність у вищій освіті.

СК05. Здатність генерувати нові ідеї щодо розвитку теорії та практики у сфері Права, виявляти, ставити та вирішувати проблеми дослідницького характеру, оцінювати та забезпечувати якість виконуваних досліджень.

СК06. Здатність ініціювати, розробляти і реалізовувати комплексні інноваційні проекти в галузі права та дотичні до неї міждисциплінарні проекти, лідерство та безперервний саморозвиток й самовдосконалення під час їх реалізації.

СК07. Здатність до формування системного наукового світогляду, професійної етики досліджень та загального культурного кругозору, а також дотримання правил академічної доброчесності в наукових дослідженнях та науково-педагогічній діяльності.

СК08. Здатність до продукування нових ідей і розв'язання комплексних проблем наукового пізнання, застосування сучасних

методологій, методів та інструментів педагогічної та наукової діяльності в галузі права.

СК09. Здатність до застосування принципів верховенства права, в тому числі, у ситуаціях законодавчої невизначеності та формування концептуального знання щодо форм впливу практики Європейського суду з прав людини на розвиток правової системи та правозастосування в Україні.

Нормативний зміст підготовки доктора філософії, сформований у термінах результатів навчання

РН01. Мати передові концептуальні та методологічні знання з галузі права і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з відповідної галузі, отримання нових знань та/або здійснення інновацій, які відповідають стандартам національного та міжнародного рівнів.

РН02. Вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні правові проблеми державною та іноземною мовами, кваліфіковано відображати результати досліджень у наукових публікаціях у провідних міжнародних наукових виданнях.

РН03. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу з використанням здобутків теорії права та інших правових наук, експериментальних досліджень (опитувань, спостережень, тощо), математичного та/або комп'ютерного моделювання, наявні літературні дані; розв'язання проблем окремої групи правових відносин з урахуванням специфіки аерокосмічної галузі.

РН04. Розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, у тому числі методи та засоби створення інформаційних технологій та програмного забезпечення, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у галузі права та дотичних міждисциплінарних напрямах з урахуванням специфіки аерокосмічної галузі.

РН05. Планувати і виконувати експериментальні та/або теоретичні дослідження з права та дотичних міждисциплінарних напрямів з використанням сучасних інструментів, критично аналізувати результати власних досліджень і результати інших дослідників (зокрема чинного законодавства, практики його застосування, розробки проєктів нормативно-правових актів із обґрунтуванням власної позиції щодо необхідності їх прийняття), у контексті усього комплексу сучасних знань щодо досліджуваної проблеми.

РН06. Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи.

РН07. Розробляти та реалізовувати наукові та/або інноваційні проекти, які дають можливість переосмислити наявне та створити нове цілісне знання та/або професійну практику і розв'язувати значущі наукові та технологічні проблеми права з дотриманням норм академічної етики і врахуванням

соціальних, економічних, екологічних та правових аспектів.

РН08. Розуміти загальні принципи та методи права, а також методологію наукових досліджень, застосувати їх у власних дослідженнях у сфері права та у науково-педагогічній практиці.

РН09. Вивчати, узагальнювати та впроваджувати в навчальний процес інновації, сучасні освітні методи та технології, методику педагогічної діяльності з права.

РН10. Здійснювати пошук та критичний аналіз інформації, концептуалізацію та реалізацію наукових проектів з права.

РН11. Уміти управляти змістом, розкладом, вартістю, якістю, ризиками, людськими ресурсами та комунікаціями науково-технічних проектів з відповідністю вимогам міжнародних стандартів з урахуванням специфіки аерокосмічної галузі.

РН12. Знати сучасні підходи та засоби моделювання досліджуваних об’єктів та процесів управління, в тому числі в аерокосмічній галузі, вдосконалювати їх, розвивати, оптимізувати та приймати рішення, вміти створювати нові.

РН13. Знати філософсько-світоглядні засади, сучасні тенденції, напрямки і закономірності розвитку вітчизняної та світової науки в умовах глобалізації й уміння їх використовувати в науково-дослідній та професійній діяльності у різних галузях, у тому числі аерокосмічній галузі.

РН14. Демонструвати необхідні знання, розуміння сутності, змісту основних правових інститутів і норм фундаментальних галузей права та застосовувати їх у різних правових ситуаціях, виокремлювати юридично значущі факти і формувати обґрунтовані правові висновки.

4. Зміст навчальної дисципліни

МОДУЛЬ 1
СУЧАСНІ ЗАГАЛЬНО-ТЕОРЕТИЧНІ ПРОБЛЕМИ КРИМІНАЛЬНОГО ПРАВА

Тема 1. Сучасні підходи до джерел кримінального права.

Обсяг аудиторного навантаження - 8 год.:

Лекція 4 год: очна-відео-он-лайн лекція: словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.), наочні (презентація теми лекції, ілюстрування, демонстрування, самостійне спостереження).

Семінарське заняття 4 год: Усне опитування, тестування. Завантажена у систему Mentor матеріалу з підготовки до семінарського заняття та оцінка викладачем

Самостійна робота: Опрацювання навчально-методичних матеріалів. Он-лайн консультація. Робота в форумі.

Зміст теми:

Ретроспектива розвитку кримінального права в Україні та світі.

Поняття та види джерел кримінального права. Сучасні підходи до визначення джерел кримінального права України, їх значення для правозастосування.

Кримінальний кодекс України як основне джерело кримінального права.

Кримінально-правове значення Конституції України. Характер зв'язку кримінального права із конституційним правом.

Міжнародні нормативно-правові акти як джерело кримінального права України.

Зв'язок кримінального права з іншими галузями права України.

Кримінально-правове значення рішень Конституційного Суду України.

Практика Європейського суду з прав людини, її вплив на застосування норм кримінального законодавства.

Проблеми застосування постанов Пленуму Верховного суду України та Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ в процесі застосування норм кримінального права.

Кримінально-правове значення практики Верховного Суду України.

Правові позиції Верховного Суду України.

Завдання для СРС:

1. Підготувати на вибір реферат, презентацію, есе чи цільової доповіді за однією з рекомендованих тем.
2. Виконання практичних завдань протягом семестру.
3. Переклад іноземних текстів установлених обсягів з актуальних питань теми.

***Формування компетентностей*:** ІК; ЗК02, ЗК03, ЗК04; СК05, СК06, СК07, СК09.

***Результати навчання*:** РН02-РН14.

Тема 2. Диференціація кримінальної відповідальності.

Обсяг аудиторного навантаження - 4 год:

Лекція 2 год: очна-відео-он-лайн лекція: словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.), наочні (презентація теми лекції, ілюстрування, демонстрування, самостійне спостереження).

Семінарське заняття 2 год: Усне опитування, тестування. Завантажена у систему Mentor матеріалу з підготовки до семінарського заняття та оцінка викладачем

Самостійна робота: опрацювання навчально-методичних матеріалів. Он-лайн консультація. Робота в форумі.

Зміст теми: Кримінальна відповідальність як вид юридичної відповідальності (ст. 2 КК). Поняття кримінальної відповідальності. Поняття диференціації кримінальної відповідальності. Питання про кримінальну відповідальність у галузі кримінального права. Кримінально-правові відносини: їх суб'єкт та зміст. Кримінальні відносини та кримінальна відповідальність. Виникнення і припинення кримінальної відповідальності.

Кримінальна відповідальність та кримінальне покарання. Філософське обґрунтування кримінальної відповідальності особи, яка вчинила злочин. Питання про свободу волі в кримінальному праві. Підстава кримінальної відповідальності. Фактична та юридична підстава кримінальної відповідальності. Питання про юридичну підставу кримінальної відповідальності в науці і законодавстві України. Значення кримінальної відповідальності та її підстав в діяльності підрозділів досудового слідства органів внутрішніх справ.

Філософсько-методологічні основи вчення про диференціацію кримінальної відповідальності. Соціальна обумовленість вчення про диференціацію кримінальної відповідальності. Соціально-правові аспекти і проблеми визначення суспільної небезпечності діяння і її вплив на диференціацію кримінальної відповідальності. Кримінально-політичні основи вчення про диференціацію кримінальної відповідальності.

Традиційна типологія моделей диференціації кримінальної відповідальності в правових системах світу. Сучасна типологія диференціації кримінальної відповідальності в законодавстві держав англосаксонської та романо-германської правових систем.

Поняття, цілі, завдання та принципи диференціації кримінальної відповідальності. Види та засоби диференціації кримінальної відповідальності. Проблеми правового регулювання і застосування обтяжуючих та пом'якшуючих ознак. Санкції статей Особливої частини КК України та диференціація кримінальної відповідальності.

Завдання для СРС:

1. Підготувати на вибір реферат, презентацію, есе чи цільової доповіді за однією з рекомендованих тем.
2. Виконання практичних завдань протягом семестру.
3. Переклад іноземних текстів установлених обсягів з актуальних питань теми.

Формування компетентностей: ІК; ЗК02, ЗК03, ЗК04; СК05, СК06, СК07, СК09.

Результати навчання: РН02, РН08, РН09, РН13-ПРН14.

Тема 3. Окремі питання вчення про кримінальні правопорушення.

Обсяг аудиторного навантаження – 8 год:

Лекція 4 год: очна-відео-он-лайн лекція: словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.), наочні (презентація теми лекції, ілюстрування, демонстрування, самостійне спостереження).

Семінарське заняття 4 год: Усне опитування, тестування. Завантажена у систему Mentor матеріалу з підготовки до семінарського заняття та оцінка викладачем

Самостійна робота: Опрацювання навчально-методичних матеріалів. Он-лайн консультація. Робота в форумі.

Зміст теми:

Застосовувати сучасні підходи до визначення поняття кримінального правопорушення як правової категорії : формальні, матеріальні та формально-матеріальні підходи. Характеристика ознак кримінального проступку і злочину. Категоризація злочинів: поняття, підстави, критерії та значення.

Правова природа обставин, що виключають кримінальність діяння.

Склад кримінального правопорушення.

Закінчене та незакінчене кримінальне правопорушення.

Завдання для СРС:

1. Підготувати на вибір реферат, презентацію, есе чи цільової доповіді за однією з рекомендованих тем.
2. Виконання практичних завдань протягом семестру.
3. Переклад іноземних текстів установлених обсягів з актуальних питань теми.

Формування компетентностей: ІК; ЗК02, ЗК03, ЗК04; СК05, СК06, СК07, СК09.

Результати навчання: РН02, РН08, РН09, РН13-ПРН14.

Тема 4. Актуальні питання визначення особи, яка підлягає кримінальній відповідальності.

Обсяг аудиторного навантаження - 8 год:

Лекція 4 год: очна-відео-он-лайн лекція: словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.), наочні (презентація теми лекції, ілюстрування, демонстрування, самостійне спостереження).

Семінарське заняття 4 год: Усне опитування, тестування. Завантажена у систему Mentor матеріалу з підготовки до семінарського заняття та оцінка викладачем

Самостійна робота: Опрацювання навчально-методичних матеріалів. Он-лайн консультація. Робота в форумі.

Зміст теми:

Поняття та ознаки суб’єкта кримінального правопорушення.

Осудність як обов’язкова ознака суб’єкта кримінального правопорушення. Формула осудності та обмеженої осудності.

Поняття неосудності, юридичний (психологічний) та медичний

(біологічний) критерії неосудності.

Вік з якого може наставати кримінальна відповідальність.

Кримінальна відповідальність за кримінальні правопорушення, вчинені у стані сп'яніння внаслідок вживання алкоголю, наркотичних засобів або інших одурманюючих речовин.

Спеціальний суб'єкт кримінального правопорушення: його поняття та види.

Завдання для СРС:

1. Підготувати на вибір реферат, презентацію, есе чи цільової доповіді за однією з рекомендованих тем.

2. Виконання практичних завдань протягом семестру.

3. Переклад іноземних текстів установлених обсягів з актуальних питань теми.

Формування компетентностей: ІК; ЗК02, ЗК03, ЗК04; СК05, СК06, СК07, СК09.

Результати навчання: РН02, РН08, РН09, РН13-ПРН14.

Тема 5. Загальні проблеми кримінально-правової кваліфікації.

Обсяг аудиторного навантаження - 4 год:

Лекція 2 год: очна-відео-он-лайн лекція: словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.), наочні (презентація теми лекції, ілюстрування, демонстрування, самостійне спостереження).

Семінарське заняття 2 год: Усне опитування, тестування. Завантажена у систему Mentor матеріалу з підготовки до семінарського заняття та оцінка викладачем

Самостійна робота: Опрацювання навчально-методичних матеріалів. Он-лайн консультація. Робота в форумі.

Зміст теми:

Поняття кримінально-правової кваліфікації та її видів.

Зміст та обсяг поняття кримінально-правової кваліфікації.

Процес кримінально-правової кваліфікації та її результат.

Структура кримінально-правової кваліфікації.

Проблемні питання та значення правильної кримінально-правової кваліфікації. ***Завдання для СРС:***

4. Підготувати на вибір реферат, презентацію, есе чи цільової доповіді за однією з рекомендованих тем.

5. Виконання практичних завдань протягом семестру.

6. Переклад іноземних текстів установлених обсягів з актуальних питань теми.

Формування компетентностей: ІК; ЗК02, ЗК03, ЗК04; СК05, СК06, СК07, СК09.

Результати навчання: РН02, РН08, РН09, РН13-ПРН14.

ЗМІСТОВНИЙ МОДУЛЬ 2.
АКТУАЛЬНІ ТЕОРЕТИКО-ПРИКЛАДНІ ПИТАННЯ ОСОБЛИВОЇ ЧАСТИНИ КРИМІНАЛЬНОГО ПРАВА

Тема 6. Актуальні питання кримінально-правової кваліфікації злочинів проти національної безпеки України.

Обсяг аудиторного навантаження – 8 год.:

Лекція 4 год: очна-відео-он-лайн лекція: словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.), наочні (презентація теми лекції, ілюстрування, демонстрування, самостійне спостереження).

Семінарське заняття 4 год: Усне опитування, тестування. Завантажена у систему Mentor матеріалу з підготовки до семінарського заняття та оцінка викладачем

Самостійна робота: Опрацювання навчально- методичних матеріалів. Он-лайн консультація. Робота в форумі.

Зміст теми:

Проблемні питання кримінальної відповідальності за злочини проти національної безпеки.

Дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади.

Посягання на територіальну цілісність і недоторканність України.

Фінансування дій, вчинених з метою насильницької зміни чи повалення конституційного ладу або захоплення державної влади, зміни меж території або державного кордону України.

Державна зрада.

Посягання на життя державного чи громадського діяча.

Завдання для СРС:

1. Підготувати на вибір реферат, презентацію, есе чи цільової доповіді за однією з рекомендованих тем.
2. Виконання практичних завдань протягом семестру.
3. Переклад іноземних текстів установлених обсягів з актуальних питань теми.

Формування компетентностей: ІК; ЗК02, ЗК03, ЗК04; СК05, СК06, СК07, СК09.

Результати навчання: РН02, РН08, РН09, РН13-ПРН14.

Тема № 7. Проблеми застосування кримінального законодавства, яке передбачає відповідальність за кримінальні правопорушення проти життя та здоров'я особи.

Обсяг аудиторного навантаження - 4 год:

Лекція 2 год: очна-відео-он-лайн лекція: словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.), наочні (презентація теми лекції, ілюстрування, демонстрування, самостійне спостереження).

Семінарське заняття 2 год: Усне опитування, тестування. Завантажена у систему Mentor матеріалу з підготовки до семінарського заняття та оцінка викладачем

Самостійна робота: опрацювання навчально-методичних матеріалів. Он-лайн консультація. Робота в форумі.

Зміст теми:

Застосування кримінального законодавства у разі вчинення простого умисного вбивства. Застосування кримінального законодавства у разі вчинення умисного вбивства за наявності обтяжуючих обставин. Застосування кримінального законодавства у разі вчинення вбивства за наявності пом'якшуючих обставин. Застосування кримінального законодавства у разі вбивства, учиненого через необережність. Застосування кримінального законодавства у разі доведення особи до самогубства.

Застосування кримінального законодавства у разі вчинення діянь із ознаками злочинів, що спричиняють шкоду здоров'ю людини. Застосування кримінального законодавства щодо злочинів, які спричиняють шкоду здоров'ю людини, і які вчинюються у сфері охорони життя та здоров'я людини від окремих видів небезпечних інфекційних хвороб. Застосування кримінального законодавства щодо злочинів, що спричиняють шкоду здоров'ю людини, які вчинюються у сфері надання медичних послуг. Застосування кримінального законодавства щодо злочинів, які спричиняють шкоду здоров'ю людини внаслідок залишення особи без допомоги або в результаті неналежного виконання винним своїх обов'язків. Застосування кримінального законодавства щодо злочинів у сфері охорони здоров'я людини, які пов'язані із незаконним розголошенням лікарської таємниці.

Завдання для СРС:

1. Підготувати на вибір реферат, презентацію, есе чи цільової доповіді за однією з рекомендованих тем.
2. Виконання практичних завдань протягом семестру.
3. Переклад іноземних текстів установлених обсягів з актуальних питань теми.

Формування компетентностей: ІК; ЗК02, ЗК03, ЗК04; СК05, СК06, СК07, СК09.

Результати навчання: РН02, РН08, РН09, РН13-ПРН14.

Тема 8. Проблеми застосування кримінального законодавства, яке передбачає відповідальність за кримінальні правопорушення проти громадської безпеки та проти громадського порядку.

Обсяг аудиторного навантаження - 4 год:

Лекція 2 год: очна-відео-он-лайн лекція: словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.), наочні (презентація теми лекції, ілюстрування, демонстрування, самостійне спостереження).

Семінарське заняття 2 год: Усне опитування, тестування. Завантажена у систему Mentor матеріалу з підготовки до семінарського заняття та оцінка викладачем

Самостійна робота: опрацювання навчально-методичних матеріалів. Он-лайн консультація. Робота в форумі.

Зміст теми:

Застосування кримінального законодавства у випадку створення злочинної організації. Специфіка застосування кримінального законодавства в разі вчинення заздалегідь не обіцяного сприяння учасникам злочинних організацій та укриття їх злочинної діяльності. Застосування кримінального

законодавства у випадку бандитизму. Застосування кримінального законодавства у випадку вчинення злочинів терористичної спрямованості. Застосування правил кримінально-правового компромісу в разі вчинення злочинів проти громадської безпеки.

Застосування кримінального законодавства в разі групового порушення громадського порядку. Застосування кримінального законодавства у випадку масових заворушень. Застосування кримінального законодавства в разі вчинення особою закликів до вчинення дій, що загрожують громадському порядку. Застосування кримінального законодавства у випадку вчинення особою діянь із ознаками хуліганства.

Завдання для СРС:

1. Підготувати на вибір реферат, презентацію, есе чи цільової доповіді за однією з рекомендованих тем.
2. Виконання практичних завдань протягом семестру.
3. Переклад іноземних текстів установлених обсягів з актуальних питань теми.

Формування компетентностей: ІК; ЗК02, ЗК03, ЗК04; СК05, СК06, СК07, СК09.

Результати навчання: РН02, РН08, РН09, РН13-ПРН14.

Тема 9. Актуальні питання правозастосовної практики кримінального права України, Європейських країн та Сполучених штатів Америки.

Обсяг аудиторного навантаження – 4 год.:

Лекція 2 год: очна-відео-он-лайн лекція: словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.), наочні (презентація теми лекції, ілюстрування, демонстрування, самостійне спостереження).

Семінарське заняття 2 год: Усне опитування, тестування. Завантажена у систему Mentor матеріалу з підготовки до семінарського заняття та оцінка викладачем

Самостійна робота: опрацювання навчально-методичних матеріалів. Он-лайн консультація. Робота в форумі.

Зміст теми:

Аналіз питань реформування кримінального законодавства України в контексті Європейських стандартів. Питання кримінального законодавства країн традиційно формалізованої романо-германської системи права та проблеми гармонізації з ним кримінального законодавства України.

Сучасні проблеми та межі імплементації норм міжнародного кримінального права в законодавство України.

Завдання для СРС:

1. Підготувати на вибір реферат, презентацію, есе чи цільової доповіді за однією з рекомендованих тем.
2. Виконання практичних завдань протягом семестру.
3. Переклад іноземних текстів установлених обсягів з актуальних питань теми.

***Формування компетентностей*:** ІК; ЗК02, ЗК03, ЗК04; СК05, СК06, СК07, СК09.

***Результати навчання*:** РН02-РН14.

ЗМІСТОВНИЙ МОДУЛЬ 3.
НОВЕЛИ КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ
(в умовах воєнного стану)

Тема 10. Застосування кримінального законодавства, яке передбачає відповідальність за колабораційну діяльність і пособництво державі-агресору.

Обсяг аудиторного навантаження – 4 год.:

Лекція 2 год: очна-відео-он-лайн лекція: словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.), наочні (презентація теми лекції, ілюстрування, демонстрування, самостійне спостереження).

Семінарське заняття 2 год: Усне опитування, тестування. Завантажена у систему Mentor матеріалу з підготовки до семінарського заняття та оцінка викладачем

Самостійна робота: опрацювання навчально-методичних матеріалів. Он-лайн консультація. Робота в форумі.

Зміст теми:

Застосування кримінального законодавства у разі колабораційної діяльності.

Застосування кримінального законодавства у випадку пособництва державі-агресору.

Завдання для СРС:

1. Підготувати на вибір реферат, презентацію, есе чи цільової доповіді за однією з рекомендованих тем.
2. Виконання практичних завдань протягом семестру.
3. Переклад іноземних текстів установлених обсягів з актуальних питань теми.

***Формування компетентностей*:** ІК; ЗК02, ЗК03, ЗК04; СК05, СК06, СК07, СК09.

***Результати навчання*:** РН02-РН14.

Тема 11. Проблеми застосування кримінального законодавства, яке передбачає відповідальність за правопорушення проти миру, безпеки людства та міжнародного правопорядку. Екоцид.

Обсяг аудиторного навантаження – 4 год.:

Лекція 2 год: очна-відео-он-лайн лекція: словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.), наочні (презентація теми лекції, ілюстрування, демонстрування, самостійне спостереження).

Семінарське заняття 2 год: Усне опитування, тестування. Завантажена у систему Mentor матеріалу з підготовки до семінарського заняття та оцінка викладачем

Самостійна робота: опрацювання навчально-методичних матеріалів. Он-лайн консультація. Робота в форумі.

Зміст теми:

Застосування кримінального законодавства у разі правопорушення проти миру, безпеки людства та міжнародного правопорядку.

Поняття екоциду в українському та міжнародному законодавстві. Застосування кримінального законодавства у випадку екоциду.

Завдання для СРС:

1. Підготувати на вибір реферат, презентацію, есе чи цільової доповіді за однією з рекомендованих тем.
2. Виконання практичних завдань протягом семестру.
3. Переклад іноземних текстів установлених обсягів з актуальних питань теми.

***Формування компетентностей*:** ІК; ЗК02, ЗК03, ЗК04; СК05, СК06, СК07, СК09.

***Результати навчання*:** РН02-РН14.

Тема 12. Проблеми застосування кримінального законодавства, яке передбачає відповідальність за кібератаки на об'єкти критичної інфраструктури, життєзабезпечення та повітряного транспорту під час військової агресії проти України.

Обсяг аудиторного навантаження – 4 год.:

Лекція 2 год: очна-відео-он-лайн лекція: словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.), наочні (презентація теми лекції, ілюстрування, демонстрування, самостійне спостереження).

Семінарське заняття 2 год: Усне опитування, тестування. Завантажена у систему Mentor матеріалу з підготовки до семінарського заняття та оцінка викладачем.

Самостійна робота: опрацювання навчально-методичних матеріалів. Он-лайн консультація. Робота в форумі.

Зміст теми:

Теоретико-правова кваліфікація кіберзлочинності.

Застосування кримінального законодавства у разі кібератак на об'єкти критичної інфраструктури та життєзабезпечення.

Застосування кримінального законодавства у випадку кібератак на об'єкти повітряного транспорту під час військової агресії проти України.

Завдання для СРС:

1. Підготувати на вибір реферат, презентацію, есе чи цільової доповіді за однією з рекомендованих тем.
2. Виконання практичних завдань протягом семестру.
3. Переклад іноземних текстів установлених обсягів з актуальних питань теми.

***Формування компетентностей*:** ІК; ЗК02, ЗК03, ЗК04; СК05, СК06, СК07, СК09.

***Результати навчання*:** РН02-РН14.

1. Загальне поняття тероризму та кібертероризму.

В умовах збройної агресії росії проти України особливої уваги набувають питання захисту об'єктів критичної інфраструктури, життєзабезпечення та аерокосмічної галузі від різноманітних кібератак з боку країни-агресора.

Як зазначається у звітах Служби безпеки України, з початку повномасштабного вторгнення росії виявили та нейтралізували понад 120 потужних кібератак на ресурси органів державної влади та військового управління України, а також ІТ-систем об'єктів критичної інфраструктури, операторів зв'язку та ЗМІ. За даними Державної служби спеціального зв'язку та захисту інформації України, за місяць війни вже сталося майже втричі більше хакерських атак різного виду, ніж за аналогічний період минулого року. Найпопулярнішими видами атак залишаються фішингові розсилання, розповсюдження шкідливого програмного забезпечення, DDoS-атаки. Як зазначає голова Держспецзв'язку Юрій Щиголь, атакують передусім державні установи, фінансовий, оборонний сектор, операторів зв'язку, місцеві органи влади, логістичні компанії, медіа. Ми також бачимо численні спроби хакерів зламати ресурси, які збирають інформацію про військові злочини рф в Україні. Держспецзв'язку докладає зусиль для забезпечення їхнього кіберзахисту.

Важливу частку сучасної кримінально-правової політики України складає протидія різноманітним терористичним загрозам. Найбільш небезпечними та руйнівними наслідками визначаються терористичні акти, пов'язані із зазіханням на об'єкти авіакосмічної галузі та критичної інфраструктури, оскільки створюють реальну загрозу стабільного функціонування таких об'єктів, що, в свою чергу, загрожує життю і здоров'ю людей, порушує роботу підприємств, установ і організацій, промислових та господарських об'єктів тощо.

Згідно із положеннями Закону України «Про боротьбу з тероризмом» тероризм – суспільно небезпечна діяльність, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя чи здоров'я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей.

Як кримінальне явище тероризм – це протиправні, кримінально-карані діяння, що виражаються у застосуванні зброї, вчиненні вибуху, підпалу чи інших дій, які створювали небезпеку для життя чи здоров'я людини або заподіяння значної майнової шкоди чи настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, міжнародного ускладнення, або з метою впливу на прийняття рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об'єднаннями громадян, юридичними особами, міжнародними організаціями, або привернення уваги громадськості до певних політичних, релігійних чи інших поглядів винного (терориста), а також погроза вчинення зазначених дій з тією самою метою (ст. 258).

Тероризм включає в себе ідеологію насильства і терористичну діяльність

в різних формах. До терористичної діяльності відносяться планування створення і (або) створення терористичних структур, залучення в терористичну діяльність, фінансування і інше сприяння даної діяльності, пропаганда насильницьких методів досягнення соціально-політичних цілей, а також власне вчинення терористичних актів.

Тероризм – багатооб'єктний злочин, головною метою якого є громадська безпека, так само як посягання на: життя і здоров'я громадян; об'єкти критичної інфраструктури; об'єкти авіаційного транспорту; природне середовище; інформаційне середовище; органи державного управління; державних і громадських діячів тощо.

Експерти-терологи виділяють близько 200 видів сучасної терористичної діяльності. Основними з них є: політичний тероризм, націоналістичний тероризм, релігійний тероризм, технологічний тероризм тощо.

Найбільш небезпечним є технологічний тероризм, що полягає в застосуванні або загрозі застосування зброї масового ураження, у тому числі й ядерної, хімічної і бактеріологічної, радіоактивних та високотоксичних хімічних, біологічних речовин, а також загрозу захоплення об'єктів авіакосмічної галузі та критичної інфраструктури, що становлять підвищену небезпеку для життя і здоров'я людей.

Відзначається зростання небезпеки кібертероризму - дій по дезорганізації автоматизованих інформаційних систем об'єктів авіакосмічної галузі та критичної інфраструктури, що створюють небезпеку загибелі людей, заподіяння значної матеріальної шкоди або настання інших суспільно-небезпечних наслідків. Основною формою кібертероризму є атака на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові інформаційної структури, що дозволяє проникати в систему, що атакується, перехоплювати управління або пригнічувати засоби мережевого інформаційного обміну, здійснювати інші деструктивні дії.

Сьогодні стрімкими темпами розвивається так званий «аерокосмічний тероризм», який набув міжнародного, глобального характеру і є реальною загрозою національній і міжнародній безпеці. Про це свідчить загальна кількість терористистичних актів і число країн, залучених до сфери діяльності терористів. Сучасний характер аерокосмічного тероризму, збільшення його масштабів в світі, викликає велике занепокоєння в світі. За даними Національного центру управління та випробування космічних засобів Державного космічного агентства України, на навколоземних орбітах перебувало 6758 космічних об'єктів. З них штучних супутників Землі - 1948 (діючих - 497), а 53% мали військове призначення. На навколоземних орбітах перебувало вже 8089 космічних об'єктів. З них штучних супутників Землі - 2370 (діючих 668). Головним чином це - космічні апарати військового і подвійного призначення. У космос регулярно виводиться апаратура для дистанційного зондування Землі, а також для здійснення наукових досліджень. Росте число країн-учасниць освоєння космічного простору. Нині вихід у космос мають США, Росія, Китай, Франція, Японія, Великобританія, Італія. Кожна з перелічених держав здатна самостійно реалізувати великі космічні програми. Крім названих країн, мають можливість запускати висотні,

геодезичні, метеорологічні та невеликі космічні апарати такі країни, як Україна, Швеція, Норвегія, Канада, Бразилія, Аргентина, Індонезія.

Під «аерокосмічним тероризмом» можна розуміти терористичні дії, що чиняться з використанням космічних систем наземного або орбітального базування. Сучасний рівень науково-технічного прогресу дозволяє говорити про такі форми прояви космічного тероризму:

- захоплення (знищення) космічних об'єктів, елементів наземних комплексів керування, центрів прийому наукової інформації, контролю космічного простору та інших елементів структур космічних агентств;
- залякування окремих значних організацій, районів, регіонів, країн вибором конкретних цілеспрямованих місць падіння захоплених космічних апаратів;
- залякування терором (діями) із космосу стосовно морських, наземних, повітряних об'єктів тощо.

Масштаби і наслідки реалізації космічних загроз можуть бути прирівняні до застосування зброї масового ураження, а відтак, становити реальну загрозу для цивілізації. При цьому варто враховувати і те, що нівелюється межа між звичайними бойовими діями в космосі та захистом (контртерористичними операціями) від терористів.

Дотепер не було виявлено випадків «аерокосмічного тероризму». Водночас, вказаний вид тероризму потребує докладного наукового аналізу. Наукова література і розробки у даному напрямку практично відсутні. І буде непростиме повертатися до цього питання після здійснення терористичних актів.

Аналіз вітчизняних та закордонних джерел дає змогу віднести до основних сучасних тенденцій розвитку тероризму наступне:

- консолідація локальних терористичних угруповань та їх стрімка інтернаціоналізація;
- посилення взаємного впливу різноманітних внутрішніх і зовнішніх соціальних, політичних, економічних та інших факторів, що сприяють виникненню і поширенню тероризму;
- підвищення рівня організованості терористичної діяльності, створення великих терористичних формувань з розвиненою інфраструктурою;
- посилення взаємозв'язку тероризму та організованої злочинності;
- зростання фінансового та матеріально-технічного забезпечення терористичних структур;
- прагнення суб'єктів тероризму опанувати засобами масового ураження людей;
- спроби використання тероризму як інструменту втручання у внутрішні справи держав;
- розробка і вдосконалення нових форм і методів тероризму, спрямованих на розширення масштабів наслідків терористичних акцій і збільшення кількості жертв тощо.

Ступінь небезпеки загроз терористичних актів обумовлюється рівнем вдосконалення форм, методів, сил і засобів терористичної діяльності, тактики її здійснення, а також ефективністю антитерористичних заходів національних

та міжнародних систем протидії тероризму.

Метою протидії тероризму в Україні є захист особистості, суспільства і держави від терористичних загроз та запобігання таким проявам.

Основними завданнями в досягненні зазначених цілей є:

- виявлення та усунення факторів, що сприяють виникненню і поширенню тероризму;
- виявлення, попередження і припинення дій осіб і організацій, спрямованих на підготовку і вчинення злочинів терористичного характеру і (або) надання сприяння такій діяльності;
- залучення до відповідальності суб'єктів терористичної діяльності відповідно до чинного законодавства нашої держави та міжнародної спільноти;
- припинення спроб перенесення на територію України діяльності міжнародних терористичних організацій, залучення до цього процесу потенціалу міжнародної антитерористичної коаліції;
- постійне вдосконалення загальнодержавній системі протидії тероризму, підтримання в стані готовності до використання сил і засобів, призначених для виявлення, попередження, припинення терористичних актів і мінімізації їх наслідків;
- забезпечення дієвого антитерористичного захисту об’єктів авіакосмічної галузі та критичної інфраструктури, життєзабезпечення та місць масового перебування людей;
- протидія поширенню ідеології тероризму, здійснення активних інформаційно-пропагандистських заходів антитерористичної спрямованості.

Загальнодержавна система протидії тероризму являє собою сукупність організаційних структур (суб'єктів протидії тероризму), які в рамках повноважень, встановлених законами і виданими на їх основі нормативно-правовими актами, здійснюють діяльність з протидії терористичним загрозам, розробляють і реалізують комплекс заходів з профілактики терористичних загроз, виявлення та припинення терористичної діяльності, мінімізації та ліквідації можливих наслідків терористичних актів.

Суб'єктами протидії тероризму є уповноважені органи державної влади та місцевого самоврядування, до компетенції яких входить проведення антитерористичних заходів, недержавні організації та об'єднання, а також окремі громадяни, які надають сприяння у здійсненні заходів в цій сфері.

2. Протидія кібератакам.

На жаль, мусимо зазначити про певні недоліки у протидії таким загрозам. Адже рівень захисту внутрішньої критичної інфраструктури та авіації не завжди відповідає сучасним світовим вимогам безпеки. Дуже часто це відбувається через корупцію або недоліки в організаційно-господарській діяльності на критичних інфраструктурних та авіаційних об’єктах.

У цьому зв’язку якісна, своєчасна та ефективна протидія кримінальним правопорушенням, пов’язаним з використанням електронних засобів, у даний час не може бути здійснена без використання спеціальних знань в області новітніх інформаційних технологій.

Згідно із положеннями Постанови Кабінету міністрів України «Про

затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», терміни вживаються у такому значенні:

критичні бізнес/операційні процеси об'єкта критичної інфраструктури - процеси організації функціонування об'єктів критичної інфраструктури, реалізація загроз на які призводить до виведення з ладу або порушення функціонування самого об'єкта критичної інфраструктури та відповідно справляє негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіює майнову шкоду та/або становить загрозу для суспільства, життя і здоров'я людей; для організації функціонування цього процесу можуть використовуватися декілька інформаційно-комунікаційних систем;

система інформаційної безпеки - сукупність організаційних та технічних заходів, а також засобів і методів захисту інформації, які впроваджуються на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури з метою запобігання кіберінцидентам, виявлення та захисту від кібератак, порушення конфіденційності, цілісності та доступності інформаційних ресурсів, що обробляються (передаються, зберігаються) на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури, запобігання порушенню режиму функціонування та/або недоступності служб (функцій) об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, порушенню функціонування компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури; забезпечення спостережності за діями користувачів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та функціонуванням засобів захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

політика інформаційної безпеки - політика, що визначає підхід підприємства, установи та організації, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури, до інформаційної безпеки, вимоги, правила, обмеження, рекомендації, що регламентують порядок дотримання та забезпечення інформаційної безпеки.

Інші терміни вживаються у значенні, наведеному в Законах України "Про основні засади забезпечення кібербезпеки України", "Про захист інформації в інформаційно-комунікаційних системах", Правилах забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 р. № 373 (Офіційний вісник України, 2006 р., № 13, ст. 878).

3. Кіберзахист об'єкта критичної інфраструктури забезпечується шляхом впровадження на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю.

4. Кіберзахист об'єкта критичної інфраструктури є складовою частиною робіт із створення (модернізації) та експлуатації об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури. Заходи з

кіберзахисту передбачаються та впроваджуються на всіх стадіях життєвого циклу об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

5. Кіберзахист об’єкта критичної інфраструктури забезпечується власником та/або керівником об’єкта критичної інфраструктури відповідно до цих Загальних вимог та законодавства в сфері захисту інформації та кібербезпеки.

6. У випадку, якщо на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, положення цих Загальних вимог повинні бути враховані під час створення (модернізації) на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури комплексної системи захисту інформації, а їх відповідність перевіряється під час її державної експертизи в сфері технічного захисту інформації.

Створення комплексної системи захисту інформації об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та її державна експертиза здійснюються відповідно до вимог законодавства в сфері захисту інформації та охорони державної таємниці.

7. У випадку, якщо на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури не обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, положення цих Загальних вимог враховуються під час створення (модернізації) системи інформаційної безпеки об’єкта критичної інфраструктури. Виконання Загальних вимог перевіряється під час незалежного аудиту інформаційної безпеки на об’єкті критичної інфраструктури.

Створення системи інформаційної безпеки об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури здійснюється відповідно до вимог технічного завдання на створення системи інформаційної безпеки.

Технічне завдання формується за результатами оцінки ризиків, які зазначаються в звіті за результатами оцінки ризиків на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури. Методичною основою для оцінки ризиків на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури є стандарт ДСТУ ISO/IEC 27005.

Власник та/або керівник об’єкта критичної інфраструктури організовує проведення незалежного аудиту інформаційної безпеки на об’єкті критичної інфраструктури згідно з вимогами законодавства в сфері захисту інформації та кібербезпеки.

8. Власник та/або керівник об’єкта критичної інфраструктури організовує невідкладне інформування урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA (у разі наявності - галузевої команди реагування на комп’ютерні надзвичайні події), а також функціонального підрозділу контррозвідувального захисту інтересів держави у сфері

інформаційної безпеки Центрального управління СБУ (Ситуаційний центр забезпечення кібербезпеки СБУ) або відповідного підрозділу регіонального органу СБУ про кіберінциденти та кібератаки, які стосуються його об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури.

9. Державні органи отримують доступ до Інтернету через систему захищеного доступу державних органів до Інтернету Державного центру кіберзахисту, через постачальників електронних комунікаційних мереж та/або послуг, які мають захищені вузли доступу до глобальних мереж передачі даних із створеними комплексними системами захисту інформації з підтвердженою відповідністю, або через власні системи захищеного доступу до Інтернету із створеними комплексними системами захисту інформації з підтвердженою відповідністю. Ця вимога не поширюється на інформаційно-комунікаційні системи закордонних дипломатичних установ України.

10. Власник та/або керівник об'єкта критичної інфраструктури з метою усунення можливих наслідків кіберінцидентів та кібератак забезпечує створення резервних копій інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та критичних бізнес/операційних процесів об'єкта критичної інфраструктури для оперативного їх відновлення у разі пошкодження або знищення.

Державні органи для збереження резервних копій своїх інформаційних ресурсів та їх оперативного відновлення використовують основний та резервний захищений дата-центр збереження державних електронних інформаційних ресурсів Державного центру кіберзахисту.

11. Державні органи з метою здійснення захищеного інформаційного обміну, зберігання резервних копій інформаційних ресурсів, підключення до системи захищеного доступу державних органів до Інтернету Державного центру кіберзахисту використовують ресурси Національної телекомунікаційної мережі.

12. Організаційні та технічні заходи з кіберзахисту, які впроваджуються на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури, повинні забезпечувати:

-формування на об'єкті критичної інфраструктури загальної політики інформаційної безпеки;

-управління доступом користувачів та адміністраторів до об'єктів захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

-ідентифікацію та автентифікацію користувачів та адміністраторів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

-реєстрацію подій компонентами об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та їх періодичний аудит;

-мережевий захист компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

-доступність та відмовостійкість компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

-визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

-визначення умов використання програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

-визначення умов розміщення компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

Перелік базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури, які повинні бути впроваджені під час створення комплексної системи захисту інформації (системи інформаційної безпеки) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, наведено у додатку.

Перелік базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури може бути доповнено відповідно до технології обробки інформації на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури, особливостей функціонування та програмно-апаратного складу об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, складу інформаційних ресурсів та компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, які підлягають захисту, тощо.

Під час доповнення переліку базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури для кожної загрози об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури передбачаються захід або комплекс заходів, що забезпечують блокування однієї чи декількох загроз або знижують ризик її реалізації, та враховуються умови функціонування об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури. У разі коли перелік мінімальних заходів не дає можливості забезпечити блокування (нейтралізацію) усіх загроз об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, повинні бути визначені додаткові заходи, які ці загрози блокують.

Формування додаткових заходів із забезпечення кіберзахисту об’єктів критичної інфраструктури розробник комплексної системи захисту інформації (системи інформаційної безпеки) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури здійснює з урахуванням вимог нормативних документів у сфері технічного захисту інформації, міжнародних стандартів з питань інформаційної безпеки.

13. У разі відсутності можливості виконання окремих вимог із забезпечення кіберзахисту, наведених у додатку, і/або неможливості їх застосування до окремих об’єктів захисту чи користувачів та адміністраторів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, у тому числі внаслідок їх можливого негативного впливу на функціонування об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, або неможливості їх здійснення на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури через особливості функціонування, або відсутності складу компонентів

об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні бути розроблені і впроваджені компенсуючі заходи, що забезпечують блокування (нейтралізацію) загроз об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, або обґрунтовано виключені окремі вимоги з переліку базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури.

Власник та/або керівник об’єкта критичної інфраструктури у ході розроблення організаційних і технічних заходів щодо забезпечення кіберзахисту об’єкта критичної інфраструктури обґрунтовує застосування компенсуючих заходів або виключення окремих вимог з переліку базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури. При цьому під час проведення незалежного аудиту інформаційної безпеки об’єкта критичної інфраструктури або державної експертизи комплексної системи захисту інформації об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури має бути оцінена достатність і адекватність компенсуючих заходів, які застосовані для блокування (нейтралізації) загроз об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та зменшення ризиків об’єкта критичної інфраструктури, або обґрунтованість виключення окремих вимог з переліку базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури.

Рішення з обґрунтуванням щодо впровадження компенсуючих заходів або виключення окремих вимог з переліку базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури оформлюється окремим рішенням за підписом власника та/або керівника об’єкта критичної інфраструктури.

14. Міністерства та інші центральні органи виконавчої влади можуть розробляти конкретизовані вимоги з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування об’єктів критичної інфраструктури, які відносяться до сфери їх управління. Такі вимоги з кіберзахисту погоджуються з Адміністрацією Держспецзв’язку.

СБУ має право подавати міністерствам та іншим центральним органам виконавчої влади обов’язкові для розгляду пропозиції щодо таких вимог з кіберзахисту.

ПЕРЕЛІК базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури:

Формування на об’єкті критичної інфраструктури загальної політики інформаційної безпеки

1. Об’єкт критичної інфраструктури повинен мати у своєму складі підрозділ або посадову особу з інформаційної безпеки, що відповідають за політику інформаційної безпеки, прийняту на об’єкті критичної інфраструктури, та контроль за її дотриманням. Під час визначення відповідальних за інформаційну безпеку перевага повинна надаватися особам, які мають фахову освіту та досвід роботи у сфері технічного захисту інформації або інформаційної безпеки.

Підрозділ або посадова особа з інформаційної безпеки повинні бути підпорядковані безпосередньо керівнику об’єкта критичної інфраструктури.

Функції підрозділу або посадової особи з інформаційної безпеки можуть бути покладені на службу захисту інформації підприємства, установи, організації.

2. На об’єкті критичної інфраструктури повинні бути визначені права та обов’язки всіх категорій користувачів та адміністраторів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, обов’язки адміністраторів з обслуговування компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури (далі - компоненти об’єкта) та забезпечення її інформаційної безпеки, які оформлюються окремим рішенням за підписом власника та/або керівника об’єкта критичної інфраструктури.

На об’єкті критичної інфраструктури повинні бути призначені відповідальні за функціонування та інформаційну безпеку критичних бізнес/операційних процесів з числа керівників об’єкта критичної інфраструктури, працівники яких забезпечують функціонування цих критичних процесів.

3. На об’єкті критичної інфраструктури повинен бути визначений перелік інформаційних, програмних та апаратних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, рівень їх критичності для об’єкта критичної інфраструктури та/або функціонування об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та можливий рівень наслідків у випадку порушення конфіденційності, цілісності та доступності інформації, недоступності служб (функцій) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, порушення функціонування компонентів об’єкта.

4. На об’єкті критичної інфраструктури повинно бути затверджено політику управління ризиками інформаційної безпеки і методику їх оцінювання та оброблення. Методичною основою для вибору методики є стандарт ДСТУ ISO/IEC 27005.

5. Власник/керівник об’єкта критичної інфраструктури зобов’язаний не рідше одного разу на рік організовувати та проводити обстеження своїх об’єктів критичної інформаційної інфраструктури об’єкта критичної інфраструктури з метою оновлення даних щодо програмно-апаратного складу об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, технології обробки інформації на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури, переліку критичних інформаційних ресурсів та компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, які підлягають захисту, тощо. Методичною основою для проведення обстеження об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури є вимоги нормативного документа системи технічного захисту інформації 3.7-003-05 “Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі”.

Якщо за результатами обстеження об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури виявлено, що на об’єкті

критичної інформаційної інфраструктури об’єкта критичної інфраструктури змінено технологію обробки інформації, впроваджено нові програмні або апаратні компоненти, змінено перелік критичних інформаційних ресурсів та компонентів об’єкта, які підлягають захисту, тощо, здійснюється перегляд переліку загроз об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, ризиків інформаційної безпеки та рівня прийнятного ризику.

У випадку виявлення нових загроз та/або ризиків здійснюється оновлення технічного завдання на створення комплексної системи захисту інформації (системи інформаційної безпеки) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, іншої документації та впровадження оновлених вимог на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

6. Власник/керівник об’єкта критичної інфраструктури зобов’язаний забезпечити розроблення та підтримання в актуальному стані технічної, проектної та іншої документації на комплексну систему захисту інформації (систему інформаційної безпеки) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури (в захищеній від модифікації формі, зокрема електронній) з обов’язковим описом реалізованих у системі організаційних та технічних заходів безпеки інформації.

Мінімальний перелік документації об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури визначається в технічному завданні на створення комплексної системи захисту інформації (системи інформаційної безпеки) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

Програмні та апаратні компоненти об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні бути налаштовані відповідно до затвердженої політики інформаційної безпеки та технічної, проектної та іншої документації на комплексну систему захисту інформації (систему інформаційної безпеки) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

В інтересах національної безпеки інформація щодо програмно-апаратного складу об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, налаштування та конфігураційна інформація програмних та апаратних компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, інформація про параметри та режими їх функціонування, журнали реєстрації подій (логи) та дані аудиту компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, інформація про облікові записи користувачів, їх атрибути та права доступу, об’єкти захисту та їх атрибути доступу, інша інформація, яка розкриває параметри та особливості функціонування компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, є інформацією з обмеженим доступом. Ступінь обмеження доступу до цієї інформації визначається відповідно до закону.

7. На об’єкті критичної інфраструктури необхідно затвердити політику інформаційної безпеки, яка визначає:

-мету та основні принципи забезпечення захисту інформаційних ресурсів, критичних бізнес/операційних процесів тощо на об’єкті критичної інфраструктури;

-опис критичних бізнес/операційних процесів, який повинен включати схему кожного критичного бізнес-процесу з описом компонентів та користувачів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, які задіяні в цьому процесі;

-вимоги до порядку визначення, надання, зміни та скасування прав доступу користувачів та адміністраторів до служб (функцій), інформації та компонентів об’єкта та порядок контролю (аудиту) використання прав доступу користувачами та адміністраторами. При цьому необхідно дотримуватися принципу надання необхідних та мінімально достатніх повноважень користувачам та адміністраторам відповідно до їх службових обов’язків;

-політику фізичної безпеки та захисту об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури від навколишнього природного середовища;

-вимоги до забезпечення інформаційної безпеки під час взаємодії з постачальниками;

-політику управління обліковими записами в програмному та апаратному забезпеченні об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури. Політика повинна визначати порядок створення, блокування та зупинення облікових записів користувачів та адміністраторів в компонентах об’єкта;

-вимоги до порядку формування, надання, скасування та контролю (аудиту) за використанням автентифікаційних атрибутів користувачів та адміністраторів, у тому числі зовнішніх носіїв автентифікаційних даних, для доступу до служб (функцій), інформації та компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури. Повинні бути визначені також вимоги до складності паролів, періодичності їх зміни, блокування роботи користувача за певної кількості спроб підбору пароля, порядок поводження із зовнішніми носіями автентифікаційних даних тощо;

-політику забезпечення безперебійної роботи об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, зокрема порядок резервування даних та компонентів об’єкта, зберігання резервних копій даних, відновлення даних з резервних копій та заміни компонентів об’єкта у випадку виходу їх з ладу тощо;

-порядок дій персоналу об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури у випадках відмов або збоїв об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури в цілому або окремих його компонентів;

-порядок використання змінних (зовнішніх) пристроїв та носіїв інформації на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

-політику мережевого захисту, зокрема щодо сегментації мережі об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури,

захисту від вірусів, зловмисного коду, шкідливого програмного забезпечення, встановлення та налаштування засобів мережевого захисту тощо;

-політику проведення модернізації (оновлення) компонентів об'єкта, внесення змін до складу та в налаштування компонентів об'єкта. Повинні бути визначені відповідальні особи, які мають право проводити ці робити, а також порядок дотримання політики безпеки, яка прийнята на об'єкті критичної інфраструктури, під час проведення таких робіт;

-опис критичних бізнес/операційних процесів, який повинен включати схему кожного критичного бізнес-процесу з описом компонентів та користувачів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, які задіяні в цьому процесі;

-політику управління оновленнями (порядок отримання, перевірки, розповсюдження та застосування оновлень програмного забезпечення компонентів об'єкта);

-політику реєстрації та аудиту подій, що реєструються компонентами об'єкта. Політика повинна містити перелік подій, які реєструються кожним компонентом об'єкта, параметри ведення журналів (логів) реєстрації подій та їх архівування, порядок та періодичність аудиту журналів (логів) реєстрації подій адміністраторами об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури на предмет виявлення ознак кібератак або кіберінцидентів;

-політику управління інцидентами кібербезпеки, яка повинна містити перелік подій, що кваліфікуються як кіберінциденти, описи дій користувачів та адміністраторів у разі їх виникнення, порядок інформування посадових осіб об'єкта критичної інфраструктури, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA (у разі наявності - галузевої команди реагування на комп'ютерні надзвичайні події);

-політику використання електронної пошти користувачами об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

-політику проведення внутрішнього аудиту інформаційної безпеки об'єкта критичної інфраструктури.

Політика інформаційної безпеки може затверджуватися окремими рішеннями за підписом власника та/або керівника об'єкта критичної інфраструктури. Повинен бути встановлений порядок внесення змін до таких документів.

8. Вимоги затвердженої на об'єкті критичної інфраструктури політики інформаційної безпеки повинні бути доведені під підпис або в інший спосіб до всіх його працівників. На об'єкті критичної інфраструктури повинна бути визначена відповідальність його співробітників за порушення встановленої політики інформаційної безпеки.

9. Власник/керівник об'єкта критичної інфраструктури повинен впровадити програми підвищення обізнаності/навчання працівників з питань інформаційної безпеки та забезпечити щорічний контроль рівня обізнаності.

10. У підрозділі або посадової особи з інформаційної безпеки об'єкта критичної інфраструктури повинен бути створений та підтримуватися в актуальному стані перелік програмного та апаратного забезпечення, що

використовується на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури в захищеній від модифікації формі, зокрема електронній.

Управління доступом користувачів та адміністраторів до об’єктів захисту об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури

11. Механізм розподілу прав доступу до об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинен:

-охоплювати всі інформаційні ресурси об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури (інформацію, яка зберігається та обробляється на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури, технологічну інформацію програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, журнали реєстрації подій тощо);

-визначати права на виконання операцій для всіх користувачів та адміністраторів (за необхідності також активних процесів) над інформаційними ресурсами об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури (читання, модифікація, створення, видалення тощо);

-за необхідності також визначати права доступу користувачів та адміністраторів до служб (функцій) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

12. За можливості реалізації на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинна надаватися перевага централізованому поширенню інформації щодо налаштувань прав та атрибутів доступу, параметрів реєстрації подій, інших параметрів безпеки та системних налаштувань компонентів об’єкта.

Ідентифікація та автентифікація користувачів та адміністраторів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури

13. Користувачі та адміністратори об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури (за необхідності також активні процеси) повинні отримувати доступ до служб (функцій), інформації та компонентів об’єкта в межах визначених їм прав доступу тільки після успішного проходження процедури автентифікації на підставі унікального персоніфікованого ідентифікатора (імені) користувача і деякої інформації, що вводиться користувачем (пароль), та/або фізичного ідентифікатора, що надається користувачем (ключ, сертифікат, токен тощо).

14. Засоби об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні надавати можливість ідентифікації кожної операції користувача та адміністратора на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури та їх протоколювання в журналах реєстрації подій.

15. Для надання доступу до служб (функцій) та інформації об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинна використовуватися багатофакторна автентифікація користувачів та

адміністраторів. Допускається використання двофакторної автентифікації тільки в тому програмному забезпеченні компонентів об’єкта, яке не підтримує багатофакторну автентифікацію.

16. На об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні бути заблоковані або змінені облікові записи адміністраторів та їх паролів, встановлені за замовчуванням, в усіх компонентах об’єкта. Забороняється використовувати облікові записи та паролі за замовчуванням в програмному та апаратному забезпеченні об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

17. На об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні бути видалені або заблоковані неперсоналізовані і гостьові облікові записи користувачів і адміністраторів та використовуватися виключно персоналізовані облікові записи користувачів і адміністраторів в усіх компонентах об’єкта. Під час звільнення з посади працівника його обліковий запис повинен бути негайно заблокований або видалений в усіх компонентах об’єкта.

18. Обладнання, яке підключається до системи управління технологічними процесами об’єкта критичної інфраструктури, повинно бути ідентифіковане (наприклад, за IP-адресою, MAC-адресою тощо), а також повинні бути вжиті заходи, які унеможливлюють роботу обладнання в мережі без відповідної ідентифікації.

Реєстрація подій компонентами об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та їх періодичний аудит

19. Компоненти об’єкта повинні забезпечити реєстрацію, збереження в електронних журналах та захист від модифікації інформації щонайменше про такі події:

-доступ та дії з інформацією, яка зберігається та обробляється на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури, а також з налаштуваннями програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, журналами реєстрації подій тощо (читання, модифікація, створення, видалення тощо);

-реєстрація подій, пов’язаних із встановленням та зміною прав доступу до служб (функцій), інформації та компонентів об’єкта;

-вхід/вихід користувачів та адміністраторів в/із компонентів об’єкта;

-невдалі спроби входу користувачів та адміністраторів на об’єкт критичної інформаційної інфраструктури об’єкта критичної інфраструктури та перевищення граничної кількості спроб введення пароля;

-реєстрація, видалення (блокування) облікових записів користувачів та адміністраторів у компонентах об’єкта;

-зміна пароля користувача в компонентах об’єкта;

-реєстрація подій, пов’язаних із зміною конфігураційних налаштувань компонентів об’єкта;

-спроби здійснення несанкціонованого доступу до ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

-негативні результати перевірок цілісності даних та програмного і

апаратного забезпечення об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

-всі дії адміністратора з журналами реєстрації подій компонентів об’єкта та налаштування ним параметрів реєстрації.

Повний перелік подій, які реєструються компонентами об’єкта, визначається виходячи із встановленої на об’єкті критичної інфраструктури політики інформаційної безпеки.

20. Журнали реєстрації подій компонентів об’єкта повинні містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнали реєстрації повинні містити інформацію, достатню для встановлення користувача, процесу і мережевого об’єкта, що мали відношення до кожної зареєстрованої події.

21. Має бути забезпечений захист журналів реєстрації подій компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури від несанкціонованого доступу, модифікації або руйнування. Електронні журнали реєстрації подій повинні зберігатися не менше ніж один рік з дати реєстрації останньої події.

22. На об’єкті критичної інфраструктури повинно бути впроваджено систему збору та аналізу журналів реєстрації подій програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури. Така система повинна мати можливість встановлення фільтрів, які дозволяють робити вибірку і аналіз журналів та подій за різними критеріями та за потреби мати інтерфейси обміну з іншими системами.

Оброблення журналів реєстрації подій не повинно впливати на функціонування критичних бізнес/операційних процесів об’єкта критичної інфраструктури.

23. На об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинна бути забезпечена можливість роботи з архівними журналами реєстрації подій за попередні періоди шляхом завантаження журналів на об’єкт критичної інформаційної інфраструктури об’єкта критичної інфраструктури із зовнішнього джерела. При цьому дані, що завантажуються, повинні тільки доповнювати існуючі журнали, але не затирати і не змінювати інформації, що вже зберігається в них.

Архівні журнали реєстрації подій зберігаються на фізично відокремленому компоненті об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури або окремому носії даних не менше року з дати їх утворення.

Забезпечення мережевого захисту компонентів та інформаційних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури

24. На об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні використовуватися засоби захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів. Повинно бути забезпечене централізоване управління засобами захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів.

25. Доступ адміністраторам до компонентів об’єкта повинен надаватися виключно з IP-адрес (робочих станцій), які визначені для адміністрування об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

26. У разі неможливості фізичного розділення зовнішньої мережі та об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури на межі (периметрі) між зовнішніми мережами, іншими інформаційно-комунікаційними системами, що обслуговують об’єкт критичної інфраструктури, та об’єктом критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні бути встановлені засоби мережевого захисту, що виконують щонайменше такі функції захисту:

-захист від атак “нульового дня” (вразливості програмного забезпечення, які ще невідомі користувачам чи розробникам програмного забезпечення та проти яких ще не розроблені механізми захисту), виявлення зловмисного коду та шкідливого програмного забезпечення;

-фільтрація трафіку та розмежування доступу між мережею об’єкта критичної інфраструктури та зовнішніми мережами за критеріями дозволених та заборонених служб, протоколів, портів, мережевих адрес, мережевих з’єднань, небажаних веб-сайтів тощо. Блокування трафіку та з’єднань, які не відповідають визначеним критеріям;

-фільтрація та аналіз трафіку за визначеними відповідно до політики інформаційної безпеки критеріями;

-моніторинг трафіку на наявність зловмисного коду, вірусів зловмисного програмного забезпечення та за іншими визначеними відповідно до політики інформаційної безпеки критеріями;

-виявлення та запобігання атакам та вторгненням, спрямованим на програмні та апаратні компоненти та інформацію об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

-захист від атак типу “відмова в обслуговуванні”;

-захист від несанкціонованого доступу через Інтернет;

-балансування навантаження;

-маскування структури і мережевих адрес мережі;

-завершення з’єднання з вузлом у разі атаки;

-здійснення реєстрації подій, що мають відношення до безпеки.

Для захисту об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні використовуватися програмно-апаратні засоби, потужність яких визначається виходячи із потужності трафіку, який передбачається в мережі, з урахуванням його потенційного збільшення.

27. На об’єкті критичної інфраструктури необхідно здійснити розподіл об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури на фізичному та/або логічному рівні (сегментацію мережі) і обмежити доступ між сегментами мережі з використанням міжмережевих екранів або аналогічних за функціональністю засобів мережевого захисту.

28. Реалізована архітектура об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинна надавати можливість розподілу мережі щонайменше на такі частини / зони:

-зовнішня зона (DMZ-zone): зона із зовнішніми діапазонами адресації мережі для розміщення зовнішніх (публічних) інформаційних ресурсів та сервісів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

-зона прикладних застосувань об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури (APP-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення серверів застосувань, доступна для виконання функціональних запитів користувачів інформаційних сервісів;

-зона сховищ даних об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури (DB-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення баз даних, для доступу за запитами прикладних застосувань зони (APP-zone);

-зона прикладних застосувань системи безпеки (Security-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для розміщення сервісів та служб захисту інформації;

-тестова зона (Test-zone): захищена внутрішня зона із внутрішньою адресацією, призначена для тестування нових компонентів та/або оновлень програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, перед тим як впровадити їх в промислову експлуатацію на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

29. Сервери та обладнання, що забезпечують функціонування сервісів та віддалений доступ клієнтів / користувачів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури із зовнішніх мереж, повинні бути розміщені в зовнішній зоні об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури. З’єднання серверів та обладнання, які розміщені в зовнішній зоні, із серверами та обладнанням внутрішньої мережі об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні захищатися міжмережевим екраном.

30. Робочі станції, з яких виконуються дії щодо адміністрування програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, а також серверні частини засобів захисту інформації повинні бути розміщені в зоні прикладних застосувань системи безпеки (Security-zone) мережі, захищеної за допомогою міжмережевого екрана.

31. Сегмент інформаційної інфраструктури об’єкта критичної інфраструктури, в якому перебуває система керування технологічними процесами, повинен бути відокремленим від інших систем об’єкта критичної інфраструктури. У випадку логічного відокремлення на межі сегмента повинен бути встановлений міжмережевий екран.

32. Повинні бути визначені та відключені (заблоковані) програмні порти компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, які є небезпечними для забезпечення кібербезпеки.

33. Власник/керівник об’єкта критичної інфраструктури зобов’язаний проводити перевірку ефективності заходів щодо захисту об’єкта критичної

інформаційної інфраструктури об’єкта критичної інфраструктури від зовнішнього проникнення шляхом виконання періодичних (не рідше одного разу на рік) тестів на проникнення (Penetration test). У разі отримання негативних результатів після проведення тестів необхідно вжити заходів для усунення їх причин.

34. На об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури передача даних бездротовими мережами повинна здійснюватися виключно захищеними з’єднаннями із забезпеченням її конфіденційності та цілісності. Забороняється використання на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури технологій Wi-Fi та Bluetooth.

35. Для захисту даних, які передаються через незахищене середовище між віддаленими користувачами, адміністраторами та об’єктом критичної інформаційної інфраструктури об’єкта критичної інфраструктури, між компонентами об’єкта (поза контрольованою територією об’єкта критичної інфраструктури), між об’єктом критичної інформаційної інфраструктури об’єкта критичної інфраструктури та іншими (зовнішніми) інформаційно-комунікаційними системами, необхідно використовувати захищені з’єднання із забезпеченням конфіденційності та цілісності цих даних.

36. Систему управління технологічними процесами об’єкта інфраструктури дозволяється підключати до глобальних мереж передачі даних, зокрема до Інтернету, тільки у випадку неможливості функціонування технологічного процесу без підключення до Інтернету та за умови впровадження всіх заходів захисту відповідно до Загальних вимог до кіберзахисту об’єктів критичної інфраструктури або конкретизованих вимог з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування об’єкта критичної інфраструктури, який відноситься до відповідної сфери управління.

37. До глобальних мереж передачі даних, зокрема Інтернету, об’єкти критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні підключатися через тих постачальників електронних комунікаційних мереж та/або послуг, які мають захищені вузли доступу до глобальних мереж передачі даних із створеними комплексними системами захисту інформації з підтвердженою відповідністю. У договорі з надавачем цих послуг зазначаються зобов’язання щодо виконання тієї частини Загальних вимог до кіберзахисту об’єктів критичної інфраструктури, які він надає об’єкту критичної інформаційної інфраструктури об’єкта критичної інфраструктури, та наявність комплексної системи захисту інформації з підтвердженою відповідністю.

Забезпечення доступності та відмовостійкості компонентів та інформаційних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури

38. Інформаційна інфраструктура об’єкта критичної інфраструктури повинна будуватися на базі відмовостійкого підходу. Для забезпечення відмовостійкості об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинно здійснюватися, як мінімум, таке:

-періодичне створення резервних копій інформаційних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та критичних бізнес/операційних процесів об’єкта критичної інфраструктури, включаючи інформацію, яка зберігається на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури, технологічну інформацію компонентів об’єкта та образів серверів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, а також їх відновлення у випадку втрати або пошкодження;

-резервування критичних для функціонування об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та бізнес/операційних процесів об’єкта критичної інфраструктури програмних та апаратних компонентів для забезпечення його сталого функціонування у випадку виходу з ладу одного з критичних компонентів. У разі використання на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури віртуальних серверів необхідно забезпечити їх резервування;

-дублювання (кластеризація) критичних для функціонування об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та бізнес/операційних процесів об’єкта критичної інфраструктури програмних та апаратних компонентів об’єкта для забезпечення його сталого функціонування, зниження навантаження та збільшення продуктивності;

-використання засобів балансування навантаження;

-використання джерел безперебійного живлення для критичних компонентів об’єкта;

-зв’язок з Інтернетом з використанням двох та більше каналів передачі даних, які надаються різними операторами мережі передачі даних (провайдерами), - для об’єкта критичної інфраструктури, які надають свої послуги через Інтернет.

39. Під час розроблення, модернізації або оновлення компонентів системи управління технологічними процесами об’єкта критичної інфраструктури необхідно використовувати тестову програмно-апаратну платформу, яка підключена до окремого (тестового) виділеного сегмента його мережі для тестування нових компонентів та/або оновлень програмного та апаратного забезпечення, перед тим як впровадити їх в промислову експлуатацію.

Визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури

40. На об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинна проводитися перевірка всіх змінних (зовнішніх) пристроїв та носіїв інформації перед кожним їх використанням на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури засобами захисту від зловмисного коду, шкідливого програмного забезпечення та вірусів.

41. На об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинна здійснюватися ідентифікація всіх змінних (зовнішніх) пристроїв та носіїв інформації за допомогою унікального ідентифікатора.

Повинно бути унеможливлено використання змінних (зовнішніх) пристроїв та носіїв інформації, які не зареєстровані на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

42. На об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинно бути відключено автоматичний запуск програм із змінних (зовнішніх) пристроїв та носіїв інформації.

43. Порти компонентів мережевого обладнання, робочих станцій та серверів, які не використовуються, мають бути заблоковані адміністраторами об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

Визначення умов використання програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури

44. На об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинна проводитися перевірка на цілісність та автентичність оновлень компонентів об’єкта. У разі порушення цілісності або непідтвердження автентичності оновлення воно повинно бути відхилене і не повинно застосовуватися, а цю подію необхідно запротоколювати в журналі подій.

45. У складі об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинно використовуватися програмне та апаратне забезпечення, для якого не припинено підтримку виробника. Повинні використовуватися офіційні стабільні версії прикладного програмного забезпечення та драйверів.

На об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинна надаватися перевага програмному забезпеченню, яке має більш вищий рівень гарантій відповідно до нормативного документа системи технічного захисту інформації 2.5-004-99 “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу”, за результатами державної експертизи у сфері технічного захисту інформації.

46.На об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинно блокуватися самостійне встановлення або видалення користувачами програмного забезпечення на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури. Право на встановлення або видалення програмного забезпечення повинен мати тільки уповноважений адміністратор.

47. Засоби об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні забезпечувати неприйняття файла/повідомлення в обробку у разі отримання негативного результату перевірки електронного підпису файла/повідомлення, що надійшов/надійшло. Ця подія повинна відображатися в журналі реєстрації подій.

48. Програмні та апаратні засоби, які використовуються у складі об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, не повинні мати походження з іноземної держави, до якої застосовано санкції згідно із Законом України “Про санкції”, чи бути розроблені/виготовлені

юридичною особою - резидентом такої іноземної держави або юридичною особою, частка статутного капіталу якої перебуває у власності зазначеної іноземної держави, або юридичною особою, яка перебуває під контролем юридичної особи такої іноземної держави.

Визначення умов розміщення компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури

49. Компоненти та/або інформація об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, крім систем управління технологічними процесами, можуть перебувати в сторонньому (не власному) центрі обробки даних тільки за умови, що центр обробки даних розташований на території України (за винятком тимчасово окупованої території України), а власником центру обробки даних є резидент України. При цьому у договорі із центром обробки даних повинні зазначатися його зобов’язання щодо виконання тієї частини Загальних вимог до кіберзахисту об’єктів критичної інфраструктури, які він надає об’єкту критичної інфраструктури.

Компоненти та інформація (дані) систем управління технологічними процесами об’єкта критичної інфраструктури повинні бути розміщені тільки у власному центрі обробки даних.

50. З метою створення резервних копій своїх інформаційних ресурсів та їх оперативного відновлення у разі пошкодження або знищення державні органи використовують основний та резервний захищений дата-центр збереження державних електронних інформаційних ресурсів Державного центру кіберзахисту.

51. Компоненти об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні розміщуватися у приміщеннях, які унеможливлюють несанкціонований фізичний доступ до них сторонніх осіб.

Повинен бути забезпечений контрольований фізичний доступ до приміщень та/або комутаційних шаф, де розташовані робочі станції, сервери, мережеві компоненти та комутаційні вузли структурованої кабельної системи об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

52. Забороняється підключати робочі місця адміністраторів та операторів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури до інших інформаційно-комунікаційних систем.

53. Схеми (креслення) розміщення обладнання структурованої кабельної системи та кабельних каналів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, схеми підключення обладнання, таблиці маркування кабелів структурованої кабельної системи та кабельних з’єднань зберігаються в актуальному стані.

3. Особливості виявлення і дослідження криміналістично-значимої комп’ютерної інформації пов’язані, перш за все, з тим, що дана область спеціальних знань включає в себе ряд досить різнорідних наукомістких напрямів, таких як електроніка, електротехніка, інформаційні системи і процеси, радіотехніка та зв’язок, обчислювальна техніка (у т.ч. програмування) і автоматизація. Злочини розглянутих категорій носять найчастіше латентний характер, не залишають видимих слідів і складні з точки

зору розкриття і збирання доказової інформації в зв’язку з широким застосуванням засобів віддаленого доступу, захисту даних тощо.

до спеціальних знань у сфері комп'ютерної інформації та комп'ютерної техніки, можуть бути віднесені пізнання в різних областях науки, в тому числі техніки, мистецтва і ремесла стосовно області комп'ютерної інформації та сфері високих технологій, отримані в рамках професійної чи спеціальної освіти, професійної діяльності, що включають знання теорії, навички та вміння, і використовувані учасниками судочинства з метою встановлення обставин, що підлягають доказуванню по конкретній справі, в порядку, передбаченому відповідним процесуальним законодавством України. Спеціалізація обізнаних осіб в області комп'ютерних технологій визначається через наявність поглиблених знань і досвіду роботи з певними операційними системами і програмним забезпеченням, комп'ютерними мережами і технічними пристроями. У зв'язку з цим, залучаючи обізнаних осіб до участі в слідчих діях, призначаючи експертизу, слід враховувати предметну спеціалізацію експертів і фахівців.

Як і будь-який інший рід судової експертизи, потреба в якому виникла з кінця XX століття з появою нових видів злочинів і вдосконаленням технічних засобів (генетична, лінгвістична), комп'ютерна експертиза пройшла всі стадії розвитку - від формулювання предмета і завдань, визначення термінології до формування сучасної академічної та методичної школи, що відповідає вимогам кримінального процесу, технічним вимогам дослідження об'єктів високих технологій. На різних стадіях формування даного роду експертиз застосовувалися різні найменування (програмно-технічна, інженерно-комп'ютерна, судово-технічна експертиза інформаційно-обчислювальних систем, інформаційно-технічна, інформаційно-технологічна експертиза, судово-кібернетична експертиза). Сьогодні використовується термін «комп'ютерно-технічна експертиза» (далі – КТЕ), який застосовується в судово-експертних установах Міністерства юстиції України. При цьому ми вважаємо, що сучасна термінологія не є остаточною. Використання термінів прямо чи опосередковано пов'язане з появою нових чи моральним старінням технічних засобів, тому в подальшому можливо як поява нових видів комп'ютерно-технічної експертизи, так і зміна самого її найменування. Однак, незалежно від назви, незмінним залишається її висока технократичність і потреба з боку як правоохоронних органів, так і суспільства в цілому.

Основним завданням експертів, при здійсненні ними комп'ютерно-технічної експертизи є відповідь на питання, що вимагають спеціальних знань в області «форензік» (комп'ютерної криміналістики) - знань про методи пошуку, закріплення і дослідження цифрових доказів за злочинами, пов'язаними з комп'ютерною інформацією (кіберзлочинів).

Комп'ютерно-технічна експертиза дозволяє сформувати цілісну побудову доказової бази шляхом вирішення більшої частини діагностичних та ідентифікаційних питань, тобто вирішує завдання, пов'язані з пошуком, виявленням, оцінкою і аналізом інформації, що міститься в комп'ютерній системі. В результаті ТКЕ, що проводиться під час розслідування злочинів, пов'язаних з порушенням інформаційної безпеки у відкритих комп'ютерних

мережах, розкраданням (руйнуванням, модифікацією) інформації та порушенням інформаційної безпеки, формується інформація про уразливість процесів переробки інформації в інформаційних системах. При цьому результати ТКЕ можуть бути використані фахівцями з інформаційної безпеки для вдосконалення існуючих засобів захисту інформації та забезпечення інформаційної безпеки.

З огляду на розробки закордонних та вітчизняних вчених , сучасний рівень розвитку науки і техніки, практичний досвід здійснення комп'ютерно-технічної експертизи, зрозуміло, що в якості основних областей досліджень фахівців у царині КТЕ є інтегровані та вбудовані системи, відкриті системи, системи зв'язку, а також мультимедійні об'єкти. У більшості випадків метою подібних досліджень є вирішення діагностичних та ідентифікаційних завдань при дослідженнях інформаційної системи, отримання доступу до електронного обладнання й інформації. Так, особлива увага при дослідженнях мобільних терміналів приділяється телекомунікаційним сервісів SMS, EMS, MMS, тому що вони можуть надавати відомості про осіб, причетних до вчинення кримінальних дій, в тому числі і в мережах мобільного зв'язку .

Великий обсяг роботи експертів вітчизняних судово-експертних установ та їх закордонних колег (наприклад, в Нідерландах, Чехії, Італії), пов'язаний із дослідженням відкритих систем, які охоплюють різні операційні системи, їх архітектури, апаратно-програмні комплекси. Апаратними об'єктами експертизи в цих випадках є різні комп'ютерні системи: від мініатюрних персональних комп'ютерів до надзвичайно великих суперкомп’ютерів. Для цих систем характерна наявність різноманітних електронних накопичувачів даних: від жорстких і флоппі-дисків, стрічок, CD-ROM, DVD, магнітооптичних накопичувачів до RAID-масивів, тобто здійснюється аналіз комп'ютерного середовища. В цілому експертами успішно застосовуються при розслідуванні злочинів та отриманні інформації з електронних носіїв, такі операції як: злом захистів під паролем; моделювання пам'яті вилучених електронних апаратів в пам'яті комп'ютера (органайзерів, стільникових телефонів, сім-карт, смарт-карт і модулів, смартфонів та фнших носіїв інформації, за допомогою апаратного програмного інструментарію (Cardreader CardLabs) тощо.

Географічні інформаційні системи та комунікаційні інформаційні системи є наступним перспективним напрямом експертів, що спеціалізуються у мережевих відкритих системах. Основними завданнями тут є аналіз різних інформаційних потоків з метою їх виявлення, інтерпретації повідомлень, відновлення інформації, розкодування даних, виявлення використаних різних алгоритмів тощо. Головне місце в експертному дослідженні займає вивчення протоколів передачі даних, в тому числі повного стека протоколів за рівнями OSI . Ця модель включає до себе маршрутизовані і транспортні протоколи. Окремим видом є проведення досліджень телекомунікаційних мереж забезпечення стільникового зв'язку GSM, GPS, GPRS - комунікацій. Однак дії фахівців з перехвату сигналів зв'язку, їх аналізу, ідентифікації систем локального і глобального зв'язку, географічної області, локалізації користувача/ адресата, найчастіше пов'язані з проведенням оперативно-

розшукової діяльності та використовуються експертами лише у прикладних цілях для вирішення окремих завдань. Подібна ситуація спостерігається і в дослідженнях, пов'язаних із розслідуванням різноманітних злочинів у глобальних мережах. Ця область спеціальних знань включає до себе як завдання ідентифікації та діагностики користувачів мережі, їх ресурсів, так і аналіз роботи провайдерів, характеристик досліджуваних трафіків та інформаційних систем Internet, активне використання різних програм-браузерів тощо. Сучасні Інтернет технології, технології розробки програмного забезпечення (OLE, ActiveX), різні plug-ins, Java-аплети значно розширюють список можливих форматів даних та об'єктів програмного забезпечення, що потрапляють до уваги експертів.

Даний перелік напрямів комп'ютерно-технічної експертизи не є вичерпним, і може бути змінений та доповнений з урахуванням сучасного розвитку комп'ютерної техніки, високих технологій та програмного забезпечення, а також розробок нових методик дослідження технічних і програмних засобів. Такий підхід, на нашу думку, дозволяє забезпечити більш ефективний підбір окремих експертів, які володіють спеціальними знаннями при виявлення і розслідування злочинів у сфері комп'ютерної інформації та високих технологій, а також скоротити час проведення експертиз за рахунок чіткого визначення завдань їх розподілу між відповідними фахівцями.

5. Індивідуальні завдання

Навчальним планом не передбачено.

Реферати, аналітичні огляди та інше – це індивідуальні завдання, які сприяють розширенню та поглибленню теоретичних знань з окремих тем навчальної дисципліни, формують навички самостійної роботи з навчальною та науковою літературою, кримінальним законодавством, судовою практикою.

6. Методи навчання

Проведення аудиторних лекцій, практичних занять, індивідуальні консультації (при необхідності), самостійна робота студентів за матеріалами, опублікованими кафедрою (методичні посібники), проведення олімпіад, словесні (пояснення, розповідь, бесіда, навчальна дискусія та ін.), наочні (ілюстрування, демонстрування, самостійне спостереження)

7. Методи контролю

Поточний контроль: опитування на семінарських та практичних заняттях; вирішення конкретних правових ситуацій; проведення письмових контрольних робіт з окремих правових інститутів; проведення програмованого контролю (тестування); проведення групових та індивідуальних консультацій.

Підсумковий контроль: складання модульного контролю; складання іспиту.

8. Критерії оцінювання та розподіл балів, які отримують здобувачі

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Модуль 1			
Самостійна робота з навчально-методичними матеріалами	0…2	3	0…6
Виконання практичних робіт	0..2	1	0...2
Семінарські заняття	0…2	2	0…4
Рішення тестових завдань	0-10	1	0-10
Усього за модуль			1-22
Модуль 2			
Самостійна робота з навчально-методичними матеріалами	0…2	8	0…16
Виконання практичних робіт	0...2	8	0…16
Рішення тестових завдань	0-11	1	0-10
Усього за модуль			1-42
Модуль 3			
Самостійна робота з навчально-методичними матеріалами	0…2	5	0…10
Виконання і захист практичних робіт	0..2	5	0...1 0
Рішення тестових завдань	0-10	1	0-16
Усього за модуль			1-36
Усього за курс			**60…100**

Білет для іспиту/заліку складається з**:**

І. Теоретична частина (питання для перевірки отриманих знань): складається з 2 запитань кожне оцінюється максимально 20 балів.

Приклад

1. Поняття та ознаки транспортного кримінального правопорушення - 20 балів

2. Типові тактичні операції початкового етапу розслідування кримінальних правопорушень у сфері екологічної безпеки на об'єктах критичної інфраструктури.

ІІ. Практична частина (завдання для виявлення рівня сформованості умінь та практичних навичок професійної діяльності). – максимальна оцінка 60 балів

Всього – максимальна оцінка 100 балів.

Під час складання семестрового іспиту/заліку студент має можливість отримати максимум 100 балів.

Критерії оцінювання роботи здобувача протягом семестру

Відповідно до п. 3.2. Положення про рейтингове оцінювання досягнень студентів у Національному аерокосмічному університеті ім. М.Є. Жуковського «Харківський авіаційний інститут» студенту можуть призначатися бали за інші активності, пов'язані з навчальною дисципліною, які нараховуються та можуть бути враховані у загальній оцінці за семестр. Бали зокрема можуть призначатися за такі активності, пов'язані з навчальною дисципліною, як:

- участь у науковому комунікативному заході (конференції, семінарі, круглому столі тощо) із написанням тез наукової доповіді за предметом навчальної дисципліни (20 балів);
- участь у другому турі Всеукраїнської олімпіади відповідного напряму 20 балів);
- участь (прослуховування) не менше у 5 вебінарах, пов'язаних з навчальною дисципліною (3-15 балів);
- участь у тренінгу, пов'язаному з навчальною дисципліною (15 балів);
- проходження он-лайн курсу, пов'язаного з навчальною дисципліною (20 балів);
- участь та отриманні рейтингового місця у тематично пов'язаному із предметом навчальної дисципліни студентському конкурсі (30 балів);
- розробка та створення дидактичного матеріалу за тематикою предмету навчальної дисципліни (15 балів) (підтвердження - дидактичний матеріал);
- проведення право освітнього заходу із учнями шкіл та інших навчальних закладів за тематикою навчальної дисципліни (20 балів);
- написання реферату (5 балів);
- участь у не менше 2-х заходах, що проводяться студентськими професійними об`єднаннями за спеціальністю (5-15 балів);
- інші активності, пов'язані з навчальною дисципліною, за попереднім погодженням із науково-педагогічним працівником, який викладає навчальну дисципліну.

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	

60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

9. Політика навчального курсу

1. Письмові роботи:

Планується виконання студентами обов'язкових та додаткових декількох видів письмових робіт: письмових робіт за результатами самостійної роботи за темами курсу, тестових завдань за модулями (перелік та зміст завдань за темами курсу міститься на сторінці **в: Ошибка! Недопустимый объект гиперссылки.**), письмових експрес-опитувань на семінарських заняттях тощо.

2. Академічна доброчесність:

Очікується, що студенти будуть дотримуватися принципів академічної доброчесності, усвідомлюючи наслідки її порушення. Порушення академічної доброчесності регулюється відповідно до Положень «Про систему забезпечення якості освітньої діяльності та вищої освіти СУЯ ХАІ-НМВ-П/011:2017» та «Про академічну доброчесність» СУЯ ХАІ-НМВ-П/004:2019 від 21.06.2019(зі змінами від 22.01.2020) (https://khai.edu/ua/university/normativnabaza/polozheniya1/polozhennya-yaki-regulyuyut-poryadok-zdijsnennya osvitnogo-procesu/; https://khai.edu/assets/files/polozhennya/polozhennya-pro-akademichnu-dobrochesnist.pdf).

3. Відвідування занять:

Відвідання занять є важливою складовою навчання. Очікується, що всі студенти відвідають лекції і практичні заняття курсу.

Пропуски семінарських (практичних, лабораторних) занять відпрацьовуються в обов'язковому порядку. Студент зобов'язаний відпрацювати пропущене заняття впродовж двох тижнів з дня пропуску заняття. За пропущені лекційні заняття без поважних причин в обсязі, що перевищує 10% від загальної кількості лекційних годин, які відведені на навчальну дисципліну відповідно до робочого навчального плану, керівник курсу віднімає 5 балів від підсумкового семестрового балу студента (https://khai.edu/ua/university/normativna-baza/polozheniya1/polozhennya-pro-organizaciyu-sistemi-upravlinnya-yakistyu/polozhennya-pro-sistemu-zabezpechennya-yakosti/).

10. Методичне забезпечення

1. Навчально-методичне забезпечення обов'язкової навчальної дисципліни «Актуальні проблеми кримінального права», другий рівень вищої освіти (магістерський) / Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т" ; уклад. І. Р. Шинкаренко. Харків. Нац. аерокосм. ун-т ім. М. Є. Жуковського "Харків. авіац. ін-т", 2022.
2. Mentor: https://mentor.khai.edu/course/view.php?id=1686

11. Рекомендована література

Основні нормативні акти:

1. Конституція України: Закон України від 28.06.1996 р. № 254к/96-ВР. URL: http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

2. Конвенція Організації Об'єднаних Націй проти корупції: підписана відімені України 11.12.2003 р.; ратифікована 18.10.2006 р.; набрала чинності для України 01.01.2010 р. *Офіційний вісник України*. 2010. № 10. Ст. 506.

3. Конвенція про захист прав людини і основоположних свобод. URL: http://www.echr.coe.int/Documents/Convention_UKR.pdf.

4. Рекомендація Rec (2004)4 Комітету міністрів Ради Європи державам-членам про роль Європейської конвенції з прав людини в університетській освіті та професійній підготовці. URL: http://zakon3.rada.gov.ua/laws/show/994_573.

5. Загальна декларація прав людини. Прийнята і проголошена резолюцією 217 А (III). Генеральної Асамблеї ООН від 10 грудня 1948 року. URL: http://zakon3.rada.gov.ua/laws/show/995_015.

6. Окінавська хартія глобального інформаційного суспільства (2000 р.). URL: http://zakon3.rada.gov.ua/laws/show/998_163.

7. Міжнародний пакт про економічні, соціальні і культурні права (1966 р.). URL: http://zakon3.rada.gov.ua/laws/show/2148-08.

8. Кримінальна конвенція про боротьбу з корупцією: підписана від імені України 27.01.1999 р.; ратифікована 18.10.2006 р., набрала чинності для України 01.03.2010 р. *Офіційний вісник Украї*ни. 2010. № 15. Ст. 717.

9. Кримінальний кодекс України: Закон від 05.04.2001 р. № 2341-III. URL: http://zakon3.rada.gov.ua/laws/show/2341-14. (Дата звернення 10.02.2018 р.).

10. Кримінальний процесуальний кодекс України. Закон від3.04.2012 № 4651-VI. URL: http://zakon3.rada.gov.ua/laws/show/4651-17

11. Кодекс України про адміністративні правопорушення: Закон від07.12.1984 № 8073-X. URL: http://zakon5.rada.gov.ua/laws/show/80731-10

12. Закон України «Про заходи протидії незаконному обігу наркотичних засобів, психотропних речовин і прекурсорів та зловживанню ними». URL: https://cutt.ly/TJ4YPV9.

13. Про запобігання корупції: Закон України від 14.10.2014 р. № 1700-VII. URL: http://zakon5.rada.gov.ua/laws/show/1700-18/print1511514732405635*Підзаконні акти:*

1. Про судову практику у справах про необхідну оборону: Постанова ПВСУ від 26.04.2002 р. №1 // База даних «Законодавство України». URL: http://zakon.rada.gov.ua/laws/show/995_011 .

2. Про умовно-дострокове звільнення від відбування покарання і заміну не відбутої частини покарання більш м'яким: Постанова ПВСУ від

26.04.2002 р. №2 // База даних «Законодавство України». URL: http://zakon.rada.gov.ua/laws/show/795_015 .

3. Про практику розгляду судами справ про застосування примусових заходів виховного характеру: Постанова ПВСУ від 15.05.2002 р. № 2 // База даних «Законодавство України». URL:http://zakon.rada.gov.ua/laws/show/895_014 .

4. Про практику призначення судами кримінального покарання: Постанова ПВСУ від 24.10.2003 р. №7 // База даних «Законодавство України». URL: http://zakon.rada.gov.ua/laws/show/225_016 .

5. Про практику застосування судами України законодавства про погашення і зняття судимості: Постанова ПВСУ від 26.12.2003 р. №16 // База даних «Законодавство України». URL: http://zakon.rada.gov.ua/laws/show/335_075 .

6. Про практику призначення військовослужбовцям покарання у виді тримання в дисциплінарному батальйоні: Постанова ПВСУ від 28.12.1996 р. №15 (Із змінами, внесеними згідно з Постановою ПВСУ №17 26.12.2003 р.) // База даних «Законодавство України». URL:http://zakon.rada.gov.ua/laws/show/956_009 .

7. Про практику застосування судами України законодавства у справах про злочини неповнолітніх: Постанова ПВСУ від 16.04.2004 р. №5. // Базаданих «Законодавство України». URL:http://zakon.rada.gov.ua/laws/show/978_012 .

8. Про практику застосування судами примусових заходів медичного характеру та примусового лікування: Постанова ПВСУ від 16.04.2004 р. №5 // База даних «Законодавство України». URL:http://zakon.rada.gov.ua/laws/show/456_011 .

9. Про практику розгляду судами кримінальних справ про злочини, вчинені стійкими злочинними об'єднаннями: Постанова ПВСУ від 23.12.2005 р. №13 // База даних «Законодавство України». URL: http://zakon.rada.gov.ua/laws/show/934_011 .

10. Про практику застосування судами України законодавства про звільнення особи від кримінальної відповідальності: Постанова ПВСУ від 23.12.2005 р. № 12 // База даних «Законодавство України». URL: http://zakon.rada.gov.ua/laws/show/923_034 .

11. Про внесення змін та доповнень до постанови Пленуму Верховного Суду України від 24 жовтня 2003 року № 7 „Про практику призначення судами кримінального покарання: Постанова Пленуму Верховного Суду України від 12 червня 2009 р. № 8 // База даних «Законодавство України». URL: http://zakon.rada.gov.ua/laws/show/235_012 .

12. Про внесення доповнення до постанови Пленуму Верховного Суду України від 24 жовтня 2003 року № 7 «Про практику призначення судами кримінального покарання: Постанова Пленуму Верховного Суду України від 6 листопада 2009 р. № 11 // База даних «Законодавство

України». URL: http://zakon.rada.gov.ua/laws/show/678_045 .

13. Про звернення до Конституційного Суду України з конституційним поданням щодо офіційного тлумачення положень частини другої статті 4, частин першої та четвертої статті 5, частини третьої статті 74 Кримінального кодексу України, статті 73 Закону України “Про Конституційний Суд України: Постанова Пленуму Верховного Суду України від 4 червня 2010 року № 4 // База даних «Законодавство України». URL:http://zakon.rada.gov.ua/laws/show/235_013

14. Про введення воєнного стану в Україні. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №64/2022. URL: https://www.president.gov.ua/documents/642022-41397

15. Про рішення Ради національної безпеки і оборони України від 06.05.2015 р. «Про Стратегію національної безпеки України»: Указ Президента України від 26.05.2015

16. Постанова Кабінету Міністрів України від 06.05.2000 № 770 «Про затвердження переліку наркотичних засобів, психотропних речовин і прекурсорів». URL: https://cutt.ly/xJ4OF9G.

17. Результати міжнародного дослідницького проєкту «Куріння, вживання алкоголю та наркотичних речовин серед підлітків, які навчаються: поширення й тенденції в Україні» (ESPAD). URL: https://cutt.ly/DJ6skn6.

18. Розпорядження Кабінету Міністрів України від 27.11.2019 № 1335-р «Про затвердження Плану заходів з реалізації Національної стратегії реформування системи юстиції щодо дітей на період до 2023 року». URL: https://cutt.ly/3J4GlU2.

19. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури. Постанова КМУ від 19 червня 2019 р. № 518. Із змінами, внесеними згідно з Постановою КМ № 991 від 02.09.2022.

20. Наказ Міністерства освіти і науки України від 02.10.2018 № 1047 «Про затвердження Методичних рекомендацій щодо виявлення, реагування на випадки домашнього насильства і взаємодії педагогічних працівників із іншими органами та службами». URL: https://cutt.ly/7J56qtr.

21. A/CONF.6/1. Доповідь Першого конгресу ООН із запобігання злочинності й поводженню з правопорушниками (Женева, 22 серп. – 3 вер. 1955 р.). URL: http://daccess- dds-ny.un.org/doc/UNDOC.

22. 3 A/CONF.26/7. Доповідь Третього конгресу ООН із запобігання злочинності й поводженню з правопорушниками (Стокгольм, 9–18 серп. 1965 р.). URL: http://daccess- dds-ny.un.org/doc/UNDOC.

23. A/CONF.87/14/Rev.1. Доповідь Шостого конгресу ООН із запобігання злочинності й поводженню з правопорушниками (Каракас, 25 серп. – 5 вер. 1980 р.). URL: http://daccess-dds-ny.un.org/doc/UNDOC.

24. A/CONF.144/28/Rev.1. Доповідь Восьмого конгресу ООН із запобігання злочинності й поводженню з правопорушниками (Гавана, 27 серп. – 7 вер. 1990 р.). URL: http://daccess-dds-ny.un.org/doc/UNDOC.

25. A/CONF.203/18. Доповідь Одинадцятого Конгресу ООН із запобігання злочинності і кримінального правосуддя (Бангкок, 18–25 квіт. 2005 р.). URL: http://daccess- dds-ny.un.org/doc/UNDOC.

26. АЖЕ8/65/230. Доповідь Дванадцятого Конгресу ООН із запобігання злочинності і кримінального правосуддя (Бразилія, 12–19 квітня 2010 року). URL: http://daccess-dds- ny.un.org/doc/UNDOC.

27. ADO 15/33/688. Доповідь Тринадцятого Конгресу ООН із запобігання злочинності і кримінального правосуддя (Доха, 12–19 квітня 2015 року) URL: http://daccess-dds-ny.un.org/doc/UNDOC

28. Про практику застосування судами кримінального законодавства про повторність, сукупність і рецидив злочинів та їх правові наслідки: Постанова Пленуму Верховного Суду України від 4 червня 2010 року № 7 // База даних
«Законодавство України».

Підручники:

1. Актуальні проблеми кримінально-правової кваліфікації: навч. посіб. / за заг. ред. В.В. Топчія; наук. ред. В.І. Антипова. Вінниця: ТОВ «Нілан-ЛТД», 2017. 896 с.

2. Баулін Ю.В., В.І. Борисов, В.І. Тютюгін та ін. Кримінальне правоУкраїни: Загальна частина: підручник. Харків: Право, 2010. 456 с.

3. Баулін Ю.В., В.І. Борисов, В.І. Тютюгін та ін. Кримінальне правоУкраїни: Особлива частина: підручник. Харків: Право, 2010. 608 с.

4. Вереша Р.В. Суб'єктивні елементи підстави кримінальноївідповідальності: Підручник. Київ: Атіка, 2006. 740 с.

5. Велика українська юридична енциклопедія: у 20 т. Харків: Право, 2016. Т. 17: Кримінальне право / редкол.: В.Я. Тацій (голова), В.І. Борисов (заст. голови) та ін.; Нац. акад. прав. наук України; Ін-т держави і права ім.В.М. Корецького НАН України; Нац. юрид. ун-т ім. Ярослава Мудрого. 2017. 1064 с.:

6. Корупційні схеми: їх кримінально-правова кваліфікація і досудове розслідування / за ред. М.І. Хавронюка. К.: Москаленко О.М., 2019. 464 с.

7. Матишевський П.С. Кримінальне право України. Загальна частина: Підруч. для студ. юрид. вузів і фак. Київ: А.С.К., 2001. 352 с.

8. Настільна книга детектива, прокурора, судді: коментар антикорупційного законодавства: вид. друге, перобл. і доповн. / за ред. М.І.Хавронюка. К.: ВД «Дакор», 2017. 514 с.

9. Науково-практичний коментар Закону України «Про запобігання корупції» / Н.О. Армаш, Т.О. Коломоєць, Д.В. Приймаченко, В.В. Шаблистийта ін.; за заг. ред. Т.О. Коломоєць, В.К. Колпакова. Запоріжжя: Видавничий дім
«Гельветика», 2019. 588 с.

10. Науково-практичний коментар Закону України «Про запобігання корупції» / В.С. Ковальський, О.І. Миколенко, Є.Л. Стрельцов, О.І. Клименко. К.: Юрінком Інтер, 2019. 380 с.

11. Науково-практичний коментар Кримінального кодексу України / Д.С. Азаров, В.К. Грищук, А.В. Савченко [та ін.]; за заг. ред. О.М. Джужі, А. В. Савченка, В. В. Чернєя. К.: Юрінком Інтер, 2016. 1064 с.

12. Науково-практичний коментар Кримінального кодексу України /

за заг. ред. О.М. Литвинова. К.: «Центр учбової літератури», 2016. 536 с.

13. Науково-практичний коментар Кримінального кодексу України / за ред. М.І. Мельника, М.І. Хавронюка. 9-те вид., переробл. і допов. К.: Юридичнадумка, 2012. 1316 с.

Навчальні посібники, інші дидактичні та методичні матеріали:

Монографії та інші наукові видання:

1. Алфьоров С.М., Шаблистий В.В. Кримінальна відповідальність за погрози застосуванням фізичного насильства: монографія. Запоріжжя: ФОП Зеленкевич Л.П., 2011. 212 с.

2. Андрушко П.П. Злочини проти виборчих прав громадян та їх права брати участь у референдумі: кримінально-правова характеристика: Монографія.КИЇВ:КНТ, 2007. 328 с.

3. Антипов В.В., Антипов В.І. Обставини, які виключають застосування кримінального покарання: Монографія. КИЇВ:Атіка, 2004. 208 с.

4. Анчукова М.В. Виправданий ризик як обставина, що виключає злочинність діяння: Монографія. Харків.: Видавець ФО-ПВапнярчукН.М., 2006.168 с.

5. Баулін Ю.В. Звільнення від кримінальної відповідальності: Монографія. КИЇВ: Атіка, 2004. 296 с.

6. Берзін П.С. Злочинні наслідки: поняття, основні різновиди, кримінально-правове значення: Монографія. КИЇВ: Дакор, 2009. 736 с.

7. Борисов В.І., Пащенко О.О. Злочини проти безпеки виробництва: поняття та види. Кримінальна відповідальність за порушення правил ядерної або радіаційної безпеки: Монографія. Харків: Видавець СПД ФОП Вапнярчук Н.М., 2006. 224 с.

8. Бурдін В.М. Кримінальна відповідальність за злочини, вчинені встані сп'яніння: Монографія. КИЇВ:Атіка, 2005. 160 с.

9. Бурдін В.М. Особливості кримінальної відповідальностінеповнолітніх в Україні: Монографія. КИЇВ: Атіка, 2004. 240 с.

10. Вербенський М.Г., Мінка Т.П., Негодченко Д.О. Протидія торгівлілюдьми в Україні: Монографія. Дніпропетровськ, ДДУВС, 2010. 236 с.

11. Вереша Р.В. Поняття вини як елемент змісту кримінального праваУкраїни: Монографія. КИЇВ: Атіка, 2005. 224 с.

12. Вечерова Є.М. Нормативність кримінального права: теоретико-прикладне дослідження: монографія. Одеса: Вид. дім «Гельветика», 2018. 460 с.

13. Гладкова Є.О. Стратегія й тактика протидії наркозлочинності в Україні: монографія. Харків: Діса плюс, 2019. 464 с.

14. Голіна В.В. Судимість: Монографія. Харків: Харків юридичний,2006. 384 с.

15. Горох О.П. Сучасні кримінально-правові проблеми звільнення відпокарання та його відбування: монографія; за наук. ред. А.А. Музики. Київ: ВД «Дакор», 2019. 676 с.

16. Гороховська О.В. Вбивство через необережність: Монографія /Наук. ред. Музика А.А. КИЇВ: Видавець ПАЛИВОДА А.В., 2007. 180 с.

17. Грищук В.К. Філософсько-правове розуміння відповідальності людини: монографія. 2-ге вид., перероообл. і доповн. Хмельницький: Хмельн. ун-т управління і права, 2013. 768 с.

18. Дудоров О.О. Злочини у сфері господарської діяльності: кримінально-правова характеристика: Монографія. КИЇВ:Юридична практика, 2003. 924 с.

19. Жаровська Г.П. Транснаціональна організована злочинність в Україні: феномен, детермінація, протидія: монографія. Чернівці: Чернівец. нац. ун-т, 2018. 568 с.

20. Зеленецький В.С., Ємельянов В.П., НастюкВ.Я. та ін. Проблеми систематизації та комплексного розвитку антитерористичного законодавстваУкраїни / За заг. ред. Зеленецького В.С., Ємельянова В.П.: Монографія. Харків:Право, 2008. 96 с.

21. Іващенко В.О. Торгівля жінками та дітьми (кримінологічні та кримінально-правові аспекти боротьби): Монографія. КИЇВ:Атіка, 2004. 112 с.

22. Ізетов А.Е. Втягнення у вчинення терористичного акту: кримінально-правове дослідження: Монографія. Харків: Право, 2010.174 с.

23. Катеринчук К.В. Злочини проти здоров'я особи: проблеми кримінально-правової теорії та практики: монографія. Київ: ФОП Маслаков, 2018. 408 с.

24. Козак О.С. Ефективність звільнення від кримінальної відповідальності в Україні: монографія / за ред. О.М. Бандурки. Київ: Освіта України, 2009. 204 с.

25. Коржанський М.Й. Предмет і об'єкт злочину: Монографія. Дніпропетровськ: Юридична академія МВС; Ліра ЛТД, 2005. 252 с.

26. Коржанський М.Й. Презумпція невинуватості і презумпція вини: Монографія. КИЇВ:Атіка, 2004. 216 с.

27. Коржанський М.Й. Проблеми кримінального права: Монографія. Дніпропетровськ: Юридична академія Міністерства внутрішніх справ, 2003. 200с.

28. Корнякевич-Танасійчук Ю.В. Кримінально-правова політика України: монографія. Івано-Франківськ: Прикарпат. нац. ун-т ім. Василя Стефаника, 2019. 336 с.

29. Корупційна злочинність: витоки, сучасний стан, стратегія протидії: монографія / Т.В. Корнякова, О.Л. Соколенко, І.Г. Алєксєєнко та ін.; за заг. ред. д-ра юрид. наук, проф. Т.В. Корнякової. Дніпро: ліра, 2017. 276 с.

30. Котовенко О.М. Кримінальна відповідальність за пошкодження об'єктів магістральних нафто-, газо- та нафтопродуктопроводів: Монографія. Харків: Консум, 2004. 136 с.

31. Кузнецов В.В. Кримінальна відповідальність за крадіжки: Монографія. КИЇВ: Вид. ПАЛИВОДА А.В., 2005. 158 с.

32. Куц В.М., Кириченко Ю.В. Кримінальна відповідальність за

незаконне використання електричної або теплової енергії: Монографія. КИЇВ: Центр учбової літератури, 2010. 160 с.

33. Лень В.В. Осудність у кримінальному праві і законодавстві: Монографія. Дніпропетровськ: Дніпроп. держ. ун-т внутр. справ; Ліра ЛТД, 2008. 180 с.

34. Лень В.В., Книга М.М. Примусові заходи медичного характеру: історія, стан, тенденції. Запоріжжя: Дніпровський металург, 2010. 212 с.

35. Лень В.В., Книга М.М. Примусові заходи медичного характеру: цілії підстави застосування. Запоріжжя: Дніпровський металург, 2011.92 с.

36. Марін О.К. Кваліфікація злочинів при конкуренції кримінально-правових норм: Монографія. КИЇВ:Атіка, 2003. 224 с.

37. МарітчакТ.М. Помилки у кваліфікації злочинів: Монографія. КИЇВ:Атіка, 2004. 188 с.

38. Матвійчук В.К., Голуб С.А. Незаконне полювання: відповідальність, протокольна форма провадження, розслідування і запобігання: Монографія. КИЇВ:КНТ, 2006. 304 с.

39. Машлякевич Д.С. Литвинов О.М. Стратегії запобігання і протидії корупції в Україні: монографія / за загальною редакцією д-ра юрид. наук, проф. О. М. Литвинова. Харків: ТОВ «В деле», 2016. 260 с.

40. Медицький І.Б. Вплив соціальних факторів на злочинність в умовахстановлення незалежної Української держави: монографія. Івано-Франківськ, 2007. 222 с.

41. Мельник М.І. Корупція – корозія влади (соціальна сутність, тенденції та наслідки, заходи протидії): монографія. К.: Юридична думка, 2004.

400 с. Михайленко Д.Г. Протидія корупційним злочинам засобами кримінального права: концептуальні основи: монографія. Одеса: Видавничий дім «Гельветика», 2017. 582 с.

42. Микитчик О.В. Філософія злочину: монографія. КИЇВ: Київський нац. ун-т внутр. справ, 2006. 188 с.

43. Миронова В.О. Проблеми кримінальної відповідальності за порушення законів та звичаїв війни: Монографія. Харків: Право, 2007. 152 с.

44. Мисливий В.А. Злочини проти безпеки дорожнього руху та експлуатації транспорту: Монографія. Дніпропетровськ: Юридична академія Міністерства внутрішніх справ, 2004. 380 с.

45. Митрофанов І.І. Кримінально-правове забезпечення охорони довкілля: Монографія. Кременчук: Видавець «ПП Щербатих О.В.», 2010. 272 с.

46. Митрофанов І.І., СлободяникТ.М. Кримінальна відповідальність осіб, які вчинили злочин у співучасті: Монографія. Кременчук: Видавець «ПП Щербатих О.В.», 2009. 280 с.

47. Музика А.А. Відповідальність за злочини у сфері обігу наркотичнихзасобів: Монографія. КИЇВ: Логос, 1998. 324 с.

48. Методика розслідування вбивств, вчинених на замовлення / Волобуєв А.Ф., Матюшкова Т.П., Філіпенко Н.Є. // Актуальні питання

діяльності слідчих підрозділів ОВС України: зб. наук. Праць ННІПФСД ХНУВС за 2011 р. / за загал. ред. д-ра юрид. наук, проф. О.М.Бандурки. Х.: НікаНова, 2012. С. 257-298.

49. Методичні рекомендації щодо виявлення, документування та розслідування злочинів, передбачених ст. 315 КК України, в умовах нового кримінального процесуального та оперативно-розшукового законодавства / Степанюк Р.П., Галкін Д.В., Сафронов С.О. Філіпенко Н.Є. // Актуальні питання діяльності органів внутрішніх справ України: зб. наук. праць факультету підготовки фахівців для підрозділів слідства ХНУВС за 2014 р. / за загал. ред._д-ра юрид. наук, чл.- кор. НАПрН України, засл. юриста України_С.М. Гусарова. Х.: ХНУВС, НікаНова, 2015. С. 414-479.

50. Новітні кримінально-правові дослідження – 2019 : альманах наукових досліджень / за ред. О. В. Козаченка, О. М. Мусиченко. – Миколаїв : СПД Румянцева Г. В., 2019. 278 с. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/11514/Almanax.pdf?sequence=1&isAllowed=y.

51. Наден О.В. Найманство як соціальне та кримінально-правове явище: сутність, новітні тенденції розвитку та проблеми протидії: Монографія. КИЇВ:Атіка, 2005. 264 с.

52. Наден О.В. Спеціальні види звільнення особи від кримінальної відповідальності за злочини у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів: Монографія. Харків: Право, 2003. 224 с.

53. Наден О.В. Торгівля жінками як кримінально-правова та соціальна проблема сучасності: Монографія. КИЇВ:Атіка, 2004. 288 с.

54. Науково-практичний коментар Кримінального кодексу України: Злочини проти власності/ За ред. М.І. Хавронюка. - Київ: ВД «Дакор», 2017. 448 с.

55. Науково-практичний коментар Закону України «Про запобігання корупції» / Н.О. Армаш, Т.О. Коломоєць, Д.В. Приймаченко, В.В. Шаблистийта ін.; за заг. ред. Т.О. Коломоєць, В.К. Колпакова. Запоріжжя: Видавничий дім
«Гельветика», 2019. 588 с.

56. Орлеан А.М. Кримінально-правова характеристика торгівлі людьми: Монографія. Харків: СІМ, 2005. 180 с.

57. Осадчий В.І. Кримінально-правовий захист правоохоронної діяльності: Монографія. КИЇВ: Атіка, 2004. 336 с.

58. Пономаренко Ю.А. Чинність і дія кримінального закону в часі: Монографія. КИЇВ: Атіка, 2005. 288 с.

59. Пономаренко Ю.А. Штраф як вид покарання у кримінальному праві України (за результатами реформи 2011 р.): наук. нарис / наук. ред. Ю.В. Баулін. Х.: Право, 2012. 80 с.

60. Попрас В.О. Штраф як вид покарання за кримінальним правом України: монографія. Х.: Право, 2009. 224 с.

61. Присяжнюк Т.І. Потерпілий від злочину: проблеми правового захисту. КИЇВ:Центр учбової літератури, 2007. 240 с.

62. Протидія інформаційному тероризму та його фінансуванню в сучасних умовах: монографія / В.В. Крутов, М.П. Стрельбицький, О.А. Шевченко; ред.: В.В. Крутов; Нац. акад. прав. наук України. Київ. Ужгород: Вид-во НАПрНУ: ІВА, 2014. 309 с.

63. Романов С.Ю. Криминальный обман: Монография. Харьков: ООО «Прометей-Прес», 2005. 272 с.

64. Савченко А.В. Кримінальне законодавство України та федеральне кримінальне законодавство Сполучених Штатів Америки: комплексне порівняльно-правове дослідження: Монографія. КИЇВ:КНТ, 2007. 596 с.

65. Савченко А.В. Мотив і мотивація злочину: Монографія. КИЇВ: Атіка, 2002. 144 с.

66. Семикін М.В. Створення терористичної групи чи терористичної організації: кримінально-правове дослідження: Монографія / За заг. ред. проф. В.П. Ємельянова. Харків: Вид-во Нац. ун-ту внутр. справ, 2003. 145 с.

67. Спіцина Г. О., Філіпенко Н. Є. Терористична діяльність: кримінально-правова політика протидії // Кримінально-правові та кримінологічні засоби протидії злочинам проти громадської безпеки та публічного порядку : зб. тез доп. міжнар. наук.-практ. конф. до 25-річчя ХНУВС (18 квіт. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ ; Кримінол. асоц. України. Харків : ХНУВС, 2019. С. 188-191.

68. Спіцина Г. О., Філіпенко Н. Є., Акулова А. О. Віктимологічний аспект попередження майнових злочинів на транспорті. Злочинність і протидія їй в умовах сингулярності: тенденції та інновації : зб. тез доп. наук.-практ. конф., присвяч. пам'яті члена Правління Кримінологічної асоціації України, професора Тетяни Андріївни Денисової (м. Харків, 16 квіт. 2021 р.) / МВС України, Харків. нац. ун-т внутр. Справ, Кримінол. асоц. України. Харків : ХНУВС, 2021. С. 143-145.

69. Титаренко О.О. Кримінологічна характеристика та протидія економічним злочинам у вугільній промисловості: Монографія. Дніпропетровськ: ДДУВС, 2008. 196 с.

70. Тростюк З.А. Понятійний апарат Особливої частини кримінального кодексу України: Монографія. КИЇВ:Атіка, 2003. 144 с.

71. Трубников В.М., Орел Ю.В. Кримінальна відповідальність за злісну непокору вимогам адміністрації виправної установи: Монографія. Харків: Харків юридичний, 2009. 356 с.

72. Трубников В.М., Шинкарьов Ю.В. Арешт як вид кримінального покарання та особливості його застосування: Монографія. Харків: Харків юридичний, 2007. 288 с.

73. Ус О.В. Кримінальна відповідальність за підбурювання до злочину: Монографія. Харків.: Видавець ФОП Вапнярчук Н.М.,2007.264с.

74. Усатий Г.О. Кримінально-правовий компроміс: Монографія. КИЇВ:Атіка, 2001. 128 с.

75. Філіпенко Н. Є. Кримінологічна діяльність судово-експертних установ України : монографія. Харків : Коллегіум, 2020. 392 с.

76. Фріс П.Л. Кримінально-правова політика Української держави: теоретичні, історичні правові проблем: Монографія. КИЇВ: Атіка, 2005. 332 с.

77. Фріс П.Л. Нарис історії кримінально-правової політики України: Монографія / За заг. ред. М.В. Костицького. КИЇВ: Атіка, 2005. 124 с.

78. Хавронюк М.І. Історія кримінального права європейських країн: Монографія. КИЇВ:Істина, 2006. 192 с.

79. Хавронюк М.І. Кримінальне законодавство України та інших держав Континентальної Європи: порівняльний аналіз, проблеми гармонізації: Монографія. К. Юрисконсульт, 2006. 1048 с.

80. Хавронюк М.І. Сучасне загальноєвропейське кримінальне законодавство: проблеми гармонізації: Монографія. КИЇВ: Істина, 2005. 264 с.

81. Харитонов С.О. Кримінальна відповідальність за військові злочини за кримінальним правом України: монографія. Харків: Право, 2018. 328 с.

82. Храмцов О.М. Насильство як категорія загальної частини кримінального права України (теорія, практика, зарубіжний досвід): монографія. Харків: Колегіум, 2017. 260 с.

83. Шаблистий В. В. Безпековий вимір кримінального права України: людиноцентристське дослідження: монографія. Дніпропетровськ: Дніпроп. держ. ун-т внутр. справ: Ліра ЛТД, 2015. 420 с. Шаблистий В.В., Александрова А.Ю. Кримінальна відповідальністьза ухилення від призову за мобілізацією: монографія. за заг. ред. д.ю.н., доц. В.В. Шаблистого. Дніпро: Видавець Біла К.О., 2019. 200 с.

84. Шаблистий В.В., Галемін О.А. Кримінальна відповідальність за хуліганство, пов'язане з опором особам, наділеними владними повноваженнями під час виконання службових обовязків, чи іншим громадянам, які припиняли хуліганські дії: монографія. Дніпро: Дніпроп. держ. ун-т внутр. справ; Ліра ЛТД, 2017. 164 с.

85. Шаблистий В.В., Ткаченко А.В. Кримінальна відповідальність за дії, що дезорганізують роботу установ виконання покарань: монографія. за заг. ред. д.ю.н., доц. В.В. Шаблистого. Дніпро: Видавець Біла К.О., 2018. 152 с.

86. Шаблистий В.В., Якименко Л.Г. Запобігання проникненню заборонених предметів до установ виконання покарань: монографія. Дніпро: Дніпроп. держ. ун-т внутр. справ; Ліра ЛТД, 2017. 168 с.

87. Шаблистий В.В. Тілесне ушкодження як злочин проти життя та здоров'я людини за кримінальним правом України: монографія / В.В. Шаблистий, В.Ю. Коломієць; за заг. ред. д-ра юрид. наук, доц. В.В. Шаблистого. Дніпро: Видавець Біла К. О., 2020. 164 с.

88. Кримінальна відповідальність за невиконання рішення суду у кримінальному провадженні: моногр. / В. В. Шаблистий, О. В. Чорна; за заг. ред. д-ра юрид. наук, доц. В.В. Шаблистого. Дніпро: Видавець Біла К. О., 2020. 164 с.

89. Шакун В.І. Суспільство і злочинність: Монографія. КИЇВ:Атіка,

2003. 784 с.

90. Шемшученко Ю.С., Титаренко Ю.Л., СкибицкийВ.В., ФилоновА.В. Уголовноенаказание: Монография. Киев-Донецк: Институтгосударства и праваим. В.М. Корецкого НАН Украины, Донецкий інститут внутреннихдел МВД Украины, 1997. 320 с.

91. Шеремет А.П. Злочини проти статевої свободи: Монографія. Чернівці: ТОВ «Видавництво «Наші книги», 2007. 216 с.

92. Шинкаренко І.Р. Основи боротьби з тероризмом: навч. посіб. для вищих навчальних закладів МВС України / Шинкаренко І.Р., Ханькевич А.М., Никифорчук Д.Й. та ін. МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. – Луганськ: РВВ ЛДУВС, 2011. 403 с.

93. Шинкаренко І.Р., Спіціна Г.О. Безпека об'єктів інфраструктури авіаційного транспорту: теоретичні аспекти. Вісник Дніпропетровського державного університету внутрішніх. 2020. №2. С. 253-262. включено до міжнародної науково метричної бази Index Copernicus International (Республіка Польща, Варшава), «Перелік Б МОН України» DOI: DOI: 10.31733/2078-3566-2020-2-253-262

94. Ященко А.М. Застосування заходів кримінально-правового характеру: монографія. Х.: НікаНова, 2014. 388 с.

95. Mykola Nechyporuk, Oleksandr Kliuiev, Aleksandar Ivanović, Nataliia Filipenko (2021) Development Strategy of International Cooperation of Forensic Science Institutions of Ukraine with Foreign Experts in Prevention of Terrorist Attacks on Aerospace Industry and Critical Infrastructure. Integrated Computer Technologies in Mechanical Engineering – 2021. Synergetic Engineering Pp. 825-848. Presents the proceedings of the ICTM´21 Conference held in Kharkov, Ukraine, at November 28–29, 2021. ISBN: 978-3-030-94259-5 (eBook). URL: https://link.springer.com/chapter/10.1007/978-3-030-94259-5_64

96. Nataliia Filipenko, Svetlana Andrenko (2021) Principles of criminological activity of forensic science institutions of Ukraine Sud ekspertizasi: kecha va bugun. Respublika ilmiy-amaliy konferensiya materiallari // Mas'ul muharrir: A.U.Xalilov. X.Sulaymonova nomidagi Respublika sud ekspertizasi markazi. – Toshkent: Respublika sud ekspertizasi markazi, 2021 (Материалы научно-практической конференции "СУДЕБНАЯ ЭКСПЕРТИЗА: ВЧЕРА И СЕГОДНЯ", посвящённой 70-летию Республиканского центра судебной экспертизы им. Х. Сулаймановой 30 июнь – 1 июль 2021 года). P. 46-49.

97. Filipenko N., & Bublikov A. As for determination of certain stages of preventive forensic expert activity. Права людини в Україні: минуле, сьогодення, майбутнє : тези доп. учасників Всеукр. наук.-практ. конф. (Харків, 10 груд. 2020 р.). Харків: НДІ ППСН, 2020. С. 136-138. URL: https://library.pp-ss.pro/index.php/ndippsn_20201120/article/view/filipenko.

98. Vladislav Fedorenko & Natalia Filipenko & Inesa Shumilo & Volodymyr Nesterovych & Svitlana Nischymna, (2021) Entrepreneurial activity of the IT sector in the conditions of the COVID-19 pandemic and in the post-quarantine period. Entrepreneurship and Sustainability Issues, VsI Entrepreneurship and Sustainability Center, vol. 8(4), pages 697-712, June.

Handle: RePEc:ssi:jouesi:v:8:y:2021:i:4:p:697-712DOI: 10.9770/jesi.2021.8.4(43) (Wed of Science)

99. Dzhuzha, O. M., Vasylevych, V. V., Telefanko, B. M., & Filipenko, N. E. 2021 The Criminological Principles of Crime Prevention in the Field of Physical Culture and Sports of Ukraine. DIXI, 23(2), 1-25. https://revistas.ucc.edu.co/index.php/di/article/view/3980/3174 (Wed of Science).

100. Nechyporuk, M., Pavlikov, V., Ivanović, A., Filipenko, N. (2021) Forensic Science Posibilities Within The Framework Of Criminal Proceedings While Aviation Accidents (Review Article). Archives of Criminology and Forensic Sciences. 1(3). 56-66. DOI: https://doi.org/10.32353/acfs.3.2021.05

101. Mykola Nechyporuk, Volodymyr Pavlikov, Nataliia Filipenko, Hanna Spitsyna, Ihor Shynkarenko Cyberterrorism Attacks on Critical Infrastructure and Aviation: Criminal and Legal Policy of Countering. Conference on Integrated Computer Technologies in Mechanical Engineering–Synergetic Engineering ICTM 2020: Integrated Computer Technologies in Mechanical Engineering. 2020 pp 206-217(Indexed by SCOPUS, INSPEC, WTI Frankfurt eG, zbMATH, SCImago More information about this series at. URL: http://www.springer.com/series/15179 https://doi.org/10.1007/978-3-030-66717-7.

102. Filipenko N. Ye., Spitsyna H. O. Forensic prevention: the concept of implementation in Ukraine. Challenges of legal science and education: an experience of EU countries and introduction in Ukraine : Collective monograph. Riga, Latvia : “Baltija Publishing”, 2020. P. 408-431. DOI https://doi.org/10.30525/978-9934-26-007-0-23.

103. Nataliia Filipenko, Hanna Spitsyna, Ihor Shynkarenko, Vitalii Tsymbalistyi. Implementation of Preventive Activity; Foreign Experience in Criminological Work of Forensic Science Institutions Socrates: Rīgas Stradiņa universitātes Juridiskās fakultātes elektroniskais juridisko zinātnisko rakstu žurnāls = Rīga Stradiņš University Faculty of Law Electronic Scientific Journal of Law. Rīga: RSU, 2021, Nr. 1 (19). P. 32-39.

104. Vladislav Fedorenko & Natalia Filipenko & Inesa Shumilo & Volodymyr Nesterovych & Svitlana Nischymna, 2021 Entrepreneurial activity of the IT sector in the conditions of the COVID-19 pandemic and in the post-quarantine period. Entrepreneurship and Sustainability Issues, VsI Entrepreneurship and Sustainability Center, vol. 8(4), pages 697-712, June.Handle: RePEc:ssi:jouesi:v:8:y:2021:i:4:p:697-712 DOI: 10.9770/jesi.2021.8.4(43).

105. Filipenko N. Ye. Identification of crime determinants while performing forensic expert activities // Proceedings of VI International scientific conference “Scientific achievements during the rapid technological development”. Berlin, tredition GmbH, 2019. P. 161-167.

12. Інформаційні ресурси

1. Правовий портал «Ліга: Закон» - законодавство України: http://search.ligazakon.ua/

2. Верховна Рада України. URL : https://www.rada.gov.ua/
3. Президент України. URL : https://www.president.gov.ua/ru
4. Верховний Суд. URL: https://supreme.court.gov.ua/supreme/gromadyanam /perelik_sprav/
5. Офіс Генерального прокурора України. URL: https://www.gp.gov.ua/ua/index.html
6. Національна академія правових наук України. URL: http://www.aprnu.kharkiv.org/
7. Конституційний Суд України. URL : https://ccu.gov.ua/.
8. Газета "Урядовий кур'єр" URL : http://ukurier.gov.ua/uk/
9. Газета "Юридична практика" URL : http://presa.ua/juridicheskaja-praktika.html
10. Міністерство внутрішніх справ України. URL : https://mvs.gov.ua/uk/contacts/ministry-internal-affairs.
11. Міністерства Юстиції України www.gdo.kiev.ua
12. Єдиний державний реєстр судових рішень. URL : https://reyestr.court.gov.ua/
13. Національна бібліотека України ім. В. І. Вернадського. URL : http://www.nbuv.gov.ua/
14. Бібліотечно-бібліографічні ресурси Верховної Ради України. URL : http://lib.rada.gov.ua/static/about/wellcome.html
15. Національна бібліотека України імені Ярослава Мудрого. URL : https://nlu.org.ua/
16. Науково-технічна бібліотека Національного аерокосмічного університету ім. М.Є Жуковського (ХАІ). URL : https://library.khai.edu/