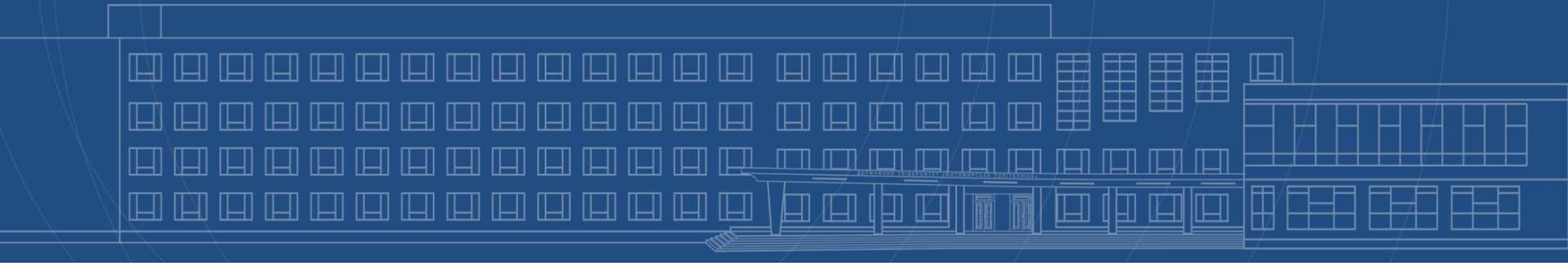
ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

@ZTUEDUUA

Тема 14. Правові механізми протидії кіберзлочинності



ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

@ZTUEDUUA

ПЛАН ЛЕКЦІЇ

1. Правова природа кіберзлочинів та їх класифікація.
2. Система суб’єктів протидії кіберзлочинності.
3. Кримінально-правові та кримінально-процесуальні механізми протидії кіберзлочинам
4. Міжнародні правові механізми протидії кіберзлочинності

Вступні питання для дискусії:

1. Чи може держава повноцінно контролювати свій інформаційний простір, якщо фізична інфраструктура (сервери, супутники Starlink) належить приватним іноземним корпораціям? Де закінчується суверенітет України в мережі Інтернет?
2. Чи можна вважати кібератаку «збройним нападом» у розумінні Статуту ООН? Чи має право держава відповісти на цифрову атаку реальною зброєю?
3. Як Ви вважаєте, чи є криптовалютні маніпуляції та «фішинг» загрозою національній економічній системі, чи це лише приватні спори між банком та клієнтом?
4. Головна проблема кіберпростору – анонімність. Як юридично довести, що за атакою хакерів стоїть конкретна держава-агресор, а не група «фрілансерів»? Які стандарти доказування мають бути застосовані?»
5. Чи має право держава в умовах воєнного стану на тотальний моніторинг трафіку громадян для виявлення диверсантів? Де межа між «кіберзахистом» та «цифровим тоталітаризмом»?

Кіберзлочинність можна розглядати як трансформацію способу посягання на фундаментальні права людини, інтереси суспільства та безпеку держави.

Кіберпростір – віртуальний простір, де цифрова інформація є об'єктом, засобом і середовищем вчинення правопорушення. Правова природа кіберзлочину полягає в тому, що він порушує цілісність (integrity), доступність (availability) та конфіденційність (confidentiality) даних

В межах концепції кримінальних правопорушень проти економічної системи, кіберзлочини розглядаються як використання високотехнологічних економічних інструментів (цифрові активи, платіжні шлюзи, бази даних) для незаконного збагачення або дестабілізації державних інститутів.

Юридична природа кіберзлочину заперечує класичний принцип територіальності (злочинець у Києві, сервер у Панамі, потерпілий у Берліні). Це створює потребу в уніфікації кримінального права на міжнародному рівні.

Об’єкт та суб’єкт кіберзлочину

Юридичні ознаки кіберзлочину:

- висока латентність: велика частина злочинів залишається нелатентною через небажання бізнесу повідомляти про злами (репутаційні ризики);
- дистанційність: відсутність фізичного контакту між злочинцем та жертвою.
- швидкість: злочин може тривати секунди, а його наслідки (наприклад, банкрутство банку) бути незворотними;
- складність доказування: необхідність роботи з «цифровими слідами», які легко видалити або підробити.

Родовий об’єкт: Суспільні відносини щодо забезпечення інформаційної безпеки та правомірного використання електронно-обчислювальних машин (ЕОМ).

Безпосередній об’єкт: Право власності на інформацію, цілісність автоматизованих систем, стабільність критичної інфраструктури.

Предмет: Суспільні відносини щодо забезпечення інформаційної безпеки та правомірного використання електронно-обчислювальних машин (ЕОМ).

Суб’єкт: Характеризується «цифровим розривом» — часто це особи з високим інтелектуальним рівнем, що потребує специфічних методів профілювання.

Традиційний підхід, закріплений у Будапештській конвенції про кіберзлочинність, поділяє їх на чотири основні групи:

1. Злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем:

I. ннезаконний доступ (Hacking) – порушення встановлених правил доступу до системи.
II. езаконне перехоплення – технічні засоби перехоплення непублічних передач даних.
III. втручання у дані – пошкодження, видалення, погіршення чи зміна комп'ютерних даних.
IV. втручання у роботу системи – серйозне перешкоджання функціонуванню системи (наприклад, DDoS-атаки).

2. Злочини, пов'язані з комп'ютерами (Computer-related offences):

Комп'ютерне шахрайство

- введення,
- зміна,
- видалення даних з метою отримання економічної вигоди (ключовий елемент економічних злочинів).

Комп`ютерне підроблення

Створення фальшивих цифрових документів

3. Злочини, пов'язані з контентом (Content-related offences):

Розповсюдження матеріалів, що пропагують насильство, жорстокість, тероризм або дитячу порнографію.

4. Злочини, пов'язані з порушенням авторського права та суміжних прав: масштабне піратство та незаконне використання інтелектуальної власності в мережі.

В контексті національної безпеки України (згідно зі Стратегією кібербезпеки), доцільно виділяти:

- кіберзлочинність (Cybercrime) – корисливі злочини приватних осіб;
- кібертероризм (Cyberterrorism) – атаки на критичну інфраструктуру з метою залякування (енергетика, водопостачання, транспорт);
- кібершпигунство (Cyberspionage) – крадіжка державних таємниць або інтелектуальної власності в інтересах інших держав;
- кіберагресія (Cyber warfare) – координовані атаки суб'єктів іноземних держав як складник гібридної війни.

Основним профільним законом у цій сфері є Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року (№ 2163-VIII), виконує три ключові функції:

1. **Легалізація термінології** – вперше на законодавчому рівні закріпив визначення таких понять, як «кібербезпека», «кіберзахист», «кіберзлочинність», «кібертероризм», «критично важливі об'єкти інфраструктури» та «інцидент кібербезпеки». Без цих дефініцій неможлива кваліфікація злочинів у суді..

***2. Р*озподіл повноважень** – розмежовує функції СБУ, Кіберполіції, Держспецзв'язку ;

***3.* Впроваджує принцип державно-приватного партнерства,** зобов'язуючи приватні компанії (банківські системи, енергомережі) співпрацювати з державними органами у разі атак.

Окрім базового закону, правове поле кібербезпеки формують:

1. **Форми Закон України «Про захист інформації в інформаційно-комунікаційних системах»:** Регулює технічні вимоги до захисту даних.
2. **Закон України «Про критичну інфраструктуру»:** Визначає перелік об'єктів, кіберзахист яких є пріоритетом №1 для держави.
3. **Стратегія кібербезпеки України: (Затверджується Указом Президента) –** програмний документ, що визначає актуальні загрози на найближчі роки (наприклад, протидія російській цифровій агресії).
4. **Міжнародний профільний акт –** Конвенція про кіберзлочинність (Будапештська конвенція), ратифікована Україною. Вона є частиною національного законодавства і визначає міжнародні стандарти, до яких Україна адаптувала свій Кримінальний кодекс.

Система суб’єктів протидії кіберзлочинності та забезпечення кібербезпеки

Координаційні органи:

1. Рада національної безпеки і оборони України (РНБО): здійснює стратегічне управління.
2. Національний координаційний центр кібербезпеки (НКЦК): робочий орган РНБО. «Ааналітичний хаб», де здійснюється обмін інформацією між державними органами та приватним сектором у режимі реального часу.

Основні суб’єкти

Згідно зі ст. 8 профільного Закону, виділяють наступних суб’єктів:

1. **Державна служба спеціального зв’язку та захисту інформації України (Держспецзв’язку)** – регулятор та головний виконавець технічного захисту.
CERT-UA (Державна команда реагування на комп’ютерні надзвичайні події) – захист державних інформаційних ресурсів та критичної інфраструктури, методичне керівництво, сертифікація засобів захисту.

2. **Служба безпеки України (СБУ). Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки (ДКЗІБ).** Сфера відповідальності: боротьба з кібертероризмом, кібершпигунством, протидія деструктивному впливу спецслужб агресора, захист об’єктів критичної інфраструктури від диверсій.

3. **Національна поліція України. Департамент кіберполіції.** Сфера відповідальності: боротьба з «класичною» кіберзлочинністю (фішинг, кардинг, комп’ютерне шахрайство, розповсюдження вірусів, несанкціоноване втручання). Саме кіберполіція є головним органом досудового розслідування кіберзлочинів.

4. **Міністерство оборони України та Генеральний штаб ЗСУ.** Сфера відповідальності: відсіч збройній кіберагресії, ведення кіберрозвідки, забезпечення кіберзахисту інформаційно-комунікаційних систем ЗСУ. Україна офіційно формує Кібервійська як окремий рід сил.

5. **Розвідувальні органи (СЗРУ, ГУР МО).** Сфера відповідальності: здобуття інформації про загрози в кіберпросторі з боку інших держав та угруповань поза межами України.

6. **Національний банк України (НБУ).** Сфера відповідальності: кібербезпека в банківській та фінансовій сферах. НБУ створив власний Центр кіберзахисту (CSIRT-NBU) для моніторингу загроз фінансовій стабільності.

Суб’єкти приватного сектору та громадянське суспільство

Оператори критичної інфраструктури: (обленерго, водоканали, телеком-оператори) зобов’язані забезпечувати захист власних мереж згідно з державними вимогами.
Кіберспільнота та «White Hat Hackers»: залучення етичних хакерів (Bug Bounty програми) для виявлення вразливостей у державних системах.

ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

@ZTUEDUUA

ПИТАННЯ ДЛЯ ОБГОВОРЕННЯ

Де закінчується компетенція Кіберполіції (шахрайство) і починається компетенція СБУ (кібертероризм), якщо атака вчинена кримінальним угрупованням, але за гроші агресора?

Кримінально-правова характеристика (Розділ XVI КК України)

Основою протидії кіберзлочинності в Україні є Розділ XVI Особливої частини КК України («Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку»).

Основні склади злочинів:

Стаття 361. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних мереж.

Об'єкт: цілісність та доступність систем.

Стаття 361-1. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів (віруси, шифрувальники).

Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в системах, вчинені особою, яка має право доступу до неї (інсайдерська корупція/злив даних).

Стаття 363-1. Перешкоджання роботі систем шляхом масового розповсюдження повідомлень (DDoS-атаки, спам).

Бланкетність норм:

- для правильної кваліфікації необхідно звертатися до Закону «Про захист інформації в інформаційно-комунікаційних системах».

- На відміну від класичних економічних злочинів, шкода в кіберзлочинах часто виражається не в грошах, а в порушенні цілісності даних або призупиненні роботи сервісів.

Кримінально-процесуальні механізми (Робота з електронними доказами)

Процесуальна діяльність у сфері кібербезпеки регламентується КПК України з урахуванням специфіки «цифрового сліду».

1. Електронні докази (ст. 99 КПК України):

Електронним документом є документ, інформація в якому зафіксована у вигляді електронних даних.

Проблема автентичності: *Як довести в суді, що скріншот листування або лог-файл сервера не був змінений? Це потребує обов'язкового створення хеш-суми (цифрового відбитка) під час вилучення.*

2. Особливості слідчих дій:

- Тимчасовий доступ до речей і документів: найчастіше застосовується до провайдерів телекомунікацій для отримання IP-адрес та даних про трафік.
- Зняття інформації з електронних комунікаційних мереж (ст. 263 КПК): НСРД, що дозволяє перехоплювати дані в реальному часі.
- Огляд та обшук: вилучення техніки має проводитися із залученням спеціаліста (кіберполіцейського) для уникнення дистанційного знищення даних (remote wipe).

Важливо:

Кіберзлочин є високотехнологічним способом вчинення традиційних злочинів (шахрайство – ст. 190, легалізація доходів – ст. 209).
Використання вразливостей банківських систем (SWIFT, API) для виведення капіталу за межі держави.
Кіберзлочинність є основою для «тіньової цифрової економіки» (Darknet), яка підриває фінансову стабільність держави.

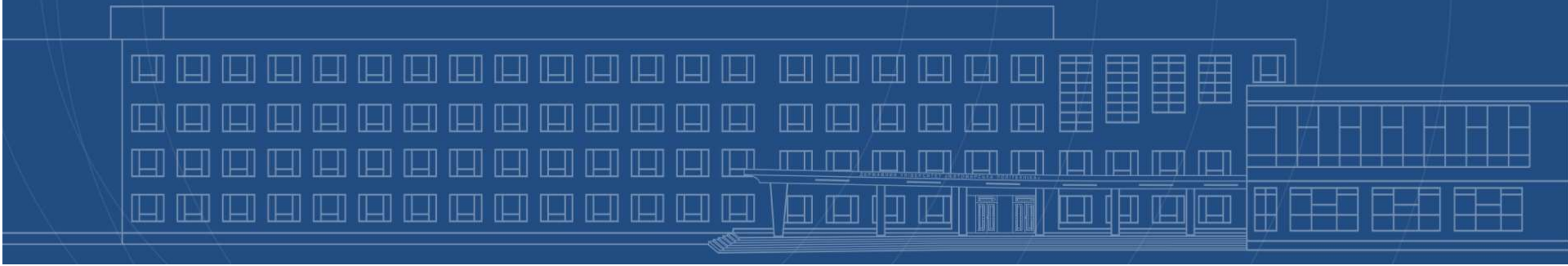
3. Міжнародна співпраця (24/7 Network):
Згідно з Будапештською конвенцією, Україна є частиною мережі цілодобової допомоги.
Це дозволяє негайно (протягом годин) заблокувати сервер у США чи ЄС за запитом українських слідчих до винесення офіційної ухвали суду.

ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

@ZTUEDUUA

ПИТАННЯ ДЛЯ ОБГОВОРЕННЯ

Чи може цифрова копія жорсткого диска вважатися оригіналом доказу, якщо оригінальний носій був знищений під час бойових дій? Як змінюються стандарти доказування в умовах хмарного зберігання даних (Cloud Computing), коли фізично сервер знаходиться поза юрисдикцією України?



Міжнародно-правове регулювання у цій сфері базується на принципах гармонізації кримінального законодавства та спрощення процедур надання правової допомоги.

Конвенція про кіберзлочинність (Будапештська конвенція, 2001) – єдиний юридично обов'язковий міжнародний договір у цій сфері, який став фундаментом для українського законодавства.

Базується на:

1. *Гармонізації*. Вимога до держав-учасниць криміналізувати однакові діяння (незаконний доступ, втручання в дані тощо).
2. *Процесуальні повноваження*. Встановлення процедур вилучення комп'ютерних даних, їх збереження та перехоплення в реальному часі.
3. *Міжнародна допомога*. Створення системи швидкого реагування.
4. *Мережа 24/7:* Спеціальний пункт зв'язку в кожній країні (в Україні – у структурі Кіберполіції), який працює цілодобово для надання негайної допомоги у транскордонних розслідуваннях.
5. *Другий додатковий протокол (2022):* Найновіший інструмент, спрямований на пряму співпрацю з сервіс-провайдерами (наприклад, Google, Meta) в інших юрисдикціях для отримання даних без тривалих процедур MLA.

Європейські механізми та Директиви ЄС

В межах євроінтеграції Україна адаптує свої норми до стандартів ЄС:

1. **Директива NIS (2016) та NIS2 (2022):** Встановлюють вимоги до безпеки мережевих та інформаційних систем для критично важливих секторів (енергетика, транспорт, охорона здоров'я).

2. **EU Cybersecurity Act**: Посилює роль ENISA (Агентства ЄС з питань кібербезпеки) та запроваджує загальноєвропейську сертифікацію кібербезпеки для IT-продуктів.

3. **GDPR (Загальний регламент про захист даних)**: Хоча це акт про приватність, він містить жорсткі вимоги до кібербезпеки персональних даних, порушення яких тягне величезні штрафи.

Регіональні та двосторонні угоди:

- Співпраця з Європолом та Інтерполом: Участь України в об'єднаних слідчих групах (JIT) для ліквідації транснаціональних ботнетів та крипто-шахрайських мереж.
- Двосторонні меморандуми: Наприклад, активна співпраця між Україною та США (FBI/CISA) у боротьбі з російськими державними хакерськими угрупованнями (APT).

Проблема атрибуції та «Талліннське керівництво» (Tallinn Manual 2.0)

Це найавторитетніше науково-правове видання (хоч і не є договором), що аналізує, як міжнародне право війни застосовується до кіберпростору.
Атрибуція: Проблема доказування зв'язку між хакером та державою.
Право на самооборону: Коли кібератака вважається "збройним нападом", що дає право на відповідь відповідно до ст. 51 Статуту ООН?

ВАЖЛИВО:

Міжнародні механізми сьогодні трансформуються від «допомоги у справах проти хакерів-одинаків» до системної протидії державному тероризму в цифровій сфері.
Кіберзлочинність використовується агресором як інструмент економічного виснаження жертви.
Міжнародні санкції за кібератаки стають окремим видом правового реагування (Cyber Sanctions Regime ЄС).

Питання для дискусії:

1. Чи має нести кримінальну або цивільну відповідальність розробник програмного забезпечення (наприклад, Microsoft або Apple), якщо через критичну вразливість у їхньому коді сталася атака на об’єкт критичної інфраструктури України?
2. Що є більш ефективним інструментом стримування державних хакерських угруповань: оголошення їх у міжнародний розшук чи накладення секторальних санкцій на ІТ-сектор країни-агресора?

Питання для рефлексії:

I. *Як ви ставитеся до діяльності «хактивістів» (наприклад, IT-army of Ukraine), які здійснюють атаки на інфраструктуру ворога? Чи може благородна мета виправдовувати вчинення діянь, що мають ознаки складів злочинів Розділу XVI КК України?*

II. *Як поява «цифрових слідів» змінює роль класичного слідчого та адвоката? Чи повинен сучасний юрист володіти навичками кодування, щоб бути ефективним у справах про кіберзлочини?*

III. *Чи готові ви особисто поступитися частиною своєї приватності (наприклад, надати державі доступ до зашифрованих месенджерів), якщо це гарантуватиме 100% захист країни від кібертероризму?*

Кіберпростір – це новий домен ведення війни та боротьби за економічне домінування, де право має стати не перешкодою, а надійним щитом

ЖИТОМИРСЬКА ПОЛІТЕХНІКА
ДЕРЖАВНИЙ УНІВЕРСИТЕТ

@ZTUEDUUA

Завдання для самостійної роботи

1. Проаналізувати правову природу та класифікацію кіберзлочинів.
2. Дослідити систему суб’єктів протидії кіберзлочинності.
3. Підготувати аналітичний огляд міжнародно-правових механізмів протидії кіберзлочинності

Лектор
Віталій Вихристюк - заступник начальника Поліського управління кіберполіції (до 2017 р). начальний безпеки ПП QOOBIX, IT LAB

@ZTUEDUUA

ЖИТОМИРСЬКА ПОЛІТЕХНІКА

ДЕРЖАВНИЙ УНІВЕРСИТЕТ

- **Розвиваємо лідерів**
- **Створюємо інновації**
- **Змінюємо світ на краще**