Міністерство освіти і науки України
Чорноморський національний університет імені Петра Могили
Факультет політичних наук
Кафедра міжнародних відносин та зовнішньої політики

# ІНФОРМАЦІЙНА БЕЗПЕКА КРАЇН ЄС: СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ

**АВТОРЕФЕРАТ**

дипломної роботи

на здобуття освітнього ступеню «магістр»

Виконав:
студент VI курсу групи 691
Спеціальність: 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
**Білоусов Микита Валерійович**
Науковий керівник:
к.і.н., доцент кафедри МВ та ЗП
**Вовчук Людмила Анатоліївна**

Миколаїв – 2021

# ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

**Актуальність теми.** Необхідно зазначити, що інформація – це важливий ресурс людства у XXI столітті. Глобалізація ставить нові виклики перед країнами ЄС, адже інформаційне суспільство стане в найближчі роки рушійною силою економічних, соціальних та технологічних змін і впливатиме на функціонування суспільства в цілому, надаючи більш широкі можливості зв'язку й обміну інформацією, зокрема, на транскордонному рівні, через глобалізацію широко доступних для суспільства мереж і служб. Важливе значення це має на європейському рівні, насамперед, стосовно культурної і мовної різноманітності та з економічного погляду.

Для Європейського Союзу інформаційна безпека має важливе значення, оскільки є невід'ємною складовою безпеки держави, кожного окремого громадянина, безпеки всієї організації. Усі ці складові врівноважує ЄС у принципах інформаційної безпеки, які застосовує в зазначеному напрямку. Вироблені в ЄС підходи до забезпечення інформаційної безпеки, що відображають узгоджену волю держав-членів та інституцій ЄС, можна розглядати як європейські рамкові стандарти в цій сфері, які можуть успішно застосовуватися різними країнами з урахуванням їх адаптації до особливостей національних правових систем і соціокультурної специфіки.

Досвід Європейського Союзу у цій сфері може бути задіяний й щодо України, де питання «інформаційної безпеки», враховуючи загострені двосторонні відносини з Російською Федерацією (створення за підтримки «східного агресора» терористичних організацій «ДНР», «ЛНР», окупація Криму) є номером один. Успішність реалізації програм інформаційної безпеки ЄС доводить вдале подолання інформаційних небезпек цією європейською структурою. Це власне й визначає актуалізацію даної тематики.

**Об'єктом дослідження** є інформаційна безпека країн ЄС.

**Предметом дослідження** є стан та перспективи розвитку інформаційної безпеки країн ЄС.

**Хронологічні рамки** дослідження охоплюють період з 2001 по 2020 рр.. *Нижня межа* пояснюється впровадженням основ європейської політики щодо забезпечення мережевої інформаційної безпеки (2001 р.). *Верхня межа* - реалізацією Закону про захист персональних даних в ЄС (2020 р.). Потрібно зазначити, що автор виходить за дані хронологічні рамки з метою більш ґрунтовного висвітлення досліджуваної тематики.

**Територіальні рамки** цього дослідження охоплюють територію країн-членів Європейського Союзу (Австрія, Бельгія, Болгарія, Греція, Данія, Естонія, Ірландія, Іспанія, Італія, Кіпр, Латвія, Литва, Люксембург, Мальта, Нідерланди, Німеччина, Польща, Португалія, Румунія, Словаччина, Словенія, Угорщина, Фінляндія, Франція, Хорватія, Чехія, Швеція), а також США.

**Мета** роботи полягає у аналізі стану та перспектив розвитку інформаційної безпеки країн ЄС.

Відповідно до мети поставлені наступні **завдання:**

- висвітлити стан наукової розробки теми, джерельну базу та теоретико-методологічну основу дослідження;
- розглянути базові принципи інформаційної політики безпеки ЄС та охарактеризувати засади сучасної кіберстратегії ЄС;
- проаналізувати загальну концепція політики інформаційної безпеки ЄС;
- дослідити ЗМІ та соціальні мережі як інструменти маніпулювання електоральною поведінкою громадян західноєвропейських кран;
- охарактеризувати безпеку е-врядування та захист персональних даних в країнах ЄС як основний принцип політики інформаційної безпеки;
- сформувати практичні рекомендації щодо розвитку політики провідних країн ЄС у сфері інформаційної безпеки.

**Наукова новизна** дослідження визначається актуальністю досліджуваної проблеми і тим, що запропонована тема є недостатньо вивченою у вітчизняній історіографії та полягає у тому, що у рамках проведеного наукового дослідження:

- здійснений комплексний аналіз принципів інформаційної політики безпеки ЄС, засад сучасної кіберстратегії ЄС, загальної концепції політики інформаційної безпеки ЄС;
- отримала подальшої систематизації історіографія проблеми та джерельна база дослідження;
- запропоновані практичні рекомендації щодо розвитку політики провідних країн єс у сфері інформаційної безпеки.

**Практичне значення роботи** полягає в тому, що магістерську роботу написано в наукових і навчальних цілях. Матеріали дипломної роботи можуть бути використані при написанні дисертаційних робіт, навчальних посібників і підручників, а також під час викладання загальних і спеціальних курсів, таких як «Міжнародні відносини та світова політика», «Україна та ЄС», «Зовнішня політика країн Європейського Союзу», «Міжнародна та європейська безпека».

**Апробація результатів дослідження.** Основні положення та висновки цього дослідження були представлені на розгляд у вигляді виступів на наукових конференціях, зокрема, у IX Всеукраїнській науковій конференції «Історико-філософські дослідження молодих учених» (м. Суми, СумДПУ імені А. С. Макаренка, 22-23 квітня 2021 р.); Міжнародній науково-практичній конференції «Принциповий прагматизм ЄС – наслідки для Східної та Південно-Східної Європи: політичні, економічні, правові та комунікаційні аспекти» (м. Київ, Інститут міжнародних відносин КНУ ім. Тараса Шевченка, 21-22 травня 2021 р.).

**Публікації.** За темою дослідження було опубліковано двоє тез (у збірниках вищевказаних конференцій) та статтю у співавторстві з

к.і.н., доцентом кафедри міжнародних відносин та зовнішньої політики А.О. Хмель у науковому журналі «Вісник Львівського університету».

**Структура роботи** відбиває поставлені перед дослідженням цілі та завдання. Загальний обсяг її становить 103 сторінки, з них основного тексту – 91 сторінка. Дипломна робота складається зі вступу, 4 розділів, 8 підрозділів, висновків, списку використаних джерел і літератури (98 найменувань українською, російською, англійською мовами).

## ОСНОВНИЙ ЗМІСТ МАГІСТЕРСЬКОЇ РОБОТИ

У **вступі** обґрунтовано актуальність теми, визначено мету та завдання роботи, об'єкт та предмет дослідження; зазначено методи дослідження, сформульовано наукову новизну, з’ясовано практичне значення отриманих результатів, їх апробація, окреслено структуру роботи.

У першому розділі **«Концептуально-теоретичні засади дослідження, джерельна база та стан наукової розробки проблеми»** подається аналіз стану наукової розробки та джерельної бази, проаналізовано понятійно-категоріальний апарат, принципи, підходи та методи дослідження проблеми. Використану в роботі літературу автор класифікував за територіальним критерієм, виділяючи роботи вітчизняних авторів, праці російських науковців і англомовних авторів.

На думку автора вітчизняні науковці останнім часом активно опікуються дослідженням даної тематики, але їх увага більше прикута до розгляду стану інформаційної безпеки України, що абсолютно логічно. Характеризуючи джерельну базу роботи, автор підкреслює, що вона є достатньою для розкриття теми і складається переважно з іншомовних джерел (зокрема, англійською мовою), що відповідно вимагає від автора більш ґрунтовного підходу до їх опрацювання. Такої історіографічної та джерельної баз виявилося цілком достатньо для того аби здійснити об’єтивне, насичене фактами дослідження.

Окрім того, у першому розділі автор дійшов висновку, що *«інформаційна безпека»* – це стан захищеності інформації та інфраструктури, яка її підтримує від випадкових або навмисних впливів природного або штучного характеру (інформаційних загроз, загроз інформаційній безпеці), які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин.

Під час дослідження інформаційної політики країн ЄС автор використовує комплекс загально-історичних та загальнонаукових методів. Зокрема автор звернувся до методів аналізу і синтезу, індукції та дедукції, узагальнення, описового, хронологічного, діахронного методу, методу узагальнення, групування. Комплексне дослідження було б неможливе без використання системного методу, який дозволяє дослідити об'єкт дипломної роботи, враховуючи вплив як зовнішніх так і внутрішніх факторів.

У другому розділі **«Сутність і зміст інформаційної безпеки в ЄС»** надається інформація щодо базових принципів інформаційної політики безпеки ЄС та засад сучасної кіберстратегії ЄС. Автор схиляється до думки, що до принципів забезпечення інформаційної безпеки в ЄС можна віднести: законність, баланс інтересів особистості, суспільства і держави, комплексність, системність, інтеграцію з міжнародними системами безпеки, економічну ефективність і т.д.

Найбільш важливим в інформаційній політиці ЄС є принцип безперервності вдосконалення і розвитку системи інформаційної безпеки. Суть його полягає в постійному контролі функціонування системи, у виявленні її слабких місць, можливих каналів витоку інформації і несанкціонованого доступу, оновлення та доповнення механізмів захисту в залежності від зміни характеру внутрішніх і зовнішніх загроз, обґрунтуванні і реалізації на цій основі найбільш раціональних методів, способів і шляхів захисту інформації.

Одним з семи стовпів Стратегії «Європа – 2020», запропонованої Європейською Комісією, є «Цифровий порядок денний для Європи»,

пов’язаний з використанням потенціалу ІКТ для стимулювання інновацій, економічного зростання і прогресу. Включення її в зміст базового стратегічного документа ЄС на найближче десятиліття показує, що розвиток ІКТ та інформаційного суспільства залишаються одним з найважливіших стратегічних пріоритетів ЄС і розглядаються як необхідна умова подальшого прогресу європейських країн. Основною метою цієї ініціативи є розвиток єдиного цифрового ринку для забезпечення розумного, стійкого і загального зростання в Європі. Мета стратегії кібербезпеки ЄС «Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace» (Стратегія кібербезпеки ЄС: відкритий, надійний та безпечний кіберпростір) – підвищення стійкості і нарощування потенціалу в області кібербезпеки держав-членів ЄС (посилення боротьби з кіберзлочинністю, формування ефективної інфраструктури забезпечення безпеки, розробка принципів міжнародної політики в області кібербезпеки).

У третьому розділі «**Механізми та правове забезпечення захисту інформації в європейських країнах**» також акцентується увага на розкритті Загальної концепції політики інформаційної безпеки ЄС. Активна діяльність інститутів ЄС у сфері гарантування безпеки інформаційного суспільства здійснювалася насамперед в рамках першої (Європейське Співтовариство) і третьої опори (співробітництво поліцій і судів у кримінально правовій сфері).

Після тривалих консультацій у липні 2005 р. Міністр закордонних справ Швеції Марго Вальстрем представила Комісії свої пропозиції щодо модернізації практики комунікацій («План дій щодо культури інформаційної політики в країнах ЄС»). Під її керівництвом було також розроблено «План Д: демократія, діалог та дебати» (жовтень 2005 р.) і, нарешті, «Біла книга щодо комунікаційної політики ЄС».

Також автор магістерської роботи стверджує, що для західноєвропейських країн тривалий час доволі актуальним питанням був перехід від традиційних форм політичної участі до більш сучасних. На сучасному етапі інформаційні технології у політичних процесах набули

особливого пожвавлення, що в політичній науці відобразилося появою такого поняття як електронна демократія. В епоху цифрових технологій під час виборчих кампаній соціальні медіа та ЗМІ демонструють значну пріоритетність над традиційними засобами впливу на електоральну поведінку громадян. Відбулася трансформація відносин між світом політики, ЗМІ та громадянами.

Для підвищення довіри до цифрового середовища необхідно забезпечити захист персональних даних і захист об'єктів критичної інфраструктури. Зрозуміло, що збій в роботі об'єктів критичної інфраструктури може відбитися на безпеці і добробут не тільки окремих держав, а й самого ЄС в цілому. Серйозні наслідки може мати втрата контролю над персональними даними. Сьогодні уже сформувалася «тіньова» цифрова економіка, в якій ключовим товаром є дані. Для усунення прогалин у наднаціональному регулюванні протидії атакам на об'єкти критичної інфраструктури в 2016 р. була прийнята Директива про мережеву та інформаційну безпеки «The Directive on security of network and information systems» («Директива про безпеку мережевих та інформаційних систем» (NIS Directive)).

У четвертому розділі «**Практичні рекомендації щодо розвитку політики провідних країн ЄС у сфері інформаційної безпеки**» автор наполягає на тому, що для реалізації стратегій кібербезпеки країн ЄС приватний і державний сектори повинні працювати в тісній співпраці, яка повинна здійснюватися за допомогою обміну інформацією, передовими практиками (наприклад, в сфері управління інцидентами), а також навчаннями на державному і пан-європейському рівні. Для досягнення цієї мети передбачається реалізація провідними країнами ЄС системи таких заходів забезпечення безпеки і довіри у сфері інформації: 1) посилення політики в сфері мережевої та інформаційної безпеки; 2) протидія кібератакам на інформаційні системи; 3) впровадження Європейської платформи з кіберзлочинності («European cybercrime platform»); 4) вивчення необхідності створення Європейського центру з кіберзлочинності («European

cybercrime centre»); 5) посилення боротьби з кіберзлочинністю на міжнародному рівні; 6) підтримка готовності до дій щодо забезпечення кібербезпеки на загальноєвропейському рівні; 7) вивчення способів повідомлення користувачів про випадки порушення системи безпеки (втрати, розкрадання або зміни персональних даних); 8) контроль за виконанням телекомунікаційних правил про приватне життя; 9) підтримка механізму повідомлень про незаконний он-лайн контент і кампанії підвищення обізнаності про правила забезпечення безпеки дітей в Інтернеті; 10) стимулювання корпоративного саморегулювання в сфері використання он-лайн послуг.

У **висновках** узагальнено головні результати магістерського дослідження.

1. Питання інформаційної безпеки активно вивчається як вітчизняними, так і закордонними фахівцями, результати досліджень яких можна знайти в їх працях. Серед вітчизняних науковців слід згадати напрацювання У. Хельберг, С. Кудрявцевої, А. Чічановського, В. Карпенка, Г. Почепцова, В. Брежка, Є. Макаренка, О. Юдіна, Л. Куренди, М. Пахніна, М. Лабенської, К. Шапранової, М. Овсіюка, Т. Ткачука, С. Трояна, О. Запорожець.

Слід зазначити, що інформаційна безпека країн ЄС на сучасному етапі досить активно досліджується російськими та західними вченими. На сьогодні існує значний теоретичний та емпіричний матеріал щодо цього питання, який можна віднайти у роботах Ю. Громова, М. Арєєва, Ю. Куришевої, Н. Степанової, В. Гафнера, Дж. Крістова, Дж. Ховорта, У. Могенсена, М. Цану. На основі критичного осмислення теоретичних підходів до інформаційної безпеки вище вказаних науковців можуть бути сформульовані основи єдиної державної політики в галузі забезпечення інформаційної безпеки країнах ЄС: підготовка і реалізація невідкладних заходів щодо вдосконалення політико-правового, методичного, науково-технічного і організаційного забезпечення інформаційної безпеки; розробка цільової комплексної програми боротьби з комп’ютерною злочинністю.

Особливу увагу приділено питанням гідного захисту інформації. Це тим більш актуально, якщо врахувати, що в сучасній дійсності почала даватися взнаки чергова крайність – прагнення до максимальної інформаційної відкритості, полегшено-зневажливі відносин до питань конфіденційності та секретності в роботі з документами.

За допомогою джерельної бази, яка представлена офіційними документами, можна краще зрозуміти, проаналізувати та зробити самостійні висновки, базуючись на різних матеріалах при проведенні цієї дослідницької роботи. Джерельна база дослідження охоплює коло джерел, частина яких вводиться до наукового обігу вперше. Матеріали, використані при написанні роботи, умовно можуть бути поділені на дві групи: 1) міжнародні угоди та договори світового значення; 2) офіційні документи глав держав і урядів країн-учасниць ЄС та документів створених РЄ. Незважаючи на те, що не всі документи є рівнозначними за змістом, їх сукупності, інформаційності та насиченості виявилося достатньо для розкриття теми та досягнення зазначеної перед автором мети.

Методологічну основу дослідження було обрано відповідно до визначеної мети та поставлених завдань. Методологію складають сукупність філософських та загальнонаукових підходів до проблеми реалізації інформаційної безпеки країн ЄС. Для дослідження інформаційної безпеки країн ЄС було використано як загальнонаукові, так і конкретно-наукові методи дослідження обраної теми. Зокрема автор звернувся до методів аналізу і синтезу, індукції та дедукції, узагальнення, історичного методу, тощо.

Автор дійшов висновку, що аналіз існуючих принципів та підходів пізнання, наукових методів та інформаційних джерел дозволяє визначити методологію дослідження інформаційної безпеки країн ЄС. Теоретико-методологічною основою дослідження є метод системного аналізу міжнародних відносин і зовнішньої політики. Використання наукових методів політичного дослідження дозволяє вивчити інформаційну безпеку

ЄС як комплексний процес, виявити фактори, що впливали на формування без пекової політики провідних країн ЄС, визначити місце останніх у системі міжнародних відносин.

2. До принципів забезпечення інформаційної безпеки в ЄС можна віднести: законність, баланс інтересів особистості, суспільства і держави, комплексність, системність, інтеграцію з міжнародними системами безпеки, економічну ефективність і т.д. Найбільш важливим в інформаційній політиці ЄС є принцип безперервності вдосконалення і розвитку системи інформаційної безпеки. Можна визначити 5 пріоритетів сучасної кіберстратегії ЄС: 1) досягнення кіберживттєстійкості; 2) значне скорочення кіберзлочинності; 3) розвиток політики кіберзахисту; 4) розвиток промислових і технологічних ресурсів для кібербезпеки; 5) створення гармонійної міжнародної політики в сфері кіберпростору. У стратегії наголошується, що ЄС вже веде активну роботу щодо захисту громадян від кіберзлочинності. Одним з результатів цієї роботи стало створення Європейського центру протидії кіберзлочинності. Стратегія передбачає розвиток і фінансування мережі національних центрів протидії кіберзлочинності.

3. Загальна концепція інформаційної безпеки ЄС полягає у: а) плані реагування на широкомасштабні кібератаки; б) зміцненні глобальної стабільності через міжнародне співробітництво; в) усуненні загроз онлайн-платформам і надання їм можливості здійснювати позитивний внесок у суспільство; г) підтримці малих і середніх підприємств у конкурентній боротьбі в цифровій економіці; д) інвестування у використання штучного інтелекту. Протягом останніх років європейська інформаційна політика реалізується через стратегії, програми і проекти міжурядових регіональних організацій, таких як Рада Європи, ОБСЄ, Центральноєвропейська Ініціатива, в рамках яких розглядаються і вирішуються проблеми розвитку «інфраструктури», інформаційних комунікаційних магістралей,

телекомунікаційних мереж та проблеми інформаційної економіки, електронної торгівлі тощо.

4. Для вирішення проблем маніпулювання необхідно підвищити рівень грамотності населення щодо небезпеки, що виникає в результаті використання технологій політичного маніпулювання, розвивати культуру споживання інформації та критичність її сприйняття. Обмеження маніпулювання має полягати в проведенні великої кампанії по формуванню критичного ставлення до самого явища.

У пропонованому законі «Про протидію політичному маніпулюванню в Інтернеті» для західноєвропейських країн повинні бути чітко кваліфіковані маніпулятивні техніки і їх специфічні ознаки, а також санкції за маніпулювання в політичній практиці, щоб уникнути загрози легалізації державної цензури і обмеження свободи слова, що в підсумку призведе до монополізації політичного маніпулювання державою. Закон повинен передбачати обмеження маніпулювання незалежно від того, хто передає такі повідомлення і з якими цілями. У відповідному законі має бути передбачено покарання за використання антигуманних способів інформаційного насильства будь-яким актором, а також визначені чіткі рамки інституціоналізації нових маніпулятивних технологій в політиці. Одним з технічних підходів до вирішення проблеми політичного маніпулювання в Інтернеті може стати функція пошукових систем, що класифікує текстову інформацію за вмістом у ній маніпулятивних елементів.

5. Іншим ключовим завданням для розвитку цифрових відносин є захист персональних даних. У 2016 р., у рамках масштабної зміни правового регулювання даної сфери був прийнятий т.зв. званий Загальний регламент щодо захисту даних «General Data Protection Regulation» («Загальний регламент про захист даних» (GDPR)), який замінює Директиву ЄС щодо захисту даних 95/46/ЄС. Цей Регламент покликаний захистити права фізичних осіб щодо обробки персональних даних усіма компаніями, що пропонують свої послуги на європейському ринку.

У 2017 р. ЄК внесено також проект Регламенту про повагу приватного життя та захист персональних даних в електронних комунікаціях. Два цих документа повинні закласти основи регулювання захисту персональних даних в ЄС. При цьому за загальним правилом, Регламенти матимуть пряму дію в державах-членах ЄС без необхідності імплементації їх положень на рівні національного законодавства. Очевидним, таким чином, стає прагнення до уніфікації правового регулювання цієї сфери на всій території ЄС. Більш того, беручи до уваги транскордонний характер передачі даних, частина положень загального Регламенту поширюється на осіб, заснованих за межами ЄС. Сьогодні не зрозуміло, чи будуть провідні торгові партнери ЄС адаптувати своє законодавство з урахуванням цих змін, але можливо Загальний регламент вплине на загальносвітовий порядок обробки персональних даних.

6. Автор магістерської роботи вважає за доцільне запропонувати комплекс таких заходів щодо розвитку політики провідних країн ЄС у сфері інформаційної безпеки:

- оцінити функціонування різних інструментів захисту інформації і представити, якщо це необхідно законодавчі та інші ініціативи для ефективного забезпечення ефективного застосування принципів інформаційної безпеки країн ЄС;
- розробити і внести рекомендації для переговорів з питань захисту інформації, а також угоди з обміну інформацією між правоохоронними органами з США, грунтуючись на виконаній роботі в рамках Високої групи переговірників ЄС-США з питань поширення інформації, захисту приватного життя та персональних даних;
- розглянути основні елементи для угод про захист інформації з третіми країнами в правоохоронних цілях, які можуть включати в міру необхідності конфіденційне зберігання інформації, засноване на високому рівні захисту інформації;

- вдосконалення механізму виконання принципів захисту даних через розвиток відповідних нових технологій, включаючи взаємодію між публічним і приватним секторами, зокрема в дослідницькій сфері;
- вивчення стану впровадження європейської системи сертифікації технологій, продуктів і послуг «конфіденційність-обізнаність» («privacy-aware»);
- проведення інформаційних кампаній, зокрема щодо підвищення обізнаності суспільства.

**Наукові праці, в яких опубліковано основні наукові результати магістерської роботи:**

*Статті в наукових виданнях*

1. Хмель А., Білоусов М. Механізми та правове забезпечення захисту інформації в ЄС // Вісник Львівського університету. Серія філос.-політолог. студії. 2020. Випуск 33. С. 167-176.

*Тези*

2. Білоусов М. Безпека е-врядування та захист персональних даних в країнах ЄС як основний принцип політики інформаційної безпеки // Матеріали IX Всеукраїнської наукової конференції «Історико-філософські дослідження молодих учених» (м. Суми, СумДПУ імені А.С. Макаренка, 22-23 квітня 2021 р.). Суми. 2021 р. у друці.

3. Білоусов М. Інформаційна політика ФРН // Матеріали Міжнародної науково-практичної конференції «Принциповий прагматизм ЄС – наслідки для Східної та Південно-Східної Європи: політичні, економічні, правові та комунікаційні аспекти» (м. Київ, Інститут міжнародних відносин КНУ ім. Тараса Шевченка, 21-22 травня 2021 р.). Київ. 2021 р. у друці.

# АНОТАЦІЯ

**Білоусов М.В. Інформаційна безпека країн ЄС: стан та перспективи розвитку.** – На правах рукопису.

Дипломна робота на здобуття освітнього ступеню «магістр».

Чорноморський національний університет імені Петра Могили. – Миколаїв, 2021.

Дослідження присвячено аналізу стану та перспектив розвитку інформаційної безпеки країн ЄС. Вироблені в країнах ЄС підходи до забезпечення інформаційної безпеки, що відображають узгоджену волю держав-членів та інституцій ЄС, можна розглядати як європейські рамкові стандарти в цій сфері, які можуть успішно застосовуватися різними країнами з урахуванням їх адаптації до особливостей національних правових систем і соціокультурної специфіки.

Для країн ЄС інформаційна безпека має важливе значення, оскільки зав'язана на безпеці держави, кожного окремого громадянина, безпеці ЄС як організації і дотриманні прав і свобод людини. Всі ці складові врівноважує ЄС у принципах інформаційної безпеки, які застосовує в зазначеному напрямку. Комплексна політика інформаційної безпеки країн ЄС включає в себе розробку, виробництво і установку технічних засобів захисту, а також регулярне проведення перевірок використовуваного інформаційного обладнання. Відповідно приклад ЄС для нашої країни може стати вкрай важливим, адже успішність країн ЄС в цьому напрямку доводить вдале подолання інформаційних небезпек цією європейською структурою.

***Ключові слова:*** інформація, інформаційна політика, інформаційна безпека, ЄС.

# SUMMARY

**Bilousov M. Information security of EU countries: state and development prospects.** – Manuscript.

Graduate work for obtaining an educational degree «Master». Petro Mohyla Black Sea National University. – Mykolaiv, 2021.

The study analyzes the state and development prospects of information security in the EU countries. The approaches to ensuring information security developed in the EU countries, reflecting the agreed will of the member states and EU institutions, can be considered as European framework standards in this area, which can be successfully applied by various countries, taking into account their adaptation to the peculiarities of national legal systems and socio-cultural specifics.

For the EU countries, information security is important, since it's tied to the security of the state, each individual citizen, the security of the EU as an organization and the observance of human rights and freedoms. All these components are balanced by the EU in the principles of information security applied in this direction. The comprehensive information security policy of the EU countries includes the development, production and installation of technical means of protection, as well as regular inspections of the information equipment used. According to the example of the EU, it can become extremely important for our country, because the success of the EU countries in this direction proves the successful overcoming of information hazards by this European structure.

***Key words:*** information, information policy, information security, EU.