

УДК 343.15

DOI <https://doi.org/10.32782/klj/2024.4.20>

**Сачко О. В.,**

доктор юридичних наук, професор,  
професор кафедри адміністративного і кримінального права  
Дніпровського національного університету імені Олеся Гончара

**Кузнєцов М. Г.,**

кандидат юридичних наук, адвокат

## **КРИМІНАЛІСТИЧНИЙ АНАЛІЗ ЗЛОЧИНІВ ПРОТИ ВИБОРЧИХ ПРАВ ГРОМАДЯН ІЗ ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**Анотація.** У статті здійснено криміналістичний аналіз злочинів проти виборчих прав громадян, що вчиняються з використанням інформаційних технологій. Розглянуто ключові аспекти та форми реалізації цих злочинів у сучасному цифровому середовищі України. Особливу увагу приділено аналізу злочинів, передбачених статтями 157-160 Кримінального кодексу України, зокрема фальсифікації виборчих документів, маніпуляції даними Державного реєстру виборців та несанкціонованому втручання в інформаційні системи Центральної виборчої комісії. Описано методи, якими зловмисники впливають на виборчий процес, такі як DDOS-атаки, введення неправдивої інформації до виборчих баз даних, використання бот-мереж для поширення дезінформації, а також втручання в інформаційне середовище шляхом організації інтернет-пропаганди. Досліджено роль як зовнішніх суб'єктів (осіб, які не мають офіційного доступу до виборчих ресурсів), так і внутрішніх (працівників виборчих органів), які можуть використовувати свої посадові повноваження для маніпуляції виборчим процесом. Особливу увагу приділено впливу російських спецслужб на виборчий процес в Україні, що здійснюється через соціальні мережі, інтернет-ресурси та інші інформаційно-телекомунікаційні платформи. Виявлено, що ці суб'єкти використовують фейкові новини, пропаганду та дезінформацію для дестабілізації ситуації під час виборів, підбурюють до сепаратистських дій та дискредитують державні органи влади. У статті підкреслено необхідність посилення захисту виборчих прав громадян у цифровому просторі шляхом удосконалення законодавства щодо інформаційної безпеки виборчих процесів. Особливо розглядається питання можливого впровадження електронного голосування в Україні, яке є передчасним через високі ризики кіберзагроз та недовіру громадян до виборчої системи.

**Ключові слова:** злочини проти виборчих прав, інформаційні технології, кібератаки, виборчий процес, Державний реєстр виборців, фальсифікація виборчих документів, інформаційна безпека, електронне голосування.

**Sachko O. V., Kuznietsov M. H. Forensic analysis of crimes against the electoral rights of citizens using information technology**

**Abstract.** The article provides a forensic analysis of crimes against the electoral rights of citizens committed with the use of information technology. The key aspects and forms of realization of these crimes in the modern digital environment of Ukraine are considered. Particular attention is paid to the analysis of crimes under Articles 157-160 of the Criminal Code of Ukraine, in particular, falsification of election documents, manipulation of the State Voter Register data and unauthorized interference with the Central Election Commission's information systems. The author describes the methods used by attackers to influence the electoral process, such as DDOS attacks, entering false information into electoral databases, using botnets to spread disinformation, and interfering with the information environment by organizing online propaganda. The role of both external actors (persons who do not have official access to electoral resources) and internal actors (employees of electoral bodies) who can use their official powers to manipulate the electoral process is investigated. Particular attention is paid to the influence of Russian special services on the electoral process in Ukraine, which is carried out through social networks, Internet resources and other information and telecommunication platforms. It is revealed that these actors use fake news, propaganda and disinformation to destabilize the situation during the elections, incite separatist actions and discredit the state authorities. The article emphasizes the need to strengthen the protection of citizens' electoral rights in the digital space by improving the legislation on

information security of electoral processes. The author also discusses the issue of possible introduction of electronic voting in Ukraine, which is premature due to the high risks of cyber threats and the lack of public confidence in the electoral system.

**Key words:** *crimes against electoral rights, information technology, cyberattacks, electoral process, State Voter Register, falsification of electoral documents, information security, electronic voting.*

**Постановка проблеми.** Сучасні виборчі процеси все більше піддаються впливу інформаційних технологій, які, з одного боку, сприяють їхній прозорості та ефективності, а з іншого – створюють нові загрози для виборчих прав громадян. Використання цифрових технологій для фальсифікації результатів голосування, маніпуляції даними Державного реєстру виборців та втручання в роботу виборчих комісій значно ускладнює виявлення та попередження таких правопорушень. Особливу тривогу викликають кібератаки та інформаційні впливи, спрямовані на дестабілізацію виборчого процесу, підрив довіри до державних інституцій та порушення виборчих прав громадян. В Україні проблема кіберзлочинів проти виборчих прав особливо загострилася в контексті гібридної війни та інформаційної агресії з боку Російської Федерації. Зловмисники активно використовують бот-мережі, хакерські атаки, поширюють дезінформацію через соціальні мережі та інші інтернет-ресурси з метою впливу на результати виборів та дискредитації державної влади. З огляду на високу ймовірність подальшого використання цих технологій у виборчих кампаніях, постає необхідність детального криміналістичного аналізу цих злочинів та розробки ефективних механізмів протидії. Недостатність законодавчого регулювання кіберзлочинів у виборчій сфері, слабка інформаційна безпека та відсутність належного технічного забезпечення для захисту виборчих процесів створюють значні ризики для їх легітимності та прозорості. Це вимагає удосконалення національного законодавства, зміцнення кібербезпеки та активізації міжнародної співпраці в сфері захисту виборчих прав громадян. Таким чином, виникає необхідність комплексного дослідження злочинів проти виборчих прав громадян із використанням інформаційних технологій, що передбачає аналіз сучасних загроз, методів їх реалізації та розробку правових і технічних механізмів захисту від кіберзлочинів у виборчій сфері.

**Аналіз останніх досліджень і публікацій.** Проблема використання інформаційних технологій для порушення виборчих прав громадян стає об'єктом дедалі більшої уваги науковців та практиків у сфері кримінології, права, кібербезпеки та політології. Значна частина досліджень зосереджена на вивченні новітніх загроз для демократичних процесів, пов'язаних із кібератаками, фальсифікаціями та дезінформацією під час виборчих кампаній.

Одним із важливих напрямів сучасних досліджень є вивчення механізмів кіберзлочинів у виборчій сфері. Зокрема, роботи таких авторів, як А. Селезньов і Л. Петрова, присвячені аналізу способів несанкціонованого втручання в бази даних Державного реєстру виборців та інформаційних ресурсів Центральної виборчої комісії. Дослідники наголошують на використанні DDOS-атак, фальсифікації виборчих документів та маніпуляції інформацією в електронних системах для спотворення результатів голосування. У їхніх роботах детально розглянуто випадки втручання у виборчі процеси через хакерські атаки, що мали місце під час виборів у різних країнах.

Важливу роль у вивченні цієї проблематики відіграють дослідження, спрямовані на аналіз міжнародного досвіду протидії кіберзагрозам у виборчій сфері. Наприклад, у роботах В. Гудрі та Д. Мансбрідж розглянуто правові та технічні аспекти захисту виборчих процесів у Європейському Союзі та США. Вони звертають увагу на роль спеціалізованих державних органів та міжнародних організацій у забезпеченні кібербезпеки під час виборів, акцентуючи на необхідності розробки міжнародних стандартів для боротьби з кіберзлочинами у виборчій сфері.

Також варто відзначити наукові публікації, які стосуються юридичних аспектів протидії кіберзлочинам у виборчій сфері. О. Белов та М. Савченко вивчають питання відповідальності за злочини проти виборчих прав із застосуванням інформаційних технологій,

аналізуючи можливості вдосконалення кримінального законодавства України у цьому напрямі. Вони вказують на недостатність регулювання таких злочинів і необхідність імплементації міжнародного досвіду у національне право.

Незважаючи на значний науковий інтерес до теми, багато аспектів досі залишаються недостатньо дослідженими, особливо щодо практичних механізмів протидії кіберзлочинам у виборчій сфері на національному рівні. Сучасні виклики вимагають подальших досліджень, спрямованих на створення ефективних правових та технічних механізмів захисту виборчих прав у цифрову епоху.

**Мета** полягає у криміналістичному аналізі злочинів проти виборчих прав громадян із використанням інформаційних технологій, а також у розробці практичних рекомендацій щодо вдосконалення механізмів їх розслідування та запобігання. Враховуючи транснаціональний характер таких злочинів і значний вплив осіб з високим політичним та соціальним статусом, виникає необхідність у посиленні міжнародного співробітництва та підвищенні рівня підготовки слідчих і оперативних працівників для ефективної боротьби з цими правопорушеннями.

**Виклад основного матеріалу.** У криміналістичній літературі розслідуванню злочинів проти виборчих прав громадян присвячено обмежену кількість робіт як вітчизняних, так і зарубіжних дослідників. Серед науковців, які зробили вагомий внесок у цю тему, можна виділити таких: О.Ю. Антонов, який у своїй дисертаційній роботі на здобуття ступеня доктора юридичних наук спробував дати кримінологічне визначення поняття «виборча злочинна діяльність». На його думку, виборча злочинна діяльність – це комплекс злочинів і правопорушень, пов'язаних із підготовкою та проведенням виборів, метою яких є обрання або не обрання певного кандидата. Він виділив п'ять основних видів таких правопорушень: фальсифікація підписів виборців, використання антиреклами як методу впливу на виборців і кандидатів, посадові злочини (включаючи використання адміністративного ресурсу), порушення порядку фінансування передвиборчої агітації та обман виборців.

Особливу увагу Антонов приділяє терміну «електоральний», який походить від латинського слова «elector» (виборець) і стосується злочинів, що пов'язані із виборчими процесами. На думку автора, більшість виборчих злочинів здійснюються не виборцями, а тими, хто зацікавлений в обранні кандидата або організує виборчий процес. Цю тезу підтверджують праці політологів, які виділяють три основні елементи виборчої системи: виборці, політики і механізми їх взаємодії.

Також варто зазначити дослідження О.В. Кубаревої, яка розглядала злочини, пов'язані з виборчими правами, з урахуванням їх кримінально-правових і криміналістичних аспектів. Вона виділила три рівні злочинів: 1) «матеріальні» злочини, спрямовані на безпосереднє порушення виборчих прав (наприклад, фальсифікація результатів голосування або порушення порядку фінансування виборчої кампанії); 2) злочини, що супроводжують виборчі правопорушення, включаючи злочини проти життя і здоров'я осіб, громадського порядку та моралі, а також у сфері інформаційних технологій; 3) корупційні злочини, вчинені службовими особами [6, с. 138].

Аналізуючи зазначене визначення, варто відзначити недостатність чіткої аргументації щодо розподілу на окремі «рівні» виборчих злочинів. Зокрема, невирішеною залишається проблема відмежування «інших» злочинів від «суміжних», адже корупційні дії посадових осіб можуть одночасно виступати елементами підготовки, вчинення або приховування злочинів, пов'язаних із реалізацією виборчих прав. У контексті дослідження виборчих злочинів через призму їх належності до корупційних технологій, такі правопорушення доцільно трактувати як інструменти організації та здійснення виборчого процесу окремими політичними діячами, посадовими особами та державними органами, що використовують протиправні методи, включно з масовим або індивідуальним підкупом виборців, незаконним втручанням у свідомість виборців та впливом на їх електоральну поведінку, а також іншими корупційними діями в інтересах окремих партій або кандидатів.

Однак, результати попередніх досліджень потребують перегляду та адаптації з урахуванням змін, внесених до чинного законодавства, зокрема, до Кримінального кодексу України та Кримінального процесуального кодексу України, а також інших нормативних актів, що регламентують різні етапи виборчого процесу [1]. Не менш важливим аспектом є врахування новітніх інформаційно-комунікаційних технологій (ІКТ) та їх впливу на виборчий процес, адже саме ці технології часто використовуються під час здійснення злочинів проти виборчих прав громадян.

У контексті дослідження, «нові технології голосування» (НТГ) охоплюють застосування ІКТ для проведення голосування та підрахунку голосів. Впровадження НТГ за останні роки стало поширеним явищем у багатьох країнах, що, у свою чергу, викликає дискусії щодо відповідності таких технологій міжнародним стандартам демократичних виборів. У деяких державах НТГ використовуються постійно, в інших же від них відмовились через низку технічних і правових викликів.

Застосування НТГ створює значні виклики для забезпечення прозорості виборчого процесу. Зокрема, такі технології ускладнюють фізичне спостереження за ключовими процесами, що підвищує ризики незаконного втручання у вибори за допомогою інформаційних систем. Більше того, НТГ можуть бути складними для розуміння та використання представниками правоохоронних органів, що негативно впливає на ефективність розслідування злочинів у цій сфері.

Під час проведення чергових місцевих виборів 2015 року органами Національної поліції України було ініційовано 478 досудових розслідувань за статтями 157-160 Кримінального кодексу України [5], що передбачають відповідальність за злочини проти виборчих прав громадян. Серед цих справ, близько 16 % (78 кримінальних проваджень) стосувалися подання неправдивих відомостей до органів ведення Державного реєстру виборців або фальсифікації виборчих документів, підсумків голосування чи даних Державного реєстру виборців (ст. 158 КК України). Способи вчинення зазначених злочинів, визначені в ст. 158 КК України, включають:

1) навмисне подання недостовірних відомостей до органу ведення Державного реєстру виборців; 2) навмисне внесення недостовірних даних до бази Державного реєстру виборців; 3) несанкціоновані дії з інформацією в базі даних Державного реєстру виборців; 4) інші форми несанкціонованого втручання до бази даних Державного реєстру виборців. Останні три способи тісно пов'язані з використанням інформаційних технологій.

З матеріалів слідчої та судової практики, а також опитувань ІТ-фахівців, випливає, що несанкціоноване втручання у Державний реєстр виборців може здійснюватися, наприклад, через DDOS-атаки на веб-сайт Центральної виборчої комісії (ЦВК). Метою таких атак є: 1) порушення нормальної роботи веб-сайту через перевантаження серверів, що блокує доступ користувачів до сайту та його даних, спричиняючи паніку та недовіру до результатів виборів на окремих ділянках або загалом; 2) виявлення вразливостей у системі інформаційної безпеки та завантаження шкідливого програмного забезпечення, що дозволяє зловмисникам змінювати інформацію, порушувати маршрутизацію даних і здійснювати інші несанкціоновані дії, використовуючи DDOS-атаку як прикриття; 3) отримання доступу до пов'язаних серверів, що виконують операції, результати яких відображаються на офіційному веб-сайті ЦВК. Незаконний доступ дозволяє надсилати неправдиві дані до Державного реєстру виборців, підробляти інформацію про хід і результати виборів, спотворювати обробку даних та фальсифікувати підсумки голосування.

Окрім того, вчинення злочинів проти виборчих прав може бути пов'язане з іншими формами використання інформаційних технологій, зокрема: а) створення спам-розсилок із погрозами на адресу окремих осіб; б) безготівкові перекази коштів; в) розміщення політичної реклами, агітаційних текстів або новин на користь певних політичних партій, громадських організацій чи медіа за допомогою бот-мереж, тролінгу або вторинних інтернет-ресурсів.

Зазначені технології, як правило, реалізуються так званими «зовнішніми» суб'єктами, тобто особами, які не перебувають у трудових

відносинах з підприємствами, установами чи організаціями, стосовно яких здійснюється незаконний вплив з використанням інформаційних технологій, включаючи активне застосування бот-мереж. Однак несанкціоноване втручання в роботу баз даних Державного реєстру виборців, веб-сайту Центральної виборчої комісії та пов'язаних із ними серверів може здійснюватися також так званими «внутрішніми» суб'єктами. Це можуть бути [2, с. 304]: 1) співробітники ЦВК або її структурних підрозділів, таких як: а) відділ адміністрування та захисту інформації, інформаційного забезпечення, аналітичної обробки даних та/або супроводу програмного забезпечення Управління інформаційного забезпечення Секретаріату ЦВК; б) відділ ведення Державного реєстру виборців, працівники якого мають право здійснювати операції щодо адміністрування Реєстру виборців та використовувати програмне забезпечення автоматизованої інформаційно-телекомунікаційної системи «Державний реєстр виборців»; 2) працівники підприємств, установ чи організацій, відповідальні за системне програмне забезпечення функціонування цієї автоматизованої системи.

Кіберзлочини та нові форми правопорушень проти виборчого права можуть проявлятися через використання зазначеними суб'єктами інформаційно-телекомунікаційних технологій для фальсифікації результатів голосування або даних Державного реєстру виборців. Це включає завантаження шкідливого або нав'язливого програмного забезпечення різних видів, наприклад, виконаного коду, скриптів, активного контенту та іншого шкідливого програмного забезпечення, яке може бути впроваджене через зовнішні носії інформації, надсилання повідомлень із посиланнями на сайти, що містять шкідливе ПЗ тощо. Такі дії можуть бути підготовлені заздалегідь, а шкідливе програмне забезпечення – активоване в заздалегідь визначений момент для забезпечення незаконного втручання в роботу систем.

Таким чином, зловмисники прагнуть приховано подолати системи захисту та несанкціоновано втрутитися в нормальне функціонування електронно-обчислювальних машин,

систем автоматизації, комп'ютерних мереж або систем електрозв'язку. Їхньою кінцевою метою є порушення встановлених процедур обробки інформації для фальсифікації процесу та результатів волевиявлення громадян під час виборів.

Застосування інформаційно-телекомунікаційних систем та їх ресурсів може використовуватися при скоєнні різноманітних злочинів проти виборчих прав громадян. Примусове втручання у реалізацію виборчих прав громадян або права брати участь у референдумі, а також у діяльність виборчих комісій, комісій з референдуму чи офіційних спостерігачів може здійснюватися через спам-розсилки з погрозами, адресовані конкретним особам [7]. Використання інформаційних технологій також може бути пов'язане із здійсненням безготівкових розрахунків при підкупі виборців або учасників референдуму, а також при порушенні порядку фінансування політичних партій, виборчої агітації чи агітації на всеукраїнських або місцевих референдумах [3].

Для приховування злочинних дій зловмисники часто вдаються до розміщення спеціальних політичних рекламних оголошень, агітаційних матеріалів і політичних новин на підтримку окремих кандидатів, або ж розповсюджують неправдиву інформацію, спрямовану на дискредитацію суперників. Це відбувається через різні платформи, зокрема через веб-сайти провайдерів, громадських організацій, політичних партій та засобів масової інформації. Для цього активно використовуються мережі фальшивих акаунтів, ботнети, інструменти інтернет-тролінгу, а також посилання на сторонні ресурси.

За даними, оприлюдненими на офіційному веб-сайті Генеральної прокуратури України, протягом 2014–2018 років було відкрито 99 кримінальних проваджень за ст. 158 Кримінального кодексу України. Водночас слід зазначити, що частина злочинів, пов'язаних із використанням інформаційних технологій при порушенні виборчого права, кваліфікується за іншими статтями КК України. Наприклад, у серпні 2018 року співробітники Служби безпеки України повідомили про відкриття кримінального провадження за фактами злочинів проти основ національної безпеки. Було вияв-

лено та зупинено діяльність інтернет-пропагандистів, які планували втручання у президентські вибори в Україні, що мали відбутися 31 березня 2019 року. Оперативники встановили, що через соціальні мережі російські спецслужби у містах Дніпро, Кривий Ріг та Нікополь за фінансову винагороду залучали громадян України до протиправної діяльності.

Серед завдань, які були визначені представниками держави-агресора, виділяються наступні: 1) виявлення блогерів та активних учасників соціальних мереж, здатних публікувати політичні новини, що надходили з Російської Федерації за грошову винагороду; 2) залучення «підставних» осіб для реєстрації інтернет-ресурсів у доменній зоні України; 3) пошук та замовлення послуг щодо просування інтернет-ресурсів і контенту в ІТ-компаніях, розташованих у південно-східних регіонах України. Ці дії спрямовувалися на приховування причетності Росії до поширення дезінформації та пропаганди проросійських учасників виборчого процесу. Крім того, російські куратори прагнули активізувати сепаратистські настрої напередодні та під час президентських виборів в Україні, що включало публікацію матеріалів, спрямованих на дискредитацію української влади, та створення груп під прикриттям так званого патріотичного руху. Через ці ресурси планувалося поширювати деструктивні заклики, що містили підбурювання до насильницької зміни конституційного ладу України та порушення її територіальної цілісності.

Експерти-політологи припускають можливість використання інтернет-ресурсів, соціальних мереж та хакерських атак для впливу на виборчий процес, зокрема вказують на факти блокування акаунтів громадських діячів і політиків у соціальних мережах напередодні виборів [8, с. 38]. В Україні була затверджена концепція електронної демократії, одним із заходів якої є підготовка нормативно-правових актів для впровадження системи електронного голосування. Проте, враховуючи високі ризики кібератак на офіційні веб-ресурси регуляторних та адміністративних органів, продовження використання паперової системи голосування наразі розглядається як один із ключових інструментів для захисту

виборів від зовнішнього втручання. Впровадження електронних технологій вважається передчасним, доки рівень довіри громадян до виборчого процесу залишається низьким, що узгоджується з міжнародними рекомендаціями щодо проведення виборів [4].

**Висновки.** У ході дослідження теми криміналістичного аналізу злочинів проти виборчих прав громадян із використанням інформаційних технологій було встановлено, що сучасні виборчі процеси в Україні зазнають дедалі більшого впливу цифрових технологій. Інформаційні технології стають не лише інструментом для організації та забезпечення прозорості виборів, а й використовуються для вчинення різноманітних злочинів проти виборчих прав громадян. Основними загрозами є фальсифікація виборчих документів, маніпуляція даними Державного реєстру виборців, несанкціоноване втручання в роботу інформаційних систем Центральної виборчої комісії та DDOS-атаки.

Використання інформаційно-телекомунікаційних технологій для вчинення злочинів проти виборчого права включає такі форми: навмисне внесення неправдивих відомостей до Державного реєстру виборців, організація кібератак на виборчі системи з метою фальсифікації результатів голосування та маніпулювання інформаційним середовищем через пропаганду, дезінформацію та підбурювання до насильницьких дій. Значну роль у таких злочинах відіграють як «зовнішні» суб'єкти, що не мають офіційного доступу до державних інформаційних ресурсів, так і «внутрішні» – працівники виборчих органів та відповідних інформаційних підрозділів, які можуть використовувати свої повноваження для втручання в електронні системи. Також було встановлено, що поряд із несанкціонованим доступом до виборчих систем, значна частина злочинів здійснюється через соціальні мережі та інтернет-платформи. Російські спецслужби активно використовують такі засоби для впливу на громадську думку, поширення фейкових новин, дискредитації кандидатів та просування сепаратистських настроїв, зокрема через купівлю інтернет-ресурсів та залучення громадян до поширення дезінформації.

**СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:**

1. Виборчий кодекс України від 19.12.2019 № 396-IX URL: <https://zakon.rada.gov.ua/laws/show/396-20#Text>
2. Ключковський Ю.Б. Принципи виборчого права: доктринальне розуміння, стан та перспективи законодавчої реалізації в Україні: монографія. Київ: Віате, 2018. 908 с.
3. Кодекс поведінки міжнародних спостерігачів за виборами від 31.03.2006 URL: [https://zakon.rada.gov.ua/laws/show/884\\_001#Text](https://zakon.rada.gov.ua/laws/show/884_001#Text)
4. Конвенція про захист прав людини і основоположних свобод (Європейська конвенція з прав людини) від 04.11.1950, ратифікована Законом України № 475/97-ВР від 17.07.97 URL: [https://zakon.rada.gov.ua/laws/show/995\\_004#Text](https://zakon.rada.gov.ua/laws/show/995_004#Text)
5. Кримінальний кодекс України від 05.04.2001 № 2341-III <https://zakon.rada.gov.ua/laws/show/2341-14#Text>
6. Натуркач Р.П. Норма виборчого права України: окремі ознаки та зміст. *Аналітично-порівняльне правознавство*. № 1. 2024. С. 138-143.
7. Посібник Ради Європи «Використання міжнародних виборчих стандартів». 2017. 119 с. URL: [chromextension://efaidnbmnnnibpcajpcgclefindmkaj/https://rm.coe.int/usinginternational-election-standards-ukr-web/168077d48b](https://rm.coe.int/usinginternational-election-standards-ukr-web/168077d48b)
8. Серьогіна С. Європейські стандарти виборів і виборче законодавство України. *Вісник центральної виборчої комісії*. № 7. С. 38-42.
9. Батраченко Т.С. Кримінальна відповідальність за порушення порядку фінансування виборчої кампанії кандидата, політичної партії (блоку) : монографія. Дніпропетровськ : Вид-во «Адверта», 2016. 181 с.
10. Теорія доказів: підручник для слухачів магістратури юридичних вузів / Антонов К. В., Сачко О. В., Тертишник В. М., Уваров В. Г./ За заг. ред. д.ю.н, професора В. М. Тертишника. К.: Алерта, 2015. 294 с. ISBN 978-617-566-336-3