Юридичні науки

УДК 347.963

Ковалів Мирослав Володимирович
кандидат юридичних наук, професор
Львівський державний університет внутрішніх справ
Ковалив Мирослав Владимирович
кандидат юридических наук, профессор
Львовский государственный университет внутренних дел
Kovaliv Myroslav
PhD in Law, Professor
Lviv State University of Internal Affairs
ORCID: 0000-0002-9730-8401

Хмиз Мар'яна Василівна
доктор філософії, викладач
Львівський національний університет імені Івана Франка
Хмыз Марьяна Васильевна
доктор философии, преподаватель
Львовский национальный университет имени Ивана Франко
Khmyz Mariana
PhD, Lecturer
Ivan Franko National University of Lviv
ORCID: 0000-0003-3553-8022

Кайдрович Христина Іванівна
кандидат економічних наук, доцент
Заклад вищої освіти «Львівський університет бізнесу та права»
Кайдрович Христина Ивановна
кандидат экономических наук, доцент
Учреждение высшего образования «Львовский университет бизнеса и права»

Kaydrovych Khrystyna
PhD in Economics, Associate Professor
Institution of higher education «Lviv University of Business and Law»
ORCID: 0000-0002-0362-7779

Єсімов Сергій Сергійович
кандидат юридичних наук, доцент
Львівський державний університет внутрішніх справ
Есимов Сергей Сергеевич
кандидат юридических наук, доцент
Львовский государственный университет внутренних дел
Yesimov Serhii
PhD in Law, Associate Professor
Lviv State University of Internal Affairs
ORCID: 0000-0002-9327-0071

Князь Святослав Володимирович
доктор економічних наук, професор
Національний університет «Львівська політехніка»
Князь Святослав Владимирович
доктор экономических наук, профессор
Национальный университет «Львовская политехника»
Kniaz Sviatoslav
D. Sc. (Economics), Professor
Lviv Polytechnic National University
ORCID: 0000-0002-7236-1759

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ОРГАНАХ ПРОКУРАТУРИ УКРАЇНИ

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ПРОКУРАТУРЫ УКРАИНЫ

PROBLEMS AND PROSPECTS OF ENSURING INFORMATION SECURITY IN THE PROSECUTOR'S OFFICE OF UKRAINE

Анотація. *У статті на підставі методології комплексного системного аналізу правових явищ досліджено проблеми та перспективи забезпечення інформаційної безпеки в органах прокуратури України. Зміст діяльності прокуратури у всіх напрямах тісно пов'язане з обробкою інформації. Ця робота характеризується різноманіттям джерел, наростаючим обсягом і великою питомою вагою процедур обробки, багаторазовим повторенням циклів отримання та відправки у встановлені терміни, необхідністю забезпечення конфіденційності у використанні окремих її частин, надзвичайною важливістю у підготовці та прийнятті рішень. Перехід на електронний документообіг та електронна взаємодія є сучасними трендами розвитку управління. Ігнорування цього фактора може знизити ефективність прокурорської діяльності в перспективі. На підставі аналізу нормативно-правової бази напрямами використання інформаційних технологій у діяльності прокуратури є: електронний документообіг у внутрішній діяльності органів прокуратури, а також при направленні запитів і отримання відповідей від інших органів державної влади, громадських організацій, юридичних та фізичних осіб, у межах Концепції розвитку електронного урядування в Україні; застосування широкосмугового доступу при здійсненні функцій прокурорського нагляду в інформаційно-комунікативній мережі Інтернет; доступ до баз зберігання даних для цілей здійснення прокурорської діяльності. Розвиток і вдосконалення навичок використання інформаційних технологій доцільно розглядати як один з перспективних*

напрямів навчання прокурорів. В якості практичної пропозиції щодо підвищення ефективності використання інформаційних технологій, у тому числі щодо забезпечення інформаційної безпеки, у діяльності прокуратури України можна розглядати пропозицію про створення єдиної Концепції інформатизації та впровадження інформаційних технологій в діяльність прокуратури.

Ключові слова: *органи прокуратури, інформація, інформаційна безпека, інформаційні технології, цифрові компетентності.*

Аннотация. *В статье на основании методологии комплексного системного анализа правовых явлений исследованы проблемы и перспективы обеспечения информационной безопасности в органах прокуратуры Украины. Содержание деятельности прокуратуры по всем направлениям тесно связано с обработкой информации. Эта работа характеризуется многообразием источников, нарастающим объемом и большим удельным весом процедур обработки, многократным повторением циклов получения и отправки в установленные сроки, необходимостью обеспечения конфиденциальности в использовании отдельных ее частей, чрезвычайной важностью в подготовке и принятии решений. Переход на электронный документооборот и электронное взаимодействие являются современными трендами развития управления. Игнорирование этого фактора может снизить эффективность прокурорской деятельности в перспективе. На основании анализа нормативно-правовой базы направлениям использования информационных технологий в деятельности прокуратуры являются: электронный документооборот во внутренней деятельности органов прокуратуры, а также при направлении запросов и получения ответов от других органов государственной власти, общественных организаций, юридических и физических лиц в пределах Концепции развития электронного управления в*

Украине; применение широкополосного доступа при осуществлении функций прокурорского надзора в информационно-коммуникативной сети Интернет; доступ к базам хранения данных для целей осуществления прокурорской деятельности. Развитие и совершенствование навыков использования информационных технологий целесообразно рассматривать как одно из перспективных направлений обучения прокуроров. В качестве практической предложения по повышению эффективности использования информационных технологий, в том числе по обеспечению информационной безопасности, в деятельности прокуратуры Украины можно рассматривать предложение о создании единой Концепции информатизации и внедрения информационных технологий в деятельность прокуратуры.

Ключевые слова: *органы прокуратуры, информация, информационная безопасность, информационные технологии, цифровые компетентности.*

Summary. *In the article based on the methodology of a comprehensive systemic analysis of legal phenomena, the problems and prospects of ensuring information security in the prosecutor's office of Ukraine are investigated. The content of the activities of the prosecutor's office in all areas is closely related to the processing of information. This activity is characterized by a variety of sources, an increasing volume and a large proportion of processing procedures, multiple repetitions of receiving and sending cycles in a timely manner, the need to ensure confidentiality in the use of its individual parts, and is extremely important in preparation and decision-making. The transition to electronic document management and electronic interaction are modern trends in the development of management. Ignoring this factor can reduce the effectiveness of prosecutorial activities in the future. Based on the analysis of the regulatory framework, the directions for the use of information technologies in the*

activities of the prosecutor's office are: electronic document flow in the internal activities of the prosecutor's office, as well as when sending requests and receiving answers from other government bodies, public organizations, legal entities and individuals within the framework of the Concept for the development of electronic management in Ukraine; the use of broadband access in the implementation of the functions of prosecutorial supervision in the information and communication network of the Internet; access to databases for storing data for the purpose of carrying out prosecutorial activities. It is advisable to consider the development and improvement of skills in the use of information technologies as one of the promising areas of training for prosecutors. As a practical proposal to improve the efficiency of the use of information technologies, including ensuring information security, in the activities of the prosecutor's office of Ukraine one can consider the proposal to create a unified Concept of informatization and the implementation of information technologies in the activities of the prosecutor's office.

Key words: *prosecutor's office, information, information security, information technology, digital competencies.*

Постановка проблеми. Використання інформаційно-комунікаційних технологій і систем – необхідна складова, важливий елемент наукової організації праці в прокурорській, як і в будь-який інший діяльності, яка передбачає комплексний підхід до її здійснення. У Стратегії розвитку прокуратури України на 2021-2023 роки передбачено поступове впровадження в практичну діяльність високотехнологічного нагляду, заснованого на інформаційно-комунікаційних технологіях та впровадженні новітньої комп'ютерної техніки. У числі розв'язуваних завдань виділяються підвищення ефективності забезпечення інформаційної безпеки інформаційних ресурсів прокуратури шляхом впровадження сучасних та перспективних інформаційних технологій обробки первинної

інформації в усіх видах наглядової діяльності, підвищення оперативності прокурорського реагування на порушення закону тощо. Тому окреслена проблематика сьогодні є особливо актуальною, доцільною та важливою.

Аналіз останніх досліджень і публікацій. Питання правового забезпечення діяльності органів прокуратури України, у тому числі щодо застосування інформаційних технологій, були предметом наукових досліджень таких вчених і практиків: А. Войтенка, М. Косюти, В. Малюги, І. Марочкіна, М. Мички, О. Михайленка, В. Підгородинського, М. Потебенька, Є. Поповича, М. Руденка, Н. Рибалки, Р. Скриньковського, Л. Сопільника, В. Сухоноса, П. Шумського, М. Якимчука та інших учених і практиків.

Розвиток нових інформаційно-комунікаційних технологій обумовлює збільшення технологічного розриву між вимогами захищеності інформаційних ресурсів і можливостями використовуваних при забезпеченні інформаційної безпеки програмно-апаратних засобів. Це зумовлює потребу в науково обґрунтованих методах організації та вдосконаленні системи забезпечення інформаційної безпеки в органах державної влади, у тому числі в органах прокуратури.

Мета статті. Метою статті є дослідження проблем та перспектив забезпечення інформаційної безпеки в органах прокуратури України.

Виклад основного матеріалу дослідження. Відповідно до чинного Закону України «Про інформацію» від 02.10.1992 р. № 2657-XII (із змінами та доповненнями) [1] інформація – це відомості, повідомлення, дані незалежно від форми подання. Різноманіття форм відтворення та широка палітра носіїв інформації дають підстави зробити висновок про виняткову цінність інформаційного контенту. З розвитком суспільства, ускладненням політичного життя держави і посиленням боротьби за владу значимість певних видів інформації все більше зростає роль забезпечення інформаційної безпеки.

Цінною стає та інформація, володіння якою дозволить наявному й потенційному власнику отримати переваги: матеріальні, політичні, військові. Проблема захисту інформації від стороннього доступу та небажаних впливів на неї виникла давно.

У недалекому минулому завдання захисту інформації можна було ефективно вирішувати за допомогою: організаційних заходів і окремих програмно-апаратних засобів; розмежування доступу та шифрування. Широке поширення комп'ютерної техніки, локальних і глобальних мереж, хмарних технологій, супутникових каналів зв'язку, технічної розвідки істотно загострило потребу в захисті інформації.

У сучасному світі проблема надійного забезпечення схоронності інформації є однією з найважливіших. Динамічно розвивається напрям пошуку рішень для управління базами даних і аналітики. Щорічне зростання послуг, що надаються у даній сфері – більше 8,0 %.

Незмінно високий попит зберігається на рішення з управління ресурсами підприємства та відносинами з клієнтами щодо забезпечення безпеки контенту.

Питання забезпечення інформаційної безпеки не обійшли стороною органи прокуратури. Зміст діяльності прокуратури у всіх напрямах тісно пов'язане з обробкою інформації. Ця робота характеризується різноманіттям джерел і споживачів інформації, наростаючим обсягом і великою питомою вагою процедур обробки, багаторазовим повторенням циклів отримання та відправки у встановлені часові періоди (декада, місяць, квартал, рік), необхідністю забезпечення конфіденційності у використанні окремих її частин, надзвичайною важливістю у підготовці та прийнятті рішень.

Серед важливих характеристик інформації відзначимо достовірність і повноту. Інформація не повинна спотворювати справжнього стану речей і повинна бути достатньою для розуміння ситуації та прийняття рішень.

Незважаючи на значну кількість облікових документів, єдина система збору, реєстрації, обробки та зберігання інформації, яка характеризувала б з вичерпною повнотою той чи інший напрям діяльності, відсутня.

Від правильної організації інформаційно-аналітичної роботи, в першу чергу, залежать результати прокурорської діяльності, внесок прокуратури у зміцнення законності та правопорядку в країні. Велика частина помилок і прорахунків, що відзначаються в роботі окремих прокуратур, має в основі недооцінку керівниками значення інформаційно-аналітичної роботи і використання сучасних методів її організації, включаючи інструментарій забезпечення інформаційної безпеки. Ігнорування забезпечення інформаційної безпеки тягне ослаблення ефективності діяльності органів прокуратури, негативно відбивається на стані законності.

Інформаційна безпека є пріоритетним напрямом діяльності органів прокуратури, що можна розглядати у контексті наказу Офісу Генерального Прокурора України від 12 січня 2021 року № 3 «Про створення служби захисту інформації кваліфікованого надавача електронних довірчих послуг органів прокуратури України», який ставить на порядок денний вирішення низки завдань внутрішнього та зовнішнього характеру [2]. Важливим є те, що метою забезпечення інформаційної безпеки є встановлення критеріїв походження програмного забезпечення, регламентація і організація обміну інформацією.

Незважаючи на значну кількість літератури з різних аспектів прокурорської діяльності, питання, що стосуються організації саме інформаційної безпеки органів прокуратури, не знайшли повноцінного та всебічного висвітлення у науковій літературі. Це пов'язано зі складністю діяльності зі збору необхідної інформації, правильної обробки, аналізу та винесення на підставі цього ефективного управлінського рішення.

О. Баранов [3] зазначає, що об'єктом інформаційних правовідносин

є: програмно-технічні комплекси, інформаційні системи, інструменти зв'язку і комунікацій, завдяки яким відбувається передавання інформації; інформація, інформаційні ресурси, інформаційні продукти, інформаційні послуги; доменні імена; права та свободи в сфері інформації; інтереси особи, суспільства, держави в інформаційній сфері; інформаційна цілісність та інформаційний суверенітет держави; інформаційна безпека; сукупність технічних систем і комплексів, що взаємодіють і складаються із мікропроцесорів, сенсорів, пристроїв, систем передавання даних, локальних і/або розподілених обчислювальних ресурсів і програмних засобів, включаючи програми штучного інтелекту, призначених для здійснення суспільних відносин, зокрема пов'язаних із наданням послуг і проведенням робіт за безпосередньої участі або без участі суб'єктів (юридичних або фізичних осіб) на основі використання мережі Інтернет [3, с. 33].

Причинами витоку інформації, її змінення або знищення можуть бути людський фактор, вразливість програмного забезпечення, недотримання запропонованих заходів.

З огляду на те, що діяльність кожного прокурора при здійсненні нагляду тісно пов'язана з обробкою інформації з різноманітних джерел, обсяг якої постійно наростає, з багаторазовим повторенням циклів отримання та відправки у визначений час, потенційних загроз несанкціонованого поширення інформації є чимало.

Істотно підвищує ймовірність витоку службової інформації з використання цифрових технологій. Важливими напрямами використання інформаційних технологій у діяльності прокуратури є: електронний документообіг у внутрішній діяльності органів прокуратури, а також при направленні запитів і отримання відповідей від інших органів державної влади, громадських організацій, юридичних і фізичних осіб, у межах Концепції розвитку електронного урядування в Україні; застосування

широкосмугового доступу при здійсненні функцій прокурорського нагляду в інформаційно-комунікативній мережі Інтернет; доступ до баз зберігання даних (державних органів) для цілей здійснення функції прокурорського нагляду.

Велика кількість нового програмного забезпечення, перехід на електронний документообіг та електронну взаємодію є сучасними трендами розвитку виробництва і сфери послуг. Ігнорування цього фактора може знизити ефективність прокурорського нагляду в перспективі. Водночас створення умов безпечної інформаційної взаємодії у цифровому середовищі є не менш важливим, ніж створення самого цифрового середовища.

С. Гайдай [4] зазначає, що інформатизація прокурорської діяльності розглядається як стан сприятливого середовища для впровадження комп'ютеризації, інформаційно-комунікаційних, мережевих, аналітичних та автоматизованих технологій в управлінську (адміністративну) та процесуальну діяльність прокурорів органів прокуратур, що реалізується за допомогою системного організаційно-правового та фінансового забезпечення [4, с. 124].

Реалізація даного завдання зажадала застосування нових підходів до інформатизації органів прокуратури, що знайшло своє відображення у Стратегії розвитку прокуратури України на 2021–2023 роки, а також в Концепції розвитку цифрових компетентностей до 2025 року [5; 6].

З урахуванням потреб громадян і суспільства в оперативному отриманні якісних та достовірних відомостей, відповідно до Національної економічної стратегії на період до 2030 року, ведуться роботи з впровадження електронно-цифрових технологій, створення високотехнологічної цифрового середовища взаємодії органів прокуратури, бізнесу та громадян, що забезпечує прозорість і ефективність наглядової діяльності, оперативність прокурорського реагування на

порушення закону. З міністерствами та відомствами України передбачається обмін даними за допомогою інтеграції інформаційних систем [7].

Інформаційна безпека – це стан захищеності особи, суспільства та держави від внутрішніх і зовнішніх інформаційних загроз, при якому забезпечуються реалізація конституційних прав і свобод людини та громадянина, якість і рівень життя громадян, суверенітет, територіальна цілісність, сталий соціально-економічний розвиток України, оборона та безпека держави.

Закон України «Про основні засади забезпечення кібербезпеки України» передбачає створення системи захисту електронних технологій, включає ряд етапів, аналогічних етапів створення інформаційних систем: аналіз можливих загроз для інформаційної системи; розробку системи захисту; впровадження системи захисту; підтримку системи захисту. Крім того, управління електронними ресурсами не може здійснюватися без такого превентивного заходу безпеки, як аналіз ризику [8].

У напрямах, що визначають стимулювання впровадження рішень у сфері інформаційних технологій в діяльність органів прокуратури України, розвиток культури адаптації інновацій в прокуратурі України щодо Стратегії розвитку прокуратури на 2021-2023 роки, позначені наступні завдання у галузі забезпечення захисту інформації: оцінка стану інформаційної безпеки, прогнозування та виявлення інформаційних загроз, визначення пріоритетних напрямів запобігання та ліквідації наслідків їх прояву; планування, здійснення і оцінка ефективності комплексу заходів щодо забезпечення інформаційної безпеки; забезпечення конфіденційності, цілісності та доступності інформації. Сьогодні ризики кібератак, інших способів незаконного заволодіння інформацією дуже високі.

Несанкціоноване вилучення (чи копіювання), розповсюдження службової інформації може не тільки завдати іміджевий збиток органам

прокуратури, а й зашкодити правам і законним інтересам тих осіб, відомості щодо яких були розголошені.

Загальновизнаними рівнями захисту інформації є: а) законодавчий; б) адміністративний (накази та інші дії керівництва організацій, пов'язаних з захищеними інформаційними системами); в) процедурний (заходи безпеки, орієнтовані на людей); г) програмно-технічний. Сукупність заходів, спрямованих на забезпечення безпеки інформаційного контенту, може бути найбільш ефективним засобом захисту. Прикладом може бути створення робочої групи з питань запровадження функціоналу «кабінет реєстратора» в інформаційній системі «Єдиний реєстр досудових розслідувань» [9].

Політика безпеки – це комплекс законів, правил і практичних рекомендацій, на основі яких будується управління важливою інформацією, її охорона та поширення у певній системі.

Розглядаючи кожен з рівнів захисту окремо, слід констатувати, що навіть законодавчий рівень далекий від досконалості. Багато процесів, що відбуваються у цифровому просторі, вимагають нормативного врегулювання. Є явне соціальне замовлення на регламентацію правовідносин у кіберпросторі, що означає необхідність в розробці нових положень законодавства.

Зокрема, чинне законодавство України обмежується поняттями комп'ютерної атаки та комп'ютерного інциденту, які, на наш погляд, можна піддати серйозній критиці. У жодному нормативному акті немає визначення моделі порушення, тим більше класифікації порушень. Для порівняння, у кримінальному законодавстві злочин класифікується по тяжкості, наявності умислу, наслідків від вчинених діянь.

Доцільно було б кваліфікувати негативні дії або бездіяльність користувача щодо техніки, програмного забезпечення та інформаційного контенту.

Складно поставити тотожність між навмисними діями суб'єкта, у результаті яких певні бази даних для службового користування були скопійовані та надані третім особам, з необережною дією, внаслідок якої сповільнилася робота комп'ютерної системи. Це є порушенням інформаційної безпеки, вимагає залучення винного до юридичної відповідальності, але міра цієї відповідальності в названих випадках ідентичною бути не може.

Реалізація більшості адміністративних заходів щодо захисту інформації в органах прокуратури у даний час здійснюється в тестовому режимі. Накопичуються, узагальнюються і аналізуються результати проведених заходів. Одним з найбільш вразливих рівнів забезпечення інформаційної безпеки залишається процедурний.

Більшість користувачів персональних комп'ютерів, у тому числі значна частка працівників прокуратури, не в повній мірі усвідомлюють серйозність і масштаби загроз інформаційній безпеці. У зв'язку з цим слід підкреслити, що антивірус не може виявляти 100 % шкідливих файлів. Тому для захисту від проникнення шкідливих програм потрібно ставити оновлення та обмежувати права користувачів персональних комп'ютерів. Сучасні шкідливі програми є комплексами з багатьох частин. Завантажувачі вірусів приходять першими, аналізують обстановку, впроваджують вірусну програму і самостійно видаляються.

У підсумку до дослідників потрапляє весь шкідливий комплекс, крім завантажувача вірусів, так як метод зараження (вразливість у системі) залишається невідомим і зараження може відбутися повторно. Коли практично кожен працівник прокуратури отримає доступ до великих баз даних і електронних систем взаємодії, ціна безпеки у даній сфері багаторазово зросте.

Виходячи з вищевикладеного, а також враховуючи інформацію у працях [10–15], можна зробити висновок, що з впровадженням цифрових

технологій в повсякденну діяльність органів прокуратури неминуче з'явиться новітня дисциплінарна практика. Недотримання вимог інформаційної безпеки загрожує багатьма негативними наслідками, серед яких як мінімум нанесення шкоди іміджу органів прокуратури та порушення прав та свобод людини і громадянина.

Висновки. Вимоги інформаційної безпеки за значимістю в доступній для огляду перспективі можна буде порівняти з вимогами Кодексу професійної етики та поведінки прокурорів і іншими важливими нормами, що регламентують діяльність працівника прокуратури [16]. За ігнорування даних норм повинна неминуче наступати юридична відповідальність. Крім застосування каральних заходів, зі співробітниками прокуратури необхідно проводити регулярні заняття, спрямовані на підвищення грамотності у сфері комп'ютерних технологій та інформаційної безпеки.

Обов'язковість регулярного оновлення знань з питань інформаційної безпеки обґрунтована безперервним протистоянням між корисним і шкідливим програмним забезпеченням. Неодмінною умовою професійної придатності для проходження служби в органах прокуратури найближчим часом стане наявність високого рівня володіння комп'ютерною технікою. Постійний розвиток і вдосконалення даних навичок доцільно розглядати як один з перспективних напрямів навчання прокурорів. В якості практичної пропозиції щодо підвищення ефективності використання інформаційних технологій, у тому числі щодо забезпечення інформаційної безпеки, у діяльності прокуратури України можна розглядати пропозицію про створення єдиної Концепції інформатизації та впровадження інформаційних технологій в діяльність прокуратури.

Література

1. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII (із змінами та доповненнями). URL:

https://zakon.rada.gov.ua/laws/show/2657-12#Text

2. Про створення служби захисту інформації кваліфікованого надавача електронних довірчих послуг органів прокуратури України: Наказ Офісу Генерального прокурора України від 12.01.2021 р. № 3. URL: https://zakon.rada.gov.ua/laws/show/v0003905-21#Text
3. Баранов О. А. Інтернет речей (IoT): мета застосування та правові проблеми // Інформація і право. 2018. № 2 (25). С. 31–44. URL: http://nbuv.gov.ua/UJRN/Infpr_2018_2_5
4. Гайдай С. Інформатизація прокурорської діяльності: теоретико-правові засади // Актуальні проблеми правознавства. 2019. Вип. 1(17). С. 120–125. URL: http://nbuv.gov.ua/UJRN/aprpr_2019_1_22
5. Про затвердження Стратегії розвитку прокуратури на 2021–2023 роки: Наказ Офісу Генерального прокурора України від 16.10.2020 р. № 489. URL:https://www.gp.gov.ua/ua/iord?_m=publications&_t=rec&id=262782
6. Кабмін схвалив Концепцію розвитку цифрових компетентностей до 2025 року // Офіційний веб-сайт Міністерства та Комітету цифрової трансформації України, 03.03.2021 р. URL: https://thedigital.gov.ua/news/kabmin-skhvaliv-kontseptsiyu-rozvitku-tsifrovikh-kompetentnostey-do-2025-roku
7. Про затвердження Національної економічної стратегії на період до 2030 року: Постанова Кабінету Міністрів України від 03.03.2021 р. № 179. URL: https://zakon.rada.gov.ua/laws/show/179-2021-%D0%BF#n25
8. Про основні засади кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII (із змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
9. Про створення робочої групи з питань запровадження функціоналу «кабінет реєстратора» в інформаційній системі «Єдиний реєстр досудових розслідувань»: Наказ Офісу Генерального прокурора України від 08.09.2020 р. № 415. URL:

https://www.gp.gov.ua/ua/iord?_m=publications&_t=rec&id=262782

10. Войтенко А. Б. Роль і місце прокуратури України в суспільстві як суб'єкта державної влади // Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки». 2021. № 5. doi: https://doi.org/10.25313/2520-2308-2021-5-7216
11. Сопільник Л. І., Скриньковський Р. М., Войтенко А. Б. Деякі аспекти покращення роботи прокурора та підвищення довіри суспільства до органів прокуратури України // Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки». 2021. № 6. doi: https://doi.org/10.25313/2520-2308-2021-6-7250
12. Войтенко А. Б., Скриньковський Р. М. Міжнародні (європейські) стандарти оцінювання роботи прокурорів // Міжнародний науковий журнал «Інтернаука». 2021. № 6. doi: https://doi.org/10.25313/2520-2057-2021-6-7225
13. Малашко О. Є., Скриньковський Р. М. Пріоритетні напрями удосконалення інформаційної безпеки України // Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки». 2020. № 6(28). С. 13–19.
14. Скриньковський Р. М., Малашко О. Є. Структурно-класифікаційна характеристика забезпечення інформаційної безпеки // Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки». 2020. № 7(29). С. 25–32.
15. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави: монографія / Центр навчально-наукових та науково-практичних видань Національної академії Служби безпеки України, 2014. 196 с.
16. Кодекс професійної етики та поведінки прокурорів: Затверджено Всеукраїнською конференцією прокурорів 27.04.2017 р. URL: https://zakon.rada.gov.ua/laws/show/n0001900-17#Text