УДК 343.1:004
DOI https://doi.org/10.32782/TNU-2707-0581/2024.6/19

Каланча І.Г.
Новоселицький відділ Чернівецької окружної прокуратури

Юрчишин Ю.В.
Чернівецька обласна прокуратура

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПРОКУРОРА ПІД ЧАС РОБОТИ З ЕЛЕКТРОННИМ СЕГМЕНТОМ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ В УКРАЇНІ

У статті досліджено потенційні небезпеки для прокурора під час роботи з електронним сегментом кримінального провадження, запропоновано превентивні заходи для їх запобігання. Вказано, що специфіка роботи прокурора обумовлює щоденне використання різних електронних як: Єдиний реєстр досудових розслідувань, Облік та статистика органів прокуратури, Система електронного документообігу органів прокуратури України. Різний правовий статус вказаних інформаційних систем та підходи до автентифікації та авторизації прокурора, як реєстратора чи користувача, обумовлюють різні підходи до забезпечення безпеки прокурора при роботі з інформаційними системами. Вказано, що забезпечення надійності паролів актуальне як для автентифікації та авторизації в електронних системах, так і для контролю доступу до облікового запису комп'ютера у зв'язку з чим досліджено вимоги до паролів а також можливі види заволодіння паролями, наведено підходи до ефективної протидії. Констатовано, що особливістю роботи з ЄРДР, на відміну від всіх інших електронних систем та баз даних, є його процесуальний статус, обумовлений наявністю в КПК України вимог щодо внесення до ЄРДР ключових відомостей під час досудового розслідування. Наголошено, що найважливішим для прокурора з точки зору ризиків розголошення інформації та наслідків дисциплінарного характеру є комплексне забезпечення безпеки засобів автентифікації та авторизації прокурора в ЄРДР як ключової електронної системи, що застосовується у кримінальній процесуальній діяльності. Проаналізовано практику притягнення прокурорів до дисциплінарної відповідальності за проступки, пов'язані з порушенням правил роботи з ЄРДР або електронним підписом до ЄРДР за результатами чого зроблено висновок, що основним порушенням є дублювання електронного підпису до ЄРДР та паролю для нього керівництвом окружних прокуратур. Наголошено, що важливим аспектом є забезпечення безпеки прокурора під час роботи прокурора з електронними (цифровими) доказами, що передбачає: гарантування цілісності; належне зберігання; забезпечення контролю доступу; застосування ефективних методів шифрування; документування процесу роботи; навчання прокурорів.; забезпечення прокурорів програмними та технічними засобами; дотримання норм КПК України та профільних законів; моніторинг та аудит робочих процесів.

Ключові слова: *прокурор, безпека, електронний сегмент, пароль, кримінальний процес, електронні докази, цифрові докази, гешування.*

Постановка проблеми. З розвитком технічного прогресу ефективність та безпека функціонування різних сфер сучасного життя дедалі більше залежить від забезпечення інформаційної безпеки. Зазначене особливо актуально з огляду на тенденції інноваційного вдосконалення кримінального процесу України. Роботу сучасного прокурора неможливо уявити без застосування комп'ютера. Зберігання службової інформації, відомостей щодо стану досудового розслідування кримінальних проваджень в електронному форматі в його модулях пам'яті є об'єктивною дійсністю сьогодення.

Аналіз останніх досліджень і публікацій. Питанням безпеки прокурора присвячений науково-практичний посібник «Особиста безпека прокурора» авторства Туркота М. С. та Столітнього А. В. (2019, також суміжній темі присвятили наукові свої статті Дегтярьова О. В. щодо забезпечення інформаційної безпеки у кримінальному провадженні (2020), та Топчій Н. С. щодо забезпечення інформаційної безпеки в електронному кримінальному провадженні в Україні (2024). Однак вказані дослідження не охоплюють сфери дослідження нашої статті, що обумовлює її актуальність.

Постановка завдання. Метою даної роботи є виявлення потенційних небезпек для прокурора під час роботи з електронним сегментом кримінального провадження, вироблення превентивних заходів для їх запобігання.

Виклад основного матеріалу. Важливим аспектом роботи прокурора є використання електронних інформаційних систем та баз даних. Специфіка роботи прокурора обумовлює щоденне використання таких електронних систем як: Інформаційна система «Єдиний реєстр досудових розслідувань» (далі – ЄРДР, Реєстр), Інформаційно-аналітична система «Облік та статистика органів прокуратури» (далі – ІАС «ОСОП») та Інформаційна система «Система електронного документообігу органів прокуратури України» (далі – ІС «СЕД»). Різний правовий статус вказаних інформаційних систем та підходи до автентифікації та авторизації прокурора, як реєстратора чи користувача, обумовлюють різні підходи до забезпечення безпеки прокурора при роботі з інформаційними системами.

Можна виділити кілька рівнів захисту, що мають бути організовані прокурором для безпечної роботи з електронними системами: 1. Безпека комп'ютера та службової інформації, що зберігається в електронному вигляді в його модулях пам'яті; 2. Безпека засобів автентифікації та авторизації прокурора в ІАС «ОСОП» та ІС «СЕД»; 3. Комплексне забезпечення безпеки засобів автентифікації та авторизації прокурора в ЄРДР.

Забезпечення прокурором безпеки комп'ютера та службової інформації, що зберігається в електронному вигляді в його модулях пам'яті передбачає: використання виключно ліцензійного програмного забезпечення (операційна система, офісні програми тощо), що дає можливість для постійного оновлення програмного забезпечення; використання для роботи з електронними системами та документами окремого облікового запису в операційній системі Windows без прав адміністратора; встановлення пароля на вхід до облікового запису, забезпечення його надійності та таємності; вимкнення функції віддаленого доступу та автоматичного завантаження сторонніх програм, що дозволяють віддалене управління комп'ютером, невикористання програм віддаленого управління комп'ютером; використання захищених вузлів доступу до мережі Інтернет; запобігання впливу шкідливого програмного забезпечення (використання актуальних антивірусних баз даних, періодичне здійснення антивірусної перевірки комп'ютера, дотримання безпеки електронного листування – при користуванні електронною поштою не відкривати електронні листи від невідомих адресатів, особливо з прикріпленими файлами, не переходити за наведеними в них посиланнями).

Робота з ІАС «ОСОП» та ІС «СЕД» передбачає особливості функціоналу на які прокурор не може вплинути а відтак й забезпечити їх безпеку. Позитивним моментом в забезпеченні безпеки інформації при роботі прокурора з ІАС «ОСОП» та ІС «СЕД» є те, що доступ до їх функціоналу можливий лише з визначених IP-адрес, тобто з приміщень відповідних прокуратур. Водночас, логіни до даних електронних систем є простою транслітерацією комбінації анкетних даних відповідного прокурора з додаванням однієї чи кількох цифр, однакової для працівників однієї прокуратури. Тобто для досить широкого кола суб'єктів, що володіють мінімумом інформації підбір логіна є більш ніж легким завданням, що негативно впливає на забезпечення безпеки.

В свою чергу, пароль для автентифікації та авторизації прокурора в ІАС «ОСОП» та ІС «СЕД» формується прокурором самостійно. Таким чином, забезпечення прокурором безпеки засобів автентифікації та авторизації прокурора в ІАС «ОСОП» та ІС «СЕД» передбачає формування надійного пароля та забезпечення його таємності.

Варто зауважити, що забезпечення надійності паролів актуальне як для автентифікації та авторизації в електронних системах, так і для контролю доступу до облікового запису комп'ютера. Насамперед прокурору необхідно відмовитись від практики застосування простих паролів та застосування однакових паролів для автентифікації в різних електронних системах.

Експерти менеджера паролів NordPass щорічно аналізують мільйони вкрадених паролів в мережі Інтернет і складають список з найбільш популярних з них. В 2023 році до його топ-25 увійшли: 123456, 123456789, qwerty, password, 1234567, 12345678, 12345, iloveyou, 111111, 123123, abc123, qwerty123, 1q2w3e4r, admin, qwertyuiop, 654321, 555555, lovely, 7777777, welcome, 888888, princess, dragon, password1, 123qwe [14]. Неефективність застосування подібних комбінацій як паролів вбачається очевидною.

Необхідно зауважити, що науковці відзначають, що найбільш раціональним для забезпечення функціональної безпеки систем бездротового зв'язку, за рахунок вдосконалення парольних політик, є спосіб генерування випадкових паро-

лів [11, с. 63]. Водночас, випадково згенеровані паролі, зазвичай, важко запам'ятати, що потребує їх письмової фіксації а відтак підвищує ризик дискредитації. Таким чином, часто застосовувані паролі доцільно формувати самостійно.

Загальні вимоги до формування надійного пароля передбачають, що він має містити: 1) не менш ніж 8 символів; 2) символи з будь-яких двох з наведених груп: а) латинські букви (прописні й рядкові): «A, B, C...» і «a, b, c...»; б) цифри: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9; в) символи (всі символи, що не належать до букв або цифр): ` ~ ! @ # $ % ^ & * ( ) _ + – = { } | [ ] \ : " ; ' < > ? , . / .

Підвищення ефективності паролів може бути забезпечено також іншими способами. По-перше, різні перестановки слів, включаючи заміну першої літери на прописну, заміну всіх літер на прописні, інверсія слова, заміна літери О на цифру 0, літери І на цифру 1 (або на знак оклику), заміна літери S на цифру 5, перетворення в множину (househouses). Цей спосіб дає близько 1000000 варіантів для перебирання. По-друге, різні перестановки слів, що не перекривають перший спосіб, заміна однієї малої літери на прописну (Olexander, oleXander, olexaNder та ін.), заміна двох (трьох і т.д.) малих літер (OlexaNder, OleXanDer). Другий спосіб за умови заміни однієї літери дає 400 000 варіантів, 2-х – 1 500 000 варіантів, 3-х – 3 000 000 варіантів для їх перебирання. Найбільш складний і захищений варіант – це пароль, що складається з двох коротких слів зі знаком пунктуації між ними. Через пароль, що складається з двох слів довжиною від 3 до 5 символів і знаку пунктуації між ними, дається близько 90 000 000 варіантів для перебирання (і це без використання першого та другого способів) [13, с. 174].

Також необхідно розуміти можливі види заволодіння паролями для ефективної протидії, серед них: підглядання за користувачем, коли той вводить пароль, що дає право на роботу з операційною системою; одержання пароля з файлу, в якому цей пароль був збережений користувачем, який не бажає утрудняти себе введенням пароля при під'єднанні до мережі (як правило, такий пароль зберігається у файлі в незашифрованому вигляді); пошук пароля, що користувачі записують на календарях, у записних книжках чи на зворотному боці комп'ютерних клавіатур; крадіжка зовнішнього носія з парольними даними (дискети чи електронного ключа, на яких зберігається пароль користувача) [12, с. 22].

Однак найважливішим для прокурора з точки зору ризиків розголошення інформації та наслідків дисциплінарного характеру є комплексне забезпечення безпеки засобів автентифікації та авторизації прокурора в ЄРДР як ключової електронної системи, що застосовується у кримінальній процесуальній діяльності.

Відповідно до п. 3 глава 1 розділу І Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення, затвердженого наказом Генерального прокурора № 231 від 17.08.2023 (далі – Положення про ЄРДР), Реєстр – електронна інформаційно-комунікаційна система, призначена для збирання, зберігання, захисту, оброблення, обліку, пошуку, узагальнення даних, зазначених у пункті 1 глави 1 розділу ІІ цього Положення, які використовуються для формування звітності, а також надання інформації про відомості, внесені до Реєстру, з дотриманням вимог кримінального процесуального законодавства та законодавства, яким урегульовано питання захисту персональних даних та доступу до інформації з обмеженим доступом [3].

Особливістю роботи з ЄРДР, на відміну від всіх інших електронних систем та баз даних, є його процесуальний статус, обумовлений наявністю в КПК України вимог щодо внесення до ЄРДР ключових відомостей під час досудового розслідування (ст. ст. 214, 218, 278, 280-282, 282 КПК України та ін.). З огляду на вказані норми КПК України, відомості ЄРДР є складовою кримінального провадження та на них розповсюджується відповідний процесуальний статус та процесуальні гарантії. Насамперед, щодо відомостей ЄРДР, як невід'ємної складової кримінального провадження, поширюються вимоги ст. ст. 221, 222 КПК України.

Відповідно до п.п. 1, 2 розділу VI Положення про ЄРДР адміністратор здійснює комплекс організаційних, технологічних та програмних заходів щодо захисту відомостей, які містяться в Реєстрі, від несанкціонованого доступу з урахуванням вимог до захисту такої інформації. Адміністратор за кожним фактом компрометації Реєстратором чи Користувачем особистих ключів для доступу до ЄРДР (втрата або пошкодження носія ключової інформації, розголошення ідентифікаторів тощо) невідкладно вживає заходів до його блокування та повідомляє про це керівництво органу прокуратури чи досудового розслідування, у якому працює такий Реєстратор чи Користувач. Повторна видача особистого ключа здійснюється після призначення службового розслідування чи перевірки обставин компрометації з обов'язковим подальшим інформуванням адміністратора Реєстру про

вжиті заходи до недопущення аналогічних порушень у майбутньому.

Автентифікація та авторизація користувача в ЄРДР здійснюється за допомогою електронного ключа доступу щодо якого встановлено суворі вимоги щодо зберігання та використання

Для використання електронного підпису як інструменту автентифікація та авторизація прокурора в ЄРДР необхідні носії ключової інформації, що надаються Адміністратором ЄРДР (Офіс Генерального прокурора та обласні прокуратури (за винятком спеціалізованих.

Надання послуг електронного підпису працівникам органів прокуратури здійснює Кваліфікований надавач електронних довірчих послуг органів прокуратури України (КНЕДП ОПУ), що є підрозділом Офісу Генерального прокурора.

Пунктами 23, 26, 27 частини першої статті 1 Закону України «Про електронні довірчі послуги» від 05 жовтня 2017 року № 2155-VIII (далі – Закон № 2155-VIII) передбачено, що кваліфікований електронний підпис – удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа [1].

Компрометація особистого ключа – будь-яка подія, що призвела або може призвести до несанкціонованого доступу до особистого ключа. Користувачі електронних довірчих послуг – підписувачі, створювачі електронних печаток, відправники та отримувачі електронних даних, інші фізичні та юридичні особи, які отримують електронні довірчі послуги у надавачів таких послуг відповідно до вимог цього Закону.

Згідно з частиною другою статті 12 Закону № 2155-VIII користувачі електронних довірчих послуг зобов'язані забезпечувати конфіденційність та неможливість доступу інших осіб до особистого ключа; невідкладно повідомляти надавача електронних довірчих послуг про підозру або факт компрометації особистого ключа.

Одним із основних напрямів державної інформаційної політики, згідно зі статтею 3 Закону України «Про інформацію» від 02 жовтня 1992 року № 2657-XII є забезпечення інформаційної безпеки України. Відповідно до статті 27 цього закону порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно із законами України [2].

Регламентом роботи кваліфікованого надавача електронних довірчих послуг органів прокуратури України, який 10 лютого 2022 року затверджено Генеральним прокурором та погоджено головою Державної служби спеціального зв'язку та захисту інформації України (далі – Регламент), передбачено обов'язковість його норм для усіх користувачів кваліфікованих електронних довірчих послуг, у тому числі підписувачів – працівників органів прокуратури [9].

Згідно з пунктом 4.20.1 Регламенту компрометація ключа підписувача – це факт, або обґрунтована підозра того, що особистий ключ став відомий або доступний до використання іншим особам.

Відповідно до приписів Інструкції щодо поводження з ключовими документами і носіями, затвердженої заступником Генерального прокурора України 05 листопада 2012 року: – носій ключової інформації разом з особистим ключем є об'єктом суворого зберігання; – посадова особа, яка є власником ЕЦП, несе персональну відповідальність за збереження цілісності ключового носія і відповідного ключа, а також за недопущення доступу до ключового носія інших осіб; – ключовий носій повинен зберігатись у службовому сейфі посадової особи або належної користувачу чарунці сейфа, яка повинна надійно зачинятись і опечатуватись; – власник має право зробити резервний запис паролю доступу до особистого ключа тільки на аркуші паперу, який буде зберігатись у запечатаному конверті в тому ж сховищі, що і ключовий носій. Робити інші записи паролю доступу заборонено; – під час тимчасового припинення виконання своїх службових обов'язків посадовою особою – власником особистого ключа (у зв'язку з відпусткою, хворобою тощо), він повинен подати в ЦСК або регіональний центр реєстрації заяву про блокування сертифіката (може бути подано усно за телефоном з використанням фрази-паролю).

Власник особистого ключа зобов'язаний: вживати всіх заходів до забезпечення безпечного зберігання ключового носія; зберігати в таємниці пароль доступу до особистого ключа; використовувати ключ тільки особисто та лише в службових цілях.

Категорично заборонено копіювати ключові дані з ключового носія на будь-які інші носії, передавати ключовий носій іншим особам. Розголошення пароля, а також втрата ключового носія або його потрапляння до інших осіб є фактом компрометації особистого ключа.

Згідно із пунктом 2 розділу VII Положення про ЄРДР, Реєстратори та Користувачі відповідають за порушення вимог цього Положення, отри-

мання, призупинення, поновлення та припинення доступу до Реєстру відповідно до службових повноважень, компрометацію особистих ключів електронного підпису для доступу до ЄРДР (втрату або пошкодження носія ключової інформації, розголошення ідентифікаторів тощо) [3]. Відповідальність за порушення вимог чинного законодавства під час користування ЄРДР Реєстраторами чи Користувачами органів прокуратури України настає за результатами розгляду відповідної скарги Кваліфікаційно-дисциплінарною комісією прокурорів (далі – КДКП). КДКП, діючи на засадах верховенства права, законності, незалежності, відкритості і гласності, колегіальності, змагальності, неупередженості, об'єктивності та дотримання гарантій незалежності прокурора, визначає рівень фахової підготовки осіб, які виявили намір зайняти посаду прокурора, та вирішує питання щодо дисциплінарної відповідальності прокурорів, переведення та звільнення прокурорів з посади (частина перша статті 73 Закону України «Про прокуратуру», пункт 7 Положення про порядок роботи відповідного органу, що здійснює дисциплінарне провадження).

За результатами опрацювання практики притягнення до дисциплінарної відповідальності прокурорів КДКП за проступки, пов'язані з порушенням правил роботи з ЄРДР або електронним підписом до ЄРДР можна зробити висновок, що основним порушенням є дублювання електронного підпису до ЄРДР та паролю для нього керівництвом окружних прокуратур.

Наприклад, рішенням КДКП [10] Особа_3 притягнуто до дисциплінарної відповідальності та накладено дисциплінарне стягнення у виді догани за порушення вимог Інструкції щодо поводження з ключовими документами і носіями від 05.12.2012. Встановлено, що в одному з кримінальних проваджень (за ознаками кримінального правопорушення, передбаченого ч. 3 ст. 368 КК України), крім осіб, які його переглядали у зв'язку з безпосереднім виконанням своїх службових обов'язків, здійснювався з використанням електронного цифрового підпису для входу до ЄРДР Особа_3 9 разів із різних Ір-адрес (протягом липня-вересня 2017 року). Згідно з інформацією ГПУ за період з червня по вересень 2017 року Особа_3 здійснив перегляд 356 кримінальних проваджень, у яких інформації (спецповідомлення) до ГПУ відділом не готувалися, до виконання завдань, доручень, аналітичних досліджень працівники очолюваного ним відділу не залучалися, що свідчить про можливе використання ним інформації із ЄРДР в особистих цілях. Крім цього, під час перебування Особа_3 у відпустці (за межами України) з використанням його особистого електронного цифрового підпису систематично здійснювався вхід до ЄРДР з різних Ір-адрес. З червня по липень 2017 року з використанням особистого ключа Особа_3 вхід у кримінальне провадження Номер_1 здійснювався 19 разів, у тому числі 6 разів упродовж однієї доби. Окрім Ір-адрес прокуратури Н-ської області та Н-ської місцевої прокуратури, вхід до ЄРДР з використанням особистого ключа Особа_3 здійснювався також з інших динамічних Ір-адрес, що не використовуються в діяльності органів прокуратури Н-ської області, в тому числі в робочий та позаробочий час, вночі. Також під час перевірки встановлено, що сертифікат особистого ключа Особа_3 на період його відпустки не був заблокований, чим порушено вимоги Інструкції щодо поводження з ключовими документами і носіями від 05.11.2012, якою передбачено, що під час тимчасового припинення виконання своїх службових обов'язків посадовою особою – власником особистого ключа (у зв'язку з відпусткою, хворобою та ін.), вона повинна подати у регіональний центр реєстрації заяву про блокування сертифікату.

Таким чином, під час дисциплінарного провадження в діях Особа_1 КДКП встановлено, що Особа_3, у порушення абзаців 2, 6 розділу «Носій ключової інформації разом із особистим ключем є об'єктом суворого зберігання» Інструкції щодо поводження з ключовими документами і носіями від 05.11.2012, яка передбачає, що ключовий носій повинен зберігатися у службовому сейфі посадової особи або належної користувачу чарунці сейфа, не подавши в ЦСК або регіональний центр реєстрації заяву про блокування сертифікату, умисно вивіз за кордон ключовий носій, з яким перебував там та в цей час за його допомогою здійснював входження до ЄРДР.

Також варто звернути увагу на випадок притягнення Наказом прокурора Н-ської області до дисциплінарної відповідальності та оголошення догани ОСОБА_4 за неналежне виконання службових обов'язків, що виразилось у недбалому зберіганні службового посвідчення посадової особи органів прокуратури України, невжитті заходів для безпечного зберігання ключового носія, внаслідок чого вони були втрачені [4].

Встановлено, що у ОСОБА_4, в період перебування на лікарняному, було викрадено сумку з документами, службовим посвідченням та ключовим носієм реєстратора ЄРДР. Після цього

ОСОБА_4 було негайно викликано поліцію та подано заяву про злочин, відомості про вказану подію внесено до ЄРДР. Приступивши до виконання своїх службових обов'язків ОСОБА_4 звернувся з усною заявою до регіонального Центру приймання дзвінків Центру сертифікації ключів та повідомив про крадіжку ключового носія та службового посвідчення. За фактом втрати службового посвідчення та ключового носія проведено службове розслідування яким встановлено, що ОСОБА_4 у період тимчасової непрацездатності, у порушення пункту 4.1 Інструкції про службове посвідчення працівника прокуратури України, затвердженої наказом Генерального прокурора України №55 від 11.06.2012, у результаті недбалого ставлення до своїх службових обов'язків не забезпечив належного зберігання службового посвідчення, внаслідок чого воно було втрачено. У порушення пункту 4.5 Інструкції про службове посвідчення працівника прокуратури України, ОСОБА_4 негайно не повідомив керівника прокуратури про втрату посвідчення. Також, ОСОБА_4 у порушення вимог ст. 7 Закону України «Про електронний цифровий підпис», Інструкції про поводження з ключовими документами і носіями від 05.11.2012, не вжив необхідних заходів для безпечного зберігання ключового носія, не повідомив Центр сертифікації ключів (ЦСК) або адміністратора ЦСК у Н-ській області про тимчасове припинення виконання своїх службових обов'язків у зв'язку з, що призвело до втрати ключового носія та створило умови для розголошення конфіденційної інформації, що міститься у ЄРДР.

Судом першої інстанції адміністративний позов ОСОБА_4 до Прокуратури Н-ської області про визнання дій протиправними, визнання протиправним та скасування наказу задоволено частково, визнано протиправним та скасовано наказ про оголошення догани ОСОБА_4 за неналежне виконання службових обов'язків [8]. Судом апеляційної інстанції рішення суду першої інстанції скасовано, прийнято нову постанову якою в позові ОСОБА_4 відмовлено [7]. Судом касаційної інстанції рішення суду апеляційної інстанції залишено без змін [4]. Колегія суддів касаційної інстанції погодилася з висновком суду апеляційної інстанції про те, що під час тимчасового припинення виконання своїх службових обов'язків через хворобу ОСОБА_4 як власник особистого ключа не подав в ЦСК або регіональний центр реєстрації заяву (у будь-якій формі) про блокування сертифікату. Крім того, всупереч вимогам наведеної вище Інструкції щодо поводження з ключовими документами і носіями від 05.11.2012, ОСОБА_4 не забезпечив належного зберігання ключового носія, а мав його при собі під час перебування на лікарняному. Таким чином, виявлені в ході службового розслідування обставини є достатньою підставою для притягнення ОСОБА_4 до дисциплінарної відповідальності за неналежне виконання службових обов'язків. При цьому, приймаючи наказ про оголошення ОСОБА_4 догани за неналежне виконання службових обов'язків, відповідачем враховано обставини, що можуть обтяжувати або пом'якшувати ступінь і характер відповідальності ОСОБА_4, його особисті характеристики, і притягнуто до найлегшого виду дисциплінарного стягнення.

Також варто звернути увагу на випадки притягнення до дисциплінарної відповідальності, якими прокурорів звільнено з посади у зв’язку з, в тому числі, порушенням Інструкції щодо поводження з ключовими документами і носіями від 05.11.2012, яке полягає у неподанні заяви про блокування електронного ключа доступу до ЄРДР на час відпустки та допущенням доступу до свого особистого електронного цифрового ключа доступу до Єдиного реєстру досудових розслідувань. При чому, в обох випадках з вказаними рішення погодились суди всіх інстанцій, підтвердивши наявність порушень в наведеній частині [5, 6].

Описані нами практичні кейси вказують на важливість дотримання прокурором вимог чинного законодавства України щодо поводження з ключовими документами і носіями при користуванні електронними ключами доступу до ЄРДР.

Невід’ємною складовою правового аспекту інформаційної безпеки ЄРДР є *усвідомлення прокурором потенційної кримінальної відповідальності за незаконні дії* як з ЄРДР, так і з даними, що в ньому містяться. Вказані протиправні дії в контексті норм Кримінального кодексу України (далі – КК України) передбачає таку потенційну кваліфікацію діянь: несанкціоноване втручання в роботу ЄРДР – за ст. 361 КК України; несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в ЄРДР – за ст. 361-2 КК України; несанкціоновані дії з інформацією, яка оброблюється в ЄРДР або зберігається в ньому, вчинені особою, яка має право доступу до ЄРДР – за ст. 362 КК України; порушення правил експлуатації ЄРДР або порядку чи правил захисту інформації, яка в ньому оброблюється – за ст. 363 КК України; службове підроблення в частині внесення неправдивих відомостей до ЄРДР – за ст. 366 КК України; роз-

голошення відомостей ЄРДР як даних досудового розслідування – за ч. 2 ст. 387 КК України.

Ще одним важливим аспектом є забезпечення безпеки прокурора під час роботи прокурора з електронними (цифровими) доказами, що передбачає: 1. *Гарантування цілісності електронних (цифрових) доказів*: Прокурор має вжити заходів для забезпечення того, щоб електронні (цифрові) докази не були змінені, пошкоджені або знищені,. Для цього використовуються засоби фіксації їхнього стану (найефективнішим з яких є гешування) та обов'язкове ведення журналу всіх дій з доказами; 2. *Належне зберігання електронних (цифрових) доказів*: Електронні (цифрові) докази, що розміщені на фізичних носіях повинні зберігатися в спеціально організованих місцях з дотриманням експлуатаційних рекомендацій, забезпечення їх конфіденційності та цілісності а також їх резервні копії повинні зберігатися централізовано на сервері органу досудового розслідування або органу прокуратури; 3. *Забезпечення контролю доступу до електронних (цифрових) доказів.* Обмеження доступу до електронних (цифрових) доказів має бути належним та відповідати вимогам КПК України. Доступ до доказів повинні мати лише уповноважені особи, і цей доступ має фіксуватися та реєструватися для забезпечення можливості подальшого контролю; 4. *Застосування ефективних методів шифрування електронних (цифрових) доказів*. Для захисту цифрових доказів від несанкціонованого доступу використовуються методи шифрування. Це особливо важливо при передачі даних або при їх зберіганні на зовнішніх фізичних носіях; 5. *Документування процесу роботи з електронними (цифровими) доказами (chain of custody)*. Усі етапи роботи з електронними (цифровими) доказами (від вилучення до зберігання і використання в суді) мають бути детально задокументовані, що включає фіксацію часу, місця, осіб, які мали доступ до доказів, а також інструментів і методів, що використовувались під час роботи з ними; 6. *Навчання прокурорів.* Прокурори та інші особи, які працюють з електронними (цифровими) доказами, повинні проходити регулярне навчання щодо правильного поводження з такими доказами та щодо нових методів захисту; 7. *Забезпечення прокурорів програмними та технічними засобами*, що передбачає використання прокурорами спеціалізованих програмних та апаратних засобів для виявлення, фіксації, аналізу та зберігання електронних (цифрових) доказів, які забезпечують максимальний рівень безпеки; 8. *Дотримання норм КПК України, профільних законів та ДСТУ під час роботи з електронними (цифровими) доказами.* Це передбачає, що прокурор має діяти відповідно до вимог КПК України, профільних законів та ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) "Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів", що регулюють використання роботи з електронними (цифровими) доказами. Це передбачає дотримання норм щодо конфіденційності, прав людини та забезпечення належного процесу доказування; 9. *Моніторинг та аудит процесів роботи з електронними (цифровими) доказами*, що передбачає постійний аудит і моніторинг доступу та використання електронних (цифрових) доказів та дозволятиме вчасно виявити порушення і запобігти потенційним загрозам. Наведені заходи мають на меті забезпечення безпеку прокурора під час роботи з електронними (цифровими) доказами і гарантувати їх цілісність та достовірність.

Висновки. Дотримання прокурором вимог безпеки під час роботи з електронним сегментом кримінального провадження є невід'ємно складовою загальної системи забезпечення особистої безпеки прокурора та ефективного виконання прокурором службових повноважень. Електронне середовище, як одне з найбільш важливих та найменш вивчених прокурорами потребує особливої уваги та вжиття вичерпних заходів щодо: забезпечення безпеки комп'ютера та службової інформації, що зберігається в електронному вигляді в його модулях пам'яті, забезпечення безпеки засобів автентифікації та авторизації прокурора інформаційних системах та роботи з електронними (цифровими) доказами.

Список літератури:

1. Про електронні довірчі послуги : Закон України від 05 жовтня 2017 року № 2155-VIII (зі змін. і доп.). URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text

2. Про інформацію : Закон України від 02 жовтня 1992 року № 2657-XII (зі змін. і доп.). URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

3. Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення, затв. наказом Генерального прокурора № 231 від 17.08.2023. URL: https://zakon.rada.gov.ua/laws/show/v0298905-20#Text

4. Постанова Верховного Суду у складі колегії суддів Касаційного адміністративного суду від 05.03.2018 у справі № 804/2948/17. URL: https://zakononline.com.ua/court-decisions/show/72693440

5. Постанова Верховного Суду у складі колегії суддів Касаційного адміністративного суду від 30.04.2020 у справі № 821/677/17. URL: https://reyestr.court.gov.ua/Review/89012942

6. Постанова Верховного Суду у складі колегії суддів Касаційного адміністративного суду від 24.06.2020 у справі № 826/6147/17. URL: https://reyestr.court.gov.ua/Review/90029742

7. Постанова Дніпропетровського апеляційного адміністративного суду від 21.11.2017 у справі № 804/2948/17. URL: https://reyestr.court.gov.ua/Review/70546264

8. Постанова Дніпропетровського окружного адміністративного суду від 21.07.2017 у справі № 804/2948/17. URL: https://reyestr.court.gov.ua/Review/67887163

9. Регламентом роботи кваліфікованого надавача електронних довірчих послуг органів прокуратури України, який 10 лютого 2022 року затверджено Генеральним прокурором та погоджено головою Державної служби спеціального зв'язку та захисту інформації України. URL: https://ca.gp.gov.ua/uk/pro-knedp/reglament-knedp

10. Рішення Кваліфікаційно-дисциплінарної комісії прокурорів №69дп-17 від 30.08.2017. URL: https://www.kdkp.gov.ua/decision/2017/08/30/850

11. Бурячок В.Л. А.В Платоненко, О.В. Семко Вибір раціонального способу генерування паролів серед множини існуючих // Безпека інформації. 2019. Том 25, № 1. С. 59–64.

12. Франчук В.М. Захист інформаційних ресурсів: криптографічні та стеганографічні методи захисту даних. Посібник для викладачів, вчителів та студентів інформатичних спеціальностей. К.: НПУ імені М.П. Драгоманова, 2012. 120 с.

13. Франчук В.М. Захист даних. Засоби парольної ідентифікації та адміністрування // Науковий часопис НПУ імені М.П. Драгоманова. Серія 2 : Комп'ютерно-орієнтовані системи навчання. 2017. № 19. С. 170-174.

14. NordPass password manager. 2019. URL: https://nordpass.com/most-common-passwords-list/

Kalancha I.H., Yurchyshyn Yu.V. ENSURING THE SAFETY OF PROSECUTORS WHEN WORKING WITH THE ELECTRONIC SEGMENT OF CRIMINAL PROCEEDINGS IN UKRAINE

In the article, the authors study the potential dangers for a prosecutor when working with the electronic segment of criminal proceedings and propose preventive measures to prevent them. The authors point out that the specifics of the prosecutor's work determine the daily use of various electronic tools: The Unified Register of Pre-trial Investigations, Accounting and Statistics of Prosecutor's Offices and the Electronic Document Management System of the Prosecutor's Office of Ukraine. Different legal status of these information systems and approaches to authentication and authorisation of the prosecutor as a registrar or user determine different approaches to ensuring the security of the prosecutor when working with information systems. The authors point out that ensuring the reliability of passwords is relevant both for authentication and authorisation in electronic systems and for controlling access to a computer account, and in this regard, the author examines the requirements for passwords and possible types of password theft, and provides approaches to effective counteraction. The authors establish that the peculiarity of working with the URPTI, unlike all other electronic systems and databases, is its procedural status due to the requirements in the CPC of Ukraine to enter key information into the URPTI during the pre-trial investigation. The authors emphasise that the most important thing for a prosecutor in terms of the risks of information disclosure and disciplinary consequences is to ensure comprehensive security of the means of authentication and authorisation of a prosecutor in the URPTI as a key electronic system used in criminal proceedings. The authors analyse the practice of bringing prosecutors to disciplinary liability for misconduct related to violation of the rules of work with the URPTI or electronic signature to the URPTI, and conclude that the main violation is duplication of the electronic signature to the URPTI and its password by the management of district prosecutor's offices. The authors emphasize that an important aspect is to ensure the prosecutor's security when working with electronic (digital) evidence, which includes: ensuring integrity; proper storage; ensuring access control; application of effective encryption methods; documenting the work process; training of prosecutors; providing prosecutors with software and hardware; compliance with the provisions of the CPC of Ukraine and relevant laws; monitoring and auditing of work processes.

Key words: *prosecutor, security, electronic segment, password, criminal procedure, electronic evidence, digital evidence, hashing.*