УДК: [343.13+342.9](477):004
ORCID: 0000-0002-2886-9379
e-mail: stoleta@ukr.net

Anton V. Stolitnii,
Head of the Poltava Region Prosecutor's Office
(Poltava Region Prosecutor's Office)

Столітній Антон Володимирович,
Керівник Полтавської обласної прокуратури
(Полтавська обласна прокуратура)

КОНЦЕПЦІЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ДЕРЖАВНОГО БЮРО РОЗСЛІДУВАНЬ

THE CONCEPT OF INFORMATION AND TELECOMMUNICATION SYSTEM OF THE STATE BUREAU OF INVESTIGATIONS

Анотація. У статті представлено Концепцію інформаційно-телекомунікаційної системи Державного бюро розслідувань та сформульовано її ключові положення, серед яких: завдання інформаційно-телекомунікаційної системи, етапи та заходи створення, її суб'єкти, категорії та види їх ролей, функціональна архітектура, інформаційна безпека, кібербезпека, схема інтеграції до електронного інформаційного поля органів кримінальної юстиції. Запропоновано етапи реалізації Концепції та її інтеграції до електронного інформаційного поля органів кримінальної юстиції, процесуальною надбудовою якого є Електронне кримінальне провадження.

Ключові слова: кримінальне провадження, Державне бюро розслідувань, інформаційно-телекомунікаційна система, Україна, етапи створення, суб'єкти, функціональна архітектура, інформаційна безпека, інтеграція.

Summary. The article introduces the Concept of information and telecommunication system of the State Bureau of Investigations and defines its key provisions: information and telecommunication system objectives, development phases and activities, its entities, their role types and categories, functional architecture, information security, cyber security, integration scheme to the electronic information field of the criminal justice agencies. The paper suggests the Concept implementation phases and those of its integration to the electronic information field of the criminal justice agencies, its procedural superstructure being the Electronic criminal proceeding system.

Key words: criminal proceeding, State Bureau of Investigations, information and telecommunication system, Ukraine, development phases, entities, functional architecture, information security, integration.

Постановка проблеми. Державне бюро розслідувань (далі – ДБР) перебуває в процесі становлення електронного сегменту своєї діяльності, що актуалізує питання створення відомчої інформаційно-телекомунікаційної системи (далі – ІТС).

Положення п. 10 ч. 1 ст. 6, п. 7 ч. 1 ст. 7 Закону України «Про Державне бюро розслідувань» [2, с. 1] (далі – Закон) визначають повноваження ДБР щодо самостійного створення інформаційних систем. Зазначене доцільно реалізувати шляхом створення відомчої ІТС, інтегрованої з Єдиним реєстром досудових розслідувань (далі – ЄРДР) як чинним електронним кримінальним процесуальним правореалізаційним засобом та потенційним процесуальним інструментом електронного кримінального провадження (далі – ЕКП). Реалізація вказаної технологічної складової роботи ДБР потребує розробки Концепції ІТС ДБР.

Пропонована Концепція ІТС ДБР створена за моделлю уніфікованої Концепції інформаційно-телекомунікаційної системи органу досудового розслідування [7, с. 14-23] та є логічним продовженням Концепції електронного

кримінального провадження [8, с. 24-35] в частині залучення ДБР як учасника кримінального провадження до єдиного електронного інформаційного поля органів кримінальної юстиції.

Стан опрацювання обраної теми, аналіз останніх публікацій та досліджень. Теоретичні, організаційні та процесуальні аспекти діяльності ДБР досліджували Є.Д. Скулиш (2015), О.Ю. Бусол (2016),М.А. Погорецький (2018), Деревянко Б.В. (2019), Дрозд О.Ю. (2020) та інші українські вчені. Водночас, питання забезпечення системної інформатизації діяльності ДБР та реалізація повноважень щодо самостійного створення інформаційних систем залишились поза увагою науковців.

Метою даної роботи є формулювання ключових положень Концепції ІТС ДБР, серед яких: завдання ІТС ДБР, етапи та заходи її створення, суб'єкти ІТС ДБР, категорії та види ролей суб'єктів, адміністративний та технічний аспекти інформаційної безпеки ІТС ДБР, кібербезпека ІТС ДБР, функціональна архітектура ІТС ДБР, схема інтеграції ІТС ДБР до єдиного електронного інформаційного поля органів кримінальної юстиції.

Методологічною основою цієї роботи є сукупність загальнонаукових та спеціально-юридичних методів: діалектичний, системно-структурний, аналогії, системного аналізу, формально-юридичний, моделювання, синергетичний тощо.

Виклад основного матеріалу. Стрімкий розвиток інформаційних технологій, що охопив всі сфери життя суспільства, перехід «діалогу» з державою в електронний формат, ведення електронних державних реєстрів та баз даних створюють передумови для інформатизації роботи ДБР шляхом створення відомчої ІТС, спрямованої на інформаційно-технологічне супроводження діяльності органу досудового розслідування та інтегрованої до єдиного електронного інформаційного поля органів кримінальної юстиції. Створення ІТС ДБР забезпечуватиме дотримання вимог ст. 2 Кримінального процесуального кодексу України (далі – КПК України) щодо швидкого, повного та

неупередженого розслідування, сприятиме ефективному розслідуванню та розкриттю правопорушень, адже економитиме час та ресурси.

Нормативною підставою створення ІТС ДБР є п. 10 ч. 1 ст. 6, п. 7 ч. 1 ст. 7 Закону, щодо: самостійного створення інформаційних систем та ведення оперативного обліку в обсязі і порядку, що визначаються завданнями, покладеними на ДБР, із дотриманням законодавства про захист персональних даних (п. 10 ч. 1 ст. 6); створення інформаційних систем та ведення оперативного обліку у цілях оперативно-розшукової та слідчої діяльності, в обсязі і порядку, передбачених законодавством (п. 7 ч. 1 ст. 7). Вимоги до ІТС ДБР необхідно визначати з урахуванням потреби реалізації в електронному інформаційному середовищі таких повноважень ДБР як: доступу як користувача до інформаційних систем органів державної влади, перелік яких встановлюється Кабінетом Міністрів України (п. 10 ч. 1 ст. 6); безоплатно одержувати в порядку, передбаченому КПК України, за письмовими запитами Директора ДБР, його уповноваженого заступника, директорів територіальних управлінь ДБР або їхніх уповноважених заступників інформацію, необхідну у справах про злочини, що знаходяться у провадженні ДБР, у тому числі з автоматизованих інформаційних і довідкових систем, реєстрів та банків даних, держателем (адміністратором) яких є органи державної влади або органи місцевого самоврядування, у тому числі інформацію з обмеженим доступом (п. 2 ч. 1 ст. 7); здійснення інформаційно-аналітичних заходів щодо встановлення системних причин та умов проявів організованої злочинності та інших видів злочинності, протидію яким віднесено до компетенції ДБР, вжиття заходів до їх усунення (п. 2 ч. 1 ст. 6). Також в КПК України визначено завдання ДБР як органу досудового розслідування, що обумовлює відображення в ІТС ДБР відповідного функціоналу. На виконання положень абз. 3 п. 5.12. Стратегії реформування судоустрою, судочинства та суміжних правових інститутів на 2015–2020 роки, необхідно забезпечити інтеграцію ІТС ДБР до єдиного електронного інформаційного поля органів кримінальної юстиції. З урахуванням визначеного обсягу функцій в ІТС ДБР

доцільно реалізувати забезпечення завдань з: внутрішньої електронної комунікації; електронної організації роботи та управління шляхом постановки завдань та контролю їх виконання; ведення уніфікованого обліку (реєстрації) інформації; автоматизованого); виконання автоматизації ведення статистики; аналізу діяльності (в тому числі інших адміністративних функцій (трудових, фінансових, господарських тощо); ведення оперативного обліку; зовнішньої електронної комунікації.

Виходячи з адміністративної складової органу та функцій ДБР щодо здійснення досудового розслідування доцільно створення трьох блоків ІТС ДБР: *адміністративний* (організація роботи, безпеки, документообіг та внутрішня ділова переписка, кадрова робота тощо), *процесуальний* (інтеграція з програмним забезпеченням Електронного кримінального провадження як процесуальної надбудови електронного інформаційного поля органів кримінальної юстиції) та *оперативний* (діяльність оперативних підрозділів ДБР в інформаційній сфері).

Створення ІТС ДБР включає в себе заходи з **розробки** (нормативної основи роботи та програмного забезпечення), **впровадження** в роботу та **інтеграції** до електронного інформаційного поля. Реалізація зазначених заходів пропонується за сімома послідовними етапами:

1. Створення нормативної основи (розробка та затвердження: Технічного завдання на розробку програмного забезпечення ІТС ДБР; Технічного завдання для серверної системи апаратної частини ІТС ДБР (аналітична); Специфікації (технічні вимоги) до ІТС ДБР; Положення про порядок ведення ІТС ДБР; Правил розмежування прав доступу до ресурсів ІТС ДБР (затверджених Директором ДБР), Положенням про обмін даними між ІТС ДБР та ЄРДР (затвердженого Директором ДБР та Генеральним прокурором) тощо);

2. Створення програмного забезпечення (розробка програмного забезпечення ІТС ДБР (включаючи комплексну систему захисту інформації ІТС ДБР): проектування, розробка, тестування функціональності, застосовності та

безпеки, аудит інформаційної та криптографічної безпеки програмного забезпечення, тестування дієвості та продуктивності ІТС ДБР. **Функціональна архітектура ІТС ДБР** відображає структуру програмного забезпечення електронної системи відповідно до її завдань та розподілена за наступними складовими: Система інформаційної безпеки ІТС ДБР (включає підсистему автентифікації користувачів (система паролів доступу до електронної системи), підсистему управління повноваженнями користувачів та підсистему фіксації та аналізу дій користувачів); Підсистема організації роботи та управління (включає Модуль організації внутрішнього документообігу); Електронний кабінет (включає Комунікаційний модуль); Підсистема аналізу; Підсистема обліку та статистики; Підсистема управління персоналом (облік кадрів); Підсистема управління фінансово-господарськими процесами; Підсистема ведення оперативного обліку; Інтеграційна шина обміну даних між ІТС ДБР та зовнішніми електронними інформаційними ресурсами; Модуль обміну структурованою електронною інформацією з підсистемою Електронного кримінального провадження;

3. Створення (розширення) технічної інфраструктури (створення центру зберігання та обробки даних ІТС ДБР; забезпечення підрозділів ДБР пристроями для оцифрування документів, отриманих у паперовій формі; збільшення пропускної здатності мережевого підключення приміщень підрозділів ДБР для забезпечення суб`єктів кримінального провадження можливістю працювати з відео-файлами та іншими матеріалами великого об’єму);

4. Запровадження пілотного проекту ІТС ДБР (апробація електронної системи у формі пілотного проекту в одному з територіальних підрозділів ДБР строком від 1 до 3 місяців; проведення (за потреби) коригування програмного забезпечення ІТС ДБР відповідно до отриманих зауважень). **Інтерфейс** ІТС ДБР для її користувачів представлений у формі електронного робочого столу, функціонал якого визначатиметься залежно від ролі користувача в електронні

системі, що потребують попереднього тестування користувачами та оптимізації перед впровадженням в роботу. Також **функціональність** ІТС ДБР передбачатиме **для кожної з експлуатаційних ролей** користувачів додаткові опції, спеціалізований функціонал, модифікації інтерфейсу, налаштування Електронного кабінету, що також потребують тестування користувачами та оптимізації;

5. Навчання суб'єктів ІТС ДБР роботі з функціоналом електронної системи (навчання роботі з ІТС ДБР; створення спеціалізованих програм-тренажерів для самостійного дистанційного навчання роботі з функціоналом ІТС ДБР);

6. Впровадження ІТС ДБР в роботу органу досудового розслідування (проведення приймальних випробувань ІТС; перевірки технічної інфраструктури ІТС ДБР; отримання сертифікату відповідності за результатами державної експертизи ІТС ДБР у сфері технічного захисту інформації; оцінки результатів апробації електронної системи у формі пілотного проекту; оцінки ступеня готовності користувачів, за результатами навчання роботі з функціоналом ІТС ДБР; затвердження відомчого документу про впровадження ІТС в експлуатацію та її обов'язкове застосування);

7. Інтеграція ІТС ДБР до електронного інформаційного поля органів кримінальної юстиції, в тому числі Електронного кримінального провадження як його процесуальної надбудови (розробка та затвердження Положенням про обмін даними між ІТС ДБР та ЄРДР, затвердженим Директором ДБР та Генеральним прокурором; функціональне та технічне підключення до інтеграційного середовища Електронного кримінального провадження (Рис. 1) для забезпечення обміну даними в порядку електронного кримінального провадження з ЄРДР) [7, с. 15-21].

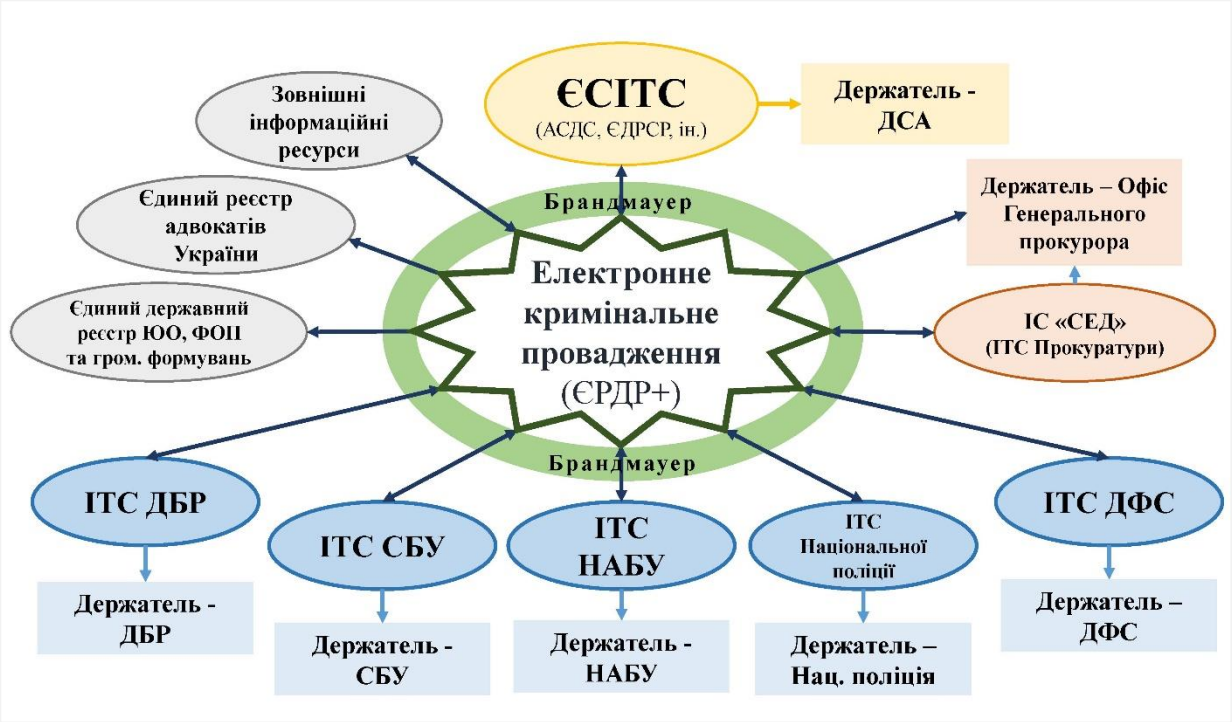

Рис. 1. *Схема інтеграції ІТС ДБР до єдиного електронного інформаційного поля органів кримінальної юстиції.*

Послідовна реалізація запропонованих етапів дозволить забезпечити швидке проектування та ефективне запровадження ІТС ДБР, належну апробацію її функціоналу та врахування інтересів користувачів.

Одним з ключових положень функціонування ІТС ДБР є її суб'єкти, до яких належать: **держатель, адміністратори та користувачі**. Ефективне розмежування повноважень суб'єктів ІТС ДБР в частині доступу до його ресурсів обумовлює визначення їх ролей в електронній системі, що поділяються на дві категорії: *адміністративні ролі: адміністратор безпеки* – забезпечує захищеність ресурсів ІТС; надання забезпечує доступ користувачам до ресурсів згідно з їх повноваженнями; забезпечує контроль за виконанням користувачами та іншими адміністраторами вимог політики безпеки; *адміністратор мережевих сервісів* – налаштовує та обслуговує операційні системи активного мережевого обладнання, створює резервні копії та відновлює функціонування цього обладнання; *системний адміністратор* –інсталює, налаштовує та обслуговує операційні системи серверів, встановлює на них програмного забезпечення; *адміністратор баз даних* – інсталює, налаштовує та обслуговує системи

керування базами даних, розгортає та обслуговує бази даних ІТС [6, с. 18]; *експлуатаційні ролі*: *«користувач»* – має доступ до функціоналу ІТС ДБР в обсязі, визначеному займано посадою, наданими процесуальними та/або адміністративними повноваженнями [7, с. 16-17].

Експлуатаційні ролі (користувачі) визначаються відповідно до займаної посади, наданих процесуальних та/або адміністративних повноважень, тобто структури ДБР та утворюють доцентрову комунікаційну структуру з Підсистемою організації роботи та управління ІТС (Рис. 2).

Рис. 2. *Комунікаційна структура ролей користувачів ІТС ДБР.*

Забезпечення належного рівня безперервного функціонування електронної системи та захисту інформації дозволяє суміщення двох або більше адміністративних ролей за виключенням ролі адміністратора безпеки. При цьому заборонено суміщення адміністративних та експлуатаційних ролей [6, с. 19].

Інформаційна безпека є Невід'ємним аспектом ефективної роботи ІТС ДБР. Її варто розглядати в адміністративному (організаційному) та технічному аспектах. Відповідно до ч. 2 ст. 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», державні інформаційні ресурси

або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Комплексна система захисту інформації – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації (абз. 11 ст. 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах») [4, с. 1]. Створення комплексної системи захисту інформації здійснюється відповідно до Порядку проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі НД ТЗІ 3.7-003-2005 [7, с. 19]. Вимоги до інформаційної безпеки ІТС ДБР повинні відповідати таким, що визначено для інформаційної безпеки електронного кримінального провадження [6, с. 11-22].

Адміністративний (організаційний) аспект інформаційної безпеки ІТС ДБР включає адміністративні (організаційні) заходи захисту апаратного забезпечення ІТС ДБР та адміністративні (організаційні) заходи захисту інформації ІТС ДБР. Адміністративні (організаційні) заходи захисту апаратного забезпечення ІТС ДБР визначаються комплексною системою захисту інформації. Процес розроблення і реалізації організаційних заходів захисту інформації визначено в п. 6.2 ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт». Зазначений документ регулює загальні положення відповідного процесу. Володільцем інформації ІТС ДБР (в розумінні абз. 4 ст. 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [4, с. 1]) необхідно визначити держателя електронної системи, тобто ДБР. На відміну від вимог до інформаційної безпеки електронного кримінального провадження [6, с. 11-22], яка має три категорії інформації, що підлягають захисту (обумовлено процесуальною природою електронної системи), інформацію ІТС ДБР, що підлягає захисту варто поділити на чотири категорії: *конфіденційну*, *службову*, *технологічну* та *відкриту* [7, с. 19-20]. Правовий режим інформації ІТС ДБР та порядок доступу до неї

пропонується врегулювати шляхом затвердження Директором ДБР «Правил розмежування прав доступу до ресурсів ІТС ДБР».

Технічний аспект інформаційної безпеки ІТС ДБР включає інженерно-технічні заходи захисту апаратного забезпечення ІТС ДБР та технічні заходи захист інформації ІТС ДБР. Інженерно-технічні заходи захисту апаратного забезпечення ІТС ДБР визначено комплексною системою захисту інформації. Забезпечення технічного захисту інформації ІТС ДБР передбачається розробку програмного модуля (як складової software) «Система інформаційної безпеки», ключовими функціями якого є: автентифікація користувачів; авторизація користувачів; надання доступу до ІТС ДБР з урахуванням повноважень користувачів; фіксація та аналіз дій користувачів ІТС ДБР. Також варто вказати про необхідність забезпечення кібербезпеки ІТС ДБР.

Невід'ємним аспектом ефективного функціонування ІТС ДБР є його інтеграція до єдиного електронного інформаційного поля органів кримінальної юстиції, що узгоджується з положеннями абз. 3 п. 5.12. Стратегії реформування судоустрою, судочинства та суміжних правових інститутів на 2015–2020 роки та норми профільного закону. Зокрема, відповідно до п. 10 ч.1 ст. 6 Закону [2, с. 1], ДБР має доступ як користувач до інформаційних систем органів державної влади, перелік яких встановлюється Кабінетом Міністрів України.

Електронні цифрові контури ІТС ДБР мають бути технологічно сумісні та логічно продовжувати особистий віртуальний кабінет ЄРДР. Обмін інформації з ЄРДР здійснюватиметься автоматично, за допомогою захищеної системи обміну даними, у обсягу інформації, визначеному Положенням про обмін даними [7, с. 21].

Висновки та пропозиції. Створення Електронного кримінального провадження [8, с. 24-35] як логічний етап інноваційної еволюції кримінального процесу України передбачає системну інформатизацію всіх суб'єктів кримінального провадження, в тому числі діяльності ДБР. Така системна інформатизація передбачає створення для ДБР ефективного процесуального та

адміністративно-організаційного правореалізаційного електронного інструменту, що забезпечуватиме здійснення повноважень в електронному інформаційному середовищі.

Література

1. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: http://zakon2.rada.gov.ua/laws/show/4651-17. (дата звернення: 11.06.2020).

2. Про Державне бюро розслідувань: Закон України від 12.11.2015 №794-VIII. URL: https://zakon.rada.gov.ua/laws/show/794-19. (дата звернення: 10.06.2021).

3. Про електронні довірчі послуги: Закону України від 05.10.2017 № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19. (дата звернення: 24.07.2021).

4. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 05.07.1994№ 80/94-ВР. URL: http://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80. (дата звернення: 20.07.2021).

5. Стратегія реформування судоустрою, судочинства та суміжних правових інститутів на 2015-2020 роки. URL: https://zakon2.rada.gov.ua/laws/show/276/2015. (дата звернення: 18.06.2021).

6. Каланча І. Інформаційна безпека електронного кримінального провадження України. *Науковий часопис Національної академії прокуратури України.* 2018. № 3. С. 11-22.

7. Столітній А., Каланча І. Концепція інформаційно-телекомунікаційної системи органу досудового розслідування. *Юридичний часопис Національної академії внутрішніх справ*. 2019. №18. С.14-23.

8. Столітній А. Концепція електронного кримінального провадження в Україні. *Вісник Національної академії прокуратури України.* 2018. № 4. С. 24-35.