УДК 343.13:004+342.9

Столітній А. В. – доктор юридичних наук, доцент, радник директора Державного бюро розслідувань, м. Київ
ORCID: https://orcid.org/0000-0002-2886-9379;

Каланча І. Г. – кандидат юридичних наук, прокурор Київської місцевої прокуратури № 2 міста Києва, м. Київ
ORCID: https://orcid.org/0000-0002-5246-7337

Концепція інформаційно-телекомунікаційної системи органу досудового розслідування

Мета *статті полягає у формулюванні ключових положень Концепції інформаційно-телекомунікаційної системи органу досудового розслідування.* ***Методологія.*** *Методологічною основою цієї роботи є сукупність загальнонаукових і спеціально-юридичних методів: діалектичний, системно-структурний, аналогії, системного аналізу, формально-юридичний, моделювання, синергетичний тощо.* ***Наукова новизна.*** *У публікації представлено Концепцію інформаційно-телекомунікаційної системи органу досудового розслідування, яка визначає систему поглядів на забезпечення інформатизації органу досудового розслідування шляхом створення відомчої інформаційно-телекомунікаційної системи, спрямованої на інформаційно-технологічне супроводження роботи органу досудового розслідування. Сформульовано ключові положення зазначеної Концепції, серед яких: завдання, етапи й заходи її створення, суб'єкти, категорії та їх ролі, функціональна архітектура, інформаційна безпека, схема інтеграції до єдиного електронного інформаційного поля органів кримінальної юстиції. Запропоновано етапи реалізації Концепції інформаційно-телекомунікаційної системи органу досудового розслідування. Розроблено схему інтеграції інформаційно-телекомунікаційної системи органу досудового розслідування до єдиного електронного інформаційного поля органів кримінальної юстиції, процесуальною надбудовою якого є електронне кримінальне провадження.* ***Висновки.*** *З огляду на одночасну потребу реформування й уніфікації наявних відомчих інформаційно-телекомунікаційних систем органів досудового розслідування, а також доцільність упровадження єдиної інформаційно-телекомунікаційної системи для реалізації всіх аспектів роботи певного органу досудового розслідування, вбачається, що пропонована Концепція є ефективною та універсальною для організації відповідних процесів.*

Ключові слова: кримінальне провадження; орган досудового розслідування; інформаційно-телекомунікаційна система; суб'єкт; функціональна архітектура; інформаційна безпека; інтеграція.

Вступ

В умовах системної інформатизації кримінального процесу України ефективна робота органів досудового розслідування (далі – ОДР) об'єктивно неможлива без застосування сучасних інформаційних технологій.

Повноваження щодо створення інформаційних систем визначено для більшості ОДР у профільних законах. Крім того, нині деякі ОДР використовують електронні системи: Національна поліція – Інтегровану інформаційно-пошукову систему Національної поліції України (ІІПС «АРМОР»), Систему централізованого управління нарядами поліції «ЦУНАМІ» (Krasnobryzhyi, Prokopov, & Ryzhkov, 2018) тощо, НАБУ – систему багатофункціонального електронного документообігу АСКОД. Загалом налічується кілька десятків електронних систем і баз даних органів правопорядку, у структурі яких функціонують електронні системи ОДР. Однак усі вони не виконують на належному рівні завдання щодо комплексного інформаційно-технологічного супроводження роботи ОДР і частково технологічно застаріли. Зазначені електронні системи не інтегровані між собою та з електронними кримінальними процесуальними правореалізаційними засобами, передбаченими КПК України: автоматизованою системою документообігу суду (ст. 35); Єдиним реєстром адвокатів України (ст. 45); Єдиним реєстром досудових розслідувань (далі – ЄРДР) (ст. 214); Єдиним державним реєстром судових рішень (ст. 535); Єдиним державним реєстром юридичних осіб, фізичних осіб – підприємців та громадських формувань (ст. 535). З огляду на функціонал застосовуваних ОДР інформаційних систем, така інтеграція технічно складна та потребує комплексного доповнення й уніфікації функціоналу наявних в ОДР електронних систем, а отже, недоцільна як концептуально, так і фінансово.

Зазначене зумовлює необхідність створення в усіх ОДР відомчих інформаційно-телекомунікаційних систем (далі – ІТС), що забезпечуватимуть реалізацію відповідними органами своїх функцій в електронному середовищі.

Питання забезпечення системної та уніфікованої інформатизації роботи ОДР і реалізації повноважень щодо самостійного створення інформаційних систем учені майже не досліджували.

Пропоновану Концепцію ІТС ОДР створено в контексті реалізації Концепції електронного кримінального провадження (Stolitnii, 2018) в частині створення для всіх ОДР електронних правореалізаційних інструментів з метою залучення їх до єдиного електронного інформаційного поля органів кримінальної юстиції.

Мета і завдання дослідження

Метою публікації є формулювання ключових положень Концепції ІТС ОДР. У статті сформульовано: завдання ІТС ОДР, етапи та заходи її створення, суб'єкти ІТС ОДР, категорії та їх ролі, функціональну архітектуру ІТС ОДР, її інформаційну безпеку, схему інтеграції ІТС ОДР до єдиного електронного інформаційного поля органів кримінальної юстиції.

Виклад основного матеріалу

Представлена Концепція ІТС ОДР визначає систему поглядів на забезпечення інформатизації ОДР шляхом створення відомчої ІТС, спрямованої на інформаційно-технологічне супроводження роботи органу й інтегрованої до єдиного електронного інформаційного поля органів кримінальної юстиції.

Повноваження щодо створення інформаційних систем, визначені для більшості ОДР у профільних законах, відображають адміністративну, слідчу (процесуальну) й оперативну спрямованість їхньої роботи. Зокрема, Національна поліція може створювати власні бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також міжвідомчі інформаційно-аналітичні системи (ч. 3 ст. 25 Закону України «Про Національну поліцію» від 2 липня 2015 року № 580-VIII); Державне бюро розслідувань – самостійно створювати інформаційні системи та вести оперативний облік; з метою оперативно-розшукової та слідчої діяльності створювати інформаційні системи та вести оперативний облік (п. 10 ч. 1 ст. 6, п. 7 ч. 1 ст. 7 Закону України «Про Державне бюро розслідувань» від 12 листопада 2015 року № 794-VIII); Служба безпеки України – в інтересах контррозвідки й оперативно-розшукової діяльності створювати інформаційні системи та вести оперативний облік (п. 12 ч. 1 ст. 25 Закону України «Про Службу безпеки України» від 25 березня 1992 року № 2229-XII); Національне антикорупційне бюро України – у межах оперативно-розшукової та слідчої діяльності створювати інформаційні системи та вести оперативний облік (п. 14 ч. 1 ст. 17 Закону України «Про Національне антикорупційне бюро України» від 14 жовтня 2014 року № 1698-VII).

Виконання положень абз. 3 п. 5.12 Стратегії реформування судоустрою, судочинства та суміжних правових інститутів на 2015–2020 роки щодо покращення управління та забезпечення сумісності інформаційних систем судів, прокуратури, адвокатури, пенітенціарної служби й інших органів юстиції потребує забезпечення інтеграції ІТС ОДР до єдиного електронного інформаційного поля органів кримінальної юстиції.

З огляду на це, ІТС ОДР має забезпечувати завдання щодо: внутрішньої електронної комунікації ОДР, ефективної електронної організації роботи й управління шляхом формулювання завдань і контролю за їх виконанням; ведення уніфікованого обліку (реєстрації) інформації; автоматизації ведення статистики; аналізу діяльності ОДР (серед яких автоматизований); виконання інших адміністративних функцій (трудових, фінансових, господарських тощо) підрозділами ОДР; ведення оперативного обліку; забезпечення електронної комунікації ОДР із суб'єктами кримінального провадження (зокрема в порядку електронного кримінального провадження); електронної комунікації ОДР з органами державної влади й управління в електронному інформаційному середовищі.

Правовий статус ОДР передбачає створення його ІТС як відомчої електронної системи, концептуальна структура (рис. 1, с. 16) якої обумовлена визначеними завданнями, функціональною спрямованістю діяльності ОДР та охоплює три складові, що формують її концептуальну структуру: *адміністративний блок* (організація роботи, безпеки, документообіг і внутрішнє ділове листування, кадрова робота тощо), *процесуальний блок* (інтеграція з програмним забезпеченням електронного кримінального провадження як процесуальної надбудови єдиного електронного інформаційного поля органів кримінальної юстиції) та *оперативні обліки* (діяльність оперативних підрозділів ОДР в інформаційній сфері).

Створення ІТС ОДР охоплює її розроблення (нормативної бази роботи та програмного забезпечення), упровадження в роботу й інтеграцію до єдиного електронного інформаційного поля, що слід реалізувати в межах окремих етапів: 1) створення нормативної бази; 2) розроблення програмного забезпечення; 3) розширення технічної інфраструктури; 4) тестування ІТС ОДР як пілотного проекту; 5) навчання суб'єктів ІТС ОДР роботи з функціоналом електронної системи; 6) упровадження ІТС ОДР у роботу правоохоронного органу; 7) інтеграція ІТС ОДР до єдиного електронного інформаційного поля органів кримінальної юстиції (зокрема електронного кримінального провадження як його процесуальної надбудови).

Рис. 1. Концептуальна структура ІТС ОДР

Перший етап – створення нормативної бази – передбачає здійснення заходів з розроблення та затвердження низки документів: Технічного завдання на розробку програмного забезпечення ІТС ОДР; Технічного завдання для серверної системи апаратної частини ІТС ОДР (аналітична); Технічного завдання для комплексної системи захисту інформації ІТС ОДР; Специфікації (технічні вимоги) до ІТС ОДР; Положення про порядок ведення ІТС ОДР; Правил розмежування прав доступу до ресурсів ІТС ОДР (затверджених керівником ОДР); Положення про обмін даними між ІТС ОДР та ЄРДР (затвердженого керівником ОДР і Генеральним прокурором) тощо.

Суб'єктами ІТС ОДР є держатель, адміністратори та користувачі.

Держатель – ОДР, який створює нормативно-правову базу для розроблення та функціонування ІТС ОДР; встановлює організаційні, методологічні принципи ведення ІТС ОДР; забезпечує функціонування ІТС ОДР; є володільцем бази даних ІТС ОДР; здійснює контроль за виконанням заходів, пов'язаних із захистом інформації, що міститься в базах даних ІТС ОДР; організовує взаємодію з іншими державними інформаційними системами, реєстрами та базами даних. Держатель ІТС ОДР забезпечує розроблення Системи інформаційної безпеки ІТС ОДР і гарантує забезпечення доступу до інформації з обмеженим доступом шляхом запровадження системи автентифікації користувачів з наданням доступу до інформації в межах процесуальних та/або адміністративних повноважень її користувачів.

Адміністратор – ОДР та його територіальні підрозділи, які забезпечують: виконання заходів зі створення, упровадження й технологічного супроводження програмного забезпечення ІТС ОДР; виконання заходів із технічного та програмно-технологічного забезпечення функціонування електронної системи; виконання заходів, пов'язаних зі збереженням і захистом інформації, що міститься в базах даних ІТС ОДР; структурну систематизацію несортованої інформації, відповідно до тематичних класифікаторів; надання користувачам доступу до ІТС ОДР; надання цілодобового доступу до ІТС через телекомунікаційні мережі закритого користування.

Користувач (згідно з абз. 12 ст. 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах») – працівник ОДР, якому надано доступ до функціоналу (або його частини) електронної системи відповідно до займаної посади, а також процесуальних та/або адміністративних повноважень. Користувачам ІТС ОДР для отримання доступу до електронної системи відведено роль в електронній системі відповідно до займаної посади, процесуальних та/або адміністративних повноважень.

Ефективне розмежування повноважень суб'єктів ІТС ОДР у частині доступу до його ресурсів зумовлює визначення їхніх ролей в електронній системі, які можна поділити на дві категорії:

– *адміністративні ролі: адміністратор безпеки* забезпечує захищеність ресурсів ІТС, доступ користувачам до ресурсів згідно з їх повноваженнями, контроль за виконанням користувачами й 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, установлює на них

програмне забезпечення; *адміністратор баз даних* інсталює, налаштовує та обслуговує системи керування базами даних, розгортає й обслуговує бази даних ІТС (Kalancha, 2018);

– *експлуатаційні ролі*: *«користувач»* має доступ до функціоналу ІТС ОДР відповідно до займаної посади, процесуальних та/або адміністративних повноважень. Експлуатаційні ролі (користувачів) визначаються відповідно до займаної посади, наданих процесуальних та/або адміністративних повноважень, тобто структури ОДР.

Забезпечення належного рівня безперервного функціонування електронної системи та захисту інформації дає змогу поєднувати дві та більше адміністративних ролей, за винятком ролі адміністратора безпеки. Водночас заборонено суміщення адміністративних та експлуатаційних ролей (Kalancha, 2018).

Функціональність ІТС ОДР визначатиме для кожної з експлуатаційних ролей користувачів додаткові опції, спеціалізований функціонал, модифікації інтерфейсу та можливість персонального налаштування електронного кабінету.

Другий етап – створення програмного забезпечення – передбачає здійснення таких заходів:

– розроблення програмного забезпечення ІТС ОДР (серед яких елементи комплексної системи захисту інформації ІТС ОДР): проектування; тестування функціональності, застосовності й безпеки; аудит інформаційної та криптографічної безпеки програмного забезпечення;

– тестування дієвості та продуктивності ІТС ОДР (зокрема елементи комплексної системи захисту інформації ІТС ОДР): функціональне; дослідницьке; у сфері технічного захисту інформації.

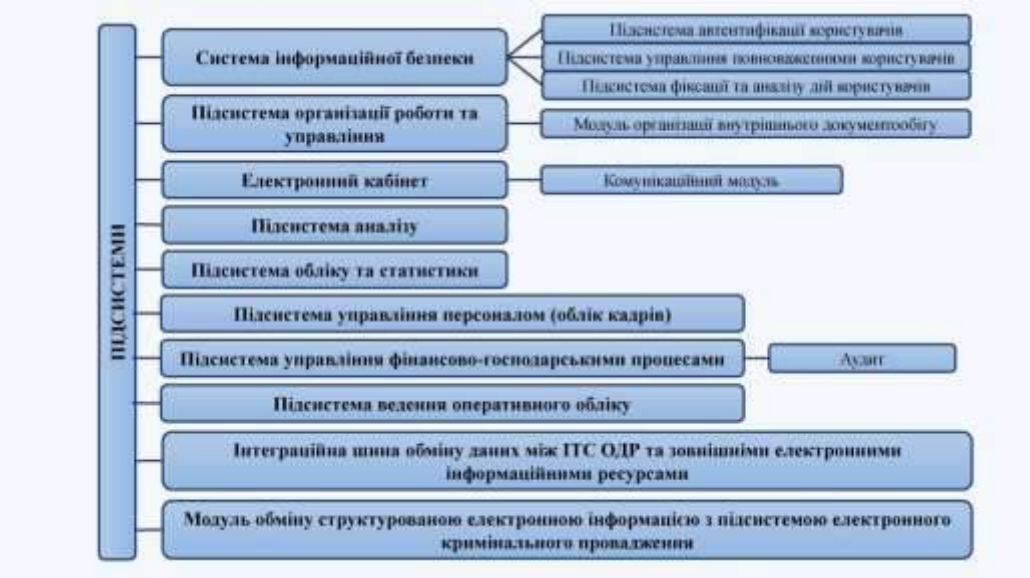

Рис. 2. Функціональна архітектура ІТС ОДР

Функціональна архітектура ІТС ОДР (рис. 2) відображає структуру програмного забезпечення електронної системи відповідно до її завдань і має такі складові:

І. Система інформаційної безпеки ІТС ОДР містить підсистему автентифікації користувачів (систему паролів доступу до електронної системи); підсистему управління повноваженнями користувачів; підсистему фіксації та аналізу дій користувачів.

Підсистема автентифікації користувачів забезпечить надання працівникам ОДР паролів доступу до електронної системи. Також ІТС ОДР дає змогу інтегрувати технологію кваліфікованого електронного цифрового підпису, розроблену відповідно до вимог Закону України «Про електронні довірчі послуги» від 5 жовтня 2017 року № 2155-VIII.

Підсистема управління повноваженнями користувачів ІТС ОДР призначена для виконання завдань автоматизації обслуговування її користувачів, серед яких: накопичення персональних даних користувачів ІТС ОДР; структуроване зберігання організаційної та штатної структури ОДР; автоматизація підготовки даних для генерування паролів доступу до ІТС ОДР; автоматизація обліку паролів доступу до ІТС ОДР; облік та управління повноваженнями користувачів. Підсистема управління повноваженнями користувачів ІТС ОДР працює надає послуги цілодобово. Перерви в роботі підсистеми можливі лише для виконання необхідних технологічних процесів і в разі виникнення непередбачуваних обставин. Окреслена підсистема містить три компоненти: серверне програмне забезпечення – відповідає за накопичення даних і надання

сервісів як зовнішнім системам, так й операторам системи; єдине програмне забезпечення генерування паролів доступу; програмне забезпечення для самостійної підготовки персональних даних потенційними користувачами ІТС ОДР. Доступ до елементів цієї підсистеми мають користувачі, адміністратори й технічний персонал з обслуговування в межах наданих їм повноважень.

Підсистема фіксації та аналізу дій користувачів: виконує завдання щодо фіксації та зберігання інформації про дії користувачів ІТС ОДР в електронній системі. Вона функціонує та надає послуги цілодобово; доступ до елементів підсистеми мають користувачі, адміністратори й технічний персонал з обслуговування в межах наданих їм повноважень.

II. Підсистема організації роботи та управління – підсистема, що відображає структуру ОДР і мережу електронних зв'язків між ними та забезпечує: формування й розподіл завдань між структурними підрозділами і працівниками шляхом накладання електронних резолюцій, ведення календаря виконання завдань, контроль за їх виконанням і реалізацію інших адміністративних функцій структурних підрозділів ДБР.

Окреслена система містить модуль організації внутрішнього документообігу, який здійснює доставляння внутрішньовідомчих електронних документів (повідомлень, файлів тощо) й електронних повідомлень від зовнішніх електронних інформаційних ресурсів, спрямованих за результатами накладання керівником електронних резолюцій.

III. Електронний кабінет – підсистема, що забезпечує доступ користувачів до функціоналу ІТС ОДР для виконання завдань щодо формування документів, обміну даними, доступу до інформації ІТС ОДР в обсязі, визначеному залежно від займаної посади, наданих процесуальних та/або адміністративних повноважень (ролі в системі). Електронний кабінет разом з модулем обміну структурованою електронною інформацією з підсистемою електронного кримінального провадження забезпечує зв'язок з електронним кримінальним процесуальним правореалізаційним середовищем.

Електронний кабінет має комунікаційний модуль – функціонал ІТС ОДР, що забезпечує формування та скерування електронних повідомлень (охоплює базу даних внутрішніх комунікацій ІТС ОДР та Базу даних електронних адрес органів державної влади, органів місцевого самоврядування, органів кримінальної юстиції тощо).

IV. Підсистема аналізу – забезпечує аналіз діяльності користувачів ІТС ОДР шляхом формування стандартизованих й авторських (на підставі заданих користувачем параметрів і змісту) аналітичних звітів у формі таблиць та візуалізацій.

V. Підсистема обліку та статистики – забезпечує облік діяльності користувачів ІТС ОДР на підставі даних, згенерованих підсистемою фіксації та аналізу дій користувачів системи інформаційної безпеки ІТС ОДР, і формування статистичних відомостей у вигляді затверджених керівником ОДР форм обліку діяльності ОДР.

VI. Підсистема управління персоналом (облік кадрів) забезпечує автоматизацію процесів кадрового обліку, формування кадрової звітності.

VII. Підсистема управління фінансово-господарськими процесами здійснює автоматизацію процесів фінансового та бухгалтерського обліку, формування фінансової та бухгалтерської звітності, автоматизацію процесів з інших питань управління фінансово-господарською діяльністю ОДР.

VIII. Підсистема ведення оперативного обліку забезпечує відображення, систематизацію та узагальнення первинних показників роботи оперативних підрозділів ОДР, здійснює їх перетворення в структуровану електронну інформацію.

IX. Інтеграційна шина обміну даних між ІТС ОДР та зовнішніми електронними інформаційними ресурсами – підсистема, що забезпечує обмін електронними даними між ІТС ОДР і зовнішніми електронними даними із зовнішніми електронними інформаційними ресурсами шляхом кодування та відправлення електронних транспортних пакетів, сформованих користувачем за допомогою комунікаційного модуля електронного кабінету, а також доставляння електронних повідомлень від зовнішніх електронних інформаційних ресурсів (до комунікаційного модуля електронного кабінету або модуля організації внутрішнього документообігу підсистеми організації роботи та управління).

X. Модуль обміну структурованою електронною інформацією з підсистемою електронного кримінального провадження – підсистема, що забезпечує двосторонній обмін електронною інформацією у формі шифрованих електронних транспортних конвертів між ІТС ОДР і процесуальною інформаційною системою електронного кримінального провадження – ЄРДР.

Слід зауважити, що програмне забезпечення ІТС ОДР, розроблене на замовлення ОДР та/або придбане ним, уся інформація баз даних ІТС ОДР є власністю держави в особі зазначеного органу.

Третій етап – створення (розширення) технічної інфраструктури – передбачає здійснення таких заходів:

– створення центру зберігання й обробки даних ІТС ОДР (центральний і резервний);

– забезпечення підрозділів ОДР пристроями для оцифрування документів, отриманих у паперовій формі; збільшення пропускної здатності мережевого підключення приміщень підрозділів ОДР для забезпечення суб'єктів кримінального

провадження можливістю працювати з відеофайлами й іншими матеріалами великого обсягу.

Четвертий етап – запровадження пілотного проекту ІТС ОДР – передбачає здійснення заходів з:

– апробації електронної системи у формі пілотного проекту (тестування зручності використання й інтерфейсу користувача) в одному з територіальних підрозділів ОДР строком від одного до трьох місяців;

– проведення (за потреби) коригування програмного забезпечення ІТС ОДР відповідно до отриманих зауважень.

Реалізація пілотного проекту ІТС ОДР покликана забезпечити апробацію електронної системи для виявлення недоліків системи, урахування досвіду користувачів для покращення функціоналу чи інтерфейсу. Наприклад, інтерфейс ІТС ОДР для її користувачів представлений у вигляді електронного робочого столу, функціонал якого буде визначено залежно від ролі користувача в електронній системі, що потребує попереднього тестування користувачами й оптимізації перед упровадженням у роботу.

П'ятий етап – навчання суб'єктів ІТС ОДР роботи з функціоналом електронної системи – передбачає здійснення таких заходів:

– професійне навчання для роботи з ІТС ОДР (для окремих працівників – також із комплексною системою захисту інформації ІТС ОДР) у відомчому (спеціалізованому) закладі вищої освіти ОДР;

– створення спеціалізованих програм-тренажерів для дистанційного навчання роботи з функціоналом ІТС ОДР.

Шостий етап – упровадження ІТС ОДР у роботу правоохоронного органу – передбачає здійснення таких заходів:

– проведення приймальних випробувань ІТС ОДР;

– перевірку технічної інфраструктури ІТС ОДР;

– отримання сертифіката відповідності за результатами державної експертизи ІТС ОДР у сфері технічного захисту інформації;

– оцінювання результатів апробації електронної системи у формі пілотного проекту;

– оцінювання ступеня готовності користувачів за результатами навчання роботи з функціоналом ІТС ОДР;

– затвердження відомчого документа про впровадження ІТС в експлуатацію та її обов'язкове застосування.

Невід'ємним аспектом ефективної роботи ІТС ОДР, без якого неможливе її впровадження, є інформаційна безпека, яку слід розглядати в адміністративному (організаційному) й технічному аспектах.

Відповідно до ч. 2 ст. 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року № 80/94-ВР, державні інформаційні ресурси або інформацію з обмеженим доступом, вимога щодо захисту якої встановлена законом, слід обробляти 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 цього Закону).

Створення комплексної системи захисту інформації здійснюють відповідно до НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».

Вимоги до інформаційної безпеки ІТС ОДР мають відповідати таким, що визначені для інформаційної безпеки електронного кримінального провадження (Kalancha, 2018).

Адміністративний (організаційний) аспект інформаційної безпеки ІТС ОДР охоплює адміністративні (організаційні) заходи захисту апаратного забезпечення ІТС ОДР й адміністративні (організаційні) заходи захисту інформації ІТС ОДР.

Адміністративні (організаційні) заходи захисту апаратного забезпечення ІТС ОДР визначені комплексною системою захисту інформації.

Процес розроблення та реалізації організаційних заходів захисту інформації окреслено в п. 6.2 ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт». Цей документ регулює загальні положення відповідного процесу.

Володільцем інформації ІТС ОДР (згідно з абз. 4 ст. 1 цього Закону) слід визначити держателя електронної системи, тобто ОДР.

На відміну від вимог до інформаційної безпеки електронного кримінального провадження (Kalancha, 2018), яка має три категорії інформації, що підлягають захисту (з огляду на процесуальну сутність електронної системи), інформацію ІТС ОДР, що підлягає захисту, можна поділити на чотири категорії: конфіденційну (дані користувачів ІТС ОДР, для яких забезпечено вимоги щодо збереження конфіденційності й цілісності персональних даних, їх доступності та спостережності дій користувачів з ними); службову (відомча інформація ОДР, що створюється внаслідок діяльності працівників ОДР в електронній системі та належить до інформації з обмеженим доступом. Для окресленої категорії інформації забезпечено вимоги щодо збереження конфіденційності й цілісності даних, їх доступності та спостережності дій користувачів з ними); технологічну (налаштування програмно-технічних засобів ІТС ОДР, права доступу її користувачів, атрибути доступу, відомості про події, які генеруються програмно-

технічними засобами електронної системи. Розмежування доступу до об'єктів, що містять технологічну інформацію, забезпечено на рівнях: операційної системи (до файлів операційної системи та файлів, створених користувачами); системи керування базами даних; активного мережевого обладнання. Технологічну інформацію містять: файли програмних і технічних засобів ІТС ОДР з їх налаштуваннями; файли програмних і технічних засобів ІТС ОДР, що мають журнали подій, зокрема: системні журнали подій операційної системи, журнали подій безпеки операційної системи, журнали подій активного мережевого обладнання (відомості про дії користувачів під час обробки конфіденційної інформації). Для зазначеної категорії інформації забезпечено вимоги щодо збереження конфіденційності й цілісності технологічної інформації, її доступності та спостережності дій користувачів з ними; відкриту (дані, що містять статистичну інформацію, нормативно-правове забезпечення діяльності ОДР та іншу інформацію, яка не потребує захисту від несанкціонованого ознайомлення сторонніми особами, а також публічну інформацію, яка належить ОДР, що не стосується інформації з обмеженим доступом (зокрема інформація, розміщена на зовнішньому веб-сайті ОДР). Для цієї категорії інформації забезпечено вимоги щодо збереження цілісності відкритої інформації, її доступності й спостережності дій користувачів з ними.

Правовий режим інформації ІТС ОДР і порядок доступу до неї запропоновано врегулювати шляхом затвердження керівником ОДР Правил розмежування прав доступу до ресурсів ІТС ОДР і реалізувати через упровадження автоматизованої системи контролю доступу до інформації ІТС ОДР (рис. 3).

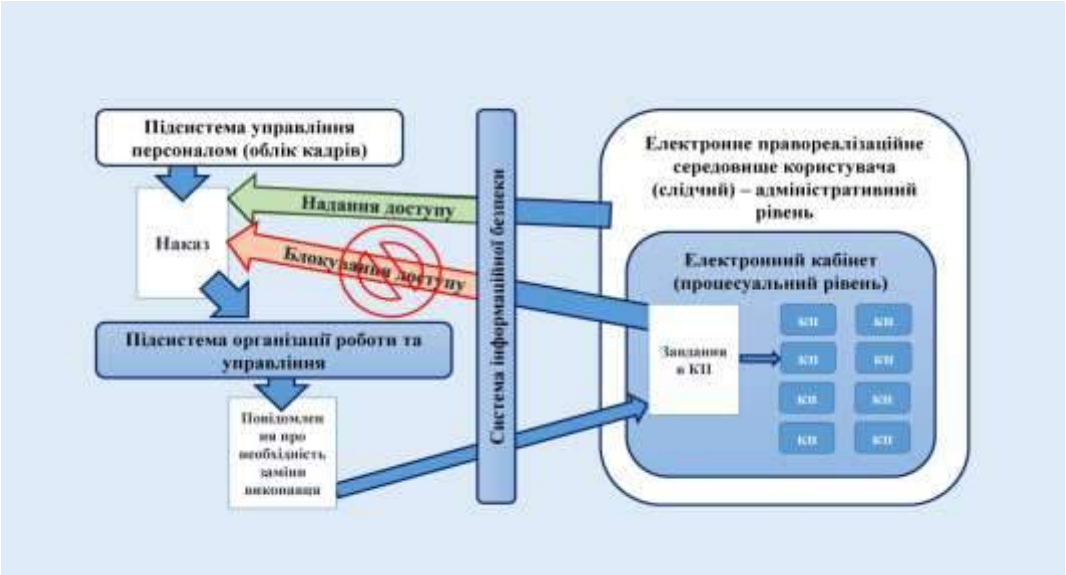

Рис. 3. Система контролю доступу до інформації ІТС ОДР

Технічний аспект інформаційної безпеки ІТС ОДР охоплює інженерно-технічні заходи захисту апаратного забезпечення ІТС ОДР і технічні заходи захисту інформації ІТС ОДР. Інженерно-технічні заходи захисту апаратного забезпечення ІТС ОДР визначені комплексною системою захисту інформації.

Забезпечення технічного захисту інформації ІТС ОДР передбачає розроблення програмного модуля (як складової software) «Система інформаційної безпеки», ключовими функціями якого є: автентифікація користувачів; авторизація користувачів; надання доступу до ІТС ОДР відповідно до повноважень користувачів; фіксація та аналіз дій користувачів ІТС ОДР.

Також слід зазначити про необхідність забезпечення кібербезпеки ІТС ОДР, що потребує застосування посилених механізмів захисту інформації: захист від DDoS-атак шляхом організації розподіленої системи серверів; застосування подвійного криптографічного захисту інформації в процесі обміну даними із зовнішніми системами; захищені тунелі обміну даними між ІТС ОДР та електронними системами й базами даних органів кримінальної юстиції, органів державної влади, місцевого самоврядування тощо.

Сьомий етап – інтеграція ІТС ОДР до єдиного електронного інформаційного поля органів кримінальної юстиції (зокрема, електронного кримінального провадження) – передбачає здійснення таких заходів:

– розроблення та затвердження Положення про обмін даними між ІТС ОДР та Єдиним

реєстром досудових розслідувань, затвердженим керівником ОДР та Генеральним прокурором;

– функціональне й технічне підключення до інтеграційного середовища електронного кримінального провадження для забезпечення обміну даними в порядку електронного кримінального провадження (Stolitnii, 2018) з ЄРДР.

Передумовою інтеграції ІТС ОДР до єдиного електронного інформаційного поля органів кримінальної юстиції (рис. 4) є положення абз. 3 п. 5.12 Стратегії реформування судоустрою, судочинства та суміжних правових інститутів на 2015–2020 роки й норми профільних законів. Національна поліція має безпосередній оперативний доступ до інформації та інформаційних ресурсів інших органів державної влади (ч. 1 ст. 27 Закону України «Про Національну поліцію» від 2 липня 2015 року № 580-VIII); Національне антикорупційне бюро України має безпосередній доступ до автоматизованих інформаційних і довідкових систем, реєстрів та банків даних, держателем (адміністратором) яких є державні органи або органи місцевого самоврядування, користується державними, зокрема урядовими, засобами зв'язку та комунікацій, мережами спеціального зв'язку й іншими технічними засобами (абз. 3 п. 3 ч. 1 ст. 17 Закону України «Про Національне антикорупційне бюро України» від 14 жовтня 2014 року № 1698-VII); Державне бюро розслідувань має доступ як користувач до інформаційних систем органів державної влади, перелік яких встановлює Кабінет Міністрів України (п. 10 ч. 1 ст. 6 Закону України «Про Державне бюро розслідувань» від 12 листопада 2015 року № 794-VIII).

Електронні цифрові контури ІТС ОДР мають бути технологічно сумісні та логічно продовжувати особистий віртуальний кабінет ЄРДР. Обмін інформацією з ЄРДР здійснюватиметься автоматично за допомогою захищеної системи обміну даними в обсязі, визначеному Положенням про обмін даними.

Реалізація окреслених вище етапів дасть змогу забезпечити послідовне проектування й запровадження ІТС ОДР, належну апробацію її функціоналу та врахувати інтереси користувачів.

Рис. 4. Схема інтеграції ІТС ОДР до єдиного електронного інформаційного поля органів кримінальної юстиції

Наукова новизна

У публікації вперше сформульовано ключові положення Концепції ІТС ОДР, а саме: завдання ІТС ОДР, етапи та заходи її створення, суб'єкти ІТС ОДР, категорії та їхні ролі, функціональну архітектуру й інформаційну безпеку ІТС ОДР, схему інтеграції ІТС ОДР до єдиного електронного інформаційного поля органів кримінальної юстиції.

Висновки

Розвиток кримінального процесу України в напрямі створення електронного кримінального провадження передбачає системну інформатизацію всіх суб'єктів кримінального провадження, зокрема ОДР. Зазначене виявляється в потребі розроблення для ОДР ефективних електронних правореалізаційних засобів, що забезпечуватимуть здійснення повноважень в електронному інформаційному середовищі. З огляду на одночасну необхідність реформування й уніфікації наявних відомчих ІТС ОДР, а також доцільність упровадження єдиної ІТС для реалізації всіх аспектів роботи певного ОДР, запропонована Концепція видається ефективною та універсальною для організації відповідних процесів.

REFERENCES

Frappaolo, C. (1995). Electronic document management system analysis report and system plan for the Environmental Restoration Program. *Delphy Consulting Group.* doi: https://doi.org/10.2172/661548.

Gordon, D. (2017). The Electronic Panopticon: A Case Study of the Development of the National Criminal Records System. *Surveillance, Crime and Social Control*, 383-411. doi: https://doi.org/10.4324/9781315242002-18.

Kalancha, I. (2018). Informatsiina bezpeka elektronnoho kryminalnoho provadzhennia Ukrainy [Information security of the electronic criminal case of Ukraine]. *Naukovyi chasopys Natsionalnoi akademii prokuratury Ukrainy, Scientific Journal of National Academy of Prosecution of Ukraine, 3,* 11-22. Retrieved from http://www.chasopysnapu.gp.gov.ua/chasopys/ua/pdf/3-2018/kalancha.pdf.

Krasnobryzhyi, I.V., Prokopov, S.O., & Ryzhkov, E.V. (2018). *Informatsiine zabezpechennia profesinoi diialnosti [Information provision of professional activity].* Dnipro: DDUVS [in Ukrainian].

Olugasa, O. (2013). *ICT for Criminal Justice System in Nigeria and Ethical Considerations.* Autónoma University, Portugal. doi: https://doi.org/10.2139/ssrn.2510444.

Poriadok provedennia robit iz stvorennia kompleksnoi systemy zakhystu informatsii v informatsiino-telekomunikatsiinii systemi. ND TZI 3.7-003-2005 [The order of work on creation of the complex system of information security in the information and telecommunication system. Regulatory document of the technical protection of information 3.7-003-2005]. (n.d.). *www.dsszzi.gov.ua.* Retrieved from http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article%3Bjsessionid=9082A42798BC38188D392292242BFBA2?showHidden=1&art_id=102232&cat_id=46556&ctime=1344503967308 [in Ukrainian].

Sangero, B., & Halpert, M. (2011). A Safety Doctrine for the Criminal Justice System. *Michigan State Law Review*. doi: https://doi.org/10.2139/ssrn.1922251.

Simmons, R. (2016). Quantifying Criminal Procedure: How to Unlock the Potential of Big Data in Our Criminal Justice System. *Ohio State Public Law Working Paper, 362,* 947-1017. doi: https://doi.org/10.2139/ssrn.2816006.

Stolitnii, A.V. (2018). Kontseptsiia elektronnoho kryminalnoho provadzhennia v Ukraini [Electronic criminal case concept in Ukraine]. *Visnyk Natsionalnoi akademii prokuratury Ukrainy, Journal of the National Prosecution Academy of Ukraine, 4,* 24-35. Retrieved from http://www.visnyknapu.gp.gov.ua/files/issues-2018/Visnyk-NAPU_4_2018.pdf [in Ukrainian].

Zakhyst informatsii. Tekhnichnyi zakhyst informatsii. Poriadok provedennia robit. DSTU 3396.1-96 [Technical protection of information. The order of works. State standard of technical specifications 3396.1-96]. (n.d.). *www.dsszzi.gov.ua.* Retrieved from http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38911&cat_id=38836 [in Ukrainian].

Zakon Ukrainy "Pro Derzhavne biuro rozsliduvani": vid 12 lystop. 2015 r. No 794-VIII [Law of Ukraine "On the State Bureau of Investigation" from November 12, 2015, No. 794-VIII]. (n.d.). *zakon.rada.gov.ua.* Retrieved from https://zakon.rada.gov.ua/laws/show/794-19 [in Ukrainian].

Zakon Ukrainy "Pro Natsionalne antykoruptsiine biuro Ukrainy": vid 14 zhovt. 2014 r. No. 1698-VII [Law of Ukraine "On the National Anti-Corruption Bureau of Ukraine" from October 14, 2014 r. No. 1698-VII]. (n.d.). *zakon.rada.gov.ua*. Retrieved from https://zakon.rada.gov.ua/laws/show/1698-18 [in Ukrainian].

Zakon Ukrainy "Pro Natsionalnu politsiiu": vid 2 lyp. 2015 r. No. 580-VIII [Law of Ukraine "On National Police" from July 2, 2015, No. 580-VIII]. (n.d.). *zakon.rada.gov.ua*. Retrieved from https://zakon.rada.gov.ua/laws/show/580-19 [in Ukrainian].

Zakon Ukrainy "Pro Sluzhbu bezpeky Ukrainy": vid 25 berez. 1992 r. No. 2229-XII [Law of Ukraine "On the Security Service of Ukraine" from March 25, 1992, No. 2229-XII]. (n.d.). *zakon.rada.gov.ua*. Retrieved from https://zakon.rada.gov.ua/laws/show/2229-12 [in Ukrainian].

Zakon Ukrainy "Pro zakhyst informatsii v informatsiino-telekomunikatsinykh systemakh": vid 5 lyp. 1994 r. No. 80/94-VR [Law of Ukraine "On the protection of information in information and telecommunication systems" from July 5, 1994, No. 80/94-VR]. (n.d.). *zakon.rada.gov.ua.* Retrieved from http://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 [in Ukrainian].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Frappaolo C. Electronic document management system analysis report and system plan for the Environmental Restoration Program. *Delphy Consulting Group.* 1995. doi: https://doi.org/10.2172/661548.

Gordon D. The Electronic Panopticon: A Case Study of the Development of the National Criminal Records System. *Surveillance, Crime and Social Control.* 2017. P. 383–411. doi: https://doi.org/10.4324/9781315242002-18.

Каланча І. Інформаційна безпека електронного кримінального провадження України. *Науковий часопис Національної академії прокуратури України.* 2018. № 3. С. 11–22. URL: http://www.chasopysnapu.gp.gov.ua/chasopys/ua/pdf/3-2018/kalancha.pdf.

Краснобрижий І. В., Прокопов С. О., Рижков Е. В. Інформаційне забезпечення професійної діяльності : навч. посіб. Дніпро : ДДУВС, 2018. 220 с.

Olugasa O. ICT for Criminal Justice System in Nigeria and Ethical Considerations. Autónoma University, Portugal, 2013. P. 15. doi: https://doi.org/10.2139/ssrn.2510444.

Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-2005. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article%3Bjsessionid=9082A42798BC38188D392292242BFBA2?showHidden=1&art_id=102232&cat_id=46556&ctime=1344503967308.

Sangero B., Halpert M. A Safety Doctrine for the Criminal Justice System. *Michigan State Law Review.* 2011. P. 34. doi: https://doi.org/10.2139/ssrn.1922251.

Simmons R. Quantifying Criminal Procedure: How to Unlock the Potential of Big Data in Our Criminal Justice System. *Ohio State Public Law Working Paper.* 2016. No. 362. P. 947–1017. doi: https://doi.org/10.2139/ssrn.2816006.

Столітній А. Концепція електронного кримінального провадження в Україні. *Вісник Національної академії прокуратури України.* 2018. № 4. С. 24-35. URL: http://www.visnyknapu.gp.gov.ua/files/issues-2018/Visnyk-NAPU_4_2018.pdf.

Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38911&cat_id=38836.

Про Державне бюро розслідувань : Закон України від 12 листоп. 2015 р. № 794-VIII. URL: https://zakon.rada.gov.ua/laws/show/794-19.

Про Національне антикорупційне бюро України : Закон України від 14 жовт. 2014 р. № 1698-VII. URL: https://zakon.rada.gov.ua/laws/show/1698-18.

Про Національну поліцію : Закон України від 2 лип. 2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19.

Про Службу безпеки України : Закон України від 25 берез. 1992 р. № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12.

Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 лип. 1994 р. № 80/94-ВР. URL: http://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

Стаття надійшла до редколегії 14.05.2019

Stolitnii A. – Doctor of Law, Associate Professor, Advisor to the Director of the State Bureau of Investigation, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-2886-9379;

Kalancha I. – Ph.D in Law, Prosecutor of the Kyiv Local Prosecutor's Office No. 2 of Kyiv city, Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-5246-7337

The Conception of Information and Telecommunication Systems of the Pre-Trial Investigation Body

*The **purpose** this study is to formulate key principles of the Conception of information and telecommunication systems of the pre-trial investigation body. **Methodology.** The methodological basis of this paper is represented by the set of general scientific and specialized judicial methods, such as: dialectical, systemic-structural, methods of analogy, system analysis, formal-judicial, modeling, synergetic etc. **Scientific novelty.** The article presents the Conception of information and telecommunication system of the pre-trial investigation body, which defines a system of views on ensuring the informatization of the pre-trial investigation body through the creation of the departmental information and telecommunication system aimed at providing the pre-trial investigation body with informational and technological support. The authors have elaborated the following key principles of the Conception of information and telecommunication systems of the pre-trial investigation body: the tasks, stages and steps of its creation, subjects, categories and types of their roles, functional framework, informational security, the scheme for integrating criminal justice bodies into a unified electronic information field. The research propounds implementation stages of the Conception of information and telecommunication system of the pre-trial investigation body. The authors have developed the scheme for integrating information and telecommunication system of the pre-trial investigation body into a unified electronic information field of criminal justice bodies. Its procedural superstructure is viewed as Electronic criminal case. **Conclusions.** Taking into account the simultaneous need for reforming and unifying the existing departmental information and telecommunication systems of all pre-trial investigation bodies as well as the expedience of introducing a unified information and telecommunication system aiming at the implementation of all aspects of a certain pre-trial investigation body operation, the proposed conception is considered effective and universal for organizing the relevant processes.*

Keywords: criminal proceedings; pre-trial investigation body; information and telecommunication system; subject; functional framework; informational security; integration.