РАДА СУДДІВ УКРАЇНИ

01601, м. Київ, вул. Липська, 18/5, тел.: (044) 277-76-29, факс: (044) 277-76-30

25 листопада 2021 року **м. Ужгород**

РІШЕННЯ

№ 57

Заслухавши та обговоривши інформацію члена Ради суддів України Чорної В.В. про погодження проєкту Положення про інформаційно-телекомунікаційну систему досудового розслідування "іКейс", відповідно до частини восьмої статті 133 Закону України "Про судоустрій і статус суддів" та Положення про Раду суддів України, затвердженого X позачерговим з'їздом суддів України 16 вересня 2010 року (зі змінами), Рада суддів України

в и р і ш и л а:

Погодити проєкт Положення про інформаційно-телекомунікаційну систему досудового розслідування "іКейс", що додається.

Голова
Ради суддів України **Б.С. Моніч**

Додаток
до рішення Ради суддів України
25 листопада 2021 року № 57

ПОГОДЖЕНО
рішення Ради суддів України
від 25 листопада 2021 року № 57

ЗАТВЕРДЖЕНО
наказ _____
Директора Національного
антикорупційного бюро України

Генерального прокурора

Положення

про інформаційно-телекомунікаційну систему досудового розслідування "іКейс"

І. Загальні положення

1. Це Положення визначає мету, основні завдання та функції, структуру, суб'єктів, користувачів, а також загальні засади функціонування інформаційно-телекомунікаційної системи досудового розслідування "іКейс" у кримінальних провадженнях, досудове розслідування в яких здійснюється детективами Національного антикорупційного бюро України.

2. Положення розроблено відповідно до положень Кримінального процесуального кодексу України, законів України «Про Національне антикорупційне бюро України», «Про прокуратуру», «Про судоустрій і статус суддів», «Про Вищий антикорупційний суд», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про телекомунікації», «Про Національну систему конфіденційного зв'язку», «Про електронні документи та документообіг», «Про електронні довірчі послуги» та інших нормативно-правових актів.

3. Терміни, що вживаються в цьому Положенні, мають таке значення:

інформаційно-телекомунікаційна система досудового розслідування "іКейс" (далі – Система) – це система, яка забезпечує створення, збирання, зберігання, пошук, оброблення і передачу матеріалів та інформації (відомостей) у кримінальному провадженні;

інтеграція Системи із системою, що функціонує в суді відповідно до статті 35 Кримінального процесуального кодексу України, – процес технічної взаємодії, що полягає в автоматизованому обміні даними між цими системами, в порядку, передбаченому пунктом 11 цього Положення;

інцидент інформаційної безпеки – будь-яка подія, яка призводить або може призвести до переривання функціонування Системи або до знищення, втрати, несанкціонованого розкриття, зміни, доступу до даних, переданих, збережених або оброблених іншим чином в Системі;

оброблення інформації в Системі – виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зміна, зчитування, зберігання, знищення, реєстрація, приймання, отримання, передавання даних, які здійснюються в системі за допомогою технічних і програмних засобів;

порушення інформаційної безпеки – факт недотримання встановлених вимог з інформаційної безпеки, який призводить або може призвести до переривання функціонування Системи або до знищення, втрати, несанкціонованого розкриття, зміни, доступу до даних, переданих, збережених або оброблених іншим чином в Системі;

управління доступом користувачів – дії адміністраторів Системи щодо додавання, вилучення, тимчасового блокування, розблокування користувача, а також управління атрибутами користувача (значення полів його профілю, в тому числі належністю користувача до відповідної організації/підрозділу та групи).

Інші терміни, що використовуються в цьому Положенні, вживаються у значенні, встановленому Кримінальним процесуальним кодексом України (далі – КПК України), законами України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про телекомунікації», «Про Національну систему конфіденційного зв'язку», «Про електронні документи та електронний документообіг», «Про електронні довірчі послуги» та іншими законами України.

ІІ. Мета, основні завдання та функції Системи

4. Метою Системи є автоматизація процесів досудового розслідування, включаючи створення, збирання, зберігання, пошук, оброблення і передачу матеріалів та інформації (відомостей) у кримінальному провадженні, а також процесів, які забезпечують організаційні, управлінські, аналітичні, інформаційно-телекомунікаційні та інші потреби користувачів системи.

5. Основними завданнями системи є:

1) створення єдиного електронного простору для суб'єктів Системи, в якому зберігаються матеріали та інформація щодо кримінальних проваджень;

2) створення умов для електронної взаємодії та автоматизації роботи суб'єктів Системи з метою підвищення ефективності виконання завдань, покладених на них законодавством, зменшення часових та фінансових витрат на здійснення досудового розслідування, управлінські, інформаційно-пошукові, аналітичні роботи, формування звітності;

3) забезпечення точними аналітичними даними для прийняття ефективних управлінських рішень, заснованих на фактах;

4) забезпечення інформаційної взаємодії з іншими інформаційними (автоматизованими), інформаційно-телекомунікаційними системами.

6. Функціями Системи є:

1) створення, збирання, зберігання, пошук, оброблення і передача матеріалів та інформації (відомостей) у кримінальному провадженні;

2) централізоване захищене зберігання матеріалів кримінальних проваджень, процесуальних та інших документів;

3) захищене зберігання, автоматизована аналітична обробка інформації;

4) обмін документами та інформацією (надсилання та отримання документів та інформації, спільна робота з документами) в електронній формі між суб'єктами Системи;

5) доступ користувачів Системи до будь-якої інформації, що в ній зберігається, в електронній формі відповідно до наданих прав доступу;

6) автоматизована взаємодія (інтеграція) Системи з іншими інформаційними (автоматизованими), інформаційно- телекомунікаційними системами;

7) автоматичне формування аналітичних звітів з наборів даних, що містяться в Системі;

8) інші функції, передбачені Положенням.

III. Структура Системи та її взаємодія з іншими інформаційними (автоматизованими), інформаційно-телекомунікаційними системами

7. До складу Системи входять:

1) ядро Системи;

2) телекомунікаційна мережа;

3) автоматизовані робочі місця користувачів Системи;

4) комплексна система захисту інформації.

8. До складу ядра Системи входять:

1) сервери;

2) системи віртуалізації;

3) системи збереження даних;

4) кластер програм та сервісів;

5) кластер баз даних;

6) інтеграційний шлюз.

9. До складу телекомунікаційної мережі входять:

1) телекомунікаційні мережі доступу;

2) технічні засоби телекомунікацій;

3) засоби криптографічного захисту інформації.

10. Система взаємодіє з Єдиним реєстром досудових розслідувань та системою, яка функціонує в суді відповідно до статті 35 Кримінального процесуального кодексу України, а також може взаємодіяти з іншими інформаційними, інформаційно-телекомунікаційними системами у випадках, передбачених законом. Порядок взаємодії Системи з Єдиним реєстром досудових розслідувань, іншими інформаційними, інформаційно-телекомунікаційними системами визначається держателями відповідних систем згідно з вимогами чинного законодавства України.

11. Порядок взаємодії Системи із системою, яка функціонує в суді відповідно до статті 35 Кримінального процесуального кодексу України,

визначається адміністраторами цих систем за погодженням із Вищим антикорупційним судом.

Цим Положенням визначається мінімальний обсяг інформації (відомостей), який повинен передаватися в процесі інтеграції Системи із системою, яка функціонує в суді відповідно до статті 35 Кримінального процесуального кодексу України.

У разі надходження на розгляд слідчого судді Вищого антикорупційного суду клопотань, заяв, інших матеріалів, сформованих у Системі на стадії досудового розслідування, інтеграція повинна забезпечувати автоматичне наповнення у системі, що функціонує в суді, відповідних полів реєстраційних та обліково-статистичних карток на матеріали такою інформацією (відомостями):

1) назва документа;
2) вид документа (категорія справи);
3) вихідна дата та номер документа;
4) прізвище, ім'я, по батькові, посада (найменування) відправника;
5) адреса відправника;
6) короткий зміст матеріалів;
7) обсяг матеріалів;
8) реквізити першого надісланого документа (у разі надіслання документів до раніше зареєстрованих);
9) номер кримінального провадження, якого стосуються подані матеріали;
10) прізвище, ім'я, по-батькові фізичної або найменування юридичної особи, щодо якої подано процесуальний документ,
11) адреса фізичної чи юридичної особи, щодо якої подано процесуальний документ;
12) статус фізичної чи юридичної особи, щодо якої подано процесуальний документ, у кримінальному провадженні.

Інтеграція забезпечує автоматичну передачу із системи, яка функціонує у Вищому антикорупційному суді відповідно до статті 35 Кримінального процесуального кодексу України, до Системи такої інформації (відомостей):

1) дата, час та місце розгляду клопотань, заяв, інших матеріалів, які надійшли на розгляд слідчому судді із Системи;
2) електронний примірник судового рішення, ухваленого за результатами розгляду клопотання, заяви, інших матеріалів, які надійшли на розгляд до суду із Системи, та створеного в системі, яка функціонує в Вищому антикорупційному суді відповідно до статті 35 Кримінального процесуального кодексу України.

IV. Суб'єкти Системи

12. Суб'єктами Системи є:
1) держатель;
2) технічний адміністратор;
3) органи, що використовують Систему.

13. Держателем Системи є Національне антикорупційне бюро України.

Держатель Системи здійснює:

1) організаційне забезпечення функціонування Системи;

2) планування розвитку Системи і необхідних для цього заходів;

3) розробку нормативно-правових актів, що регламентують порядок функціонування Системи;

4) розробку організаційних та методологічних рекомендацій щодо використання Системи;

5) моніторинг якості функціонування Системи, зокрема повноти та коректності роботи окремих модулів Системи;

6) організацію інформаційної взаємодії з питань функціонування Системи з Суб'єктами Системи;

7) аналіз роботи Системи та її функціоналу на відповідність кримінальному процесуальному законодавству та, у випадку необхідності, приведення функціоналу Системи у відповідність до вимог законодавства;

8) забезпечення модернізації і доопрацювання Системи;

9) формування вимог до забезпечення захисту інформації в Системі;

10) спеціальний облік усіх засобів криптографічного захисту інформації, які використовуються в Системі, а також їх технічну експлуатацію;

11) визначення політики інформаційної безпеки Системи, в тому числі управління рольовою та груповою політикою. Визначення та управління рольовою та груповою політикою, яка стосується органів, що використовують Систему, здійснюється за погодженням з відповідними органами.

Держатель Системи несе відповідальність за дотримання вимог інформаційної безпеки.

14. Технічне адміністрування Системи здійснює Національне антикорупційне бюро України.

Технічне адміністрування Системи передбачає здійснення:

1) адміністрування, технічну підтримку та безперебійне функціонування ядра Системи;

2) забезпечення автоматизованої взаємодії (інтеграції) Системи з іншими автоматизованими, інформаційними, інформаційно-телекомунікаційними системами;

3) організаційну та методологічну підтримку технічного персоналу органів, що використовують Систему;

4) підтримку в актуальному стані класифікаторів, довідників, реєстрів та ідентифікаторів, робочих процесів, шаблонів документів у процесі забезпечення функціонування Системи;

5) технічне обслуговування усіх компонентів ядра Системи;

6) аналіз та діагностику збоїв або припинення роботи апаратно-програмних інформаційних ресурсів Системи;

7) впровадження затверджених правил та вимог з інформаційної безпеки, реалізацію технічних та організаційних заходів із забезпечення захисту інформації, обробка якої виконується в Системі;

8) реєстрацію та аналіз подій, пов'язаних з функціонуванням технічних засобів, засобів захисту та доступом до ресурсів Системи Користувачів, фактів зміни їх повноважень тощо;

9) загальний контроль за дотриманням вимог з інформаційної безпеки всіма Суб'єктами Системи.

15. Органами, що використовують Систему, є Національне антикорупційне бюро України, Спеціалізована антикорупційна прокуратура Офісу Генерального прокурора, Офіс Генерального прокурора та Вищий антикорупційний суд.

Органи, що використовують Систему, забезпечують в межах компетенції:

1) розробку та реалізацію процедур управління доступом до Системи користувачів Системи та здійснення контролю за дотриманням таких процедур;

2) підтримання в актуальному стані кваліфікованого сертифіката відкритого ключа, скасування, блокування та поновлення кваліфікованого сертифіката відкритого ключа користувачів Системи;

3) налаштування, технічне обслуговування та фізичний захист складових Системи відповідно до пункту 7 цього Положення, а саме: телекомунікаційної мережі та автоматизованих робочих місць користувачів Системи;

4) дотримання користувачами Системи вимог цього Положення;

5) дотримання вимог з інформаційної безпеки, вжиття необхідних заходів щодо забезпечення захисту інформації, що міститься в Системі, зокрема під час роботи із Системою користувачів Системи;

6) інформування Держателя Системи про виявлені порушення інформаційної безпеки та участь в їх аналізі, формуванні висновків з метою мінімізації негативних наслідків такого порушення та недопущення їх повторення в майбутньому;

7) впроваджують рішення міжвідомчих робочих груп, комітетів тощо, спільні рішення щодо функціонування і розвитку Системи шляхом вжиття організаційних, технічних, навчальних та інших заходів.

Органи, що використовують Систему, призначають адміністраторів Системи та адміністраторів безпеки Системи, на яких покладаються обов'язки, передбачені цим Положенням та технічною документацією комплексної системи захисту інформації для Системи, в межах компетенції органу, що використовує Систему.

Для вирішення питань функціонування та розвитку Системи органи, що використовують систему, можуть утворювати міжвідомчі робочі групи, комітети тощо, приймати спільні акти та рішення.

V. Користувачі Системи (крім користувачів у Вищому антикорупційному суді) та їх права доступу до Системи

16. Користувачами Системи є уповноважені посадові особи органів, що використовують Систему та учасники кримінального провадження, яким в установленому порядку надано відповідні права доступу до Системи.

17. Користувачами Системи в Національному антикорупційному бюро України є:

1) Директор, його перший заступник та заступники;

2) керівники органу досудового розслідування, органу дізнання, що здійснюють свої повноваження відповідно до Кримінального процесуального кодексу України;

3) посадові особи, які відповідно до Кримінального процесуального кодексу України уповноважені здійснювати досудове розслідування кримінальних правопорушень, кримінальних проступків;

4) інші посадові особи Національного антикорупційного бюро України, перелік яких визначається Директором Національного антикорупційного бюро України або особою, що виконує його обов'язки.

18. Користувачами Системи у Спеціалізованій антикорупційній прокуратурі Офісу Генерального прокурора є:

1) заступник Генерального прокурора – керівник Спеціалізованої антикорупційної прокуратури, його перший заступник та заступники;

2) прокурори, що здійснюють свої повноваження відповідно до Кримінального процесуального кодексу України;

3) інші посадові особи Спеціалізованої антикорупційної прокуратури Офісу Генерального прокурора, перелік яких визначається заступником Генерального прокурора – керівником Спеціалізованої антикорупційної прокуратури або особою, що виконує його обов'язки.

19. Користувачами Системи в Офісі Генерального прокурора є:

1) Генеральний прокурор;

2) інші посадові особи Офісу Генерального прокурора, перелік яких визначається Генеральним прокурором, за наявності необхідного обґрунтування потреби цих осіб у здійсненні доступу до Системи для виконання посадових обов'язків у конкретних кримінальних провадженнях, учасниками яких вони є, а також незалежно від такої потреби – за погодженням керівника Спеціалізованої антикорупційної прокуратури або особи, що виконує його обов'язки.

20. Користувачами Системи можуть бути учасники кримінального провадження, досудове розслідування у якому здійснюється Національним антикорупційним бюро України. Порядок реєстрації таких користувачів, управління доступом до Системи, включаючи відповідні права користувачів, визначаються держателем Системи.

21. Користувачі Системи наділяються правами доступу до Системи з урахуванням прав та повноважень, наданих Кримінальним процесуальним кодексом України.

22. Порядок управління доступом до Системи користувачів Національного бюро визначається розпорядчим документом Директора Національного бюро, з урахуванням приписів Кримінального процесуального кодексу України та цього Положення.

23. Порядок управління доступом до Системи користувачів Спеціалізованої антикорупційної прокуратури Офісу Генерального прокурора визначається розпорядчим документом Генерального прокурора за погодженням керівника Спеціалізованої антикорупційної прокуратури або особи, що виконує

його обов'язки, з урахуванням приписів Кримінального процесуального кодексу України та цього Положення.

24. Порядок управління доступом до Системи користувачів Офісу Генерального прокурора визначається розпорядчим документом Генерального прокурора, з урахуванням приписів Кримінального процесуального кодексу України та цього Положення.

25. Користувачі Системи відповідно до наданих прав доступу мають право:

1) створювати, збирати, зберігати, здійснювати пошук, обробляти і передавати матеріали та інформацію (відомості) у кримінальному провадженні;

2) здійснювати аналітичну обробку інформації (відомостей) та формувати аналітичні звіти з наборів даних, що містяться у Системі;

3) обмінюватися документами та інформацією (відомостями), зокрема надсилати та отримувати документи та інформацію (відомості), спільно працювати з документами та чернетками;

4) використовувати Систему для організації роботи під час досудового розслідування, зокрема здійснювати планування, створювати нагадування, використовувати календар, обмінюватися коментарями, тощо;

5) здійснювати реалізацію інших повноважень, відповідно до наданого системою функціоналу.

26. Користувачі Системи відповідно до наданих прав зобов'язані:

1) вносити до Системи об'єктивну, достовірну та повну інформацію (відомості);

2) своєчасно завантажувати до Системи матеріали кримінального провадження, що існують в паперовій або електронній формі поза межами Системи, з урахуванням вимог щодо якості, визначених цим Положенням;

3) дотримуватися вимог цього Положення та вимог із захисту інформації під час використання Системи;

4) повідомляти Службу захисту інформації Системи про всі інциденти та порушення інформаційної безпеки для вжиття заходів реагування;

5) негайно повідомляти Службу захисту інформації Системи про факти компрометації, втрати або пошкодження засобів кваліфікованого електронного підпису та вживати необхідні заходи для їх блокування.

27. Користувачі Системи несуть відповідальність за порушення вимог цього Положення, незаконне втручання в роботу Системи, розголошення інформації, що міститься у Системі, згідно з чинним законодавством.

VI. Загальні засади функціонування Системи

28. Авторизація користувачів у Системі здійснюється з використанням кваліфікованого електронного підпису в порядку та у спосіб, визначений держателем Системи.

29. Здійснення в Системі дій, пов'язаних із кримінальним провадженням, розпочинається з моменту надходження інформації про зареєстроване кримінальне провадження з Єдиного реєстру досудових розслідувань.

30. Використання Системи користувачами Системи здійснюється відповідно до наданих прав шляхом:

1) внесення інформації (відомостей) у кримінальному провадженні;

2) створення, погодження, затвердження матеріалів кримінального провадження безпосередньо у Системі за допомогою наявних форм та шаблонів;

3) завантаження до Системи матеріалів кримінального провадження, які існують поза межами Системи;

4) дослідження матеріалів кримінального провадження, що містяться в Системі;

5) в інший спосіб, передбачений цим Положенням та функціоналом Системи.

31. В Систему вноситься інформація (відомості) про кримінальне провадження (фабула, встановлені під час досудового розслідування факти, учасники кримінального провадження, представники, кваліфікація кримінального правопорушення, тощо), а також інша інформація (відомості), необхідні для автоматизації процесів досудового розслідування, зокрема інформація про речові докази, підготовку до слідчих (розшукових) дій, тощо. Зазначена інформація (відомості) повинні бути достовірними, повними та підтримуватись в актуальному стані.

32. Матеріали кримінального провадження, зокрема клопотання, постанови, протоколи, доручення, тощо створюються в Системі з використанням форм та шаблонів.

У разі необхідності до клопотань, постанов, протоколів, інших процесуальних документів можуть додаватися додатки. Як додатки можуть обиратися документи, створені в Системі або завантажені до неї. Документи, обрані як додатки, відображаються у вигляді відповідних посилань на них у Системі.

Погодження чи відмова у погодженні, затвердження чи відмова у затвердженні процесуального документа здійснюється за допомогою відповідного функціоналу Системи із накладенням кваліфікованого електронного підпису.

У разі неможливості використання Системи для створення матеріалів кримінального провадження, зокрема у випадках відсутності доступу до Системи, її технічної несправності, відсутності в Системі необхідного функціоналу для реалізації повноважень користувача, створення матеріалів кримінального провадження може здійснюватися поза межами Системи з подальшим завантаженням таких матеріалів до Системи в порядку, передбаченому пунктом 33 цього Положення.

33. Матеріали кримінального провадження, зокрема постанови, клопотання, протоколи, доручення, запити, тощо, створені поза межами Системи слідчим, дізнавачем, прокурором, керівником органу досудового розслідування, дізнання, прокуратури, скануються та завантажуються до Системи не пізніше трьох робочих днів після їх підписання.

Матеріали кримінального провадження, отримані в ході досудового розслідування, зокрема відповіді на запити, вилучені документи, тощо, що

існують в паперовому вигляді, скануються та завантажуються до Системи до моменту винесення постанови про закриття кримінального провадження, складання клопотання про звільнення від кримінальної відповідальності чи повідомлення про завершення досудового розслідування та надання доступу до матеріалів досудового розслідування.

Матеріали кримінального провадження, отримані в ході досудового розслідування, що існують в електронному вигляді, зокрема матеріали фотозйомки, звукозапису, відеозапису, тощо, які містяться на електронних носіях інформації, завантажуються до Системи у разі необхідності за рішенням слідчого, дізнавача, прокурора.

Матеріали кримінального провадження, створені або отримані поза межами Системи в ході проведення негласних слідчих (розшукових) дій, можуть бути відскановані та (або) завантажені до Системи лише після їх розсекречування в порядку, визначеному законодавством.

Матеріали кримінального провадження, досудове розслідування в якому здійснювалося без використання Системи, зокрема, що надійшли з іншого органу досудового розслідування, виділені з матеріалів досудового розслідування, що здійснювалося без використання Системи, скануються та завантажуються до Системи до моменту винесення постанови про закриття кримінального провадження, складання клопотання про звільнення від кримінальної відповідальності чи повідомлення про завершення досудового розслідування та надання доступу до матеріалів досудового розслідування.

У випадку передачі матеріалів кримінального провадження іншому органу досудового розслідування в порядку визначення підслідності матеріали, що існують поза межами Системи, не потребують завантаження до Системи.

Матеріали кримінального провадження, що подаються для розгляду слідчому судді Вищого антикорупційного суду через Систему, повинні бути завантажені до Системи в обов'язковому порядку.

Матеріали кримінального провадження, що скануються для завантаження до Системи, повинні відповідати оригіналу, та мати достатню якість для подальшої роботи з ними в Системі.

34. У разі використання Системи користувачі можуть досліджувати матеріали кримінального провадження, що містяться в Системі, з використанням доступу до них через Систему.

35. В Системі існують допоміжні інструменти для роботи користувачів, що включають можливості планування досудового розслідування кримінального провадження, календарів та нагадувань запланованих подій та інших відомостей, аналітичного модулю в Системі. Користувачам, відповідно до наданих прав, може надаватися доступ до аналітичних інструментів Системи та інших функціональних можливостей Системи.

36. До Системи забезпечується автоматичне внесення інформації (відомостей) шляхом взаємодії з іншими автоматизованими, інформаційними, інформаційно-телекомунікаційними системами.

37. Матеріали кримінального провадження, зокрема постанови, клопотання, протоколи, доручення, запити, тощо, створені в Системі слідчим, дізнавачем, прокурором, керівниками органів досудового розслідування, дізнання, прокуратури, не можуть бути видалені з Системи чи змінені після їх підписання з використанням кваліфікованого електронного підпису.

38. Інформація (відомості), що відповідно до Кримінального процесуального кодексу України та Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення, повинні бути внесені до Єдиного реєстру досудових розслідувань, вносяться до Єдиного реєстру досудових розслідувань в автоматичному режимі внаслідок взаємодії Системи з Єдиним реєстром досудових розслідувань.

39. Матеріали досудового розслідування, які містяться в Системі, передаються, їх копії чи примірники надаються в електронній формі, а за рішенням слідчого, дізнавача, прокурора, які їх передають чи надають, – у паперовій формі.

40. Ознайомлення з матеріалами досудового розслідування, розміщеними в Системі, здійснюється слідчим, дізнавачем, прокурором шляхом надання доступу до них або надання електронних копій чи примірників таких матеріалів, з дотриманням вимог статей 221, 222 КПК України.

41. Відкриття матеріалів досудового розслідування, що містяться в Системі, здійснюється шляхом надання доступу до них або надання електронних копій таких матеріалів, засвідчених в порядку, визначеному цим пунктом.

Скановані копії матеріалів кримінального провадження, або документи в електронному вигляді, які не мають кваліфікованого електронного підпису, засвідчуються шляхом накладення такого підпису.

Електронні примірники електронного документа, підписані шляхом накладення кваліфікованого електронного підпису, вважаються оригіналом електронного документа та не потребують додаткового засвідчення.

VII. Засади функціонування Системи у Вищому антикорупційному суді. Користувачі Системи та їх права доступу до Системи

42. Користувачами Системи у Вищому антикорупційному суді є:

1) Голова Вищого антикорупційного суду, його заступник;

2) слідчі судді Вищого антикорупційного суду;

3) посадові особи апарату Вищого антикорупційного суду, перелік яких визначається наказом Голови Вищого антикорупційного суду, за наявності необхідного обґрунтування потреби цих осіб у здійсненні доступу до Системи для виконання посадових обов'язків у конкретних судових справах.

43. Порядок управління доступом до Системи користувачів у Вищому антикорупційному суді встановлюється наказом Голови Вищого антикорупційного суду, з урахуванням норм Кримінального процесуального кодексу України та цього Положення.

44. Авторизація користувачів Системи у Системі здійснюється з використанням кваліфікованого електронного підпису в порядку та у спосіб, визначений держателем Системи.

45. Користувачі Системи у Вищому антикорупційному суді відповідно до наданих прав доступу мають право:

1) переглядати клопотання, заяви, інші матеріали, які сформовані у Системі на стадії досудового розслідування та подані на розгляд слідчому судді Вищого антикорупційного суду;

2) переглядати матеріали кримінального провадження, які є додатками до зазначених клопотань, заяв, інших матеріалів;

3) досліджувати докази, подані у зазначених клопотаннях, заявах, інших матеріалах;

4) копіювати матеріали клопотань, заяв, інших поданих на розгляд процесуальних документів.

46. Користувачі Системи у Вищому антикорупційному суді зобов'язані:

1) дотримуватись вимог цього Положення та вимог із захисту інформації під час використання Системи;

2) повідомляти Службу захисту інформації Системи про інциденти та порушення інформаційної безпеки для вжиття заходів реагування;

3) невідкладно повідомляти Службу захисту інформації Системи про факти компрометації, втрати або пошкодження засобів кваліфікованого електронного підпису та вживати необхідні заходи для їх блокування.

47. Користувачі Системи у Вищому антикорупційному суді несуть відповідальність за порушення вимог цього Положення, незаконне втручання в роботу Системи, розголошення інформації, що міститься у Системі, згідно з чинним законодавством.

48. Клопотання, заяви, інші матеріали, які подані слідчому судді Вищого антикорупційного суду і можуть бути предметом розгляду слідчим суддею, реєструються у системі, яка функціонує в суді відповідно до статті 35 Кримінального процесуального кодексу України, з дотриманням хронологічного порядку їх надходження, в робочий час, із урахуванням графіка прийому судових справ і матеріалів кримінального провадження, затвердженого рішенням зборів суддів Вищого антикорупційного суду.

49. Слідчі судді Вищого антикорупційного суду, визначені для розгляду клопотання, заяви, інших матеріалів, які надійшли до суду шляхом інтеграції із Системою, можуть досліджувати матеріали поданих їм процесуальних документів безпосередньо у Системі, або із використанням системи, яка функціонує в суді відповідно до статті 35 Кримінального процесуального кодексу України.

VIII. Захист інформації в Системі

50. Інформація в Системі обробляється із застосуванням комплексної системи захисту інформації (КСЗІ) відповідно до вимог чинного законодавства.

51. Комплексна система захисту інформації Систем призначена для:

1) реалізації визначеної політики безпеки інформації;

2) розмежування доступу користувачів до інформації;

3) блокування несанкціонованих дій з інформацією, що потребує захисту, та іншими ресурсами, локалізації цих дій по відношенню до ресурсів Системи та ліквідації їх наслідків;

4) забезпечення контролю та захисту потоків інформації, яка обробляється в Системі;

5) запобігання навмисним чи ненавмисним спробам порушення конфіденційності, цілісності та доступності ресурсів в Системі.

52. Комплексна система захисту інформації Системи забезпечує захист:

1) інформації, яка обробляється та поширюється в Системі;

2) процесів обробки інформації в Системі, інформаційних технологій, регламентів і процедур збору, обробки, зберігання та передачі інформації;

3) інформаційної інфраструктури, яка включає системи обробки та аналізу інформації, технічні та програмні засоби її обробки, передачі та відображення, в тому числі канали інформаційного обміну і телекомунікації, системи та засоби захисту інформації, об'єкти і приміщення, в яких розміщені чутливі елементи інформаційного середовища Системи.

53. З метою забезпечення керованості та розвитку КСЗІ створюється Комітет інформаційної безпеки Системи (Комітет) – міжвідомча робоча група, призначена для:

1) узгодження між органами, що використовують Систему спільної позиції щодо функціонування Системи та забезпечення її інформаційної безпеки;

2) прийняття керівних рішень з питань функціонування Системи та забезпечення її інформаційної безпеки;

3) оцінки ефективності впроваджених засобів захисту;

4) прийняття керівних рішень за результатами аналізу виявлених інцидентів інформаційної безпеки, що пов'язані з Системою.

До складу Комітету інформаційної безпеки Системи залучаються представники всіх органів, що використовують Систему.

Відповідно до порядку денного засідань Комітету, за необхідністю, можуть залучатись фахівці за напрямками.

Головування в Комітеті покладено на держателя Системи.

54. З метою розробки пропозицій щодо розвитку комплексної системи захисту інформації, впровадження вимог з інформаційної безпеки та здійснення контролю за їх виконанням створюється Служба захисту інформації Системи, до складу якої входять адміністратори Системи та адміністратори безпеки Системи і яка призначена для:

1) керування ризиками інформаційної безпеки;

2) формування політик безпеки Системи;

3) формування пропозицій щодо впровадження вимог з інформаційної безпеки;

4) здійснення контролю за виконанням вимог з інформаційної безпеки;

5) керування процесом аналізу інцидентів інформаційної безпеки;

6) керування засобами криптографічного захисту;

7) проведення навчання з питань інформаційної безпеки.

Керування Службою захисту інформації покладено на держателя Системи.

До роботи Служби захисту інформації можуть залучатися фахівці з інформаційної безпеки (адміністратори та адміністратори безпеки) всіх органів, що використовують Систему.

IX. Технічна підтримка

55. Технічна підтримка ядра Системи здійснюється технічним адміністратором Системи в межах повноважень та обсягах, необхідних для забезпечення функціонування та оновлення Системи.

56. Технічний адміністратор Системи повинен мати необхідні матеріально-технічні та кадрові ресурси для забезпечення технічної підтримки Системи. У випадку необхідності технічний адміністратор Системи може залучати до технічної підтримки Системи зовнішніх експертів чи організації.

X. Прикінцеві положення

57. Використання Системи в Національному антикорупційному бюро, Спеціалізованій антикорупційній прокуратурі Офісу Генерального прокурора, Офісі Генерального прокурора розпочинається з дня, що визначається наказом, яким затверджене це Положення.

58. Використання Системи у Вищому антикорупційному суді розпочинається на підставі наказу Голови Вищого антикорупційного суду, який видається за умови забезпечення інтеграції Системи із системою, що функціонує в суді відповідно до статті 35 Кримінального процесуального кодексу України, в обсязі, визначеному абзацами 3-15 пункту 11 цього Положення.

Факт забезпечення інтеграції у зазначеному обсязі підтверджується актом про технічну готовність інтеграції Системи із системою, що функціонує в суді відповідно до статті 35 Кримінального процесуального кодексу України.

59. Використання Системи стороною захисту та іншими учасниками кримінального провадження запроваджуватиметься з урахуванням функціональної, організаційної та матеріально-технічної готовності Системи. За результатами підготовки Системи до використання зазначеними суб'єктами до цього Положення вноситимуться відповідні зміни.

XI. Перехідні положення

60. До забезпечення інтеграції Системи із системою, що функціонує в суді відповідно до статті 35 Кримінального процесуального кодексу України, клопотання, заяви, інші матеріали подаються користувачами Системи до Вищого антикорупційного суду в паперовому вигляді.

61. До початку використання Системи стороною захисту Вищий антикорупційний суд приймає через Систему виключно ті процесуальні документи (матеріали), розгляд яких згідно з нормами Кримінального процесуального кодексу України здійснюється без участі сторони захисту та судові рішення за результатами розгляду яких не підлягають оскарженню. Перелік категорій таких матеріалів визначається наказом Голови Вищого антикорупційного суду.

62. До початку використання Системи стороною захисту ознайомлення з матеріалами досудового розслідування, що містяться в Системі, здійснюється шляхом надання електронних копій чи примірників таких матеріалів, а за рішенням слідчого, дізнавача, прокурора, які їх надають, – у паперовій формі.

63. До початку використання Системи стороною захисту відкриття матеріалів досудового розслідування, що містяться в Системі, здійснюється шляхом надання електронних копій чи примірників таких матеріалів, а за рішенням слідчого, дізнавача, прокурора, які їх надають, – у паперовій формі.

64. До початку автоматизованого обміну інформацією з Єдиним реєстром досудових розслідувань інформація (відомості), що відповідно до вимог Кримінального процесуального кодексу України та положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення, повинні бути внесені до Єдиного реєстру досудових розслідувань, вносяться до Єдиного реєстру досудових розслідувань користувачем вручну.

65. До моменту створення Комітету інформаційної безпеки Системи, Служби захисту інформації Системи, передбачених пунктами 53, 54 цього Положення, їх повноваження виконують відповідні Комітет інформаційної безпеки, Служба захисту інформації Національного антикорупційного бюро України.