

Зразок заповнення звіту про результати аналізу впливу порушення безперервності виконання робочих процесів (бізнес-процесів) та оцінювання пов'язаних з ними засобів інформатизації для умовного засобу інформатизації «Інформаційно-комунікаційна система ОДА», що забезпечує функціонування систем електронного документообігу, кадрового обліку, бухгалтерського обліку та звітності.

Зверніть увагу! Наведені у цьому зразку відомості, показники, найменування, кількісні та якісні характеристики є умовними (вигаданими) та наведені виключно з метою демонстрації порядку заповнення звіту.

ЗАТВЕРДЖУЮ

Голова обласної державної адміністрації
(найменування посади керівника замовника)

(підпис, власне ім'я та прізвище)

_____ р.

ЗВІТ*

про результати аналізу впливу порушення безперервності виконання робочих процесів (бізнес-процесів) та оцінювання пов'язаних з ними засобів інформатизації

Обласна державна адміністрація, 12345678
(найменування замовника, згідно з кодом ЄДРПОУ)

I. Робочі процеси (бізнес-процеси)

1. Опис робочих процесів (бізнес-процесів) (визначаються робочі процеси (бізнес-процеси) порушення безперервності виконання яких понад встановлений Обов'язковими вимогами до створення (модернізації, модифікації, розвитку), адміністрування та забезпечення функціонування засобу інформатизації, затвердженими постановою Кабінету Міністрів України від 21 лютого 2025 р. № 205 “Деякі питання створення, адміністрування та забезпечення функціонування засобу інформатизації”, показник цільового часу відновлення (RTO) для засобів інформатизації III категорії впливу порушення функціонування засобу інформатизації (далі — категорія засобу інформатизації) може призвести до значних негативних наслідків для діяльності замовника)

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Мета (призначення) робочого процесу (бізнес-процесу)	Власник робочого процесу (бізнес-процесу)	Відповідальний за забезпечення робочого процесу (бізнес-процесу)**	Мінімально прийнятний рівень виконання робочого процесу (бізнес-процесу)***	Мінімальна кількість людей, необхідна для виконання робочого процесу (бізнес-процесу)
1	Організація електронного документообігу та контролю виконання документів	Реєстрація, розподіл, погодження, підписання, надсилання документів і контроль виконання доручень керівництва ОДА, актів органів державної влади, звернень та запитів.	Керівник апарату ОДА	Керівник служби діловодства / відповідальний за СЕД	Реєстрація та доведення до виконавців термінових документів; ведення резервного паперового журналу; контроль критичних строків; подальше внесення документів до ІКС після відновлення.	2
2	Кадрове адміністрування та ведення кадрового обліку	Забезпечення оформлення кадрових рішень, ведення особових справ, обліку штатної чисельності, відпусток, відряджень, переведень і звільнень працівників.	Керівник кадрової служби ОДА	Уповноважений працівник кадрової служби / адміністратор кадрового модуля	Оформлення невідкладних кадрових наказів, облік критичних кадрових змін у паперовому резервному журналі, захист персональних даних, подальше звірення та внесення даних до ІКС.	2
3	Бухгалтерський	Ведення	Головний	Заступник	Підготовка та	2

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Мета (призначення) робочого процесу (бізнес-процесу)	Власник робочого процесу (бізнес-процесу)	Відповідальний за забезпечення робочого процесу (бізнес-процесу)**	Мінімально прийнятний рівень виконання робочого процесу (бізнес-процесу)***	Мінімальна кількість людей, необхідна для виконання робочого процесу (бізнес-процесу)
	облік, казначейське обслуговування та фінансова звітність	бухгалтерського обліку, реєстрація бюджетних зобов'язань, підготовка платіжних документів, здійснення платежів, формування та подання фінансової й бюджетної звітності.	бухгалтер ОДА	головного бухгалтера / уповноважений бухгалтер	проведення першочергових платежів, облік критичних операцій у резервних формах, контроль граничних строків звітності, подальше відновлення даних в ІКС із перевіркою їх цілісності.	
4	Адміністрування, відновлення та забезпечення функціонування ІКС	Підтримання працездатності ІКС, керування доступом, резервне копіювання, моніторинг, реагування на інциденти та відновлення функціонування компонентів ІКС.	Керівник структурного підрозділу з питань цифрового розвитку / ІТ-служби	Системний адміністратор ІКС; адміністратор баз даних; фахівець з кіберзахисту	Відновлення доступу до критичних компонентів ІКС і резервних копій, забезпечення обмеженого доступу уповноважених користувачів, фіксація інциденту та інформування власників процесів.	2

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Мета (призначення) робочого процесу (бізнес-процесу)	Власник робочого процесу (бізнес-процесу)	Відповідальний за забезпечення робочого процесу (бізнес-процесу)**	Мінімально прийнятний рівень виконання робочого процесу (бізнес-процесу)***	Мінімальна кількість людей, необхідна для виконання робочого процесу (бізнес-процесу)
5	Реагування на інциденти та забезпечення безперервності діяльності	Координація дій у разі відмови ІКС, кібератаки, втрати зв'язку, електроживлення або іншої події, що впливає на виконання критичних процесів.	Керівник апарату ОДА / відповідальний за кіберзахист	Координатор з питань безперервності діяльності; адміністратор ІКС	Оцінка впливу інциденту, прийняття рішення про перехід на резервний порядок роботи, інформування керівництва й користувачів, координація відновлення в межах $RTO \leq 72$ годин.	2

2. Наслідки порушення виконання робочих процесів (бізнес-процесів) (заповнюється окремо для кожного робочого процесу (бізнес-процесу). Для кожного зазначеного у пункті 1 цього звіту робочого процесу (бізнес-процесу) визначається рівень впливу порушення безперервності його виконання за такими напрямками оцінювання наслідків:

операційний вплив — наслідки порушення або припинення виконання робочих процесів (бізнес-процесів), зниження ефективності діяльності, виникнення затримок або неможливості виконання визначених функцій, завдань та повноважень, у тому числі щодо надання публічних послуг;

вплив на національну безпеку та обороноздатність держави — наслідки, що можуть негативно вплинути на забезпечення національної безпеки, обороноздатності держави, громадської безпеки, захист державного кордону, функціонування сектору безпеки і оборони, діяльність суб'єктів критичної інфраструктури або виконання державою функцій в умовах кризових ситуацій та особливого періоду;

соціальний вплив — наслідки для життя, здоров'я, прав та законних інтересів фізичних осіб, у тому числі обмеження доступу або затримки у наданні соціальних, медичних, освітніх та інших суспільно важливих послуг, що можуть спричинити соціальну напругу або негативну суспільну реакцію;

правовий та регуляторний вплив — наслідки, пов'язані з порушенням вимог законодавства, міжнародних договорів, договірних зобов'язань або регуляторних вимог, що можуть призвести до застосування заходів реагування, притягнення до юридичної відповідальності або виникнення судових спорів;

інформаційний вплив — наслідки порушення конфіденційності, цілісності або доступності інформації, у тому числі несанкціонованого розголошення, втрати, модифікації інформації, порушення функціонування інформаційних (автоматизованих) та/або інформаційно-комунікаційних систем, електронних комунікаційних систем;

репутаційний вплив — наслідки, пов'язані із зниженням рівня довіри громадян, суб'єктів господарювання, органів державної влади, міжнародних партнерів або формуванням негативного сприйняття діяльності замовника;

фінансово-економічний вплив — наслідки, пов'язані з виникненням фінансових втрат, бюджетних збитків, додаткових витрат на відновлення діяльності, застосуванням штрафних санкцій або неефективним використанням ресурсів.

Наведений перелік наслідків за відповідними напрямками оцінювання не є вичерпним та може бути доповнений з урахуванням особливостей діяльності замовника, специфіки робочих процесів (бізнес-процесів) та результатів аналізу впливу порушення безперервності їх виконання)

Організація електронного документообігу та контролю виконання документів

(найменування робочого процесу (бізнес-процесу))

Категорія впливу	Рівень впливу (незначний/ обмежений/ суттєвий/ критичний)	Наслідки переривання робочого процесу (бізнес-процесу)
Операційний вплив	Суттєвий	Унеможливаються або істотно затримуються реєстрація, розподіл, погодження, підписання та надсилання документів; порушується контроль виконання доручень і строків. Зростає ризик невиконання повноважень ОДА, несвоєчасного розгляду звернень, запитів і надання публічних послуг.
Вплив на національну безпеку та/або обороноздатність держави	Суттєвий	В умовах кризової ситуації, воєнного чи особливого періоду може бути ускладнено оперативне доведення доручень органів державної влади, координацію з військовими адміністраціями, органами місцевого самоврядування, суб'єктами цивільного захисту та іншими залученими органами. Для документів із грифом терміновості наслідки можуть набути критичного характеру.
Соціальний вплив	Суттєвий	Затримується розгляд звернень громадян, запитів на публічну

Категорія впливу	Рівень впливу (незначний/ обмежений/ суттєвий/ критичний)	Наслідки переривання робочого процесу (бізнес-процесу)
		інформацію, звернень щодо соціально значущих питань та документів, пов'язаних із наданням адміністративних послуг. Це може обмежити реалізацію прав і законних інтересів осіб та спричинити негативну суспільну реакцію.
Правовий та регуляторний вплив	Суттєвий	Виникає ризик порушення встановлених законодавством строків розгляду звернень, запитів, виконання доручень і підготовки відповідей. Можливі скарги, заходи реагування, службові розслідування, судові спори та притягнення винних посадових осіб до відповідальності відповідно до законодавства.
Інформаційний вплив	Суттєвий	Порушується доступність документів, реєстраційних даних, маршрутів погодження та відомостей про стан виконання доручень. У разі кібератаки, помилки відновлення або відсутності актуальної резервної копії можливі втрата, несанкціонована модифікація чи розголошення службової інформації та персональних даних.
Репутаційний вплив	Суттєвий	Знижується довіра громадян, органів державної влади, партнерів і працівників до спроможності ОДА належно організувати документообіг та виконати покладені повноваження. Невиконання або прострочення термінових доручень може отримати публічний розголос.
Фінансово-економічний вплив	Обмежений	Виникають додаткові витрати на аварійне відновлення ІКС, залучення технічної підтримки, відновлення даних, понаднормову роботу працівників і ручне опрацювання документів. Можливі непрямі втрати через затримку управлінських рішень, закупівель, погоджень або виконання договірних зобов'язань.
Загальний рівень	Суттєвий	

Категорія впливу	Рівень впливу (незначний/ обмежений/ суттєвий/ критичний)	Наслідки переривання робочого процесу (бізнес-процесу)
впливу****		
Максимально допустимий період порушення функціонування (MTPD)	96 годин (4 календарні доби)	

Кадрове адміністрування та ведення кадрового обліку
(найменування робочого процесу (бізнес-процесу))

Категорія впливу	Рівень впливу (незначний/ обмежений/ суттєвий/ критичний)	Наслідки переривання робочого процесу (бізнес-процесу)
Операційний вплив	Обмежений	Затримується оформлення прийняття, переведення, звільнення працівників, відпусток, відряджень, заміщення посад і кадрових наказів. Ускладнюється підтвердження актуальної штатної чисельності та кадрового статусу працівників, зокрема працівників, залучених до невідкладних завдань.
Вплив на національну безпеку та/або обороноздатність держави	Обмежений	За звичайних умов вплив є обмеженим. В умовах воєнного чи особливого періоду тривала недоступність кадрового обліку може ускладнити оперативне формування складу працівників, оформлення їх залучення до завдань ОДА, відряджень та заміщення вакантних посад.
Соціальний вплив	Незначний	Можуть бути порушені трудові права працівників через несвоєчасне оформлення кадрових рішень, відпусток, довідок, змін умов праці або звільнення. Це може призвести до звернень працівників,

Категорія впливу	Рівень впливу (незначний/ обмежений/ суттєвий/ критичний)	Наслідки переривання робочого процесу (бізнес-процесу)
		трудових спорів і негативної внутрішньої реакції.
Правовий та регуляторний вплив	Обмежений	Виникає ризик порушення вимог трудового законодавства, законодавства про державну службу, захист персональних даних, правил ведення кадрової документації та строків оформлення кадрових рішень. Можливі скарги, приписи контролюючих органів, службові перевірки та судові спори.
Інформаційний вплив	Незначний	Порушується доступність і цілісність персональних даних, відомостей про трудову діяльність, штатний розпис та кадрові накази. У разі втрати, несанкціонованої модифікації чи розголошення даних можливе порушення прав працівників і вимог щодо захисту персональних даних.
Репутаційний вплив	Обмежений	Знижується довіра працівників до ОДА як роботодавця та до її спроможності належно забезпечувати кадрове адміністрування. Тривала затримка кадрових рішень може негативно вплинути на імідж установи серед кандидатів, органів влади та громадськості.
Фінансово-економічний вплив	Обмежений	Виникають витрати на ручне ведення кадрового обліку, відновлення даних, залучення технічної підтримки та понаднормову роботу працівників. Можливі непрямі витрати через помилки в кадрових документах, затримки виплат або судові спори.
Загальний рівень впливу****	Обмежений	
Максимально допустимий період порушення функціонування (MTPD)	120 годин (5 календарних діб)	

Бухгалтерський облік, казначейське обслуговування та фінансова звітність
(найменування робочого процесу (бізнес-процесу))

Категорія впливу	Рівень впливу (незначний/ обмежений/ суттєвий/ критичний)	Наслідки переривання робочого процесу (бізнес-процесу)
Операційний вплив	Критичний	Унеможливаються або істотно затримуються реєстрація бюджетних зобов'язань, підготовка платіжних документів, проведення платежів, облік господарських операцій, нарахування виплат, формування та подання фінансової і бюджетної звітності. Порушується виконання фінансових повноважень ОДА.
Вплив на національну безпеку та/або обороноздатність держави	Суттєвий	В умовах кризової ситуації, воєнного чи особливого періоду може бути затримано фінансування невідкладних заходів, закупівель, матеріально-технічного забезпечення, заходів цивільного захисту та інших видатків, необхідних для виконання функцій ОДА. Для платежів, пов'язаних із реагуванням на надзвичайні ситуації, вплив може бути критичним.
Соціальний вплив	Суттєвий	Затримка платежів може вплинути на оплату праці, відшкодування відряджень, оплату товарів і послуг, що використовуються для забезпечення діяльності ОДА та виконання суспільно важливих завдань. Це може спричинити порушення прав працівників, контрагентів та негативну суспільну реакцію.
Правовий та регуляторний вплив	Критичний	Виникає ризик порушення бюджетного законодавства, порядку казначейського обслуговування бюджетних коштів, правил бухгалтерського обліку, строків подання фінансової та бюджетної звітності. Можливі заходи реагування контролюючих органів, фінансові порушення, службові розслідування, претензії контрагентів і судові спори.
Інформаційний вплив	Критичний	Порушується доступність, цілісність і конфіденційність

Категорія впливу	Рівень впливу (незначний/ обмежений/ суттєвий/ критичний)	Наслідки переривання робочого процесу (бізнес-процесу)
		бухгалтерських даних, даних про бюджетні зобов'язання, платежі, договори, контрагентів та фінансову звітність. Втрата або некоректне відновлення даних може спричинити недостовірність обліку, подвійні чи помилкові платежі, неможливість підтвердити операції та ризик витоку службової інформації.
Репутаційний вплив	Суттєвий	Несвоєчасне здійснення платежів або подання звітності знижує довіру органів державної влади, Казначейства, контрагентів, працівників і громадськості до фінансової дисципліни та управлінської спроможності ОДА.
Фінансово-економічний вплив	Критичний	Можливі бюджетні збитки, штрафні санкції, пеня, додаткові витрати на аварійне відновлення, виправлення помилок обліку та залучення технічної підтримки. Затримка платежів може призвести до невиконання договірних зобов'язань, втрати фінансування або неефективного використання бюджетних коштів.
Загальний рівень впливу****	Критичний	
Максимально допустимий період порушення функціонування (MTPD)	96 годин (4 календарні доби)	

Адміністрування, відновлення та забезпечення функціонування ІКС
(найменування робочого процесу (бізнес-процесу))

Категорія впливу	Рівень впливу (незначний/ обмежений/ суттєвий/ критичний)	Наслідки переривання робочого процесу (бізнес-процесу)
Операційний вплив	Критичний	Неможливо забезпечити адміністрування користувачів, моніторинг працездатності, резервне копіювання, усунення технічних несправностей, відновлення серверів, баз даних та прикладних модулів. Це безпосередньо впливає на безперервність електронного документообігу, кадрового та бухгалтерського обліку, звітності й інших процесів ОДА.
Вплив на національну безпеку та/або обороноздатність держави	Суттєвий	В умовах кризової ситуації, воєнного чи особливого періоду відсутність спроможності адмініструвати та відновлювати ІКС може унеможливити оперативне відновлення доступу до критичних інформаційних ресурсів, доведення термінових документів і координацію дій ОДА з іншими органами влади. У разі кібератаки або потреби виконання невідкладних завдань вплив може бути критичним.
Соціальний вплив	Суттєвий	Тривала недоступність ІКС спричиняє затримку розгляду звернень громадян, оформлення кадрових рішень, проведення платежів, підготовки відповідей та надання публічних послуг. Це може обмежити реалізацію прав і законних інтересів фізичних осіб та спричинити негативну суспільну реакцію.
Правовий та регуляторний вплив	Суттєвий	Виникає ризик невиконання вимог щодо захисту інформації, персональних даних, резервного копіювання, збереження електронних документів, ведення обліку та своєчасного подання звітності. Можливі службові перевірки, приписи, скарги, притягнення відповідальних осіб до відповідальності та судові спори.
Інформаційний вплив	Критичний	Порушується доступність, конфіденційність і цілісність інформації

Категорія впливу	Рівень впливу (незначний/ обмежений/ суттєвий/ критичний)	Наслідки переривання робочого процесу (бізнес-процесу)
		ІКС. За відсутності належного адміністрування або відновлення можуть бути втрачені резервні копії, журнали подій, конфігурації та дані; можливі несанкціонований доступ, поширення шкідливого програмного забезпечення, модифікація або розголошення службової інформації та персональних даних.
Репутаційний вплив	Суттєвий	Знижується довіра керівництва, працівників, громадян, органів державної влади та партнерів до спроможності ОДА забезпечити стабільну й захищену роботу ІКС. Тривалий інцидент або невдале відновлення може набути публічного розголосу.
Фінансово-економічний вплив	Суттєвий	Виникають витрати на аварійне відновлення, залучення технічної підтримки, придбання або заміну обладнання і програмного забезпечення, відновлення даних, проведення розслідувань та понаднормову роботу працівників. Непрямі втрати виникають через зупинення залежних бізнес-процесів, затримку платежів і звітності.
Загальний рівень впливу****	Критичний	
Максимально допустимий період порушення функціонування (MTPD)	24 години	

Реагування на інциденти та забезпечення безперервності діяльності
(найменування робочого процесу (бізнес-процесу))

Категорія впливу	Рівень впливу (незначний/ обмежений/ суттєвий/ критичний)	Наслідки переривання робочого процесу (бізнес-процесу)
Операційний вплив	Критичний	Відсутність належного реагування на інциденти унеможливорює своєчасне виявлення, локалізацію, ескалацію та усунення наслідків відмови ІКС, кібератаки, втрати електроживлення або зв'язку. Зупинка цього процесу істотно збільшує тривалість порушення всіх залежних процесів ОДА та ризик їх невідновлення в установлені строки.
Вплив на національну безпеку та/або обороноздатність держави	Суттєвий	В умовах кризової ситуації, воєнного чи особливого періоду несвоєчасне реагування може ускладнити відновлення обміну терміновою інформацією, координацію з органами влади, військовими адміністраціями, суб'єктами цивільного захисту та іншими залученими сторонами. Для інцидентів, що впливають на виконання невідкладних державних завдань, наслідки можуть бути критичними.
Соціальний вплив	Суттєвий	Тривале нерозв'язання інциденту призводить до затримки надання публічних послуг, розгляду звернень громадян, виконання кадрових та фінансових операцій. Це може обмежити реалізацію прав і законних інтересів фізичних осіб та спричинити негативну суспільну реакцію.
Правовий та регуляторний вплив	Суттєвий	Можуть бути порушені вимоги щодо захисту інформації, персональних даних, збереження електронних документів, ведення журналів подій, повідомлення про інциденти та забезпечення безперервності діяльності. Наслідками можуть бути службові перевірки, приписи, скарги, притягнення відповідальних осіб до відповідальності або судові спори.
Інформаційний вплив	Критичний	Несвоєчасна локалізація інциденту підвищує ймовірність

Категорія впливу	Рівень впливу (незначний/ обмежений/ суттєвий/ критичний)	Наслідки переривання робочого процесу (бізнес-процесу)
		поширення шкідливого програмного забезпечення, несанкціонованого доступу, втрати, модифікації або розголошення службової інформації та персональних даних. Може бути втрачено можливість оперативно зберегти журнали подій, резервні копії та інші докази для розслідування.
Репутаційний вплив	Суттєвий	Неефективне реагування на інцидент знижує довіру керівництва, працівників, громадян, інших органів влади та партнерів до спроможності ОДА захистити інформацію й відновити роботу. Особливо значним є репутаційний ризик у разі публічного розголошення даних або тривалої недоступності сервісів.
Фінансово-економічний вплив	Суттєвий	Зростають витрати на аварійне відновлення, залучення зовнішніх фахівців, відновлення даних, ліквідацію наслідків кібератаки, понаднормову роботу та технічну підтримку. Затягування реагування може збільшити масштаби збитків, спричинених простоем залежних процесів.
Загальний рівень впливу****	Критичний	
Максимально допустимий період порушення функціонування (MTPD)	8 годин	

3. Залежність робочого процесу (бізнес-процесу) від засобів інформатизації (зазначаються засоби інформатизації (ресурси), порушення функціонування яких унеможлиблює або істотно обмежує виконання ідентифікованих у пункті 2 цього звіту робочих процесів (бізнес-процесів) з обмеженим, суттєвим або критичним загальним рівнем впливу. Відомості про робочі процеси (бізнес-процеси) відображаються незалежно від форми права власності чи користування такими засобами)

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
1.	Організація електронного документообігу та контролю виконання документів	ІКС ОДА, у складі якої функціонує система електронного документообігу (СЕД)	Внутрішня	Критичний	Унеможлиблюються реєстрація, розподіл, погодження, підписання, пошук і контроль виконання електронних документів. Допускається лише тимчасовий резервний паперовий порядок.
2.	Організація електронного документообігу та контролю виконання документів	Сервери застосунків та віртуалізаційна інфраструктура ІКС	Внутрішня	Критичний	Недоступність серверів припиняє роботу СЕД і доступ користувачів до її функціональних модулів.
3.	Організація електронного документообігу	Сервер баз даних / система	Внутрішня	Критичний	Неможливі доступ до реєстраційних даних, маршрутів погодження, електронних

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
	та контролю виконання документів	управління базами даних ІКС			документів і відомостей про стан виконання доручень; виникає ризик втрати або пошкодження даних.
4.	Організація електронного документообігу та контролю виконання документів	Файлове сховище електронних документів і резервні копії	Внутрішня	Критичний	Унеможливаються перегляд, завантаження та відновлення електронних документів і додатків; у разі втрати даних не забезпечується їх відновлення в межах RPO.
5.	Організація електронного документообігу та контролю виконання документів	Локальна комп'ютерна мережа ОДА, мережеве обладнання, Wi-Fi та VPN	Внутрішня	Суттєвий	Користувачі втрачають доступ до СЕД, серверів і спільних ресурсів; віддалені працівники не можуть виконувати дії в системі.
6.	Організація електронного документообігу	Робочі станції уповноважених працівників,	Внутрішня	Суттєвий	Окремі користувачі не можуть реєструвати, готувати, погоджувати або опрацьовувати

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
	та контролю виконання документів	керівників і діловодів			документи. Робота може бути частково продовжена з резервного робочого місця.
7.	Організація електронного документообігу та контролю виконання документів	Засоби кваліфікованого електронного підпису: КЕП, захищені носії ключової інформації, програмне забезпечення підпису	Зовнішня	Критичний	Неможливе юридично значуще підписання та погодження електронних документів; затримується надсилання офіційних листів, наказів, доручень і відповідей.
8.	Організація електронного документообігу та контролю виконання документів	Доступ до Інтернету та захищені канали електронної взаємодії	Зовнішня	Суттєвий	Ускладнюється або припиняється обмін документами з іншими органами влади, надсилання електронної кореспонденції, використання зовнішніх сервісів та віддалений доступ до ІКС.

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
9.	Організація електронного документообігу та контролю виконання документів	Система керування обліковими записами та доступом користувачів	Внутрішня	Суттєвий	Неможливе надання, зміна або блокування доступу; у разі відмови автентифікації користувачі не можуть увійти до СЕД.
10.	Організація електронного документообігу та контролю виконання документів	Електроживлення серверної, ДБЖ та резервне джерело живлення	Внутрішня	Критичний	Раптове припинення роботи серверів, мережевого обладнання та робочих місць; ризик пошкодження обладнання, втрати незбережених документів і порушення цілісності баз даних.
11.	Організація електронного документообігу та контролю виконання документів	Підтримка постачальника СЕД та/або адміністратора ІКС	Зовнішня	Суттєвий	Збільшується час усунення технічних несправностей, оновлення програмного забезпечення та відновлення працездатності СЕД.

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
12.	Кадрове адміністрування та ведення кадрового обліку	ІКС ОДА, у складі якої функціонує система кадрового обліку	Внутрішня	Критичний	Унеможлиблюється централізоване ведення кадрового обліку, робота з особовими справами, штатним розписом, кадровими наказами та відомостями про працівників.
13.	Кадрове адміністрування та ведення кадрового обліку	Сервери застосунків і віртуалізаційна інфраструктура ІКС	Внутрішня	Критичний	Припиняється робота кадрового модуля та доступ уповноважених працівників до його функцій.
14.	Кадрове адміністрування та ведення кадрового обліку	Сервер баз даних / СУБД ІКС	Внутрішня	Критичний	Неможливий доступ до даних про працівників, кадрові переміщення, відпустки, штатні посади та кадрові документи; виникає ризик втрати або пошкодження даних.
15.	Кадрове адміністрування та ведення кадрового обліку	Сховище електронних кадрових	Внутрішня	Критичний	Унеможлиблюється пошук, перегляд та відновлення особових справ, наказів, заяв, документів щодо відпусток і відряджень; не

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
		документів і резервні копії			гарантується відновлення даних у межах RPO.
16.	Кадрове адміністрування та ведення кадрового обліку	Робочі станції працівників кадрової служби	Внутрішня	Суттєвий	Неможливо оформлювати кадрові документи та вносити дані до системи з конкретного робочого місця. Може застосовуватися резервне робоче місце.
17.	Кадрове адміністрування та ведення кадрового обліку	Локальна комп'ютерна мережа ОДА, мережеве обладнання, Wi Fi та VPN	Внутрішня	Суттєвий	Втрачається доступ до кадрового модуля, серверів, сховища документів і спільних інформаційних ресурсів; унеможлиблюється віддалена робота уповноважених працівників.
18.	Кадрове адміністрування та ведення кадрового обліку	Система керування обліковими записами та	Внутрішня	Суттєвий	Працівники кадрової служби не можуть автентифікуватися в ІКС; ускладнюється оперативне блокування або надання доступу до кадрових даних.

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
		доступом користувачів			
19.	Кадрове адміністрування та ведення кадрового обліку	Засоби кваліфікованого електронного підпису: КЕП, захищені носії ключової інформації, програмне забезпечення підпису	Зовнішня	Суттєвий	Неможливе юридично значуще підписання електронних кадрових наказів, погоджень, заяв та інших документів. Може бути застосовано резервний паперовий порядок, якщо він визначений внутрішніми документами ОДА.
20.	Кадрове адміністрування та ведення кадрового обліку	Доступ до Інтернету та захищені канали електронної взаємодії	Зовнішня	Обмежений	Ускладнюється обмін електронними документами з іншими органами, отримання або передання відомостей через зовнішні сервіси та віддалений доступ. Внутрішній кадровий облік може частково продовжуватися за

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
					наявності локального доступу до ІКС.
21.	Кадрове адміністрування та ведення кадрового обліку	Електроживлення серверної, ДБЖ і резервне джерело живлення	Внутрішня	Критичний	Припиняється робота серверів, мережевого обладнання та кадрового модуля; існує ризик втрати незбережених даних або пошкодження бази даних під час аварійного вимкнення.
22.	Кадрове адміністрування та ведення кадрового обліку	Програмне забезпечення антивірусного захисту / EDR та засоби резервного відновлення	Внутрішня	Суттєвий	Зростає ризик компрометації персональних даних, зараження робочих станцій і серверів, втрати кадрової інформації або тривалого простою внаслідок кібератаки.
23.	Кадрове адміністрування та ведення кадрового обліку	Технічна підтримка постачальника кадрового програмного	Зовнішня	Суттєвий	Збільшується тривалість усунення помилок, оновлення програмного забезпечення й відновлення кадрового модуля.

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
		продукту та/або адміністратора ІКС			
24.	Бухгалтерський облік, казначейське обслуговування та фінансова звітність	ІКС ОДА, у складі якої функціонує система бухгалтерського обліку та звітності	Внутрішня	Критичний	Унеможливаються ведення бухгалтерського обліку, реєстрація операцій, формування платіжних документів, облік бюджетних зобов'язань і підготовка звітності.
25.	Бухгалтерський облік, казначейське обслуговування та фінансова звітність	Сервери застосунків і віртуалізаційна інфраструктура ІКС	Внутрішня	Критичний	Припиняється робота бухгалтерського модуля та доступ уповноважених працівників до облікових функцій.
26.	Бухгалтерський облік, казначейське	Сервер баз даних / СУБД ІКС	Внутрішня	Критичний	Недоступні дані про господарські операції, бюджетні зобов'язання, платежі, договори, контрагентів та

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
	обслуговування та фінансова звітність				звітність; виникає ризик втрати або пошкодження бухгалтерських даних.
27.	Бухгалтерський облік, казначейське обслуговування та фінансова звітність	Файлове сховище бухгалтерських документів, звітності та резервних копій	Внутрішня	Критичний	Унеможливаються пошук, перегляд, підтвердження та відновлення первинних документів, платіжних документів, реєстрів і звітів; не гарантується відновлення даних у межах RPO.
28.	Бухгалтерський облік, казначейське обслуговування та фінансова звітність	Робочі станції головного бухгалтера, уповноважених бухгалтерів та працівників, які формують платежі	Внутрішня	Суттєвий	Неможливі підготовка, перевірка, погодження та подання платіжних документів і звітності з конкретного робочого місця. Робота може бути частково продовжена з резервного робочого місця.
29.	Бухгалтерський облік,	Локальна комп'ютерна	Внутрішня	Суттєвий	Втрачається доступ до бухгалтерського модуля, баз даних,

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
	казначейське обслуговування та фінансова звітність	мережа ОДА, мережеве обладнання, Wi Fi та VPN			файлового сховища та інших внутрішніх ресурсів; унеможлиблюється віддалена робота уповноважених працівників.
30.	Бухгалтерський облік, казначейське обслуговування та фінансова звітність	Автоматизована система Державної казначейської служби України та захищені канали взаємодії з нею	Зовнішня	Критичний	Неможливі або істотно затримуються передання платіжних документів, реєстрація бюджетних зобов'язань, проведення платежів і отримання відомостей про їх стан.
31.	Бухгалтерський облік, казначейське обслуговування та фінансова звітність	Доступ до Інтернету та захищені канали електронних комунікацій	Зовнішня	Критичний	Унеможлиблюється взаємодія з Казначейством, подання електронної звітності, використання зовнішніх державних інформаційних систем і віддалений доступ до ІКС.

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
32.	Бухгалтерський облік, казначейське обслуговування та фінансова звітність	Засоби кваліфікованого електронного підпису: КЕП, захищені носії ключової інформації, програмне забезпечення підпису	Зовнішня	Критичний	Неможливе юридично значуще підписання платіжних документів, звітності, договорів та інших фінансових документів; затримуються платежі й виконання фінансових зобов'язань.
33.	Бухгалтерський облік, казначейське обслуговування та фінансова звітність	Система керування обліковими записами та доступом користувачів	Внутрішня	Суттєвий	Уповноважені працівники не можуть автентифікуватися в ІКС; ускладнюється оперативне надання, зміна або блокування доступу до фінансових даних.
34.	Бухгалтерський облік, казначейське	Електроживлення серверної, ДБЖ і	Внутрішня	Критичний	Припиняється робота серверів, мережевого обладнання та бухгалтерського модуля; виникає

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
	обслуговування та фінансова звітність	резервне джерело живлення			ризик втрати незбережених операцій, пошкодження баз даних і затримки критичних платежів.
35.	Бухгалтерський облік, казначейське обслуговування та фінансова звітність	Програмне забезпечення антивірусного захисту / EDR та засоби резервного відновлення	Внутрішня	Суттєвий	Зростає ризик компрометації фінансових даних, зараження робочих станцій або серверів, втрати даних і тривалого простою внаслідок кібератаки.
36.	Бухгалтерський облік, казначейське обслуговування та фінансова звітність	Технічна підтримка постачальника бухгалтерського програмного продукту та/або адміністратора ІКС	Зовнішня	Суттєвий	Збільшується час усунення помилок, оновлення програмного забезпечення, відновлення коректної роботи бухгалтерського модуля та формування звітності.
37.	Адміністрування, відновлення та	Адміністративні робочі станції	Внутрішня	Критичний	Неможливо керувати серверною інфраструктурою, мережевим

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
	забезпечення функціонування ІКС	системних адміністраторів			обладнанням, обліковими записами, резервними копіями та прикладними модулями ІКС.
38.	Адміністрування, відновлення та забезпечення функціонування ІКС	Сервери застосунків, сервери віртуалізації та програмні засоби керування ними	Внутрішня	Критичний	Ускладнюється або унеможлиблюється запуск, зупинка, налаштування, моніторинг і відновлення віртуальних машин та сервісів ІКС.
39.	Адміністрування, відновлення та забезпечення функціонування ІКС	Сервер баз даних / СУБД та засоби адміністрування баз даних	Внутрішня	Критичний	Неможливі контроль стану баз даних, резервне копіювання, відновлення даних, перевірка їх цілісності та усунення помилок, що впливають на функціонування прикладних систем.
40.	Адміністрування, відновлення та забезпечення	Система резервного копіювання, сховище	Внутрішня	Критичний	Неможливо створювати, перевіряти або відновлювати резервні копії даних, конфігурацій та віртуальних машин; суттєво

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
	функціонування ІКС	резервних копій та засоби відновлення			зростає ризик безповоротної втрати інформації після інциденту.
41.	Адміністрування, відновлення та забезпечення функціонування ІКС	Локальна комп'ютерна мережа ОДА, мережеве обладнання, Wi Fi та VPN	Внутрішня	Критичний	Неможливо забезпечити доступ користувачів і адміністраторів до ІКС, виконати дистанційне адміністрування, локалізувати мережевий інцидент або відновити мережеву взаємодію.
42.	Адміністрування, відновлення та забезпечення функціонування ІКС	Система керування обліковими записами, правами доступу та привілейованими обліковими записами	Внутрішня	Критичний	Неможливо надати або відкликати доступ, заблокувати скомпрометовані облікові записи, відновити права адміністраторів чи забезпечити контроль доступу після інциденту.

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
43.	Адміністрування, відновлення та забезпечення функціонування ІКС	Система моніторингу, централізованого журналювання та оповіщення	Внутрішня	Суттєвий	Ускладнюється своєчасне виявлення відмов, кібератак, перевищення порогових значень і деградації сервісів; збільшується час діагностики та відновлення ІКС.
44.	Адміністрування, відновлення та забезпечення функціонування ІКС	Засоби антивірусного захисту, EDR/XDR, міжмережеві екрани та інші засоби кіберзахисту	Внутрішня	Критичний	Неможливо оперативно виявити, ізолювати та стримати кіберінцидент; підвищується ризик поширення шкідливого програмного забезпечення, компрометації даних і тривалого простою ІКС.
45.	Адміністрування, відновлення та забезпечення функціонування ІКС	Електроживлення серверної, ДБЖ, резервне джерело живлення та система контролю	Внутрішня	Критичний	Аварійне припинення роботи серверів і мережевого обладнання, ризик пошкодження техніки, втрати даних, порушення цілісності баз даних та

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
		параметрів середовища			неможливість виконувати відновлювальні дії.
46.	Адміністрування, відновлення та забезпечення функціонування ІКС	Доступ до Інтернету, захищені канали зв'язку та віддалений адміністративний доступ	Зовнішня	Суттєвий	Ускладнюється доступ до зовнішніх оновлень, хмарних резервних копій, віддаленої технічної підтримки та адміністрування ІКС поза приміщенням ОДА.
47.	Адміністрування, відновлення та забезпечення функціонування ІКС	Технічна документація, реєстр конфігурацій, облікові дані аварійного доступу та носії програмного забезпечення	Внутрішня	Суттєвий	Збільшується ризик помилок і час відновлення; неможливо оперативно відтворити коректну конфігурацію, визначити залежності компонентів або виконати аварійні процедури.

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
48.	Адміністрування, відновлення та забезпечення функціонування ІКС	Послуги постачальників обладнання, програмного забезпечення, телекомунікацій та технічної підтримки	Зовнішня	Суттєвий	Збільшується час ремонту, заміни обладнання, отримання оновлень, ліцензійних ключів, консультацій та усунення складних технічних несправностей.
49.	Реагування на інциденти та забезпечення безперервності діяльності	Робочі станції уповноважених працівників, системних адміністраторів і координатора з безперервності діяльності	Внутрішня	Критичний	Неможливо отримати доступ до засобів моніторингу, журналів подій, адміністративних консолей, планів реагування та інструментів відновлення.
50.	Реагування на інциденти та забезпечення	Система моніторингу доступності ІКС,	Внутрішня	Критичний	Несвоєчасно виявляються відмови, деградація сервісів і критичні події; збільшується час початку

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
	безперервності діяльності	серверів, мережевого обладнання та прикладних систем			реагування, діагностики та відновлення.
51.	Реагування на інциденти та забезпечення безперервності діяльності	Система централізованого журналювання, SIEM або журнали подій серверів, мережевого обладнання та прикладних систем	Внутрішня	Критичний	Унеможлиблюються аналіз причин інциденту, визначення його масштабу, виявлення скомпрометованих облікових записів і збереження доказів для розслідування.
52.	Реагування на інциденти та забезпечення	Система резервного копіювання, сховище	Внутрішня	Критичний	Неможливо перевірити наявність актуальних резервних копій, відновити дані, конфігурації та сервіси ІКС після інциденту;

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
	безперервності діяльності	резервних копій та засоби відновлення			зростає ризик безповоротної втрати інформації.
53.	Реагування на інциденти та забезпечення безперервності діяльності	Адміністративні консолі серверів, систем віртуалізації, СУБД та прикладних систем	Внутрішня	Критичний	Неможливо локалізувати інцидент, зупинити скомпрометований сервіс, змінити конфігурацію, відновити базу даних або перезапустити критичні компоненти ІКС.
54.	Реагування на інциденти та забезпечення безперервності діяльності	Локальна комп'ютерна мережа ОДА, мережеве обладнання, міжмережеві екрани, VPN, засоби сегментації	Внутрішня	Критичний	Неможливо ізолювати скомпрометований сегмент, заблокувати шкідливий мережевий трафік, обмежити несанкціонований доступ або відновити захищену мережеву взаємодію.

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
		мережі та їх системи керування			
55.	Реагування на інциденти та забезпечення безперервності діяльності	Засоби кіберзахисту: антивірусне програмне забезпечення, EDR/XDR, засоби виявлення вторгнень	Внутрішня	Критичний	Ускладнюється виявлення, локалізація та усунення наслідків кібератаки; підвищується ризик поширення шкідливого програмного забезпечення, втрати або розголошення даних.
56.	Реагування на інциденти та забезпечення безперервності діяльності	Система керування обліковими записами та привілейованим доступом	Внутрішня	Критичний	Неможливо оперативно заблокувати скомпрометовані облікові записи, змінити паролі, відкликати права доступу або надати аварійний доступ уповноваженим адміністраторам.
57.	Реагування на інциденти та	Електронна пошта, захищені	Внутрішня	Суттєвий	Ускладнюється оповіщення керівництва, працівників,

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
	забезпечення безперервності діяльності	месенджери, корпоративний телефонний зв'язок та інші канали службової комунікації			постачальників і зовнішніх суб'єктів; затримується ескалація інциденту та координація відновлювальних дій.
58.	Реагування на інциденти та забезпечення безперервності діяльності	Резервний канал комунікації: мобільний зв'язок, альтернативний доступ до Інтернету, резервні контактні дані	Зовнішня	Суттєвий	За відсутності основних каналів зв'язку неможливо оперативно координувати дії учасників реагування та забезпечити комунікацію під час масштабного інциденту.
59.	Реагування на інциденти та забезпечення	Електронні копії планів реагування на інциденти, плану	Внутрішня	Суттєвий	Працівники не мають доступу до затверджених сценаріїв, ролей, порядку ескалації та контактів; зростає ризик неузгоджених дій і

Порядковий номер	Найменування робочого процесу (бізнес-процесу)	Найменування засобу інформатизації (ресурсу), необхідного для виконання робочого процесу (бізнес-процесу)	Тип залежності (внутрішня/зовнішня)	Рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації (незначний/обмежений/суттєвий/критичний)	Наслідки порушення доступності
	безперервності діяльності	безперервності діяльності, контактів та інструкцій з відновлення			перевищення встановлених строків відновлення.
60.	Реагування на інциденти та забезпечення безперервності діяльності	Послуги постачальників технічної підтримки, електронних комунікацій, хмарного зберігання та кіберзахисту	Зовнішня	Суттєвий	Збільшується тривалість діагностики, ремонту, заміни обладнання, відновлення сервісів та отримання спеціалізованої допомоги.

II. Засоби інформатизації (заповнюється для кожного засобу інформатизації окремо)

4. Загальні відомості про засіб інформатизації (зазначаються ідентифіковані у пункті 3 цього звіту засоби інформатизації, що перебувають у власності замовника або використовуються ним на інших законних підставах та мають обмежений, суттєвий або критичний рівень залежності робочого процесу (бізнес-процесу) від засобу інформатизації. Засоби інформатизації, що використовуються виключно для інформаційного, довідкового або допоміжного забезпечення виконання робочого процесу (бізнес-процесу), зазначаються у цьому розділі лише у разі, коли їх недоступність має істотний вплив на виконання такого процесу або призводить до значного сповільнення його виконання)

Найменування засобу інформатизації	Інформаційно-комунікаційна система ОДА
Скорочена назва засобу інформатизації (за наявності)	ІКС ОДА
Власник (держатель) засобу інформатизації	ОДА
Тип засобу інформатизації (інформаційна (автоматизована) система/ інформаційно-комунікаційна система/технологічна система/ реєстр/вебпортал/електронний сервіс/центр обробки даних/ хмарний сервіс/інше	інформаційна (автоматизована) система
Призначення засобу інформатизації	ІКС ОДА призначена для автоматизації, інформаційної підтримки та забезпечення безперервного виконання основних управлінських і забезпечувальних процесів обласної державної адміністрації. Вона забезпечує створення, реєстрацію, оброблення, зберігання, пошук, передавання та захист інформації, а також взаємодію працівників ОДА, її структурних підрозділів, інших органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій і громадян.
Основні функції засобу інформатизації	електронний документообіг, погодження, підписання документів та контроль виконання доручень;

	кадрове адміністрування, ведення кадрового обліку та захист персональних даних працівників; бухгалтерський облік, казначейське обслуговування, проведення фінансових операцій і формування звітності; підготовку управлінської інформації, аналітичних матеріалів і звітів для керівництва; інформаційну взаємодію із зовнішніми державними інформаційними системами та електронними комунікаційними мережами; керування доступом користувачів, резервне копіювання, моніторинг, кіберзахист, реагування на інциденти та відновлення працездатності інформаційних ресурсів.
Кількість користувачів (внутрішніх/зовнішніх)	100/1500
Види інформації, що обробляються засобом інформатизації (відкрита/ службова/конфіденційна/ державна таємниця/інше)	відкрита/ службова/конфіденційна
Використання хмарних технологій (так/ні)	так
Місце розміщення (локальна інфраструктура/власний центр обробки даних/орендований центр обробки даних/хмарна інфраструктура/гібридна інфраструктура)	локальна інфраструктура/хмарна інфраструктура
Рівень критичної інфраструктури (за наявності)	-

5. Інформація про персонал, залучений до забезпечення безперервності функціонування засобів інформатизації (зазначаються відомості про працівників замовника та/або технічного адміністратора, які забезпечують адміністрування, технічну підтримку, експлуатацію, відновлення функціонування та реагування на порушення роботи засобу інформатизації)

Порядковий номер	Роль у забезпеченні функціонування та відновлення засобу інформатизації	Тип ролі адміністратора (основний/дублюючий)	Власне ім'я та прізвище адміністратора	Посада адміністратора	Контактні дані (робочий та мобільний телефон, адреса електронної пошти)
1	Координація BCP/DRP, кризове управління	основний	Хмаренко Тарас Григорович	Начальник ІТ-відділу ОДА	контакт за затвердженим контакт-листом
2		дублюючий	Резервенко Олег Миколайович	Головний спеціаліст ІТ-відділу ОДА	контакт за затвердженим контакт-листом
3	Відновлення інфраструктури, мережі, резервних копій	основний	Мережко Степан Андрійович	Начальник відділу адміністрування інформаційно-комунікаційної інфраструктури ОДА	контакт за затвердженим контакт-листом
4		дублюючий	Оптенко Ірина Вікторівна	Головний спеціаліст відділу адміністрування інформаційно-комунікаційної інфраструктури ОДА	контакт за затвердженим контакт-листом

Порядковий номер	Роль у забезпеченні функціонування та відновлення засобу інформатизації	Тип ролі адміністратора (основний/дублюючий)	Власне ім'я та прізвище адміністратора	Посада адміністратора	Контактні дані (робочий та мобільний телефон, адреса електронної пошти)
5	Реагування на кіберінциденти, контроль безпечного відновлення	основний	Безпечна Леся Петрівна	Начальник відділу інформаційної безпеки ОДА	контакт за затвердженим контакт-листом
6		основний	Стійченко Павло Олександрович	Заступник начальника відділу інформаційної безпеки ОДА	контакт за затвердженим контакт-листом

6. Активи, необхідні для забезпечення функціонування засобу інформатизації (визначаються інформаційні, програмні, апаратні, технологічні та інші ресурси, необхідні для функціонування засобу інформатизації та забезпечення виконання пов'язаних з ним робочих процесів (бізнес-процесів))

Порядковий номер	Тип активу	Найменування активу	Власник (власне ім'я та прізвище/ назва організації/підрозділ)	Рівень впливу (незначний/ обмежений/ суттєвий/ критичний)	Наслідки втрати активу
1.	Дані та інформаційні ресурси	База даних ІКС IKS_PROD: реєстраційні картки СЕД, електронні документи,	Служба діловодства, відділ управління персоналом, департамент фінансів; технічний власник —	Критичний	Неможливо підтвердити факт реєстрації та виконання документів, оформити кадрові

Порядковий номер	Тип активу	Найменування активу	Власник (власне ім'я та прізвище/ назва організації/ підрозділ)	Рівень впливу (незначний/ обмежений/ суттєвий/ критичний)	Наслідки втрати активу
		кадрові накази, особові дані працівників, бухгалтерські проводки та фінансова звітність	управління цифрового розвитку ОДА		рішення, вести бухгалтерський облік і сформувані звітність; можливі втрата персональних даних та недостовірність фінансової інформації.
2.	Резервні копії та копії відновлення	Щоденні резервні копії БД IKS_PROD, щотижневі повні копії віртуальних машин VM-IKS-APP01, VM-IKS-DB01; офлайн-копія на захищеному носії	Мережко Степан Андрійович/начальник відділу адміністрування інформаційно-комунікаційної інфраструктури ОДА	Критичний	Після кібератаки, відмови сервера або помилкового видалення неможливо відновити ІКС і дані в межах RPO ≤ 24 годин.

Порядковий номер	Тип активу	Найменування активу	Власник (власне ім'я та прізвище/ назва організації/ підрозділ)	Рівень впливу (незначний/ обмежений/ суттєвий/ критичний)	Наслідки втрати активу
3.	Апаратне забезпечення	Сервер SRV-01, сервер SRV-02, мережеве сховище NAS-01, комутатор SW-CORE-01, міжмережевий екран FW-01, ДБЖ UPS-01	Управління цифрового розвитку ОДА	Критичний	Зупиняється робота серверів, баз даних, СЕД, кадрового та бухгалтерського модулів; користувачі втрачають доступ до ІКС.
4.	Віртуальні ресурси та обчислювальні ресурси (віртуальні машини, контейнери, кластерні ресурси)	Віртуальні машини: VM-IKS-APP01 — сервер застосунків; VM-IKS-DB01 — сервер БД; VM-IKS-FILE01 — файлове сховище; VM-IKS-BACKUP01 — резервне копіювання	Хмаренко Тарас Григорович/начальник ІТ-відділу ОДА	Критичний	Неможливо запустити прикладні модулі ІКС, СУБД, сховище електронних документів та сервіс резервного копіювання.

Порядковий номер	Тип активу	Найменування активу	Власник (власне ім'я та прізвище/ назва організації/ підрозділ)	Рівень впливу (незначний/ обмежений/ суттєвий/ критичний)	Наслідки втрати активу
5.	Програмне забезпечення та програмні компоненти	СЕД «АСКОД» або інша фактично використовувана СЕД; кадровий модуль; бухгалтерська програма; Microsoft Windows Server; Microsoft SQL Server; антивірусний захист; система резервного копіювання	Управління цифрового розвитку ОДА; функціональні власники — служба діловодства, відділ персоналу, департамент фінансів	Критичний	Неможливі реєстрація й погодження документів, кадровий облік, облік господарських операцій, платежі та формування звітності.
6.	Ліцензії та права використання програмного забезпечення	Ліцензія Windows Server 2022, ліцензія Microsoft SQL Server Standard, ліцензії користувачів	Відділ ІТ ОДА	Суттєвий	Неможливо отримувати оновлення та технічну підтримку; виникає ризик

Порядковий номер	Тип активу	Найменування активу	Власник (власне ім'я та прізвище/ назва організації/ підрозділ)	Рівень впливу (незначний/ обмежений/ суттєвий/ критичний)	Наслідки втрати активу
		СЕД, ліцензія на бухгалтерське ПЗ, ліцензія антивірусного захисту			використання неліцензійного ПЗ, уразливостей і припинення супроводу.
7.	Конфігурації, шаблони розгортання та засоби автоматизованого управління інфраструктурою (Infrastructure as Code, IaC)	Файл конфігурації IKS-Production-Configuration.xlsx; резервні конфігурації FW-01, SW-CORE-01; сценарій відновлення Restore-IKS.ps1; схеми віртуальної інфраструктури	Системний адміністратор ІКС	Суттєвий	Значно збільшується строк відновлення; можливе неправильне налаштування мережі, серверів, доступу користувачів і засобів захисту.
8.	Інтеграційні ресурси (внутрішні API, шини даних, сервіси інтеграції)	API обміну між СЕД і поштовим сервером; інтеграція бухгалтерського	Відділ ІТ ОДА; власники відповідних бізнес-процесів	Суттєвий	Припиняється автоматичний обмін даними; документи, платежі та звіти

Порядковий номер	Тип активу	Найменування активу	Власник (власне ім'я та прізвище/ назва організації/ підрозділ)	Рівень впливу (незначний/ обмежений/ суттєвий/ критичний)	Наслідки втрати активу
		модуля з електронним кабінетом Казначейства; шлюз електронної взаємодії			доводиться готувати вручну, зростає ризик помилок і прострочень.
9.	Зовнішні сервіси та сервіси постачальників (SaaS, PaaS, API)	Сервіс КЕП кваліфікованого надавача електронних довірчих послуг; електронні сервіси ДКСУ; хмарне резервне сховище; технічна підтримка постачальника СЕД	Відповідні постачальники; відповідальний за договори	Суттєвий	Неможливо підписувати електронні документи, проводити платежі, отримувати технічну допомогу або відновлювати дані з хмарної копії.
10.	Мережеві ресурси та засоби забезпечення підключення	Локальна мережа ОДА LAN-ODA,	Відділ ІТ ОДА; оператор електронних	Критичний	Користувачі та адміністратори не

Порядковий номер	Тип активу	Найменування активу	Власник (власне ім'я та прізвище/ назва організації/ підрозділ)	Рівень впливу (незначний/ обмежений/ суттєвий/ критичний)	Наслідки втрати активу
		канал доступу до Інтернету, VPN для віддалених працівників, DNS-сервер, комутатори та Wi-Fi	комунікацій «Постачальник-Інтернет»		мають доступу до ІКС, серверів, електронної пошти, систем Казначейства та інших зовнішніх сервісів.
11.	Облікові записи, ролі та права доступу	Облікові записи admin_iks, backup_admin, db_admin; групи доступу SED_Users, HR_Users, Finance_Users; ролі погодження та підписання документів	Відділ ІТ ОДА; керівники структурних підрозділів — власники ролей	Критичний	Уповноважені працівники не можуть увійти до ІКС; або виникає ризик несанкціонованого доступу до службової, кадрової та фінансової інформації.
12.	Сертифікати, криптографічні ключі та секрети	КЕП голови ОДА, керівника апарату, головного	Власники КЕП; технічні секрети — системний адміністратор ІКС	Критичний	Неможливо підписувати документи та платіжні

Порядковий номер	Тип активу	Найменування активу	Власник (власне ім'я та прізвище/ назва організації/ підрозділ)	Рівень впливу (незначний/ обмежений/ суттєвий/ критичний)	Наслідки втрати активу
		бухгалтера; сертифікат VPN; пароль адміністратора БД; токен інтеграції з електронним сервісом ДКСУ			доручення, встановлювати захищені з'єднання, виконувати інтеграцію із зовнішніми системами; компрометація ключів може призвести до неправомірних дій від імені ОДА.
13.	Журнали подій та аудиту	Журнали Windows Server, SQL Server, СЕД, міжмережевого екрана, VPN, антивірусного захисту та дій користувачів	Відділ ІТ ОДА; відповідальний за кіберзахист	Суттєвий	Неможливо встановити час, причину, джерело й масштаб інциденту, підтвердити дії користувачів та зібрати докази для службового розслідування.

Порядковий номер	Тип активу	Найменування активу	Власник (власне ім'я та прізвище/ назва організації/ підрозділ)	Рівень впливу (незначний/ обмежений/ суттєвий/ критичний)	Наслідки втрати активу
14.	Експлуатаційна та технічна документація	Паспорт ІКС, схема мережі, інструкція адміністратора, регламент резервного копіювання, план реагування на інциденти, план безперервності та відновлення (BCP/DRP), контакти постачальників	Керівник управління цифрового розвитку ОДА	Суттєвий	Відновлення виконується без узгодженого порядку; зростають час простою, ризик помилок, дублювання дій та перевищення встановленого RTO.
15.	Інші активи (зазначити)	Серверне приміщення № 214, система контролю доступу, кондиціонер, пожежна	Балансоутримувач приміщення ОДА; відділ ІТ ОДА	Критичний	Перегрів, пожежа, несанкціонований фізичний доступ або знеструмлення можуть призвести до пошкодження обладнання, втрати даних і

Порядковий номер	Тип активу	Найменування активу	Власник (власне ім'я та прізвище/ назва організації/ підрозділ)	Рівень впливу (незначний/ обмежений/ суттєвий/ критичний)	Наслідки втрати активу
		сигналізація, дизель-генератор			тривалої недоступності ІКС.

7. Взаємозв'язки засобу інформатизації (зазначаються внутрішні та зовнішні залежності, необхідні для забезпечення функціонування засобу інформатизації, зокрема від інших засобів інформатизації, інформаційних (автоматизованих) систем, інформаційно-комунікаційних систем, інформаційних ресурсів, технологічних компонентів, інфраструктури, каналів зв'язку, хмарних сервісів, постачальників послуг та інших ресурсів. Включаються лише залежності, порушення функціонування або відсутність яких призводить до припинення чи істотного обмеження функціонування засобу інформатизації або виконання робочих процесів (бізнес-процесів), що ним забезпечуються)

Порядковий номер	Найменування залежності/ пов'язаного ресурсу	Власник (держатель) залежності	Тип залежності (інформаційна/ технологічна/ комунікаційна/ інфраструктурна/ організаційна/інша) (зазначити)	Наявність договірних або інших зобов'язань щодо забезпечення доступності та відновлення (так/ні, визначені показники SLA/ цільовий час відновлення (RTO))	Рівень залежності (низький/ середній/ високий)	Наслідки порушення або недоступності
1.	Серверна інфраструктура ІКС: SRV-01, SRV-02, NAS-01, ДБЖ UPS-01	ОДА, управління цифрового розвитку	Технологічна, інфраструктурна	Так. Внутрішній регламент експлуатації та план відновлення ІКС; цільовий RTO ≤ 72 годин	Високий	Припиняється робота серверів застосунків, баз даних, СЕД, кадрового та бухгалтерського модулів.

Порядковий номер	Найменування залежності/ пов'язаного ресурсу	Власник (держатель) залежності	Тип залежності (інформаційна/ технологічна/ комунікаційна/ інфраструктурна/ організаційна/інша) (зазначити)	Наявність договірних або інших зобов'язань щодо забезпечення доступності та відновлення (так/ні, визначені показники SLA/ цільовий час відновлення (RTO))	Рівень залежності (низький/ середній/ високий)	Наслідки порушення або недоступності
2.	Віртуалізаційна платформа та віртуальні машини VM-IKS-APP01, VM-IKS-DB01, VM-IKS-FILE01	ОДА, управління цифрового розвитку	Технологічна	Так. Регламент резервного копіювання та відновлення; RTO ≤ 8 годин	Високий	Неможливо запустити прикладні системи, базу даних і файлове сховище; усі залежні бізнес-процеси істотно обмежуються.
3.	Система управління базами даних IKS_PROD	ОДА, управління цифрового розвитку; власники даних — служба діловодства, кадрова й бухгалтерська служби	Інформаційна, технологічна	Так. Регламент резервного копіювання БД; RPO ≤ 1 годин, RTO ≤ 8 годин	Високий	Втрачається доступ до реєстраційних карток, документів, кадрових і бухгалтерських даних; неможливі операції в СЕД та облікових модулях.
4.	Локальна комп'ютерна мережа ОДА, комутатори SW-CORE-01, SW-ACC-01, міжмережевий екран FW-01	ОДА, управління цифрового розвитку	Комунікаційна, технологічна	Так. Внутрішній регламент адміністрування мережі; показники відновлення — підлягають уточненню	Високий	Користувачі й адміністратори не мають доступу до ІКС, серверів, баз даних і внутрішніх інформаційних ресурсів.

Порядковий номер	Найменування залежності/ пов'язаного ресурсу	Власник (держатель) залежності	Тип залежності (інформаційна/ технологічна/ комунікаційна/ інфраструктурна/ організаційна/інша) (зазначити)	Наявність договірних або інших зобов'язань щодо забезпечення доступності та відновлення (так/ні, визначені показники SLA/ цільовий час відновлення (RTO))	Рівень залежності (низький/ середній/ високий)	Наслідки порушення або недоступності
5.	Канал доступу до Інтернету та резервний канал зв'язку	АТ «Умовний телеком-провайдер»; ОДА — замовник послуги	Комунікаційна, зовнішня	Так. Договір про надання електронних комунікаційних послуг; приклад SLA: доступність 99,5 %, час реакції до 4 годин, відновлення до 24 годин	Високий	Припиняється взаємодія із зовнішніми державними системами, Казначейством, КНЕДП, електронною поштою та віддалений доступ до ІКС.
6.	Захищений VPN-доступ для адміністраторів та працівників, які працюють віддалено	ОДА, управління цифрового розвитку	Комунікаційна, технологічна	Так. Регламент віддаленого доступу; RTO — підлягає уточненню	Середній	Ускладнюється віддалене адміністрування, реагування на інциденти поза приміщенням ОДА та робота уповноважених працівників.
7.	Електронний кабінет та інформаційні сервіси	Державна казначейська служба України	Інформаційна, зовнішня	Так. Нормативно визначена електронна взаємодія; фактичні показники SLA та RTO	Високий	Неможливо передати платіжні документи, зареєструвати

Порядковий номер	Найменування залежності/ пов'язаного ресурсу	Власник (держатель) залежності	Тип залежності (інформаційна/ технологічна/ комунікаційна/ інфраструктурна/ організаційна/інша) (зазначити)	Наявність договірних або інших зобов'язань щодо забезпечення доступності та відновлення (так/ні, визначені показники SLA/ цільовий час відновлення (RTO))	Рівень залежності (низький/ середній/ високий)	Наслідки порушення або недоступності
	Державної казначейської служби України			встановлює держатель сервісу		бюджетні зобов'язання, провести платежі та отримати інформацію про їх стан.
8.	Кваліфікований надавач електронних довірчих послуг і сервіси перевірки КЕП	КНЕДП, що обслуговує посадових осіб ОДА — підлягає уточненню	Інформаційна, технологічна, зовнішня	Так. Договір або інші документи про надання електронних довірчих послуг; SLA — підлягає уточненню	Високий	Неможливе юридично значуще підписання електронних документів, фінансової звітності та платіжних документів.
9.	Сервіс електронної пошти mail.oda.gov.ua	ОДА або зовнішній постачальник поштової послуги — підлягає уточненню	Комунікаційна, інформаційна	Так. Регламент користування службовою електронною поштою; SLA — підлягає уточненню	Середній	Ускладнюється обмін службовими повідомленнями, надсилання електронних документів, оповіщення про інциденти та координація відновлення.

Порядковий номер	Найменування залежності/ пов'язаного ресурсу	Власник (держатель) залежності	Тип залежності (інформаційна/ технологічна/ комунікаційна/ інфраструктурна/ організаційна/інша) (зазначити)	Наявність договірних або інших зобов'язань щодо забезпечення доступності та відновлення (так/ні, визначені показники SLA/ цільовий час відновлення (RTO))	Рівень залежності (низький/ середній/ високий)	Наслідки порушення або недоступності
10.	Система резервного копіювання та хмарне/віддалене сховище резервних копій	ОДА; за наявності хмарного розміщення — ТОВ «Умовний хмарний провайдер»	Технологічна, інфраструктурна, зовнішня	Так. Регламент резервного копіювання; договір на хмарні послуги — за наявності; RPO ≤ 24 годин	Високий	Неможливо відновити дані та конфігурації після аварії або кібератаки; зростає ризик безповоротної втрати даних.
11.	Система моніторингу, централізованого журналювання та кіберзахисту	ОДА, управління цифрового розвитку	Технологічна, інформаційна	Так. Регламент моніторингу та реагування на інциденти; цільовий час первинного реагування — підлягає уточненню	Високий	Несвоєчасно виявляються відмови, кібератаки та несанкціонований доступ; збільшуються масштаб інциденту і строк відновлення ІКС.
12.	Постачальник СЕД та технічна підтримка програмного продукту	ТОВ «Умовний постачальник СЕД» / фактичний постачальник — підлягає уточненню	Організаційна, технологічна, зовнішня	Так. Договір технічної підтримки; приклад SLA: реакція на критичний інцидент до 4 годин, обхідне рішення до 24 годин	Середній	Збільшується час усунення помилок СЕД, відновлення функціоналу, встановлення оновлень і виправлення критичних

Порядковий номер	Найменування залежності/ пов'язаного ресурсу	Власник (держатель) залежності	Тип залежності (інформаційна/ технологічна/ комунікаційна/ інфраструктурна/ організаційна/інша) (зазначити)	Наявність договірних або інших зобов'язань щодо забезпечення доступності та відновлення (так/ні, визначені показники SLA/ цільовий час відновлення (RTO))	Рівень залежності (низький/ середній/ високий)	Наслідки порушення або недоступності
						уразливостей.
13.	Приміщення серверної, електроживлення, кондиціонування, пожежна сигналізація та фізичний контроль доступу	ОДА / балансоутримувач будівлі	Інфраструктурна, організаційна	Так. Договори на електропостачання й технічне обслуговування; план аварійного реагування; RTO ≤ 2 години.	Високий	Перегрів, пожежа, знеструмлення або несанкціонований фізичний доступ можуть пошкодити обладнання та спричинити тривалу недоступність ІКС.
14.	Управління цифрового розвитку ОДА, системні адміністратори та відповідальні власники бізнес-процесів	ОДА	Організаційна	Так. Посадові інструкції, наказ про розподіл ролей, план безперервності діяльності та план реагування на інциденти	Високий	За відсутності відповідальних осіб або чіткого розподілу повноважень затримуються локалізація інциденту, ухвалення рішень, комунікація та відновлення ІКС.

8. Оцінка впливу порушення конфіденційності, цілісності та доступності інформації на функціонування засобу інформатизації (оцінювання проводиться з урахуванням видів інформації, що обробляються засобом інформатизації, її значення для

виконання визначених робочих процесів (бізнес-процесів), вимог законодавства щодо захисту інформації, а також можливих наслідків у разі несанкціонованого розкриття, зміни, знищення або недоступності інформації)

Властивість інформації	Потенційно можливий рівень впливу			Рівень впливу**** (низький/ середній/ високий)	Обґрунтування рівня впливу
	низький	середній	високий		
1. Конфіденційність	несанкціоноване розкриття чи ознайомлення з інформацією може призвести до часткового негативного впливу на робочі процеси (бізнес-процеси) замовника	несанкціоноване розкриття чи ознайомлення з інформацією може призвести до істотного негативного впливу на робочі процеси (бізнес-процеси) замовника	несанкціоноване розкриття чи ознайомлення з інформацією може спричинити тяжкий або катастрофічний вплив на робочі процеси (бізнес-процеси) замовника	високий	В ІКС обробляються персональні дані працівників ОДА: ПІБ, посади, відомості про трудову діяльність, відпустки, відрядження, кадрові накази та інші дані особових справ. Також ІКС містить службові документи, проекти управлінських рішень, листування, відомості про договори, платежі й фінансові операції. Несанкціоноване розкриття такої інформації може призвести до порушення прав суб'єктів персональних даних, розголошення службової інформації, використання даних для шахрайства або соціальної інженерії, скарг, службових

Властивість інформації	Потенційно можливий рівень впливу			Рівень впливу**** (низький/ середній/ високий)	Обґрунтування рівня впливу
	низький	середній	високий		
					перевірок і репутаційних втрат ОДА.
2. Цілісність	несанкціонована модифікація чи знищення інформації, що обробляється (оброблятиметься) у засобі інформатизації, може призвести до часткового негативного впливу на робочі процеси (бізнес-процеси) замовника	несанкціонована модифікація чи знищення інформації, що обробляється (оброблятиметься) у засобі інформатизації, може призвести до істотного негативного впливу на робочі процеси (бізнес-процеси) замовника	несанкціонована модифікація чи знищення інформації, що обробляється (оброблятиметься) у засобі інформатизації, може спричинити тяжкий або катастрофічний вплив на робочі процеси (бізнес-процеси) замовника	високий	Цілісність критична для реєстраційних даних СЕД, маршрутів погодження, кадрових наказів, штатного розпису, бухгалтерських проведень, платіжних документів і фінансової звітності. Несанкціонована або помилкова зміна даних може спричинити втрату контролю за виконанням доручень, неправомірні кадрові рішення, помилки в нарахуваннях чи платежах,

Властивість інформації	Потенційно можливий рівень впливу			Рівень впливу**** (низький/ середній/ високий)	Обґрунтування рівня впливу
	низький	середній	високий		
					недостовірну звітність, порушення бюджетної дисципліни та неможливість підтвердити юридично значущі дії користувачів.
3. Доступність	припинення доступу або використання інформації, що обробляється (оброблятиметься) у засобі інформатизації, може призвести до часткового негативного впливу на робочі процеси (бізнес-процеси) замовника	припинення доступу або використання інформації, що обробляється (оброблятиметься) у засобі інформатизації, може призвести до істотного негативного впливу на робочі процеси (бізнес-процеси) замовника	припинення доступу або використання інформації, що обробляється (оброблятиметься) у засобі інформатизації, може призвести до тяжкого або катастрофічного впливу на робочі процеси (бізнес-процеси) замовника	високий	Доступність ІКС необхідна для безперервного електронного документообігу, кадрового адміністрування, бухгалтерського обліку, казначейського обслуговування та формування звітності. Недоступність системи призводить до затримки реєстрації й погодження

Властивість інформації	Потенційно можливий рівень впливу			Рівень впливу***** (низький/ середній/ високий)	Обґрунтування рівня впливу
	низький	середній	високий		
					документів, порушення строків виконання доручень, неможливості оформлення кадрових рішень, проведення платежів і подання звітності. Для ІКС III категорії впливу цільовий час відновлення має бути не більше 72 годин, а цільова точка відновлення — не більше 24 годин.

9. Оцінка стану впровадження заходів із забезпечення безперервності функціонування (зазначаються відомості про стан впровадження організаційних та технічних заходів, спрямованих на забезпечення кібербезпеки, кіберстійкості та безперервності функціонування засобу інформатизації. У графі “Додаткова інформація” зазначаються відомості щодо реквізитів документів, дати останнього перегляду або тестування, досягнутих показників, періодичності виконання заходів та інша інформація, необхідна для підтвердження стану їх впровадження)

Найменування показника*****	Стан впровадження	Дата останньої перевірки/ тестування	Додаткова інформація
-----------------------------	-------------------	--------------------------------------	----------------------

Управління безперервністю

Найменування показника*****	Стан впровадження	Дата останньої перевірки/тестування	Додаткова інформація
1. План забезпечення безперервності діяльності (BCP)	так	01.08.2026	Затверджено наказом № 45 від 15.06.2026, переглядається щороку або після суттєвих змін архітектури
2. План відновлення після аварій (DRP)	так	01.08.2026	Затверджено наказом № 46 від 15.06.2026. Останнє комплексне тестування — 31.07.2026, RTO досягнуто за 5 год 35 хв
3. Проведення тестування відновлення функціонування	проводиться	31.07.2026	Проведено тестування сценаріїв: «Відновлення з резервних копій», «Компрометація середовища». Усі сценарії виконано успішно.
Резервування та відновлення			
4. Резервне копіювання даних	повне	31.07.2026	Виконується за схемою 3-2-1-1-0. Повне резервне копіювання — щодня, інкрементальне — щогодини
5. Перевірка відновлення з резервних копій	проводиться	31.07.2026	Відновлення виконано у середовищі clean room. Цілісність даних підтверджено контрольними сумами
6. Захищене резервне копіювання з неможливістю модифікації резервних копій (Immutable Backup)	так	31.07.2026	Використовується WORM-сховище. Період незмінності резервних копій — 30 діб
7. Реплікація даних або компонентів засобу інформатизації	так	31.07.2026	Синхронна реплікація між основним і резервним ЦОД, асинхронна — до географічно відокремленого майданчика
Управління доступом			
8. Багатофакторна автентифікація (MFA)	так	31.07.2026	MFA обов'язкова для адміністраторів і користувачів з привілейованим доступом

Найменування показника*****	Стан впровадження	Дата останньої перевірки/тестування	Додаткова інформація
9. Управління привілейованим доступом (PAM)	так	31.07.2026	Впроваджено централізоване управління привілейованими обліковими записами із записом адміністративних сесій
10. Управління правами доступу користувачів та адміністраторів засобу інформатизації (RBAC/ABAC)	впроваджено	31.07.2026	Ролі переглядаються щокварталу, принцип найменших привілеїв застосовується для всіх користувачів
Архітектура безпеки			
11. Архітектура нульової довіри (Zero Trust)	впроваджено	31.07.2026	Застосовується багаторівнева автентифікація, перевірка пристроїв та сегментація мережі
Моніторинг та реагування			
12. Централізований збір та аналіз подій безпеки (SIEM або аналогічні засоби)	повний	31.07.2026	Події надходять у режимі 24/7, середній час виявлення інциденту (MTTD) — до 15 хвилин
13. Управління журналами подій та аудиту	повне	31.07.2026	Журнали централізовано зберігаються 365 днів, контроль цілісності здійснюється автоматично
Реагування на інциденти			
14. План реагування на кіберінциденти (IRP)	так	01.08.2026	Затверджено наказом № 47 від 15.06.2026, інтегровано з BCP та DRP
15. Навчання та командно-штабні тренування (Tabletop Exercises)	проводяться	31.07.2026	Проводяться двічі на рік за участю ІТ, інформаційної безпеки та керівництва
Захист кінцевих точок			
16. Засоби виявлення та реагування на загрози (EDR/XDR)	впроваджено	31.07.2026	Розгорнуто на 100 % серверів та робочих станцій адміністраторів
Управління вразливостями			

Найменування показника*****	Стан впровадження	Дата останньої перевірки/тестування	Додаткова інформація
17. Виявлення вразливостей та управління оновленнями безпеки	здійснюється	31.07.2026	Автоматизоване сканування — щотижня, критичні вразливості усуваються не пізніше ніж за 72 години
Управління залежностями			
18. Управління ризиками ланцюга постачання	впроваджено	31.07.2026	Оцінка постачальників проводиться щорічно та перед укладенням нових договорів
Захист криптографічних ресурсів			
19. Управління сертифікатами, ключами та секретами	повне	31.07.2026	Використовується централізоване сховище секретів та автоматична ротація сертифікатів

III. Вимоги до забезпечення безперервності та відновлення (заповнюється для кожного засобу інформатизації окремо)

(найменування засобу інформатизації)

10. Вимоги до відновлення функціонування засобу інформатизації (значення показників відновлення функціонування засобу інформатизації визначаються з урахуванням результатів аналізу впливу порушення виконання робочих процесів (бізнес-процесів), залежностей, визначених активів та встановлених вимог до забезпечення безперервності діяльності)

Найменування показника	Методика визначення показника	Значення
1. Робочі процеси (бізнес-процеси), виконання яких залежить від засобу інформатизації	зазначаються процеси, визначені у пункті 3 цього звіту	Організація електронного документообігу та контролю виконання документів; кадрове адміністрування та ведення кадрового обліку; бухгалтерський облік, казначейське обслуговування та фінансова звітність; адміністрування, відновлення та забезпечення функціонування ІКС; реагування на інциденти та забезпечення безперервності діяльності

Найменування показника	Методика визначення показника	Значення
2. Максимально допустимий період порушення функціонування (MTPD)	визначається як найменше значення показника максимально допустимого періоду порушення функціонування (MTPD) серед усіх робочих процесів (бізнес-процесів), виконання яких залежить від засобу інформатизації	24 години. Після 24 годин без реагування на інцидент значно зростає ризик поширення його наслідків, втрати даних і неможливості відновити ІКС у прийнятні строки.
3. Цільовий час відновлення (RTO)	визначається з урахуванням максимально допустимого періоду порушення функціонування (MTPD) та необхідності відновлення виконання залежних робочих процесів. Цільовий час відновлення (RTO) не повинен перевищувати найменший максимально допустимий період порушення функціонування (MTPD) усіх робочих процесів (бізнес-процесів), виконання яких залежить від засобу інформатизації	16 годин
4. Цільова точка відновлення (RPO)	визначається з урахуванням критичності інформаційних активів, що обробляються засобом інформатизації, та допустимого впливу втрати або пошкодження даних	Не більше 4 годин для баз даних СЕД, кадрового та бухгалтерського модулів; для конфігурацій серверів, мережевого обладнання і віртуальних машин — не більше 24 годин.

Найменування показника	Методика визначення показника	Значення
5. Мінімальний рівень функціональності засобу інформатизації під час відновлення	визначається перелік функцій або сервісів, доступність яких має бути забезпечена на період відновлення	1) доступ адміністраторів до серверів, мережі, резервних копій та журналів подій; 2) автентифікація уповноважених користувачів; 3) реєстрація й перегляд термінових документів у СЕД; 4) доступ до актуальних даних про кадровий склад; 5) перегляд бухгалтерських даних і формування першочергових платіжних документів; 6) робота КЕП для уповноважених посадових осіб; 7) захищений канал взаємодії з ДКСУ та іншими критичними зовнішніми сервісами.
6. Пріоритетність відновлення компонентів засобу інформатизації	визначається порядок відновлення активів та компонентів відповідно до їх впливу на виконання робочих процесів	1. Електроживлення, ДБЖ, серверне приміщення, мережеве обладнання та канал зв'язку. 2. Засоби кіберзахисту, міжмережевий екран, керування обліковими записами і привілейованим доступом. 3. Платформа віртуалізації, сервери, СУБД та сховище даних. 4. Система резервного копіювання і перевірка можливості відновлення. 5. СЕД і функції реєстрації термінових документів. 6. Бухгалтерський модуль, КЕП та інтеграція з ДКСУ. 7. Кадровий модуль. 8. Звіти, аналітика, допоміжні сервіси та повний функціонал ІКС.
7. Допустимий рівень деградації функціонування засобу	визначається можливість функціонування у частково обмеженому режимі на період	Допускається тимчасова робота в обмеженому режимі: реєстрація термінових документів у резервному журналі; використання резервних робочих місць;

Найменування показника	Методика визначення показника	Значення
інформатизації	відновлення	ведення переліку критичних кадрових і фінансових операцій у контрольованих офлайн-формах; виконання лише першочергових платежів; обмін службовими повідомленнями через резервний канал зв'язку. Не допускаються: використання неперевірених резервних копій, надання необґрунтованих привілеїв доступу, передавання службової або персональної інформації незахищеними каналами та проведення фінансових операцій без визначеного порядку погодження.
8. Додаткові вимоги до відновлення	зазначаються інші вимоги, зумовлені особливостями функціонування засобу інформатизації	Відновлення виконується лише уповноваженими працівниками за затвердженим планом BCP/DRP та планом реагування на інциденти. Перед введенням ІКС у штатний режим необхідно: перевірити цілісність баз даних; перевірити журнали подій і відсутність ознак компрометації; змінити скомпрометовані паролі, ключі й сертифікати; перевірити КЕП, інтеграції та резервні копії; зафіксувати результати відновлення; інформувати керівництво та власників процесів. Тестування відновлення резервних копій проводиться щокварталу, комплексне тестування BCP/DRP — не рідше одного разу на рік.

11. Вимоги до резервування (відомості зазначаються щодо активів засобу інформатизації, визначених у пункті 6 цього звіту, порушення функціонування або втрата яких може призвести до неможливості виконання робочих процесів (бізнес-процесів) або недотримання встановлених у пункті 10 цього звіту показників безперервності діяльності (максимально допустимого періоду порушення функціонування (MTPD), цільового часу відновлення (RTO), цільової точки відновлення (RPO))

Тип активу	Найменування активу/компонента	Спосіб забезпечення резервування або відновлення	Реалізований спосіб резервування/відновлення	Стан реалізації	Періодичність резервування / відновлення	Дата останнього тестування відновлення	Результат тестування
1. Дані та інформаційні ресурси	База даних IKS_PROD: СЕД, кадровий та бухгалтерський модулі	повна реплікація даних/щоденне резервне копіювання за схемою 3-2-1/використання незмінних (immutable) резервних копій	Щоденна інкрементальна копія; щотижнева повна копія на NAS-01; зашифрована офлайн-копія	Частково впроваджено	Інкрементальне — кожні 4 години; повне — щонеділі	15.08.2026 — умовний приклад	Успішно: БД відновлено за 3 год 20 хв; втрата даних — не більше 4 годин
2. Резервні копії та копії відновлення	Сховище резервних копій NAS-01, офлайн-носій, резервна копія поза серверною	створення резервних копій/ізолюване зберігання/захист від модифікації або видалення/інший спосіб	Основна копія на NAS-01; друга копія на зашифрованому зовнішньому носії в іншому приміщенні	Частково впроваджено	Перевірка цілісності — щотижня; тест відновлення — щокварталу	15.08.2026 — умовний приклад	Успішно: усі резервні копії відкриваються; рекомендовано впровадити immutable-сховище
3. Апаратне забезпечення	Сервери SRV-01, SRV-02; сховище NAS-01; ДБЖ UPS-01; комутатор SW-CORE-01	повний набір резервного обладнання для функціонування (гаряче резервування)/повна альтернативна база, але меншої потужності, відновлення з резервних копій (тепле резервування)/деяке	Резервний сервер SRV-DR-01; запасний комутатор; ДБЖ; договір на ремонт обладнання	Частково впроваджено	Перевірка обладнання — щомісяця; тест запуску резервного сервера — щокварталу	20.08.2026 — умовний приклад	Успішно: резервний сервер запущено; виявлено потребу заміни акумуляторів ДБЖ

Тип активу	Найменування активу/компонента	Спосіб забезпечення резервування або відновлення	Реалізований спосіб резервування/відновлення	Стан реалізації	Періодичність резервування / відновлення	Дата останнього тестування відновлення	Результат тестування
		обладнання для використання в надзвичайних ситуаціях, встановлення програмного забезпечення і додатків, відновлення даних з резервної копії (холодне резервування)					
4. Віртуальні ресурси та обчислювальні ресурси (віртуальні машини, контейнери, кластерні ресурси)	VM-IKS-APP01, VM-IKS-DB01, VM-IKS-FILE01, VM-IKS-BACKUP01	резервування ресурсів/реплікація/відновлення з образів/інший спосіб	Щоденні образи VM; реплікація VM-IKS-APP01 на SRV-DR-01; відновлення VM-IKS-DB01 із резервної копії	Частково впроваджено	Образи VM — щоденно; реплікація критичної VM — кожні 12 годин	15.08.2026 — умовний приклад	Успішно: VM-IKS-APP01 відновлено за 1 год 45 хв
5. Програмне забезпечення та програмні компоненти	СЕД, кадровий модуль, бухгалтерський модуль, СУБД, операційні системи, ПЗ резервного копіювання	резервування програмних компонентів/збереження дистрибутивів/автоматизоване розгортання/інший спосіб	Дистрибутиви та оновлення зберігаються у захищеному каталозі \\NAS-01\Software; інструкції розгортання — у	Частково впроваджено	Актуалізація після кожної зміни; перевірка щокварталу	12.08.2026 — умовний приклад	Успішно: бухгалтерський модуль розгорнуто на резервній VM; час — 2 год 10 хв

Тип активу	Найменування активу/компонента	Спосіб забезпечення резервування або відновлення	Реалізований спосіб резервування/відновлення	Стан реалізації	Періодичність резервування / відновлення	Дата останнього тестування відновлення	Результат тестування
			технічний документації				
6. Ліцензії та права використання програмного забезпечення	Ліцензії на Windows Server, СУБД, СЕД, бухгалтерське ПЗ, антивірусний захист	облік ліцензій/збереження інформації про права використання/інший спосіб	Електронний реєстр ліцензій Licenses_ODA.xlsx; скан-копії договорів у захищеному сховищі	Впроваджено	Актуалізація після закупівлі або продовження; інвентаризація — щороку	01.08.2026 — умовний приклад	Успішно: ліцензії критичного ПЗ чинні; потребує уточнення строк дії ліцензії антивірусного ПЗ
7. Конфігурації, шаблони розгортання та IaC	Конфігурації FW-01, SW-CORE-01, серверів, СУБД; сценарій Restore-IKS.ps1	резервування конфігурацій/контроль версій/збереження шаблонів розгортання/інший спосіб	Експорт конфігурацій мережевого обладнання після кожної зміни; сценарії та інструкції в захищеному репозиторії	Частково впроваджено	Після кожної зміни; контрольна перевірка — щомісяця	20.08.2026 — умовний приклад	Частково успішно: конфігурацію FW-01 відновлено; потрібно запровадити централізований контроль версій
Інтеграційні ресурси (внутрішні API, шини даних, сервіси інтеграції)	Інтеграція бухгалтерського модуля з сервісами ДКСУ; поштовий шлюз СЕД;	резервування сервісів інтеграції/дублювання каналів взаємодії/інший спосіб	Резервний канал Інтернету; збережені налаштування API; резервний порядок обліку термінових	Частково впроваджено	Перевірка доступності — щодня; тест інтеграцій — щокварталу	18.08.2026 — умовний приклад	Успішно: доступ до сервісу ДКСУ через резервний канал підтверджено

Тип активу	Найменування активу/компонента	Спосіб забезпечення резервування або відновлення	Реалізований спосіб резервування/відновлення	Стан реалізації	Періодичність резервування / відновлення	Дата останнього тестування відновлення	Результат тестування
	API КЕП		операцій				
9. Зовнішні сервіси та сервіси постачальників (SaaS, PaaS, API)	КНЕДП, сервіси ДКСУ, хмарне сховище, технічна підтримка постачальника СЕД	договірні умови забезпечення доступності/альтернативний сервіс/інший спосіб	Договори з постачальниками; перелік контактів для аварійної ескалації; резервний КЕП уповноваженої особи	Частково впроваджено	Перевірка контактів і строків договорів — щокварталу	01.08.2026 — умовний приклад	Частково успішно: контакти актуальні; SLA постачальника СЕД потребує уточнення
10. Мережеві ресурси та засоби забезпечення підключення	Канал Інтернету, FW-01, SW-CORE-01, VPN, DNS, локальна мережа	резервні канали зв'язку/дублювання мережевих компонентів/інший спосіб	Основний оптичний канал і резервний 4G/5G-канал; резервна конфігурація FW-01	Частково впроваджено	Моніторинг — постійно; тест резервного каналу — щомісяця	25.08.2026 — умовний приклад	Успішно: перемикання на резервний канал — 18 хв
11. Облікові записи, ролі та права доступу	admin_iks, db_admin, backup_admin; ролі SED_Clerks, HR_Users, Finance_Users	резервування облікових записів/процедури відновлення доступу/збереження налаштувань доступу/інший спосіб	Два окремі адміністратори; аварійний обліковий запис у запечатаному порядку доступу; експорт ролей	Впроваджено	Перегляд прав — щокварталу; перевірка аварійного доступу — раз на пів року	10.08.2026 — умовний приклад	Успішно: аварійний доступ перевірено; не виявлено надлишкових прав
12. Сертифікати, криптографічні ключі та секрети	КЕП голови ОДА, керівника апарату, головного	захищене зберігання/резервування/процедури відновлення/інший	КЕП зберігаються на захищених носіях; визначені резервні підписанти;	Частково впроваджено	Контроль строку дії — щомісяця; перевірка резервного	05.08.2026 — умовний приклад	Успішно: резервний КЕП головного бухгалтера чинний; VPN-

Тип активу	Найменування активу/компонента	Спосіб забезпечення резервування або відновлення	Реалізований спосіб резервування/відновлення	Стан реалізації	Періодичність резервування / відновлення	Дата останнього тестування відновлення	Результат тестування
	бухгалтера; VPN-сертифікат; секрети API	спосіб	реєстр строків чинності сертифікатів		КЕП — щокварталу		сертифікат потребує перевипуску до 30.09.2026
13. Журнали подій та аудиту	Журнали СЕД, СУБД, Windows Server, FW-01, VPN, антивірусного захисту	резервне копіювання/архівування/централізоване зберігання/інший спосіб	Щоденне архівування журналів на NAS-01; зберігання критичних журналів не менше 180 діб	Частково впроваджено	Архівування — щоденно; перевірка доступності — щомісяця	14.08.2026 — умовний приклад	Частково успішно: журнали доступні; рекомендовано впровадити централізовану SIEM
14. Експлуатаційна та технічна документація	Паспорт ІКС, схема мережі, BCP/DRP, план реагування на інциденти, інструкції адміністратора, контакти постачальників	резервування документації/контроль версій/забезпечення доступності	Електронна копія у захищеному сховищі; паперова копія BCP/DRP у керівника ІТ-підрозділу	Впроваджено	Після кожної зміни; перегляд — щороку	01.08.2026 — умовний приклад	Успішно: документація доступна; рекомендовано актуалізувати схему мережі після модернізації
15. Інші активи (зазначити)	Серверна кімната № 214, кондиціонер, пожежна сигналізація, контроль доступу, дизель-		ДБЖ із запасом автономності 30 хв; кондиціонер; пожежна сигналізація; доступ за картками	Частково впроваджено	Перевірка ДБЖ і температури — щомісяця; комплексне тестування — щороку	20.08.2026 — умовний приклад	Частково успішно: ДБЖ працює; потрібно забезпечити резервне джерело живлення

Тип активу	Найменування активу/компонента	Спосіб забезпечення резервування або відновлення	Реалізований спосіб резервування/відновлення	Стан реалізації	Періодичність резервування / відновлення	Дата останнього тестування відновлення	Результат тестування
	генератор						понад 30 хв

IV. Підсумкові результати аналізу (заповнюється для кожного засобу інформатизації окремо)

ІКС ОДА

(найменування засобу інформатизації)

Найменування показника	Значення показника
1. Категорія впливу порушення функціонування засобу інформатизації (I/II/III)*****	I
2. Обґрунтування визначення категорії	ІКС ОДА віднесено до I категорії, оскільки порушення її функціонування може призвести до припинення або суттєвого порушення виконання критичних робочих процесів ОДА: електронного документообігу та контролю виконання документів, бухгалтерського обліку, казначейського обслуговування, фінансової звітності, кадрового адміністрування, реагування на інциденти та відновлення ІКС. Недоступність ІКС може спричинити невиконання або прострочення доручень, затримку проведення платежів і подання звітності, порушення кадрових процедур, недоступність службової, кадрової та фінансової інформації, а також ускладнення реагування на кіберінциденти. Такі наслідки визначаються ОДА як неприйнятні.

3. Загальний рівень впливу ідентифікованих робочих процесів (бізнес-процесів) (незначний/ обмежений/суттєвий/ критичний) *****	критичний
4. Встановлений максимально допустимий період порушення функціонування (MTPD) *****	8
5. Встановлений цільовий час відновлення (RTO)	4
6. Встановлена цільова точка відновлення (RPO)	1
7. Загальна оцінка стану забезпечення безперервності функціонування засобу інформатизації (відповідає/ частково відповідає/не відповідає)	частково відповідає
8. Необхідність впровадження додаткових заходів (так/ні)	так

Начальник відділу інформаційної безпеки
(найменування посади особи, відповідальної за кіберзахист)

(підпис)

Леся БЕЗПЕЧНА
(власне ім'я та прізвище)

Начальник відділу адміністрування інформаційно-комунікаційної інфраструктури
(найменування посади особи, відповідальної за проведення аналізу)

(підпис)

Степан МЕРЕЖКО
(власне ім'я та прізвище)

Дата проведення обстеження 01 вересня 2026 р.

* Звіт може бути скоригований залежно від особливостей засобу інформатизації.

** У разі коли власником робочого процесу (бізнес-процесу) є інший орган, установа, підприємство, організація або інший зовнішній суб'єкт, визначається відповідальний за взаємодію щодо забезпечення виконання такого процесу з боку замовника.

*** Мінімально прийнятий рівень виконання робочого процесу (бізнес-процесу) — визначений замовником мінімальний обсяг виконання операцій (робіт) у межах робочого процесу (бізнес-процесу), який має забезпечуватися під час порушення його безперервності для недопущення значних негативних наслідків для діяльності замовника.

**** Рівень впливу визначається за найвищим рівнем впливу порушення безперервності робочого процесу (бізнес-процесу).

**** Рівень впливу визначається за найвищим рівнем впливу порушення конфіденційності, цілісності та доступності інформації на функціонування засобу інформатизації.

***** Перелік показників, за якими проводиться оцінка стану впровадження заходів із забезпечення безперервності функціонування може бути доповнений залежно від особливостей обстежуваного засобу інформатизації.

***** Категорія засобу інформатизації визначається відповідно до пункту 31 Обов'язкових вимог на підставі результатів аналізу, наведених у розділах I та II цього звіту.

***** Загальний рівень впливу визначається за найвищим рівнем впливу серед усіх робочих процесів (бізнес-процесів).

***** Значення максимально допустимого періоду порушення функціонування (MTPD) для засобу інформатизації визначається як найменше значення максимально допустимого періоду порушення функціонування (MTPD) серед усіх робочих процесів (бізнес-процесів), виконання яких залежить від такого засобу інформатизації