ЗАТВЕРДЖЕНО

Наказ Державної служби статистики

24 липня 2024 року № 195

Політика управління ризиками кібербезпеки в інформаційній системі органів державної статистики

І. Загальні положення

1. Політика управління ризиками кібербезпеки в інформаційній системі органів державної статистики (далі – Політика) визначає загальні підходи до організації процесів управління ризиками кібербезпеки (далі – КБ) й описує методи оцінки ризиків КБ, а також методи їх обробки, які застосовуються для оперативного виявлення кіберзагроз, кібератак, кіберінцидентів, визначення їх наслідків, мінімізації їх впливу та встановлення часу відновлення функціонування інформаційної системи органів державної статистики (далі – ІС ОДС), забезпечення планового рівня функціонування та підвищення надійності ІС ОДС.

Управління ризиками здійснюється з метою інтеграції ризик-орієнтованого підходу щодо заходів забезпечення кібербезпеки та кіберзахисту в діяльність і основні завдання й функції Держстату, уключаючи забезпечення впровадження системного підходу до оцінки та обробки ризиків КБ.

2. Політика поширюється на працівників самостійних структурних підрозділів апарату Держстату, його територіальних органів, установ та організацій, що належать до сфери його управління, до повноважень яких належить функціонування ІС ОДС та її складових і стосується обробки всієї інформації, яка в ній циркулює, крім випадків, передбачених законодавством.

ІІ. Терміни та визначення

У цій Політиці терміни та визначення вживаються в таких значеннях, наведених у законах України "Про основні засади забезпечення кібербезпеки України", "Про електронні комунікації", "Про захист інформації в інформаційно-комунікаційних системах", Загальних вимогах до кіберзахисту об’єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518 (Офіційний вісник України, 2019 рік, № 50, ст. 1697), ДСТУ ISO/IEC 29147:2016 "Інформаційні технології. Методи захисту. Розкриття вразливостей", ДСТУ ISO/IEC 27000:2019 "Інформаційні

технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник".

ІІІ. Управління ризиками кібербезпеки

1. Управління ризиками КБ здійснюється шляхом:

виявлення загроз, ідентифікації та аналізу ризику КБ для встановлення найбільш імовірних сценаріїв розвитку ситуації в разі виникнення кібернебезпеки в ІС ОДС, оцінки її можливих наслідків шляхом виявлення, збору й узагальнення наявної або доступної інформації щодо всіх можливих джерел і чинників ризику КБ;

впровадження системи управління ризиками КБ;

утворення в апараті Держстату робочої групи з управління ризиками (далі – РГУР КБ), склад якої затверджується наказом Держстату.

2. Основними завданнями під час управління ризиками є:

забезпечення виконання заходів із метою ефективного функціонування системи управління ризиками КБ;

забезпечення своєчасного виявлення ризиків КБ, моніторингу та контролю за функціонуванням системи управління ризиками КБ, інформування керівництва Держстату, яке згідно з розподілом функціональних повноважень уповноважене вирішувати відповідні питання, щодо суттєвих ризиків КБ;

підготовка керівництву Держстату відповідно до розподілу функціональних повноважень пропозицій щодо вжиття заходів для попередження, пом’якшення та/або уникнення ризиків КБ;

підготовка звітів щодо ризиків КБ;

розробка та підтримка в актуальному стані методики, інструментів та моделей, що використовуються для аналізу впливу різних факторів ризиків КБ;

здійснення вимірювання ризиків КБ;

складання профілю ризиків КБ;

підготовка висновків щодо ідентифікованих і задокументованих ризиків КБ;

участь у розробленні внутрішніх документів з питань управління ризиками КБ.

3. Ризики КБ уключають, зокрема:

ризики, до яких належать ризики доступу до складових ІС ОДС (фізичний доступ до об’єктів інформаційної інфраструктури Держстату);

ризики КБ та інформаційної безпеки – ризики для інформаційних, комунікаційних та інформаційно-комунікаційних систем, їх частин, які забезпечують стале функціонування ІС ОДС;

ризики, пов’язані з людським фактором – ризики КБ, які створюють працівники органів державної статистики як користувачі ІС ОДС;

ризики договірних відносин (ланцюжок постачання) – ризик зриву виконання договору, злочинного або ненавмисного використання ланцюжків постачання, що призводить до порушення стійкості ІС ОДС.

IV. Оцінка ризиків кібербезпеки

1. Оцінку ризиків КБ проводиться РГУР КБ поетапно та передбачає визначення вірогідності, джерел ризиків, характеристик інцидентів КБ, імовірності та вагомості їх наслідків і сценаріїв розвитку, а також методів управління ризиками КБ та їх ефективності.

Під час оцінки ризиків КБ проводяться: ідентифікація ризиків КБ, аналіз ризиків КБ, оцінка відповідності ризиків КБ варіантам рішень щодо їх обробки.

2. З метою організації проведення оцінки ризиків РГУР КБ складає план оцінки ризиків КБ за формою, наведеною в Таблиці 1.

Таблиця 1

№ з/п	Етап оцінки ризиків КБ	Відповідальний самостійний структурний підрозділ	Опис заходів
1	2	3	4
1.	Збір і актуалізація інформації про ІС ОДС	РГУР КБ, департамент інформаційних технологій	Для здійснення оцінки ризиків КБ РГУР КБ отримує оновлену інформацію про наявне апаратне та програмне забезпечення відповідно до результатів щорічної інвентаризації (реєстр ІТ-активів).
2.	Виявлення та оцінка вразливостей в ІС ОДС, пріоритизація усунення вразливостей	РГУР КБ, департамент інформаційних технологій, департамент координації процесу збирання даних	РГУР КБ у взаємодії із департаментом інформаційних технологій, департаментом координації збирання даних (іншими самостійними підрозділами апарату Держстату за необхідності) оцінюють вразливі місця, які існують в апаратному та програмному забезпеченні, та за формою, наведеною в додатку 2 до процесу управління вразливостями, складають реєстр вразливостей, а також визначають пріоритет усунення цих вразливостей.
3.	Виявлення загроз	РГУР КБ	РГУР КБ визначає загрози, які можуть використовувати вразливі місця для завдання шкоди ІС ОДС. Форму реєстру можливих загроз КБ наведено в додатку 1 цієї Політики. Цей реєстр уключає в себе зовнішні та внутрішні загрози від навмисних або випадкових (ненавмисних) джерел/подій.

1	2	3	4
4.	Визначення рівня загроз	РГУР КБ	Для виявлених загроз РГУР КБ визначає рівень загроз за процедурою, описаною у пункті 5 розділу VI цієї Політики. При визначенні рівня загроз ураховуються навмисні загрози, випадкові загрози, минулі інциденти КБ, нові події та тенденції.
5.	Розрахунок впливу загроз	РГУР КБ	На основі розрахованих рівнів загроз РГУР КБ розраховує вплив кожної загрози на апаратне й програмне забезпечення та кожну її складову за описаною в пункті 6 розділу VI цієї Політики процедурою.
6.	Розрахунок імовірності ризику КБ	РГУР КБ	Використовуючи рівні загроз і вразливостей, РГУР КБ розраховує ймовірність ризику КБ для кожної пари загроза-вразливість, як визначено в пункті 7 розділу VI цієї Політики.
7.	Обчислення ризику КБ	РГУР КБ	РГУР КБ розраховує рівень ризиків КБ для ІТ-активів, зважаючи на вірогідність ризику КБ і вартість його впливу. Процедура обчислення здійснюється згідно з пунктом 8 розділу VI цієї Політики.
8.	Підготовка та подання звіту з оцінки ризиків КБ до керівництва Держстату відповідно до розподілу функціональних повноважень	РГУР КБ	РГУР КБ готує звіт з оцінки ризиків КБ та подає його до керівництва Держстату відповідно до розподілу функціональних повноважень для ознайомлення та затвердження.

V. Виявлення й оцінка вразливостей

1. Виявлення й оцінка вразливостей проводиться як систематичний процес визначення слабкостей в ІС ОДС та/або її складових, що можуть бути використані для несанкціонованого доступу, руйнування чи модифікації статистичних даних. Цей процес уключає в себе виявлення, класифікацію, аналіз і складання реєстру вразливостей з метою подальшої їх нейтралізації.

2. Виявлення та пріоритизація вразливостей здійснюється відповідно до плану управління вразливостями, визначеного в пункті 1 розділу III процесу управління вразливостями.

3. РГУР КБ уживає заходів із виявлення та оцінки вразливостей, складає реєстр вразливостей та визначає їх рейтинг в оцінці ризиків КБ. Оцінка ризиків КБ складається за формою, визначеною в додатку 3 цієї Політики.

VI. Виявлення загроз

1. Виявлення потенційних загроз здійснюється РГУР КБ на постійній основі для забезпечення напрацювання переліку заходів блокування (нейтралізацію) усіх загроз КБ або зниження ризику їх реалізації. У разі, коли перелік напрацьованих заходів не дає можливості забезпечити блокування (нейтралізацію) виникаючих для ІС ОДС загроз КБ, мають бути визначені додаткові заходи, які ці загрози блокують.

2. РГУР КБ організовує та проводить заходи щодо виявлення потенційних загроз КБ, які передбачають створення, перегляд та/або оновлення Реєстру можливих загроз.

3. Результатом проведення заходів із виявлення потенційних загроз КБ є ідентифікований та визначений для ІС ОДС перелік загроз КБ у Реєстрі можливих загроз.

4. РГУР КБ забезпечує інформаційний обмін щодо реалізованих і потенційних загроз КБ з іншими суб'єктами забезпечення КБ.

5. Для кожної ідентифікованої загрози РГУР КБ визначає її рівень, як зазначено в Таблиці 2.

Таблиця 2

Аспект	Рівень загрози КБ			
	Низький (D)	Середній (C)	Високий (B)	Критичний (A)
1	2	3	4	5
Мотивація	Немає помітної мотивації	Є певна грошова, зловмисна або геополітична мотивація	Існує високий ступінь грошової, зловмисної або геополітичної мотивації	Існує критичний ступінь грошової, зловмисної або геополітичної мотивації
Можливість	Для використання цієї вразливості потрібні висококваліфіко-вані технічні знання та/або надзвичайно велика кількість ресурсів	Необхідні навички та ресурси доступні і їх можна придбати, доклавши певних зусиль	Легко зробити; потрібно мало навичок та/або мало ресурсів	Дуже легко зробити, не вимагає навичок; можливе випадкове використання

1	2	3	4	5
Доступність	Ціль дуже важко досягти, потрібно зламати кілька рівнів технології, ціль невідома та/або дуже мало людей можуть скористатися цією вразливістю	Дещо складно досягти цілі, потрібно зламати 1–2 рівні технології, ціль не визначена чітко та/або багато людей можуть скористатися цією вразливістю	Невеликі труднощі з досягненням цілі, рівні технології 0–1 повинні бути порушені, ціль можна знайти за допомогою певних зусиль і/або значна кількість людей здатна використати вразливість	Ніяких труднощів у досягненні мети. Ціль чітко визначена, або добре відома, або її легко знайти, і/або кожен має доступ для потенційного використання вразливості
Ресурс	Потрібна дуже дорога або вузькоспеціалізо-вана технологія	Потрібні певні інвестиції в технології	Потрібні безкоштовні та загальнодоступні ресурси	Спеціальний ресурс не потрібен
Час	Уразливість була доступна понад 12 місяців	Уразливість доступна 1 місяць	Уразливість була доступна менше 5 днів	Щойно виявлено вразливість
Історична інформація (періодич-ність)	Інциденти КБ можуть статися раз на два роки	Інциденти КБ можуть траплятися раз на рік	Інциденти КБ можуть виникати раз на 3 місяці	Інциденти КБ можуть траплятися раз на місяць або частіше

Рівень загрози залежить від рейтингу вразливості й простоти її реалізації та оцінюється відповідно до Таблиці 3.

Таблиця 3

Рейтинг вразливості					
	Критичний (A)	C	B	A	A
	Високий (B)	C	C	B	B
	Середній (C)	D	C	C	C
	Низький (D)	D	D	D	D
		Низький (D)	Середній (C)	Високий (B)	Критичний (A)
	Рівень простоти реалізації загрози КБ				

Результатом цього етапу є визначений рівень загроз, зазначений в оцінці ризиків КБ за формою, визначеною в додатку 3 до цієї Політики.

6. Розрахунок впливу загрози.

Визначення впливу загрози дає змогу більш реалістично відобразити різницю між цінністю ІТ-активів і загальною вартістю ризику КБ.

Вплив загрози на ІТ-актив визначається відповідно до Таблиці 4.

Таблиця 4

Цінність ІТ-активу	Критичний	2	3	4	4
	Високий	1	2	3	4
	Середній	1	2	2	3
	Низький	1	1	1	2
		Низький	Середній	Високий	Критичний
	Рівень загрози				

Кількісний розрахунок рівня впливу загрози:

Рівень впливу загрози =
= Цінність ІТ-активу для здійснення технологічного процесу х
х Потенційні збитки чи втрати від компрометації ІТ-активу
або інформації на ньому

Розраховані рівні впливів загроз зазначаються в оцінці ризиків КБ за формою, визначеною в додатку 3 до цієї Політики.

7. Розрахунок імовірності загрози:

Імовірність загрози =
= Кількість інцидентів КБ для кожної пари вразливість-загроза /
/ період між поточним моментом і попередньою оцінкою ризику КБ у днях

Примітка: якщо імовірність загрози > 1, правильна імовірність загрози = 1.

Для отримання більш точних результатів оцінки ризику КБ використовується середнє значення ймовірності загрози (середнє арифметичне кількості інцидентів КБ за рік).

Середня імовірність загрози =
= середній арифметичній кількості інцидентів КБ за рік.

Примітка: якщо середня імовірність загрози > 1, правильна середня імовірність загрози = 1.

Для зручності пріоритизації ризиків КБ і демонстрації результатів використовується шкала перетворення вартості, наведена в Таблиці 5.

Таблиця 5

Кількісне значення ймовірності загрози	Якісне значення ймовірності загрози
< 0,1	Низький
0,1–0,3	Середній
0,3–0,5	Високий
>= 0,5	Критичний

Після розрахунку значення ймовірності загрози оцінюється потенційний збиток чи втрата від компрометації ІТ-активу або інформації на ньому (залежно від загрози) для кожного активу, на який впливає загроза.

Потенційний збиток чи втрата від компрометації ІТ-активу або інформації на ньому – це частка цінності ІТ-активу для діяльності органів державної статистики, яка, ймовірно, буде знищена через певний ризик КБ, пов'язаний із загрозою.

Визначені ймовірності загроз зазначаються в оцінці ризиків КБ за формою, визначеною в додатку 3 до цієї Політики.

Визначені потенційні збитки чи втрати від компрометації активу або інформації на ньому в залежності від загроз зазначаються в оцінці ризиків КБ за формою, визначеною в додатку 3 до цієї Політики.

8. Обчислення рівня ризику КБ розраховується відповідно до матриці, наведеної в Таблиці 6.

Таблиця 6

Рівень впливу загрози	Критичний	2	3	4	4
	Високий	1	2	3	4
	Середній	1	2	2	3
	Низький	1	1	1	2
		Низький	Середній	Високий	Критичний
	Імовірність загрози				

Існує чотири рівні ризиків КБ, як показано в чотирьох зонах у матриці розрахунку ризиків КБ:

зона 4 (Критичний ризик КБ): неприйнятний ризик КБ із серйозним негативним впливом. Заходи безпеки (навіть тимчасові) швидко розгортаються, щоб зменшити критичні ризики КБ;

зона 3 (Високий ризик КБ): неприйнятний ризик КБ із негативним впливом. Високі ризики КБ покриваються заходами безпеки, щоб знизити їх до прийнятного рівня;

зона 2 (Середній ризик КБ): прийнятний ризик КБ, який незначно впливає на результати діяльності. Розглядається можливість розгортання заходів безпеки, що дозволяють знизити середні ризики КБ;

зона 1 (Низький ризик КБ): Це незначний ризик КБ, який не впливає на результати діяльності, або його вплив дуже низький. Обробка низького ризику КБ не проводиться але переглядається при кожній наступній оцінці ризику КБ.

Отриманим результатом виступає значення рівнів ризику КБ та визначений пріоритет його обробки. Значення рівнів ризику, пріоритет та варіант обробки ризику, контролі (заходи) безпеки, визначені заходи обробки ризику КБ тощо вносяться до плану обробки ризиків КБ, складеному за формою, визначеною у додатку 4 до цієї Політики.

Після здійсненої оцінки ризиків КБ, що повною мірою наведена в оцінці ризиків КБ за формою, визначеною в додатку 3 до цієї Політики, РГУР КБ готує звіт про оцінку ризиків КБ та подає його керівництву Держстату, яке згідно з розподілом функціональних повноважень уповноважене вирішувати відповідні питання для визначення та затвердження пріоритету обробки ризиків КБ.

Пріоритет обробки може бути змінений за рішенням керівництва Держстату, яке згідно з розподілом функціональних повноважень уповноважене вирішувати відповідні питання (наприклад, для критичних або нових ІТ-активів, які раніше не впливали на виникнення загроз). Зміни в пріоритеті обробки ризиків КБ також відображаються у Формі прийняття ризиків КБ, визначеною у додатку 5 до цієї Політики, з відповідним обґрунтуванням.

VII. Обробка ризиків КБ

1. РГУР КБ готує рекомендації щодо методів обробки ризиків КБ і організовує поетапне вжиття заходів щодо обробки кожного ризику КБ відповідно до прийнятого рішення шляхом складання плану обробки ризиків КБ за формою, наведеною в додатку 4 до цієї Політики.

2. Складений план обробки ризиків КБ надається на затвердження керівництву Держстату відповідно до розподілу функціональних повноважень.

Після проведення оцінки ризиків КБ РГУР КБ готує та надає на затвердження керівництву Держстату, яке згідно з розподілом функціональних повноважень уповноважене вирішувати відповідні питання, рекомендації щодо методів обробки ризиків КБ і вживає заходів щодо обробки кожного ризику КБ відповідно до прийнятого рішення, зафіксувавши дані в плані обробки ризиків КБ.

Кожен із методів обробки ризику КБ (зменшення, уникнення, прийняття та передача) описується нижче в розділі VIII цієї Політики як інструкція щодо визначення відповідного підходу до обробки виявлених ризиків КБ.

3. План обробки ризиків КБ описує дії та визначає відповідальних за кожний етап процесу обробки ризиків КБ.

Таблиця 7

№ з/п	Етап	Відповідальний	Опис заходів етапу
1	2	3	4
1.	Надання рекомендацій з обробки ризиків КБ для кожного ризику КБ	РГУР КБ	РГУР КБ надає рекомендації з обробки ризиків КБ (зменшення, уникнення, прийняття та передача) для кожного ризику КБ. Деталі підходів до обробки ризиків КБ наведені нижче в цій Політиці.
2.	Надання рекомендацій щодо контролів безпеки для ризиків КБ, які необхідно зменшити		РГУР КБ надає рекомендації щодо контролів безпеки для кожного з ризиків КБ (перелік можливих контролів безпеки наведено в додатку 2 до цієї Політики).
3.	Розробка плану обробки ризиків КБ		РГУР КБ розробляє план обробки ризиків КБ (форма складання плану наведена в додатку 4 до цієї Політики) із зазначенням кінцевих термінів, ресурсів та результатів, що мають бути досягнуті.
4.	Надання розробленого плану обробки ризиків КБ керівництву Держстату відповідно до розподілу функціональних повноважень для затвердження	РГУР КБ, керівництво Держстату відповідно до розподілу функціональних повноважень	РГУР КБ надає план обробки ризиків КБ керівництву Держстату відповідно до розподілу функціональних повноважень на перегляд та затвердження. У разі необхідності РГУР КБ уносить зміни до плану обробки ризиків КБ і повторне надає його на затвердження.
5.	Доведення плану обробки ризиків КБ до керівників самостійних структурних підрозділів	Керівники самостійних структурних підрозділів, РГУР КБ	Затверджений план обробки ризиків КБ передається керівникам самостійних структурних підрозділів для здійснення діяльності з обробки ризиків КБ.
6.	Упровадження дій з усунення ризиків КБ		Керівники самостійних структурних підрозділів разом із РГУР КБ організовують упровадження необхідних засобів контролю безпеки згідно із планом обробки ризиків КБ. Засоби контролю безпеки систематично переглядаються РГУР КБ, щоб забезпечити їх правильне та відповідне функціонування протягом життєвого циклу. Деталі етапу перегляду наведені нижче в цій Політиці.

VIII. Методи обробки ризиків КБ

1. Метод зменшення ризику КБ шляхом переоцінки ризику КБ.

Контролі (заходи) безпеки класифікуються за трьома основними класами:

попереджувальні (превентивні) заходи призначені для запобігання виникненню помилок або аномалій;

детективні (виявлювані) − спрямовані на виявлення випадків, коли превентивні контролі безпеки не були ефективними в запобіганні помилкам і порушенням, особливо щодо захисту активів;

коригувальні − призначені для виправлення помилок і невідповідностей та забезпечення того, щоб подібні помилки не повторювалися після їх виявлення.

Переоцінку ризику КБ за цим методом обробки ризиків КБ РГУР КБ здійснює щорічно.

Результатом переоцінки ризику КБ є проведена обробка ризику КБ, його переоцінка та відповідна фіксація етапу в плані обробки ризиків КБ, а також затверджений керівництвом Держстату, згідно з розподілом функціональних повноважень уповноважене вирішувати відповідні питання, план обробки ризиків КБ.

2. Метод уникнення ризику КБ.

Уникнення ризику КБ досягається шляхом:

відмови від ведення певної діяльності (наприклад, не використовувати мережу Інтернет для певного виду діяльності);

переміщення ІТ-активів із зони ризику КБ (наприклад, переміщення ІТ-активів із недостатньо фізично захищених зон);

рішення не обробляти чутливу інформацію (наприклад, із третіми особами, якщо не можна гарантувати достатній захист).

Переоцінку ризику КБ за цим методом обробки ризиків КБ РГУР КБ здійснює щорічно.

Результатом етапу є проведена обробка ризику КБ, його переоцінка та відповідна фіксація етапу в плані обробки ризиків КБ, а також затверджений керівництвом Держстату, яке згідно з розподілом функціональних повноважень уповноважене вирішувати відповідні питання, план обробки ризиків КБ.

3. Метод прийняття ризику КБ.

Етапи процесу прийняття ризику КБ описані в Таблиці 8.

Таблиця 8

№ з/п	Етап	Відповідальний	Опис
1	2	3	4
1.	Ініціація процесу прийняття ризику КБ	РГУР КБ, керівництво Держстату відповідно до	Прийняття ризику КБ може бути ініційоване за допомогою процесу обробки ризиків КБ (який визначено в цій Політиці).

1	2	3	4
		розподілу функціональних повноважень	Ризики КБ низького рівня приймаються автоматично. Середні ризики КБ можуть бути прийняті лише після схвалення керівництвом Держстату відповідно до розподілу функціональних повноважень. Високі та критичні ризики КБ неприйнятні. Процес прийняття ризику КБ ініціюється рішенням керівництва Держстату, яке відповідно до розподілу функціональних повноважень уповноважене вирішувати відповідні питання, прийняти ризик КБ.
2.	Підготовка пропозицій щодо прийняття ризику КБ		РГУР КБ готує пропозиції керівництву Держстату відповідно до розподілу функціональних повноважень за формою прийняття ризику КБ, наведеною в додатку 5 до цієї Політики. Заповнена форма має містити таке: короткий опис ризику КБ, який необхідно прийняти, включаючи контекст, історію та причину прийняття; період, після якого необхідно переглядати прийнятий ризик КБ (принаймні раз на рік).
3.	Надання форми прийняття ризику КБ для затвердження керівництву Держстату, яке відповідно до розподілу функціональних повноважень уповноважене вирішувати відповідні питання		РГУР КБ подає форму прийняття ризику КБ на затвердження до керівництва Держстату, яке відповідно до розподілу функціональних повноважень уповноважене вирішувати відповідні питання.
4.	Затвердження форми прийняття ризику КБ керівництвом Держстату, яке відповідно до розподілу функціональних		Керівництво Держстату, яке відповідно до розподілу функціональних повноважень уповноважене вирішувати відповідні питання затверджує форму прийняття ризику КБ або відхиляє її. РГУР КБ відповідно до прийнятого рішення переходить до наступного етапу або визначає інший метод

1	2	3	4
	повноважень уповноважене вирішувати відповідні питання		обробки ризику КБ.
5.	Зберігання форми прийняття ризику КБ		РГУР КБ зберігає форму прийняття ризику КБ як доказ рішення керівництва Держстату, яке відповідно до розподілу функціональних повноважень уповноважене вирішувати відповідні питання, прийняти ризик КБ.
6.	Переоцінка прийнятих ризиків КБ		РГУР КБ має запланувати повторну оцінку прийнятих ризиків КБ після узгодженого періоду часу (принаймні раз на рік), за винятком випадків, коли це вже було зроблено в межах процесу періодичної переоцінки ризиків КБ.

4. Метод передачі ризику КБ.

Передача ризику КБ третім сторонам є варіантом, коли Держстат не може самостійно вжити заходів щодо зниження ризику КБ до прийнятного рівня або економічно ефективніше передати його третій стороні. У цьому випадку така передача здійснюється за умовами укладеного із третьою стороною договору в установленому порядку. При цьому всі вимоги безпеки та засоби контролю включені в умови договору, щоб забезпечити достатню безпеку.

Переоцінку ризику КБ за цим методом обробки ризиків КБ РГУР КБ здійснює щорічно.

Результатом етапу є проведена обробка ризику КБ, його повторна оцінка та відповідна фіксація етапу в плані обробки ризиків КБ, а також погоджені вищезазначені дії з керівництвом Держстату відповідно до розподілу функціональних повноважень.

IX. Моніторинг засобів контролю безпеки та переоцінка ризиків КБ

1. РГУР КБ регулярно переглядає на предмет змін звіти про оцінку ризиків КБ і відповідні плани обробки ризиків КБ. Будь-яке впровадження нової складової ІС ОДС, критичні зміни в інформаційно-комунікаційній інфраструктурі та/або організаційній структурі Держстату можуть створити нові ризики КБ або вимагати змін у роботі з оцінки ризиків КБ, яка проводилася раніше. У цьому випадку відповідні ризики КБ переоцінюються, а плани обробки ризиків КБ оновлюються відповідним чином.

2. РГУР КБ відстежує та раз на рік переглядає впроваджені засоби контролю безпеки з метою забезпечення перевірки їх належного та ефективного функціонування, а також перевірки того, що зміни в середовищі ІС ОДС не довели їх неефективності.

3. РГУР КБ організовує забезпечення постійного моніторингу за:

новими ІТ-активами, які були включені до сфери управління ризиками КБ;

модифікації ІТ-активів, наприклад, через зміну вимог до діяльності;

новими загрозами, які можуть діяти як зовні, так і всередині Держстату та які не були оцінені;

можливістю того, що нові або збільшені вразливості можуть дозволити загрозам використовувати ці нові або змінені вразливості;

виявленням вразливих місць для визначення тих, які піддаються впливу нових або видозмінених загроз;

збільшенням впливу або наслідків оцінених загроз, вразливостей і ризиків КБ, що призводить до неприйнятного рівня ризику КБ;

інцидентами КБ.

4. Засоби, що використовуються під час контролю безпеки потребують технічного обслуговування та адміністративної підтримки для забезпечення їх правильного та належного функціонування протягом їх життєвого циклу. Технічне обслуговування засобів контролю безпеки здійснюють працівники самостійних структурних підрозділів, до повноважень якого належить функціонування ІТ-активу.

5. Заходи безпеки реалізовуються та вдосконалюються з урахуванням відсутніх засобів контролю безпеки, виявлених під час технічного обслуговування. Ці заходи включають (не обмежуючись):

перегляд лог-файлів, звітів сповіщень, звітів про інциденти КБ, оцінки вразливостей КБ;

перегляд контролів безпеки та їх дотримання;

оновлення елементів керування КБ, політик і процедур до нових версій.

Таблиця 9 описує дії та визначає відповідальність для кожного етапу процесу переоцінки ризиків КБ.

Таблиця 9

№ з/п	Етап	Відповідальний	Опис
1	2	3	4
1.	Ініціація процесу переоцінки ризиків КБ	РГУР КБ, ССП апарату Держстату, до повноважень яких належить функціонування ІТ-активу	РГУР КБ розпочинає процес перегляду ризиків КБ. Кожен ССП апарату Держстату, до повноважень яких належить функціонування ІТ-активу, надає РГУР КБ необхідну інформацію для аналізу ризиків КБ.
2.	Проведення планової переоцінки ризиків КБ	РГУР КБ	РГУР КБ виконує планову переоцінку ризиків КБ. Планова переоцінка ризиків КБ здійснюється раз на рік. Під час переоцінки ідентифікуються нові ризики КБ та зміни ризиків КБ,

1	2	3	4
			оцінюється робота попередньо визначених контролів безпеки (додаток 2).
3.	Оновлення плану обробки ризиків КБ	РГУР КБ	На основі результатів переоцінки ризиків КБ РГУР КБ оновлює звіти про переоцінку ризиків КБ і відповідні плани обробки ризиків КБ (додаток 4), щоб відобразити зміни в ризиках КБ та/або контролях безпеки. Деталі процесу обробки ризиків КБ наведені в розділі VIII цієї Політики.
4.	Сповіщення керівництва Держстату відповідно до розподілу функціональних повноважень про результати переоцінки ризиків КБ	РГУР КБ, керівництво Держстату відповідно до розподілу функціональних повноважень	РГУР КБ передає оновлені Звіти про переоцінку ризиків КБ і Плани обробки ризиків КБ (додаток 4) керівництву Держстату, яке відповідно до розподілу функціональних повноважень уповноважене вирішувати відповідні питання, для затвердження. Звіт про переоцінку ризиків КБ включає таке: опис ризику КБ і та необробленого рівня ризику КБ; опис ключових дій та/або засобів контролю, які діють для пом'якшення/управління ризиком КБ; опис залишкового рівня ризику КБ після застосування контролю безпеки; деталі для підтримки постійного вдосконалення процесу управління ризиками КБ.

X. Підтримка, оновлення та розповсюдження

1. Політика є легкодоступною для працівників органів державної статистики та може бути корисною для інших осіб, які матимуть доступ до ІС ОДС (за необхідності), для подальшого використання та розміщена на офіційному вебсайті Держстату.

2. РГУР КБ забезпечує організацію оновлення Політики та подає її до керівництва Держстату, яке згідно з розподілом функціональних повноважень уповноважене вирішувати відповідні питання, на затвердження. Політика переглядається щорічно для забезпечення її актуальності та відповідності потребам і цілям захисту ІС ОДС або частіше, якщо це необхідно (під час внесення суттєвих змін).

Заступник директора департаменту
інформаційних технологій Олександра ДОРОХОВА

Додаток 1
до Політики
(пункт 2 розділу IV)

Форма реєстру можливих загроз КБ

№ з/п	Область дії	Загроза КБ	Зв’язок з уразливостями
1	2	3	4
1.	КБ	Несанкціонований логічний доступ до інфраструктури (пристрої)	
2.		Модифікація мережевого трафіку, підслуховування (включаючи бездротові канали, MITM)	
3.		Фішинг, спам	
4.		DDoS атака	
5.		Введення шкідливого коду (віруси, програма-вимагач тощо)	
6.		Зловживання владою (працівники організації) – інсайдерська атака	
7.		Підвищення привілеїв	
8.		Несанкціонована модифікація, встановлення програмного забезпечення	
9.		Несанкціонований доступ до конфіденційної інформації (витік інформації, розкриття, втрата)	
10.		Атаки, пов’язані з ланцюгом поставок (використання критичного обладнання, програмного забезпечення, мікропрограмного забезпечення)	
11.		Знищення загальнодоступної інформації, поширення фейкової інформації	
12.	Фізична безпека	Недоступність засобів зв'язку, послуг, інформації внаслідок стихійного або техногенного лиха, війни, масових заворушень, зловмисних дій	
13.		Силове захоплення офісу (вторгнення офіційних/неофіційних органів)	
14.		Втрата кондиціонування	
15.		Втрата пожежної безпеки	
16.		Втрата живлення	
17.		Втрата водопостачання, повінь	

1	2	3	4
18.		Несанкціонований доступ до приміщень організації (фальсифікація/крадіжка карт доступу, недостатній контроль)	
19.		Несанкціонований фізичний доступ до інфраструктури	
20.		Установлення інструментів для незаконного збору інформації (жучки, мережеві сніфери, мікрофони, інше фізичне обладнання)	
21.		Пошкодження, втрата, недоступність комп'ютерного обладнання через природні або техногенні катастрофи, війну, масові розлади, шкідливі дії	
22.		Припинення роботи системи контролю доступу	
23.		Припинення експлуатації служб безпеки	
24.		Припинення функціонування постачальника інтернет-послуг	
25.	Управління	Відсутність взаємозамінності менеджменту	
26.		Низька надмірність ресурсів, низькі можливості масштабування	
27.		Непередбачуване закінчення терміну дії ліцензії	
28.	Юридична	Порушення договірних зобов'язань, NDA постачальниками, клієнтами, підрядниками	
29.		Порушення договірних зобов'язань, NDA працівниками	
30.		Невідповідність законодавству, внутрішнім політикам	

_____

Додаток 2
до Політики
(пункт 3 розділу VII,
пункт 5 розділу IX)

Перелік можливих контролів безпеки

№ з/п	Група заходів	Контроль безпеки
1	2	3
1.	Доступ	Визначення та реалізація матриці доступу
2.		Огляд прав доступу
3.		Персоналізація облікових записів користувачів
4.		Упровадження рішення для керування привілейованим доступом
5.		Упровадження рішення багатофакторної автентифікації
6.		Застосування парольної політики
7.	Захист від шкідливого коду	Упровадження процесу захисту від інцидентів зловмисного програмного забезпечення
8.		Установлення та обслуговування антивірусного програмного забезпечення
9.		Застосування обмежень на використання програмного забезпечення для серверів і робочих станцій/ноутбуків
10.		Упровадження централізованого керування кінцевими точками для контролю антивірусного ПЗ
11.	Захист інформації/активів	Упровадження рішення запобігання витоку інформації
12.		Установлення рішення повного шифрування жорсткого диску (включаючи знімний) на сервери/робочі станції
13.		Реалізація регулярного очищення застарілої інформації
14		Розробка та впровадження процесу шифрування інформації
15.		Упровадження рішення/процесу перегляду безпеки коду
16.		Упровадження маркування інформації відповідно до внутрішньої політики
17.		Упровадження інструментів для керування кінцевими точками
18.		Застосування шифрування інформації у стані спокою, де це можливо

1	2	3
19.		Перегляд налаштувань за замовчуванням у системах/службах
20.		Упровадження процесу управління IT-активами
21.		Упровадження процесу управління ліцензіями
22.	Управління вразливостями	Проведення регулярних внутрішніх/зовнішніх аудитів, тестування на проникнення, тестування безпеки додатків тощо.
23.		Білий список програмного забезпечення
24.		Упровадження регулярного процесу сканування вразливостей
25.	Логування і моніторинг	Упровадження протоколювання подій у системах і службах. Регулярне відстеження журналів подій
26.	Інфраструктура	Конфігурація серверів із захищеними параметрами
27.		Упровадження процесу тестування патчів безпеки
28.		Виведення активу з експлуатації
29.	Мережа	Конфігурація мережевих пристроїв із захищеними параметрами
30.		Проведення щорічного тесту на проникнення
31.		Упровадження рішень для захисту від спаму/фішингу
32.		Упровадження або посилення ізоляції активів від інших (список контролю доступу тощо)
33.	Резервне копіювання	Застосування резервних копій та/або їх періодичне тестування
34.		Упровадження плану заходів безперервності функціонування ІС ОДС
35.		Розробка та впровадження відповідної політики/процедури резервного копіювання
36.		Оновлення відповідної політики резервного копіювання
37.		Розробка та впровадження стандартного шаблону NDA/додаткової угоди для постачальників
38.	Безперервність діяльності	Упровадження захисту від DDoS
39.		Упровадження резервних каналів зв'язку
40.	Фізична безпека	Установлення та обслуговування датчиків затоплення водою
41.	Управління	Перевірка даних під час працевлаштування
42.		Регулярний перегляд договорів із підрядниками
43.		Перегляд NDA та відмова від NDA

Додаток 3
до Політики
(пункт 3 розділу V,
пункти 5–8 розділу VI)

Форма оцінки ризиків КБ

№ з/п	Загроза	ІТ-актив	Вартість активів для діяльності (якісна)	Вартість активів для бізнесу (кількісна)	Уразливість	Рейтинг вразливості	Ризик	Простота реалізації загрози	Рівень загрози	Відсоток пошкодження активу в залежності від загрози	Вплив загрози (кількісний)	Вплив загрози (якісний)	Імовірність загрози (кількісна)	Імовірність загрози (якісна)	Рівень ризику (якісний)	Рівень ризику (кількісний)	Пріоритет обробки
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	Несанкціонований доступ до конфіденційної інформації	СЕД, пошта, БД			Порушення правил управління доступом для працівників і третіх сторін (перегляд, припинення, надання, керування рівнем доступу, обов’язки не розподілені належним чином).		Витік, розголошення, втрата чутливих даних										

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	Несанкціо-нований доступ до конфіден-ційної інформації	Людські ресурси			Порушення парольної політики (паролі за замовчуванням не змінені, вимоги щодо довжини, складності, періоду використання, правил зберігання не дотримані, неадекватне керування паролями (паролі незашифровані та легко доступні іншим), використання одного пароля для різних облікових записів).		Витік, розголо-шення, втрата чутливих даних										
3	Несанкціо-нований логічний доступ до інфраструк-тури (пристроїв)	ПК			Сканування технічних вразливостей не проводиться регулярно. Патчі не встановлюються регулярно.		Витік, розголо-шення, втрата чутливих даних										
4	Збій активів/ систем	ПК, БД			Неоцінені/ неперевірені зміни, виправлення, оновлення.		Поруше-ння/збій процесів										
5	Несанкціо-нований фізичний	Мере-жеві пристрої			Порушення фізичної безпеки.		Витік, розголо-шення,										

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
	доступ до пристроїв						втрата чутливих даних										
6	Фішинг, вішинг (інші методи соціальної інженерії)	Пошта			Порушення правил використання Інтернету/електронної пошти. Налаштування безпеки за умовчанням у сервісах.		Витік, розголошення, втрата конфіденційних даних; втрата репутації										
7	Зловживання повноваженнями (працівниками організації) – інсайдерська атака	Active Directory			Відсутність контролю за діями адміністратора (не збираються та не переглядаються логи, не розподіляються обов’язки контролера).		Витік, розголошення, втрата конфіденційних даних; втрата репутації										
8	Зловживання повноваженнями (працівниками організації) – інсайдерська атака	Мережеві пристрої, серверна інфраструктура			Відсутність систематичного контролю за діями користувача (реєстрація, перегляд, не розподілені обов'язки контролера).		Витік, розголошення, втрата конфіденційних даних; втрата репутації										

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
9	Підвищення привілеїв	Active Directory			Відсутність процесу управління патчами для інфраструктури. Відсутність тестів безпеки додатків (перевірка коду, тест на проникнення, тестування безпеки додатків).		Витік, розголошення, втрата чутливих даних										
10	Введення шкідливого коду (вірусів, програм-вимагачів тощо)	ПК, віртуальна серверна інфраструктура			Порушення політики захисту від шкідливих програм.		Порушення/збій процесів; витік, розкриття, втрата чутливих даних; втрата репутації										
11	Несанкціонована модифікація, встановлення програмного забезпечення	ПК			Нестача персоналу для забезпечення контрольної функції.		Порушення/збій процесів; витік, розкриття, втрата чутливих даних										
12	Атаки на ланцюг поставок (використання	Інфраструктура постачальників послуг			Відсутність або недостатність умов кібербезпеки в договорах із третіми сторонами		Витік, розголошення, втрата конфі-										

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
	критичного обладнання, програмного забезпечення, мікропрограм)	/партнерів			(включаючи NDA, SLA).		денційних даних; втрата репутації										
13	Бекдори	Код вебсайту			Відсутність статичного та динамічного аналізу коду, нерегулярні перевірки коду.		Витік, розголошення, втрата конфіденційних даних; втрата репутації										
14	Примусове захоплення офісу (вторгнення офіційних/ неофіційних органів влади)	Офісні приміщення			Недостатній рівень послуг, засобів фізичної охорони.		Розкриття, втрата чутливих даних, втрата фізичних активів										
15	Непередбачуване закінчення терміну дії ліцензії	ПЗ			Відсутність управління ліцензіями. Відсутність процесу управління IT активами.		Витік, розголошення, втрата чутливих даних										

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
16	DDoS атака	Вебсайт			Відсутність захисту від DDoS.		Порушення/збій процесів										

Додаток 4
до Політики
(пункт 8 розділу VI,
пункти 1, 3 розділу VII)

Форма плану обробки ризиків КБ

№ з/п	Ризик	ІТ-актив	Уразливість	Загроза	Рівень ризику (якісний)	Рівень ризику (кількісний)	Варіант обробки ризику (уникнути, передати, зменшити, прийняти)	Контролі безпеки	Заходи обробки	Вартість впровадження	Відповідальний	Термін впровадження	Статус впровадження	Коментарі
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Витік, розголошення, втрата чутливих даних	СЕД, пошта, БД	Порушення політики управління доступом для співробітників і третіх сторін (перегляд, припинення, надання, керування рівнем доступу, обов’язки не розподілені належним чином).	Несанкціонований доступ до конфіденційної інформації										
2	Витік, розголошення, втрата чутливих даних	Людські ресурси	Порушення парольної політики (паролі за замовчуванням не змінені, вимоги щодо довжини, складності, періоду використання, правил зберігання не дотримані, неадекватне керування паролями (паролі	Несанкціонований доступ до конфіденційної інформації										

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
			незашифровані та легко доступні іншим), використання одного пароля для різних облікових записів).											
3	Витік, розголошення, втрата чутливих даних	ПК	Сканування технічних вразливостей не проводиться регулярно. Патчі не встановлюються регулярно.	Несанкціонований логічний доступ до інфраструктури (пристроїв)										
4	Порушення/збій процесів	ПК, БД	Неоцінені/неперевірені зміни, виправлення, оновлення.	Збій активів/систем										
5	Витік, розголошення, втрата чутливих даних	Мережеві пристрої, серверна інфраструктура	Порушення фізичної безпеки.	Несанкціонований фізичний доступ до пристроїв										
6	Витік, розголошення, втрата конфіденційних даних; втрата репутації	Пошта	Порушення правил використання Інтернету/електронної пошти. Налаштування безпеки за умовчанням у сервісах.	Фішинг, китові атаки, вішинг (інші методи соціальної інженерії)										
7	Витік, розголошення, втрата конфі-	Active Directory	Відсутність контролю за діями адміністратора (не збираються та не переглядаються логи, не	Зловживання повноваженнями (працівниками організації) -										

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	денційних даних; втрата репутації		розподіляються обов’язки контролера).	інсайдерська атака										
8	Витік, розголошення, втрата конфіденційних даних; втрата репутації	Мережеві пристрої, серверна інфраструктура	Відсутність систематичного контролю за діями користувача (реєстрація, перегляд, не розподілені обов'язки контролера).	Зловживання повноваженнями (працівниками організації) – інсайдерська атака										
9	Витік, розголошення, втрата чутливих даних	Active Directory	Відсутність процесу управління патчами для інфраструктури. Відсутність тестів безпеки додатків (перевірка коду, тест на проникнення, тестування безпеки додатків).	Підвищення привілеїв										
10	Порушення/збій процесів; витік, розкриття, втрата чутливих даних; втрата репутації	ПК, віртуальна серверна інфраструктура	Порушення політики захисту від шкідливих програм.	Введення шкідливого коду (вірусів, програм-вимагачів тощо)										

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
11	Порушення/збій процесів; витік, розкриття, втрата чутливих даних	ПК	Нестача персоналу для забезпечення контрольної функції.	Несанкціонована модифікація, встановлення програмного забезпечення										
12	Витік, розголошення, втрата конфіденційних даних; втрата репутації	Інфраструктура постачальників послуг/-партнерів	Відсутність або недостатність умов кібербезпеки в договорах із третіми сторонами (включаючи NDA, SLA).	Атаки на ланцюг поставок (використання критичного обладнання, програмного забезпечення, мікропрограм)										
13	Витік, розголошення, втрата конфіденційних даних; втрата репутації	Код вебсайту	Відсутність статичного та динамічного аналізу коду, нерегулярні перевірки коду.	Бекдори										
14	Розкриття, втрата чутливих даних, втрата	Офісні приміщення	Недостатній рівень послуг, засобів фізичної охорони.	Примусове захоплення офісу (вторгнення офіційних/нео										

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	фізичних активів			фіційних органів влади)										
15	Витік, розголо-шення, втрата чутливих даних	ПЗ	Відсутність управління ліцензіями. Відсутність процесу управління ІТ активами.	Непередбачу-ване закінче-ння терміну дії ліцензії										
16	Поруше-ння/збій процесів	Вебсайт	Відсутність захисту від DDoS.	DDoS атака										

Додаток 5
до Політики
(пункт 8 розділу VI,
пункт 3 розділу VIII)

Форма прийняття ризиків КБ

Інформація про працівника, який здійснює технічне обслуговування засобів контролю безпеки:

ПІБ:	
Посада:	
Адреса ел. пошти:	
Номер телефону:	

Резюме запиту (ризик КБ, що буде прийнято): _____

Огляд постраждалих сервісів/систем: _____

Переваги прийняття цього ризику КБ: _____

Опис інформації, яка буде пов’язана з ризиком КБ: _____

Рекомендації щодо зменшення ризику КБ: _____

Запропоновані альтернативи для усунення або зменшення ризику КБ: _____

Компенсаційні засоби контролю (для зменшення ризику КБ, пов’язаного з винятком): _____

Загальний ризик КБ для організації в результаті прийняття цього ризику КБ, уключаючи імовірність і вплив ризику КБ, якщо він відбудеться: _____

Прийняття ризику

Я розумію, що дотримання політик та стандартів кібербезпеки Держстату є обов’язковим для всіх працівників апарату Держстату. Я вважаю, що дотримання необхідних заходів контролю не може бути досягнуто із причин, задокументованих вище.

_____ _____
(підпис) (дата)

_____