

ЗАТВЕРДЖЕНО  
ЄААД.468244.185-ЛУ

Підп. та дата	
Інв. № дубл	
Взам. Інв. №	
Підп. та дата	
Інв. № ориг.	

## Центр сертифікації ключів ринку електричної енергії

Комплексна система захисту інформації

План проведення відновлювальних робіт і забезпечення  
безперервного функціонування

ЄААД.468244.185.Д3.02

2014 р.

**ЗМІСТ**

1 ОБЛАСТЬ ЗАСТОСУВАННЯ.....	3
2 НОРМАТИВНІ ПОСИЛАННЯ .....	3
3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ .....	4
4 ПОЗНАЧЕННЯ ТА СКОРОЧЕННЯ .....	4
5 ЦІЛІ СКЛАДАННЯ, ЗАВДАННЯ І ЕТАПИ ВИКОНАННЯ ПЛАНУ .....	5
6 СТИСЛИЙ ОПИС ЦСК.....	6
7 ОПИС ТИПОВИХ КРИЗОВИХ СИТУАЦІЙ В ЦСК .....	7
8 ОСНОВНІ ПОЛОЖЕННЯ З ОРГАНІЗАЦІЇ ВІДНОВЛЮВАЛЬНИХ РОБІТ .....	11
9 ОПИС ПРОЦЕДУР РЕАГУВАННЯ НА НАДЗВИЧАЙНІ СИТУАЦІЇ .....	12
10 ЗАХОДИ ПО ПОПЕРЕДЖЕННЮ НАДЗВИЧАЙНИХ СИТУАЦІЙ.....	16
11 ПОРЯДОК ПЕРЕГЛЯДУ ПЛАНУ .....	20
ДОДАТОК 1. ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ВІДНОВЛЮВАЛЬНИХ РОБІТ І ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОГО ФУНКЦІОНУВАННЯ ЦСК.....	21

## 1 ОБЛАСТЬ ЗАСТОСУВАННЯ

1.1 Вимоги цього документа поширюються на ЦСК в цілому.

1.2 Цей документ визначає основні заходи, методи і засоби зберігання (підтримки) працездатності ЦСК при виникненні різноманітних надзвичайних (далі - кризових) ситуацій, а також способи і засоби відновлення інформації і процесів її обробки у разі порушення працездатності ЦСК або його основних компонентів. Крім того, документ описує дії різних категорій персоналу системи в кризових ситуаціях, дії по ліквідації їх наслідків та мінімізації можливого збитку.

## 2 НОРМАТИВНІ ПОСИЛАННЯ

- 1) Закон України "Про електронний цифровий підпис" від 22.05.2003 р.;
- 2) Закон України "Про електронні документи та електронний документообіг" від 22.05.2003 р.;
- 3) Порядок акредитації центру сертифікації ключів. Затверджений Постановою КМУ від 13 липня 2004 р. № 903;
- 4) Правила посиленої сертифікації. Затверджені наказом ДСТСЗІ СБ України № 50 від 10.05.2006 р.;
- 5) Порядок засвідчення наявності електронного документа (електронних даних) на певний момент часу. Затверджений Постановою КМУ від 26 травня 2004 р. № 680.

### 3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ

Терміни, які вживаються у цьому документі, мають таке значення:

- відновлення - процес переведення об'єкта в працездатний стан з непрацездатного стану (ГОСТ 27.002);
- кризова (аварійна) ситуація - стан автоматизованої системи, визначений сполученням відмов і/або помилок функціонування її елементів і здатний привести до порушень функціонування системи в цілому з особливо значними технічними, економічними або соціальними втратами (тобто до аварій) (ГОСТ 24.701);
- конфігурація - спосіб, за допомогою якого організуються й взаємодіють апаратні й програмні засоби системи обробки інформації (ГОСТ ИСО/МЭК 2383-1);
- непрацездатний стан - стан об'єкта, при якому значення хоча б одного параметра, що характеризує здатність виконувати задані функції, не відповідають вимогам нормативно-технічної й (або) конструкторської (проектної) документації (ГОСТ 27.002);
- відмова - подія, що полягає в порушенні працездатного стану об'єкта (ГОСТ 27.002);
- працездатний стан; працездатність - стан об'єкта, при якому значення всіх параметрів, що характеризують здатність виконувати задані функції, відповідають вимогам нормативно-технічної й (або) конструкторської (проектної) документації (ГОСТ 27.002);
- резервування - спосіб забезпечення надійності об'єкта за рахунок використання додаткових засобів і (або) можливостей, надлишкових стосовно мінімально необхідного для виконання встановлених функцій (ГОСТ 27.002);
- збій - відмова, що самоусувається, або однократна відмова, що усувається незначним втручанням оператора (ГОСТ 27.002).

Інші терміни застосовуються у значенні, наведеному в Законах України "Про електронний цифровий підпис", "Про телекомунікації", інших нормативно-правових актах з питань інформатизації та захисту інформації.

### 4 ПОЗНАЧЕННЯ ТА СКОРОЧЕННЯ

ЕЦП	- Електронний цифровий підпис
ЛОМ	- Локальна обчислювальна мережа
НД	- Нормативний документ
НСД	- Несанкціонований доступ
ПЕОМ	- Персональна електронно-обчислювальна машина
ПЗ	- Програмне забезпечення
ПТК	- Програмно-технічний комплекс
РС	- Робоча станція
ЦСК	- Центр сертифікації ключів
GPS	- Global Positioning System (глобальна система позиціонування)

## 5 ЦІЛІ СКЛАДАННЯ, ЗАВДАННЯ І ЕТАПИ ВИКОНАННЯ ПЛАНУ

5.1 Основні цілі складання плану полягають у такому:

- мінімізація потенційних фінансових втрат ДП "ЕНЕРГОРИНОК" на проведення відновлювальних робіт і забезпечення безперервного функціонування ЦСК ;
- зменшення юридичної відповідальності ДП "ЕНЕРГОРИНОК" внаслідок неналежного виконання ЦСК своїх функцій та зобов'язань;
- скорочення часу непрацездатного стану ЦСК;
- забезпечення стабільності діяльності ЦСК;
- організоване відновлення працездатного стану ЦСК;
- зменшення навантаження на провідних співробітників ЦСК;
- краща схоронність майна ЦСК;
- забезпечення безпеки персоналу та замовників ЦСК;
- дотримання вимог законів та інших нормативно-правових актів з питань інформатизації та захисту інформації.

5.2 Основна мета у процесі виконання плану полягає в забезпеченні швидкого і повного відновлення безперервного функціонування ЦСК в захищеному режимі в обсязі функцій визначених у нормативно-правових актах [1 - 5].

У результаті виникнення будь-якої кризової ситуації або ланцюга подібних подій, поставлена мета досягається шляхом рішення керівництвом ДП "ЕНЕРГОРИНОК" та керівником ЦСК таких завдань:

- визначення порядку дій, процедур та ресурсів, необхідних для відновлення працездатного стану системи або забезпечення її стабільного функціонування;
- визначення штатного складу й основних обов'язків персоналу аварійних груп із числа співробітників ЦСК щодо реалізації заходів плану відновлення, а також порядку організації ефективної взаємодії між аварійними групами й управління ними протягом всього часу активності Плану;
- визначення порядку взаємодії і координації дій персоналу ЦСК та ДП "ЕНЕРГОРИНОК" щодо реалізації плану з іншими організаціями і структурами (пожежні, медперсонал, міліція, рятувальники тощо), які, можливо, будуть залучатися до ліквідації наслідків надзвичайних подій, що викликали порушення нормального функціонування системи.

5.3 Всі заходи щодо виконання плану можна поділити на три етапи:

- етап повідомлення (активації Плану). Основними завданнями, що розв'язуються на даному етапі, є своєчасна ідентифікація виникнення кризової ситуації, виявлення нанесених системі ушкоджень, оцінка збитків, прогноз можливості відновлення працездатного стану ЦСК і ухвалення рішення щодо необхідності активації плану відновлення системи;
- етап відновлення. Основні завдання - відновлення функціонування системи за тимчасовою схемою (з використанням резервних засобів), проведення комплексу робіт з повного відновлення працездатності системи в обсязі звичайних умов;
- етап відтворення системи. Основні завдання - повне відновлення працездатного стану ЦСК та повернення до режиму нормального функціонування.

## 6 СТИСЛИЙ ОПИС ЦСК

6.1 Центр сертифікації ключів (далі - ЦСК) є спеціалізованою інформаційно-телекомунікаційною (автоматизованою) системою, що призначена для обробки, як відкритої інформації, так і конфіденційної інформації.

ЦСК розгорнений як локальна обчислювальна мережа, що має єдину точку підключення до внутрішньої телекомунікаційної мережі ДП "ЕНЕРГОРИНОК", через які користувачі ЦСК і мережі отримують доступ до наданих їм інформаційних та апаратних ресурсів ПТК ЦСК.

В складі локальної обчислювальної мережі ЦСК функціонують центральні сервери ЦСК та сервер взаємодії, а також робочі станції (РС) адміністратора безпеки, системного адміністратора, адміністратора реєстрації, які взаємодіють через внутрішню комунікаційну мережу на основі кабельної мережі та комутаторів.

Програмно-технічний комплекс (ПТК) ЦСК взаємодіє з ПТК інших ЦСК (в тому числі і ЦЗО), ІТС користувачів (споживачів послуг ЕЦП) через сервер взаємодії. Сервер взаємодії (ПТК ЦСК) взаємодіє з зовнішньою телекомунікаційною мережею через внутрішні телекомунікаційні мережі ДП "ЕНЕРГОРИНОК" та програмно-технічного комплексу взаємодії з ЗТМ.

6.2 Згідно [1,3] під час надання послуг електронного цифрового підпису фізичним та юридичним особам, фізичним особам-підприємцям ЦСК зобов'язаний забезпечувати виконання таких вимог.

6.2.1 Цілодобовий доступ користувачів до сертифікатів ключів та відповідних електронних переліків сертифікатів через загальнодоступні телекомунікаційні канали.

6.2.2 Надання у реальному часі та/або з використанням списку відкликаних сертифікатів відповідно до регламенту роботи ЦСК достовірних даних про статус сертифікатів за запитом користувачів.

6.2.3 Цілодобовий прийом звернень про скасування, блокування та поновлення сертифікатів ключів (в автоматичному режимі, у телефонному режимі, або за письмовою заявою - на протязі робочого дня ДП "ЕНЕРГОРИНОК").

6.2.4 Перевірка законності звернень про скасування, блокування та поновлення сертифікатів ключів та збереження документів, на підставі яких були скасовані, заблоковані та поновлені сертифікати ключів.

6.2.5 Своєчасне скасування, блокування та поновлювання сертифікатів ключів у випадках, передбачених Законом [1]. Час між отриманням звернення підписувача або його уповноваженого представника про скасування, блокування сертифіката та внесенням змін до списку відкликаних сертифікатів, доступних користувачам, не повинен перевищувати двох годин.

6.2.6 Своєчасне попередження підписувача та додавання в сертифікат відкритого ключа підписувача інформацію про обмеження використання ЕЦП, які встановлюються для забезпечення можливості відшкодування збитків сторін у разі заподіяння шкоди з боку ЦСК.

6.2.7 Цілодобове надання послуги фіксування часу. Час формування, скасування, блокування та поновлення сертифікатів встановлюється за київським часом і синхронізується з Всесвітнім координованим часом (UTC) з точністю до однієї секунди.

6.2.8 Збереження сформованих сертифікатів ключів протягом строку, передбаченого законодавством для зберігання відповідних документів на папері.

6.2.9 Захист інформації в автоматизованих системах відповідно до законодавства.

## 7 ОПИС ТИПОВИХ КРИЗОВИХ СИТУАЦІЙ В ЦСК

### 7.1 Класифікація кризових ситуацій

7.1.1 Відповідно до джерел і форми прояву кризові ситуації можуть бути випадковими (ненавмисними) або навмисними (навмисний напад). Кризові ситуації можуть мати об'єктивну або суб'єктивну природу.

Під випадковою (ненавмисною) кризовою ситуацією розуміється така кризова ситуація, яка не була результатом наперед обдуманих дій і виникнення якої з'явилося результатом об'єктивних або суб'єктивних причин випадкового характеру, халатності, недбалості або випадкового збігу обставин.

Під навмисним нападом розуміється кризова ситуація, яка виникла в результаті виконання порушником в певні моменти часу наперед обдуманих і спланованих дій.

7.1.2 Для компонентів локальної обчислювальної мережі (ЛОМ) і засобів зовнішньої телекомунікаційної мережі ЦСК потенційно можливими джерелами кризових ситуацій об'єктивної природи можуть бути:

- випадкові зміни умов зовнішнього фізичного середовища (за межами будівлі або контрольованої зони об'єкту інформаційної діяльності ЦСК), такі як стихійні лиха і аварії, землетрус, повінь, пожежа або інші випадкові події;
- випадкові зміни умов внутрішнього фізичного середовища (усередині будівлі або контрольованої зони об'єкту інформаційної діяльності ЦСК), такі як аварія системи електропостачання будівлі або приміщень ЦСК, руйнування будівельних конструкцій приміщень ЦСК, затоплення приміщень унаслідок аварії інженерних комунікацій холодного водопостачання, опалювання, пожежа або інші випадкові події;
- випадкові збої і відмови в роботі обладнання і технічних засобів компонентів ЦСК або зовнішньої системи телекомунікації.

7.1.3 В ЦСК потенційно можливими кризовими ситуаціями суб'єктивної природи можуть бути:

- випадкові (ненавмисні) або навмисні зміни умов зовнішнього фізичного середовища (за межами будівлі або контрольованої зони об'єкту інформаційної діяльності ЦСК) такі як впливи (аварії, пожежа або інші навмисні події) на комутаційні вузли і канали передачі зовнішньої системи телекомунікації та ін.;
- випадкові (ненавмисні) або навмисні зміни умов внутрішнього фізичного середовища (усередині будівлі або контрольованої зони об'єкту інформаційної діяльності ЦСК) такі як аварія системи електропостачання будівлі або приміщень ЦСК, руйнування будівельних конструкцій приміщень ЦСК, затоплення приміщень унаслідок аварії інженерних комунікацій холодного водопостачання, опалювання, пожежа або інші випадкові події;
- наслідки помилок під час проектування і розробки компонентів ЦСК (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);
- помилки персоналу (користувачів) під час експлуатації обладнання і технічних засобів компонентів ЦСК ;
- навмисні дії (спроби) потенційних порушників під час експлуатації обладнання і технічних засобів компонентів ЦСК .

Джерела кризових ситуацій суб'єктивної природи у ЦСК можуть бути внутрішні (нелояльні співробітники) і зовнішні (клієнти - користувачі інших відомств, терористичні акти або їхня загроза, атаки хакерів, дії кримінальних, комерційних структур і та ін.).

7.1.4 За ступенем серйозності і розмірам завданого збитку кризові ситуації поділяються на категорії: загрозна, серйозна, звичайна.

Критерії визначення категорії кризової ситуації та імовірні наслідки її виникнення наведено в таблиці 1.

Таблиця 1 - Критерії визначення категорії кризової ситуації та імовірні наслідки її виникнення.

Категорії кризової ситуації	Позначення	Критерії визначення кризової ситуації	Імовірні наслідки виникнення кризової ситуації
Аварійна (форс-мажор)	АКС-1	Повна відмова інформаційно-телекомунікаційної системи ЦСК і її нездатність далі забезпечувати надання послуг ЕЦП фізичним та юридичним особам, фізичним особам-підприємцям з виконанням всіх вимог, що наведені в 6.2 цього документу. Термін відновлення більше 2 годин.	ДП "ЕНЕРГОРИНОК" безумовно повинне відшкодувати збитки, що можуть бути заподіяні підписувачам, користувачам та третім особам, які користуються ЕЦП ЦСК на договірних засадах.. Підписувач має право оскаржити дії чи бездіяльність ЦСК у судовому порядку. Втрата прихильності замовників, погіршення іміджу й зниження конкурентноздатності. Негативна інформація про ЦСК в пресі.
	АКС-2	Знищення, блокування, неправомірна модифікація або компрометація особистих ключів центру. Термін відновлення особистих ключів центру та сертифікатів більше 2 годин.	
Загрозлива	ЗКС-1	Відмова інформаційно-телекомунікаційної системи ЦСК і її нездатність далі забезпечувати надання послуг ЕЦП фізичним та юридичним особам, фізичним особам-підприємцям з виконанням будь-якої вимоги, що наведені в 6.2.1, 6.2.2, 6.2.3, 6.2.5, 6.2.7, 6.2.10 цього документу. Термін відновлення менше 2 годин.	ДП "ЕНЕРГОРИНОК" може бути примушене відшкодувати збитки, що можуть бути заподіяні підписувачам, користувачам та третім особам, які користуються ЕЦП ЦСК на договірних засадах. Підписувач має право оскаржити дії чи бездіяльність ЦСК у судовому порядку. Втрата прихильності замовників, погіршення іміджу й зниження конкурентноздатності. Негативна інформація про ЦСК в пресі.
	ЗКС-2	Знищення, блокування, неправомірна модифікація або компрометація особистих ключів центру. Термін відновлення особистих ключів центру та сертифікатів менше 2 годин.	
Серйозна	СКС-1	Відмова окремих компонентів ПТК ЦСК (часткова втрата працездатності), внаслідок чого - нездатність далі забезпечувати надання послуг ЕЦП фізичним та юридичним особам, фізичним особам-підприємцям з виконанням будь-якої вимоги, що наведені в 6.2.4, 6.2.6, 6.2.8, 6.2.9 цього документу. Термін відновлення менше 2 годин.	Підписувач має право оскаржити дії чи бездіяльність ЦСК у судовому порядку. Втрата прихильності замовників, погіршення іміджу й зниження конкурентноздатності.. Негативна інформація про ЦСК в пресі.
	СКС-2	Порушення цілісності і конфіденційності програм і даних в результаті несанкціонованого доступу (особистих ключів посадових осіб ЦСК, персональних даних реєстрації). Термін відновлення менше 2 годин.	
Звичайна	ЗвКС-1	Збій окремих компонентів ПТК ЦСК (часткова втрата працездатності), втрата продуктивності.	Ситуації, що виникають в результаті небажаних дій, що не завдають відчутного збитку, проте вимагають уваги і адекватної реакції. Дії у разі виникнення таких ситуацій передбачені Планом захисту (в обов'язках персоналу служби захисту інформації ЦСК ).
	ЗвКС-2	Зафіксовані невдалі спроби проникнення або несанкціонованого доступу до ресурсів системи (до критичних не відносяться).	



7.1.5 Класифікація кризових ситуацій відповідно до джерел, форм прояву та категорій утворюють множину з 12 варіантів, кожний з яких є класом однорідних по цілком визначених ознаках кризових ситуацій в ЦСК . Класи кризових ситуацій в ЦСК приведено в таблиці 2.

Таблиця 2 - Класи кризових ситуації в ЦСК

Категорія кризової ситуації	Джерела і форма прояву кризової ситуації		
	Об'єктивні	Суб'єктивні	
		випадкові	навмисні
Аварійна (форс-мажор)	1 клас	2 клас	3 клас
Загрозлива	4 клас	5 клас	6 клас
Серйозна	7 клас	8 клас	9 клас
Звичайна	10 КЛАС	11 клас	12 клас

7.2 До аварійних (форс-мажорних ) кризових ситуацій всіх класів відносяться:

- порушення подачі електроенергії в будівлю (аварія на районній підстанції) на термін більше 2 годин;
- затоплення серверного приміщення ЦСК або суміжних приміщень в будівлі внаслідок аварії систем життєзабезпечення (великий прорив трубопроводів гарячої та/або холодної води). Термін відновлення працездатності ПТК ЦСК більше 2 годин;
- велика або середня пожежа в будівлі або серверному приміщенні ЦСК або приміщенні адміністраторів ЦСК;
- відмова системи телекомунікації (порив кабелів або аварія обладнання АТС телефонної мережі загального користування) на термін більше 2 годин;
- відмова серверу взаємодії ЦСК (з втратою доступу до інформації web-сервера, LDAP-сервера тощо) на термін більше 2 годин;
- відмова (з втратою інформації) серверу ЦСК на термін більше 2 годин;
- відмова апаратного модулю підпису (АМП). Термін відновлення більше 2 годин;
- компрометація особистих ключів ЦСК. Термін відновлення особистих ключів ЦСК та сертифікатів підписувачів більше 2 годин;
- відмова приймача GPS сигналів Всесвітнього координованого часу (UTC) або серверу моніторингу та синхронізації часу.

7.3 До загрозливих кризових ситуацій всіх класів відносяться :

- перебіг в електропостачанні в будівлю, де розташовані приміщення ЦСК, з терміном відновлення менше 2 годин;
- порушення подачі електроенергії в приміщення ЦСК на термін більше 2 годин;
- аварії систем життєзабезпечення ЦСК (прорив трубопроводів гарячої й холодної води, відмова систем кондиціонування і ін.) на строк менше 2 годин;
- невелика пожежа в приміщенні адміністраторів ЦСК;
- збій системи телекомунікації (збій обладнання АТС телефонної мережі загального користування) з терміном відновлення менше 2 годин;
- відмова (без втрати інформації) серверу ЦСК з терміном відновлення менше 2 годин;
- збій (без втрати інформації) серверу взаємодії з терміном відновлення менше 2 годин;
- збій апаратного модулю підпису (АМП). Термін відновлення менше 2 годин;
- часткова втрата інформації на всіх серверах без втрати їх працездатності;
- вихід з ладу локальної мережі (фізичного середовища передачі даних).

7.4 До серйозних кризових ситуацій всіх класів відносяться:

- аварії систем життєзабезпечення (дрібний прорив трубопроводів гарячої та/або холодної води, відмова систем кондиціонування і ін.) в приміщеннях ЦСК на термін більше 2 годин;
- відмова (з втратою інформації) робочої станції ЦСК ;
- часткова втрата інформації на будь-якій робочій станції ЦСК без втрати його працездатності;
- перебіг в подачі електроенергії в приміщення ЦСК на термін менше 2 годин.

7.5 До ситуацій, що вимагають уваги відносяться:

- збій (без втрати інформації) робочої станції ЦСК ;
- несанкціоновані дії, що заблоковані засобами захисту і зафіксовані засобами реєстрації;
- відмова системи телекомунікації.

7.6. Джерелами інформації про виникнення кризової ситуації є:

- користувачі, що виявили невідповідність плану захисту або інші підозрілі зміни в роботі чи конфігурації системи, або засобів її захисту в межах своєї зони відповідальності;
- засоби захисту, що виявили передбачену Планом захисту кризову ситуацію;
- системні журнали, в яких є записи, що свідчать про виникнення або можливість виникнення кризової ситуації.

## 8 ОСНОВНІ ПОЛОЖЕННЯ З ОРГАНІЗАЦІЇ ВІДНОВЛЮВАЛЬНИХ РОБІТ

8.1 Всі користувачі, робота яких може бути порушена в результаті виникнення аварійної, загрозливої або серйозної кризової ситуації, повинні негайно доповідати про це. Подальші дії по усуненню причин порушення працездатності ЦСК, відновленню обробки і відновленню пошкоджених (втрачених) ресурсів визначаються функціональними обов'язками персоналу і користувачів системи.

8.2 Кожна кризова ситуація повинна аналізуватися службою захисту інформації ЦСК і за наслідками цього аналізу повинні вироблятися пропозиції по зміні повноважень користувачів, атрибутів доступу до ресурсів, створенню додаткових резервів, зміні конфігурації системи або параметрів настройки засобів захисту тощо.

8.3 Аварійна, загрозлива і серйозна кризова ситуація можуть вимагати оперативної заміни і ремонту обладнання, що вийшло з ладу, а також відновлення пошкоджених програм і наборів даних з резервних копій.

Оперативне відновлення програм (використовуючи еталонні копії) і даних (використовуючи резервні або архівні копії) у разі їх знищення або псування в аварійній, загрозливій або серйозній кризовій ситуації забезпечується резервним та архівним копіюванням і зовнішнім (по відношенню до основних компонентів системи) зберіганням копій.

Резервному копіюванню підлягають усі програми і дані серверів ЦСК (оперативної, резервної і архівної), що забезпечують працездатність системи і виконання нею своїх задач (у тому числі системне і прикладне програмне забезпечення, бази даних і інші набори даних, а також архіви, журнали транзакцій, системні журнали тощо).

8.4 Всі програмні засоби, що використовуються в ПЕОМ повинні мати еталонні дистрибутивні копії. Їх місцезнаходження і відомості про відповідальних за їх створіння, зберігання і використання повинні вказуватися в формулярах на кожен ПЕОМ (робочу станцію) ЦСК. Також повинні вказуватися переліки наборів даних, що підлягають резервному та архівному копіюванню, періодичність копіювання, місце зберігання, відповідальні за створення, зберігання і використання копій резервних (архівних) даних.

8.5 Необхідні дії персоналу по створенню, зберіганню і використанню резервних (архівних) копій програм і даних повинні відображатися в функціональних обов'язках відповідних категорій персоналу.

8.6 Кожний носій, що містить резервну копію, повинен мати мітку, що містить дані про ім'я файлу (каталогу), цінність, призначення інформації, яка зберігається, відповідального за створення, зберігання і використання, дату останнього копіювання, місце зберігання і ін.

8.7 Найбільш важливі апаратні компоненти серверу взаємодії та серверу ЦСК, особливо мережевий криптомодуль (МКМ), повинні резервуватися для забезпечення працездатності системи у разі відмови всіх або окремих апаратних компонентів в результаті загрозливої кризової ситуації.

8.8 Ліквідація наслідків аварійної, загрозливої або серйозної кризової ситуації має на увазі, можливо, більш повне відновлення програмних, апаратних, інформаційних і інших пошкоджених компонентів системи. Для відновлення використовуються засоби, які наведено в Додатку 1.

8.9 У разі виникнення будь-якої кризової ситуації повинно провадитися розслідування причин її виникнення, оцінка заподіяного збитку, визначення винних і вживання відповідних заходів.

Розслідування кризової ситуації проводить комісія, яка призначається наказом керівника ЦСК. Очолює комісію керівник служби захисту інформації ЦСК. Результати розслідування оформляються Актом, який представляється на розгляд і затвердження керівництва ДП "ЕНЕРГОРИНОК".

Якщо причиною загрозливої або серйозної кризової ситуації з'явилися недостатньо жорсткі заходи захисту і контролю, а збиток перевищив встановлений рівень, то така ситуація є підставою для повного перегляду плану захисту і плану проведення відновлювальних робіт і забезпечення безперервного функціонування ЦСК.

## 9 ОПИС ПРОЦЕДУР РЕАГУВАННЯ НА НАДЗВИЧАЙНІ СИТУАЦІЇ

9.1 Дії персоналу ЦСК в кризовій ситуації залежать від ступеня її тяжкості.

9.2 При описі процедур реагування у разі виникнення аварійної (форс-мажорної) або загрозової критичної ситуації застосовуються такі основні допущення:

- ЦСК непрацездатний, з урахуванням специфіки реалізації і технології роботи системи, технічні та програмні засоби можуть бути відновлені у попередньому місці розміщення не раніше, ніж через 2 години;
- заздалегідь призначено персонал ЦСК, що поінформований про дії в надзвичайних обставинах і свої обов'язки у процесі відновлення працездатності системи;
- системи контролю, аварійного оповіщення і ліквідації наслідків (протипожежні системи, контроль водопроводу й опалення тощо) справні і перебувають у працездатному стані;
- всі елементи системи забезпечені безперервним енергоживленням не менше 30 хвилин з моменту виходу з ладу основної енергосистеми. Надалі всі елементи системи можуть бути підключені до резервного фідера електроживлення приміщень ЦСК;
- актуальні резервні копії прикладного програмного забезпечення і даних не ушкоджені та доступні в резервному сховищі;
- необхідне для відновлення системи обладнання доступно в резервному сховищі;
- договори на технічне обслуговування апаратних засобів, відновлення програмного забезпечення й послуги провайдерів зв'язку включають положення, необхідні для реалізації плану відновлення функціонування системи.

9.3 Загальний порядок дії персоналу по забезпеченню відновлювальних робіт і забезпечення безперервного функціонування ЦСК .

9.3.1 У разі виникнення ситуації, що вимагає уваги, адміністратор безпеки ЦСК повинен провести її аналіз (розслідування) власними силами. Про факти систематичного виникнення таких ситуацій і вжитих заходів адміністратор безпеки ЦСК повинен доповідати керівнику начальника служби захисту інформації.

9.3.2 У разі виникнення аварійної (форс-мажорної), загрозової або серйозної критичної ситуації дії персоналу ЦСК включають такі етапи:

- негайна реакція;
- часткове відновлення працездатності і відновлення обробки;
- повне відновлення системи і відновлення обробки в повному об'ємі;
- розслідування причин кризової ситуації і встановлення винних.

9.3.3 Етапи включають такі дії користувачів і персоналу ЦСК :

9.3.3.1 Негайна реакція:

- користувач, що встановив факт виникнення кризової ситуації підсистеми ЦСК , зобов'язаний негайно сповістити про це адміністратора безпеки;
- адміністратор безпеки повинен довести до користувачів всіх суміжних підсистем про факт виникнення кризової ситуації для їх переходу на аварійний режим роботи (або припинення роботи);
- сповістити керівника ЦСК та системного адміністратора;
- визначити ступінь серйозності і масштаби кризової ситуації, розміри і область пошкодження;
- сповістити персонал взаємодіючих підсистем про характер кризової ситуації і орієнтовний час відновлення обробки.

Відповідальними за цей етап є користувач підсистеми і адміністратор безпеки.

9.3.3.2 При частковому відновленні працездатності (мінімально необхідної для відновлення роботи системи в цілому, можливо з втратою продуктивності) і відновленні обробки:

- відключити пошкоджені компоненти або перемкнутися на використання дублюючих ресурсів (гарячого резерву);
- якщо не відбулося пошкодження програм і даних, відновити обробку і сповістити про це персонал взаємодіючих (під)систем;
- відновити працездатність пошкоджених критичних апаратних засобів і іншого обладнання, при необхідності зробити заміну вузлів і блоків, що відмовили, резервними;
- відновити пошкоджене програмне забезпечення, використовуючи еталонні (резервні) копії;
- відновити необхідні дані, використовуючи резервні копії;

- перевірити працездатність пошкодженої підсистеми, упевнитися в тому, що наслідки кризової ситуації не впливають на подальшу роботу системи;
- повідомити операторів суміжних підсистем про готовність до продовження роботи;
- внести всі зміни даних за час з моменту створення останньої резервної копії (за поточний період, день), для чого повинен здійснюватися "вирівнювання баз даних" на підставі інформації з журналів транзакцій або всі пов'язані з пошкодженою підсистемою користувачі повинні повторити дії, що виконувалися протягом останнього періоду.

Відповідальними за цей етап є адміністратор безпеки та системний адміністратор ЦСК .

9.4. Для повного відновлення в період неактивності системи:

- відновити працездатність всіх пошкоджених апаратних засобів, при необхідності зробити заміну вузлів і блоків, що відмовили, резервними;
- відновити та настроїти всі пошкоджені програми, використовуючи еталонні (резервні) копії;
- відновити всі пошкоджені дані, використовуючи резервні копії і журнали транзакцій;
- настроїти засоби захисту підсистеми відповідно до плану захисту;
- про результати відновлення повідомити керівника ЦСК.

Відповідальними за цей етап є адміністратор безпеки та системний адміністратор ЦСК .

9.5. Далі необхідно провести розслідування причин виникнення кризової ситуації. Для цього необхідно відповісти на питання:

- випадкова або навмисна кризова ситуація?
- чи враховувалася можливість її виникнення в Плані захисту і Плані проведення відновлювальних робіт і забезпечення безперервного функціонування ЦСК ?
- чи можна було її передбачити?
- чи викликана вона слабкістю засобів захисту і реєстрації?
- чи перевищив збиток від неї встановлений рівень?
- чи є непоправний збиток і чи великий він?
- чи це перша кризова ситуація такого роду?
- чи є можливість точно визначити круг підозрюваних?
- чи є можливість точно встановити винного?
- в чому причина кризової ситуації?
- чи достатньо наявного резерву?
- чи є необхідність перегляду плану захисту?
- чи є необхідність перегляду плану проведення відновлювальних робіт і забезпечення безперервного функціонування ЦСК ?

Відповідальним за розслідування є керівник СЗІ ЦСК. Звіт про результати розслідування і пропозиції щодо вдосконалення ЦСК представляються керівництву ДП "ЕНЕРГОРИНОК" в установленому порядку.

9.6 Основні обов'язки системного адміністратора по забезпеченню безперервної роботи та відновлення працездатності ПТК ЦСК

В основні обов'язки системного адміністратора ЦСК входить:

- підтримка апаратних засобів і іншого обладнання, включаючи резервне (дублююче), в робочому стані та їх періодична перевірка;
- відновлення функцій апаратних засобів і іншого обладнання у разі відмов;
- оперативна заміна дефектних вузлів резервними у разі відмов;
- підготовка і оперативне включення резервних апаратних засобів і іншого обладнання у разі аварійної, загрозової або серйозної кризової ситуації.

9.7 Опис процедур поновлення працездатного стану ЦСК або окремих її компонентів при виникненні найпоширеніших кризових ситуацій наведені у таблиці 3.

Таблиця 3 - Опис процедур поновлення працездатного стану ЦСК

Збій базового або спеціального програмного забезпечення серверів або РС ЛОМ ЦСК.	Адміністратор безпеки ЦСК разом з системним адміністратором з'ясовують причину збою ПЗ. Якщо виправити помилку самостійно (у тому числі після консультації з розробниками ПЗ ПТК ЦСК) не вдалося, копія акту і супровідних матеріалів (а так саме файлів, якщо це необхідно) надсила-
--	---

	ються розробнику ПЗ.
Відключення електроенергії	Адміністратор безпеки разом з іншими адміністраторами (системним, реєстрації) ЦСК проводять аналіз на наявність втрат і (або) руйнування даних і ПЗ, а також перевіряють працездатність обладнання ЦСК. За потреби проводиться відновлення ПЗ і даних з останньої резервної копії зі складанням акту.
Збій у локальній обчислювальній мережі (ЛОМ)	Адміністратор безпеки разом з системним адміністратором проводять аналіз на наявність втрат і (або) руйнування даних і ПЗ ПТК ЦСК. За потреби проводиться відновлення ПЗ і даних з останньої резервної копії зі складанням акту.
Відмова серверу ЦСК	Адміністратор безпеки ЦСК разом із системним адміністратором проводить заходи для негайного включення в дію резервного сервера з метою забезпечення безперервності роботи ЦСК. За необхідністю проводиться роботи по поновленню ПЗ і даних з резервних копій зі складанням акту відповідно до експлуатаційної документації.
Втрата даних	При виявленні втрати даних адміністратор безпеки разом з іншими адміністраторами (реєстрації) ЦСК проводять заходи щодо пошуку і усунення причин втрати даних (антивірусна перевірка, перевірка цілісності і працездатності ПЗ, обладнання тощо). За необхідністю проводиться відновлення ПЗ і даних з резервних копій зі складанням акту.
Виявлено вірус.	При виявленні вірусу проводиться локалізація вірусу з метою запобігання його подальшого поширення, для чого варто фізично відокремити «заражений» комп'ютер від ЛОМ і провести аналіз стану комп'ютера. Аналіз проводить адміністратор безпеки. Результатом аналізу може бути спроба збереження даних, тому що після перезавантаження ПЕОМ дані можуть бути втрачені. Після успішної ліквідації вірусу, збережені дані також необхідно піддати перевірці на наявність вірусу. При виявленні вірусу необхідно керуватися інструкцією з організації антивірусного захисту, інструкцією з експлуатації антивірусного ПЗ. Після ліквідації вірусу необхідно провести позачергову антивірусну перевірку на всіх ПЕОМ ЦСК із застосуванням оновлених антивірусних баз. За необхідністю проводиться відновлення ПЗ і даних з резервних копій зі складанням акту. Проводиться службове розслідування з факту появи вірусу в ПЕОМ (ЛОМ) ЦСК.
Виявлено виток інформації	Факт виявлення витоку інформації доводиться до відома адміністратора безпеки і керівника ЦСК. Проводиться службове розслідування. Якщо витік інформації відбувся з технічних причин, проводиться аналіз захищеності системи і, якщо необхідно, приймаються заходи щодо усунення вразливості.
Злом системи (Web-сервера, LDAP-сервера й ін.) або несанкціонований доступ (НСД) з зовнішній телекомунікаційної мережі	При виявленні злому сервера це доводиться до адміністратору безпеки і керівника ЦСК. Проводиться, по можливості, тимчасове відключення сервера від мережі для перевірки на наявність вірусів і троянських закладок. За необхідністю, також можливо здійснити тимчасовий перехід на резервний сервер. З огляду на те, що програмні закладки можуть бути не виявлені антивірусним ПЗ, необхідно особливо ретельно перевірити цілісність файлів, що виконуються, відносно до еталонного програмного забезпечення, а також проаналізувати журнали сервера. Необхідно змінити всі паролі, які мали відношення до даного сервера. Якщо буде потреба проводиться відновлення ПЗ і даних з еталонного архіву і резервних копій зі складанням акту. За результатами аналізу ситуації варто перевірити ймовірність проникнення несанкціонованих програм у ЛОМ ЦСК, після чого провести аналогічні роботи з перевірки й відновлення ПЗ й даних на інших ПЕОМ ЦСК. По факту злому сервера проводиться службове розслідування.
Спроба несанкціонованого доступу (НСД)	При спробі НСД проводиться аналіз ситуації на основі інформації журналів реєстрації спроб НСД і попередніх спроб НСД. За результатами аналізу, якщо буде потреба, приймаються заходи щодо запобігання НСД, якщо є реальна погроза НСД. Так саме рекомендується провести позапланову зміну паролів. У випадку появи оновлень ПЗ, що усувають вразливості системи безпеки, варто застосувати такі оновлення.
Компрометація ключів	При компрометації ключів необхідно керуватися інструкціями до системи криптозахисту, що використовується в ЦСК.
Компрометація пароля	У разі компрометації пароля необхідно негайно змінити пароль, проаналі-

	зувати ситуацію на наявність наслідків компрометації й вжити необхідних заходів по мінімізації можливого (або нанесеного) збитку (блокування сертифікатів користувачів і т. ін.). За необхідністю, проводиться службове розслідування.
Фізичне пошкодження ЛОМ або ПЕОМ	Доводиться до відома адміністратора безпеки ЦСК. Проводиться аналіз на предмет витоку або пошкодження інформації. Визначаються причина пошкодження ЛОМ або ПЕОМ і можливі загрози безпеці інформації. У випадку виникнення підозри на цілеспрямований вивід обладнання з ладу, проводиться службове розслідування. Проводиться перевірка ПЗ на наявність шкідливих програм-закладок, цілісність ПЗ і даних. Проводиться аналіз електронних журналів. За необхідністю, проводяться заходи щодо відновлення ПЗ і даних з резервних копій зі складанням акту.
Стихійне лихо	При виникненні стихійних лих варто керуватися документами відповідних підрозділів ДП "ЕНЕРГОРИНОК".

## 10 ЗАХОДИ ПО ПОПЕРЕДЖЕННЮ НАДЗВИЧАЙНИХ СИТУАЦІЙ

10.1 Організація проведення відновлювальних робіт і забезпечення безперервного функціонування ЦСК

10.1 Безперервність процесу функціонування ЦСК і своєчасність відновлення його працездатності досягається:

- проведенням спеціальних організаційних заходів та розробкою організаційно-розпорядчих документів з питань забезпечення безперервності роботи і відновлення процесу функціонування ЦСК ;
- регламентацією процесу обробки інформації і дій персоналу ЦСК, у тому числі в кризових ситуаціях;
- призначенням і підготовкою посадових осіб, що відповідають за організацію і здійснення практичних заходів щодо забезпечення безперервності роботи і відновлення інформації та процесу функціонування ЦСК ;
- чітким знанням і дотриманням усіма співробітниками, що використовують засоби обчислювальної техніки ЦСК , вимог керівних документів по забезпеченню безперервності роботи і відновлення ЦСК ;
- застосуванням різних способів резервування апаратних ресурсів, еталонного, резервного та архівного копіювання програмних та інформаційних ресурсів системи;
- ефективним контролем посадовими і відповідальними особами за дотриманням вимог по забезпеченню безперервності роботи і відновлення ЦСК ;
- постійною підтримкою необхідного рівня захищеності компонентів системи, безперервним управлінням і адміністративною підтримкою коректного застосування засобів захисту;
- проведенням постійного аналізу ефективності вжитих заходів і способів забезпечення безперервності роботи і відновлення, розробкою і реалізацією пропозицій по їх вдосконаленню.

10.2 Забезпечення відновлення стійкого функціонування програмно-технічних засобів і засобів телекомунікації ЦСК повинно досягатися за рахунок проведення заходів, спрямованих на попередження порушення їхньої працездатності, і мінімізацію часу відновлення функціонування ЦСК при виникненні критичних ситуацій.

10.2.1 До заходів, що спрямовані на виключення випадків порушення працездатності, варто віднести:

- проведення комплексу організаційно-технічних заходів щодо забезпечення працездатності ЦСК (дублювання, резервування основних компонентів ПТК ЦСК);
- підвищення кваліфікації персоналу;
- використання сертифікованих програмно-технічних засобів і ліцензійного програмного забезпечення;
- проведення технічного обслуговування апаратних засобів і засобів телекомунікації;
- забезпечення безперебійного енергоживлення;
- обмеження доступу до програмно-технічних засобів.

10.2.2 Мінімізація часу відновлення працездатності ЦСК повинна досягатися за рахунок використання:

- резервного обладнання й резервних каналів зв'язку;
- копій системного й прикладного програмного забезпечення в процесі відновлення працездатності програмно-технічних засобів;
- копій файлів електронних документів і повідомлень, структур баз даних і матеріальних носіїв інформації;
- методичних документів, що регламентують дії персоналу при виникненні аварійних ситуацій.

10.3 В таблиці 4 наведено рекомендації з запобігання деяких типових кризових ситуацій.



Таблиця 4 - Рекомендації з запобігання деяких типових кризових ситуацій

Кризова ситуація	Рекомендації
Збій програмного забезпечення	Застосовувати ліцензійне ПЗ, регулярно здійснювати антивірусний контроль і профілактичні роботи на ПЕОМ (перевірка диска й ін.)
Відключення електроенергії	Використовувати джерела безперебійного живлення на відповідальних (а краще - на всіх) технологічних ділянках ЦСК. Розробити інструкцію з аварійного переходу на резервне джерело живлення (якщо такий є в наявності) або аварійного завершення роботи й збереження даних. Бажано мати в наявності резервне джерело електроживлення (дизель-генератор і ін.)
Збій ЛОМ	Забезпечення безперебійної роботи ЛОМ шляхом застосування надійних мережних технологій і резервних систем.
Вихід з ладу сервера ЦСК або серверу взаємодії	Застосовувати надійні програмно-технічні засоби, продуману політику адміністрування. Допускати до роботи із серверним обладнанням тільки кваліфікованих фахівців.
Втрата даних	Періодично здійснювати аналіз системних журналів роботи з метою з'ясування "вузьких" місць у технології й можливого витoku (або втрати) інформації. Проводити з співробітниками роз'яснювальні й навчальні збори. Забезпечити комплексний захист інформації в ЦСК.
Виявлено вірус	Дотримуватися вимог «Інструкції з організації антивірусного захисту».
Виявлено витік інформації	Застосовувати оновлення ПЗ по усуненню програмних «дір» у системі захисту в міру їхньої появи (виявлення). Створити комплексну систему захисту інформації в ЦСК. Регулярно проводити аналіз журналів спроб НСД і вдосконалення системи захисту інформації. Також див. «Втрата даних»
Злом системи (Web-сервера, LDAP-сервера й ін.) або несанкціонований доступ (НСД) з зовнішньої телекомунікаційної мережі	Див. «Виявлено витік інформації».
Спроба несанкціонованого доступу (НСД)	По можливості, установити реєстрацію спроб НСД на всіх технологічних ділянках, де можливий несанкціонований доступ, з оповіщенням адміністратора безпеки про спроби НСД.
Компрометація ключів	Дотримуватися вимог інструкції з управління ключовою системою.
Фізичне пошкодження ЛОМ або ПЕОМ	Фізичний захист компонентів мережі (серверів, маршрутизаторів і ін.), обмеження доступу до них. Див. також «Збій ЛОМ».
Стихійне лихо	Проводити навчальні збори й тренування персоналу ЦСК з питань цивільної оборони.

#### 10.4 Вимоги до забезпечення працездатності технічних засобів

10.4.1 Структура і конфігурація технічних засобів ЦСК, що використовуються при наданні послуг електронного цифрового підпису, повинні відповідати вимогам нормативно-правових документів України і технічної документації розробника (постачальника) програмно-технічного комплексу (ПТК) ЦСК.

10.4.2 Керівником ЦСК повинен визначатися і затверджуватися перелік і створений резерв технічних засобів, комплектуючих виробів та програмних продуктів, достатніх для відновлення працездатності програмно-технічного комплексу ЦСК.

10.4.3 Засоби, що використовуються для резервування, а також комплектуючі вироби повинні бути доступні протягом усього робочого дня для персоналу ЦСК, що забезпечує проведення відновлювальних робіт.

10.4.4 Захист технічних засобів від збоїв у роботі електричної мережі повинен забезпечуватися шляхом використання джерел безперебійного живлення достатньої потужності, а також резервуванням фідерів електроживлення.

10.4.5 Захист технічних засобів від впливу навколишнього середовища повинен забезпечуватися за рахунок створення температурно-вологісного режиму, що відповідає вимогам технічної документації виробника.

10.4.6 Підвищення рівня безвідмовної роботи технічних засобів повинне забезпечуватися шляхом проведення періодичного технічного обслуговування і тестування технічних засобів.

10.4.7 Періодичне технічне обслуговування технічних засобів повинне проводитися відповідно до вимог технічної документації виробників, але не рідше одного разу на рік за затвердженим директором ЦСК графіком.

10.4.8 Періодичне технічне обслуговування і тестування технічних засобів повинне містити в собі обслуговування та тестування всіх засобів, включаючи робочі станції, сервери, кабельні системи і мережне встаткування, джерела безперебійного живлення.

10.4.9 У процесі проведення періодичного технічного обслуговування повинні проводитися зовнішній і внутрішній огляд технічних засобів, перевірка контактних з'єднань, перевірка параметрів налаштувань працездатності технічних засобів і тестування їхньої взаємодії.

10.4.10 Проведення періодичного технічного обслуговування і тестування технічних засобів повинне фіксуватися в журналах, у яких повинні відображатися причини виникнення виявлених дефектів і заходи їхньої ліквідації.

10.4.11 Відновлення працездатності технічних засобів повинно проводитися відповідно до інструкцій розробника і постачальника технічних засобів по відновленню працездатності технічних засобів і завершуватися проведенням їхнього тестування.

10.4.12 Процедури відновлення працездатності технічних засобів повинні фіксуватися у відповідному журналі, в який заносяться:

- причина порушення працездатності;
- час відновлення роботи;
- перелік замінених комплектуючих виробів і деталей;
- прізвище фахівця, що здійснював відновлення працездатності.

**Примітка** - Допускається зазначену інформацію приводити в журналі обліку періодичного технічного обслуговування і тестування.

10.4.13 Паспорта на програмно-технічні комплекси та журнали на технічні засоби, що входять у їх склад, повинні перебувати на робочих місцях персоналу, що експлуатує зазначені комплекси і засоби.

#### 10.5 Вимоги до забезпечення працездатності програмного забезпечення

10.5.1 До складу програмного забезпечення програмно-технічних комплексів ЦСК повинно включатися системне, прикладне і комунікаційне програмне забезпечення.

10.5.2 Програмне забезпечення повинно відповідати вимогам технічної документації розробника і постачальника програмно-технічних комплексів ЦСК.

10.5.3 У складі програмно-технічних комплексів ЦСК повинно використовуватися ліцензійне системне програмне забезпечення.

10.5.4 Програмно-технічний комплекс ЦСК повинен мати позитивний експертний висновок ДССЗЗІ України.

10.5.5 Програмне забезпечення, яке придбане для використання в складі програмно-технічних комплексів ЦСК, повинно перевірятися на наявність вірусів і працездатність.

10.5.6 З придбаного програмного забезпечення повинні бути створені робочі копії на машинних носіях. Передача в архів оригіналу і копій повинна провадитися тільки після перевірки їх працездатності.

10.5.7 Працездатність придбаного програмного забезпечення повинна бути перевірена на резервному програмно-технічному комплексі, після чого це програмне забезпечення включається до складу засобів, що використовуються в процесі надання послуг ЕЦП.

10.5.8 Повинен бути виключений несанкціонований доступ до програмного забезпечення за рахунок використання засобів захисту інформації.

10.5.9 Програмне забезпечення повинно регулярно піддаватися перевіркам на наявність комп'ютерних вірусів та інших шкідливих програм.

10.5.10 Всі порушення працездатності програмного забезпечення повинні фіксуватися з наступним проведенням аналізу причин їх виникнення.

10.5.11 Відновлення працездатності програмного забезпечення повинно проводитися відповідно до інструкцій його постачальника.

10.5.12 Зберігання програмного забезпечення на машинних носіях повинно здійснюватися відповідно до вимог ГОСТ 28388 і нормативних документів [1-5].

10.5.13 Архівні копії програмного забезпечення на машинних носіях, експлуатаційна документація й інструкції з відновлення працездатності програмного забезпечення повинні бути доступними протягом усього робочого дня для персоналу ЦСК, що забезпечує його функціонування.

10.5.14 У програмному забезпеченні ПТК ЦСК повинні бути реалізовані такі вимоги до доступності програмних документів:

- наявність опису програмного середовища функціонування;
- оформлення документації відповідно до вимог Єдиної системи програмної документації;
- дотримання стандартів і правил викладу в документації;
- наявність повного переліку документації.

#### 10.6 Вимоги до забезпечення схоронності інформаційного забезпечення

10.6.1 До складу інформаційного забезпечення програмно-технічного комплексу (ПТК) ЦСК повинні включатися файли електронних документів і повідомлення, що використовуються в процесі надання послуг ЕЦП, протоколи подій і дій обслуговуючого персоналу, структури баз даних і матеріальні носії інформації (МНІ).

10.6.2 У ході технологічного процесу надання послуг ЕЦП всі електронні документи, повідомлення й супутня інформація відповідно до вимог [1-5], експлуатаційною документації розробників і постачальників ПТК ЦСК повинні копіюватися в поточні архіви.

10.6.3 Після завершення робочого дня інформація з поточних архівів, копії баз даних і МНІ повинні передаватися в архів електронних документів.

10.6.4 Створення копій файлів електронних документів і повідомлень, структур баз даних і МНІ, передача їх в архів електронних документів і використання цих копій для відновлення інформаційного ресурсу повинні реєструватися в журналі.

10.6.5 У випадку порушення цілісності інформаційного забезпечення відновлення повинно проводитися відповідно до інструкцій розробників і постачальників ПТК ЦСК.

10.6.6 Архіви електронних документів, експлуатаційна документація й інструкції з відновлення цілісності інформаційного забезпечення повинні бути доступні персоналу ЦСК, що забезпечує його функціонування, протягом усього робочого дня.

10.6.7 Повинна виключатися можливість несанкціонованого доступу до інформаційних ресурсів і архівів електронних документів.

## 11 ПОРЯДОК ПЕРЕГЛЯДУ ПЛАНУ

11.1 План проведення відновлювальних робіт і забезпечення безперервного функціонування ЦСК підлягає повному перегляду в таких випадках:

- при зміні переліку розв'язуваних задач ЦСК, конфігурації технічних і програмних засобів ПТК ЦСК, що призводять до зміни технології обробки інформації;
- при зміні пріоритетів в значущості загроз безпеці ЦСК .

11.2 План проведення відновлювальних робіт і забезпечення безперервного функціонування ЦСК підлягає частковому перегляду в таких випадках:

- при зміні конфігурації ЦСК, додаванні або видаленні програмних і технічних засобів ПТК ЦСК, які не змінюють технологію обробки інформації;
- при зміні конфігурації програмних і технічних засобів ПТК, що використовуються;
- при зміні складу, обов'язків і повноважень користувачів системи.

11.3 Профілактичний перегляд плану проведення відновлювальних робіт і забезпечення безперервного функціонування ЦСК здійснюється не менш ніж 1 раз на рік і має на меті перевірку достатності визначених даним планом заходів реальним умовам застосування ЦСК і існуючим вимогам.

11.4 У разі часткового перегляду можуть бути додані, видалені або змінені різні додатки до плану з обов'язковою вказівкою даних про те, яка особа санкціонувала та хто, коли, і з якою метою вніс зміни.

11.5 Зміни, які вносяться в план, не повинні суперечити іншим положенням плану і плану захисту та повинні бути перевірені на коректність, повноту і можливість здійснення.

11.6 Перегляд плану повинен здійснюватися спеціальною комісією, склад якої затверджується наказом директора ДП "ЕНЕРГОРИНОК". Включення представників служби захисту інформації до складу комісії по перегляду плану проведення відновлювальних робіт і забезпечення безперервного функціонування ЦСК є обов'язковим.

11.7 Особа, яка відповідальна за реалізацію даного документа, призначається наказом директора ДП "ЕНЕРГОРИНОК".

## ДОДАТОК 1. ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ВІДНОВЛЮВАЛЬНИХ РОБІТ І ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОГО ФУНКЦІОНУВАННЯ ЦСК

1. Резервному копіюванню підлягає така інформація:

- системні програми, набори даних РС і серверів ЦСК - не відновлюваному (однократному, еталонному) резервному копіюванню;
- прикладне програмне забезпечення і набори даних РС і серверів ЦСК - не відновлюваному резервному копіюванню;
- набори даних, що генеруються протягом дня і що містять цінну інформацію РС і серверів ЦСК (журнали транзакцій, системний журнал і т. ін.) - періодичному відновлюваному резервному копіюванню.

Склад програмних і інформаційних ресурсів, які підлягають резервному копіюванню в ЦСК, визначається службою захисту інформації в ЦСК з участю спеціалістів, що здійснюють обробку інформації, і спеціалістів, що здійснюють технічне обслуговування обладнання ЦСК . Результати роботи оформляються у вигляді таблиці Д.1.

Таблиця Д.1 - Програмні та інформаційні ресурси, що підлягають резервному копіюванню

Найменування інформаційного ресурсу	Де розміщується ресурс в системі	Вид резервного копіювання (період відновлюваного копіювання)	Відповідальний за резервне копіювання і порядок створення резервної копії (технічні засоби, що використовуються)	Де зберігається резервна копія (відповідальний, його телефон)	Порядок використання резервної копії (хто, в яких випадках)

Особа, на яку покладається відповідальність за своєчасність і правильність здійснення резервного копіювання і зберігання копій призначається наказом керівника ЦСК.

Місце і умови зберігання резервних копій, порядок і умови доступу до них визначаються наказом директора ДП "ЕНЕРГОРИНОК".

Безпека резервних копій забезпечується:

- зберіганням резервних копій поза системою (в інших приміщеннях, на іншій території);
- дотриманням заходів фізичного захисту резервних копій;
- регламентацією порядку використання резервних копій.

Склад технічних засобів, які підлягають дублюванню (резервуванню) в ЦСК , визначається службою захисту інформації ЦСК з участю спеціалістів підрозділів, що здійснюють обробку інформації, і спеціалістів підрозділів, що здійснюють технічне обслуговування обладнання ЦСК . Результати роботи оформляються у вигляді таблиці Д.2.

Таблиця Д.2 - Склад технічних засобів, що підлягають дублюванню (резервуванню) в ЦСК

Найменування дубльованого технічного засобу	Де розміщується даний засіб в системі	Вид резерву (груповий або індивідуальний, холодний або гарячий), час готовності резерву	Відповідальний за готовність резервного засобу (період перевірки працездатності резервного засобу)	Порядок використання (включення, настройки) резерву (для різних кризових ситуацій)	Де зберігається резервний засіб (відповідальний, його телефон)

Дублювання ресурсів і резервне копіювання забезпечують відновлення основних функцій системи протягом 1 дня у разі загрозової або серйозної кризової ситуації.

Дублювання ресурсів і резервне копіювання забезпечують відновлення основних функцій системи без припинення функціонування системи у разі звичайної кризової ситуації.