ЗАТВЕРДЖЕНО
Постанова правління
Пенсійного фонду України
11 жовтня 2021р № 28-1

РЕГЛАМЕНТ
роботи інформаційно-телекомунікаційної системи Пенсійного фонду України

І. Загальні положення

1. Регламент роботи інформаційно-телекомунікаційної системи Пенсійного фонду України (далі – Регламент) розроблено відповідно до Законів України "Про інформацію", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про захист персональних даних", "Про збір та облік єдиного внеску на загальнообов'язкове державне соціальне страхування", "Про основні засади забезпечення кібербезпеки України", Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 року № 373, Положення про реєстр застрахованих осіб Державного реєстру загальнообов'язкового державного соціального страхування, затвердженого постановою правління Пенсійного фонду України 18 червня 2014 року № 10-1, зареєстрованого в Міністерстві юстиції України 08 липня 2014 року за № 785/25562, інших нормативно-правових актів у сфері захисту інформації та з урахуванням принципів методології управління інформаційними технологіями CobiT 4.1.

2. Цей Регламент визначає порядок організації доступу, обробки та захисту інформації, внутрішнього контролю процесів та адміністрування ресурсів в інформаційно-телекомунікаційній системі Пенсійного фонду України, основні вимоги до політики безпеки та процедур функціонування інформаційно-телекомунікаційної системи Пенсійного фонду України.

Оброблення інформації з обмеженим доступом здійснюється у порядку, визначеному законодавством.

3. Інформаційно-телекомунікаційна система Пенсійного фонду України призначена для автоматизації одержання, обробки, зберігання та передачі інформації, розпорядником якої відповідно до законодавства є Пенсійний фонд України, автоматизації технологічних процесів та забезпечення інформаційної взаємодії з іншими суб'єктами обміну інформацією в електронній формі, доступу уповноважених осіб до інформаційних ресурсів Пенсійного фонду України.

4. Терміни і скорочення у Регламенті вживаються у таких значеннях:

АВПЗ – антивірусне програмне забезпечення;

АС – автоматизована система;

БД – база даних;

вебпортал – вебпортал електронних послуг Пенсійного фонду України;

ГУ – головні управління Пенсійного фонду України в областях та м. Києві;

ЕОТ – електронна обчислювальна техніка;

ІБ – інформаційна безпека;

ІКІС – Інтегрована комплексна інформаційна система Пенсійного фонду України;

ІТС – інформаційно-телекомунікаційна система Пенсійного фонду України;

користувач – працівник апарату Фонду або ГУ, який у зв'язку з виконанням професійних чи службових або трудових обов'язків має доступ до компонентів ІТС та/або інформації, яка в ній оброблюється;

КСЗІ – комплексна система захисту інформації;

логін – алфавітно-цифровий набір символів, що ідентифікує користувача;

ЛОМ – локальна обчислювальна мережа;

моніторинговий центр – моніторинговий центр функціональних процесів та захисту даних інформаційно-телекомунікаційної системи Пенсійного фонду України, що функціонує на базі Державного підприємства "Інформаційний центр персоніфікованого обліку Пенсійного фонду України";

МОПД – мережа оператора передачі даних;

ОІД – об'єкти інформаційної діяльності;

ОС – операційна система;

СКБД – система керування базами даних;

ПЗ – програмне забезпечення;

Фонд – Пенсійний фонд України;

ЦОД1 – основний центр обробки даних ІТС;

ЦОД2 – резервний центр обробки даних ІТС.

Інші терміни вживаються у значеннях, наведених у Законах України "Про збір та облік єдиного внеску на загальнообов'язкове державне соціальне страхування", "Про основні засади забезпечення кібербезпеки України", "Про захист інформації в інформаційно-телекомунікаційних системах", Положенні про реєстр застрахованих осіб Державного реєстру загальнообов'язкового державного соціального страхування, затвердженому постановою правління Пенсійного фонду України 18 червня 2014 року № 10-1, зареєстрованому в Міністерстві юстиції України 08 липня 2014 року за № 785/25562, Положенні про організацію прийому та обслуговування осіб, які звертаються до органів Пенсійного фонду України, затвердженому постановою правління Пенсійного фонду України від 30 липня 2015 року № 13-1, зареєстрованому в Міністерстві юстиції України 18 серпня 2015 року за № 991/27436.

5. Інформаційно-телекомунікаційна система Фонду організовується за ієрархічним принципом та складається із взаємопов'язаних технологічних

рівнів, які являють собою сукупність ЛОМ апарату Фонду та територіальних управлінь Фонду, що об'єднані в суцільне територіально розподілене телекомунікаційне середовище за допомогою мережі оператора передачі даних. Розміщення технологічних рівнів ІТС повторює організаційно-територіальну структуру Фонду:

1) центральний рівень (апарат Фонду, контакт-центр Фонду, ЦОД1, ЦОД2 та вебпортал);

2) регіональний (обласний) рівень (вузли ГУ);

3) місцевий (районний) рівень (вузли структурних підрозділів ГУ (сервісних центрів) по всій території України);

4) віддалені робочі місця.

Вузли структурних підрозділів ГУ (сервісних центрів) та віддалені робочі місця входять до складу вузлів відповідних ГУ.

6. Володільцем, розпорядником та адміністратором ІТС є Фонд.

Володільцем і розпорядником інформації, що обробляється в ІТС, та БД є Фонд. Розпорядником інформації, що обробляється в ЛОМ територіальних управлінь Фонду, є відповідні територіальні управління Фонду.

Розпорядником бази персональних даних реєстру застрахованих осіб Державного реєстру загальнообов'язкового державного соціального страхування є Державне підприємство "Інформаційний центр персоніфікованого обліку Пенсійного фонду України", що належить до сфери управління Пенсійного фонду України.

7. Програмно-апаратні комплекси, технічні та програмні засоби ІТС, ЛОМ вузлів ГУ, віддалених робочих місць функціонують відповідно до вимог законодавства у сфері захисту інформації.

8. Інтеграцію програмно-апаратних комплексів, технічних та програмних засобів ІТС, ЛОМ вузлів ГУ, віддалених робочих місць до ІТС, передачу даних у системі, тестування та модернізацію інформаційних систем здійснює адміністратор ІТС.

ІІ. Режими функціонування ІТС

1. Основними режимами функціонування ІТС є:

штатний режим роботи – основний режим функціонування, за якого забезпечується повнофункціональна доступність всіх ресурсів та сервісів ІТС;

регламентний режим роботи – режим функціонування в умовах планових регламентних робіт, що призвели (можуть призвести) до зупинки ресурсів та/або сервісів (окремого ресурсу або сервісу) ІТС;

аварійний режим роботи – вихід з ладу одного або декількох компонентів ресурсів та/або сервісів (окремого ресурсу або сервісу) ІТС, що призвело до порушення її повнофункціональної доступності.

2. Тимчасове обмеження повнофункціональної доступності ресурсів та сервісів ІТС (окремого ресурсу або сервісу) допускається у випадках:

виконання регламентних робіт з обслуговування програмно-апаратних комплексів, технічних та програмних засобів, передбачених експлуатаційною документацією;

виникнення позаштатних ситуацій, викликаних відмовами в роботі технічних та/або програмних засобів ІТС, МОПД, а також перевантаженням існуючих технологічних можливостей програмного та апаратного забезпечення.

ІІІ. Основні вимоги політики безпеки ІТС

1. Політика безпеки ІТС спрямована на захист інформації, яка обробляється, зберігається, передається та накопичується (далі – оброблення та зберігання інформації) в інформаційних системах, реєстрах, БД ІТС, та визначає заходи, спрямовані на керування засобами КСЗІ та регламентацію дій користувачів і контроль за цими діями.

2. Відповідно до функціонального призначення в ІТС здійснюється оброблення та зберігання:

відкритої інформації;

конфіденційної інформації (персональні дані);

технологічної інформації.

3. На адміністративному рівні користувачі, які мають доступ до об'єктів захисту ІТС, розподіляються на такі категорії:

адміністратори безпеки;

адміністратори прикладного ПЗ та БД;

адміністратори ІТС та ЛОМ.

4. Залежно від функціонального призначення та рівня захисту робочі станції поділяються на два типи:

робочі станції, за допомогою яких здійснюється інформаційна діяльність з використанням ресурсів ІТС та які входять до складу ІТС (далі – робочі станції складу ІТС);

робочі станції, які використовуються у службовій діяльності, але не входять до складу КСЗІ та не підключені до ІТС (далі – відокремлені робочі станції).

5. Всі компоненти ІТС, конфігурування та налаштування відповідного обладнання підлягають обов'язковому захисту атрибутами ІБ на підставі персональних автентифікаційних даних, якими є: логін, пароль, кваліфікований електронний підпис, сертифікат та особистий ключ CryptoAPI.

6. Логін повинен складатися не менше ніж з 8 символів, де обов'язковою складовою є:

перший символ логіна відповідає рівню користувача:
“U” або “u” – користувацький рівень;
“A” або “a” – адміністративний рівень;
другий та третій – код ГУ;
четвертий – шостий – код структурного підрозділу за довідником системи органів Фонду.

Пароль має складатись не менше ніж з 8 символів та має містити літери у верхньому та нижньому регістрах, цифри та спеціальні символи (за винятком випадків, коли експлуатаційною документацією технічного або програмного засобу передбачено використання паролів іншої складності).

Зміна пароля здійснюється не рідше ніж 1 раз на місяць шляхом зміни пароля в адміністративній підсистемі, нове значення пароля має відрізнятися від попереднього повністю за послідовністю символів.

У випадку позаштатної ситуації, що спричиняє ризик компрометації автентифікаційних даних, пароль змінюється невідкладно.

7. Користувач є відповідальним за складність, збереження, безпечну та своєчасну зміну пароля.

8. Робочі станції повинні мати унікальне ім’я та IP-адресу або інші статичні ідентифікатори, про що ведеться відповідний облік адміністратором ЛОМ.

9. Підключення робочих станцій до ІТС здійснюється виключно адміністраторами ЛОМ згідно з відповідною експлуатаційною документацією.

Забороняється несанкціоноване підключення або зміна унікального імені та/або IP-адреси робочих станцій, інших статичних ідентифікаторів, підключення робочих станцій, які не знаходяться на обліку.

10. На всі сегменти ІТС створюються графічні схеми фізичного та логічного підключення телекомунікаційного обладнання, робочих станцій, серверів, інших мережевих пристроїв. Адміністраторами ЛОМ складається та підтримується в актуальному стані таблиця прив’язки MAC-адрес робочих станцій та іншого мережевого обладнання, їх IP-адрес та портів мережевих комутаторів.

11. Виконання завдань на робочих станціях складу ІТС повинне забезпечуватись у функціонально замкнутому середовищі, в межах якого доступ забезпечується лише до ресурсів ІТС, що є необхідним для виконання службових обов’язків, та в межах контрольованої зони, визначеної документацією КСЗІ.

12. На відокремлених робочих станціях та робочих станціях складу ІТС доступ користувача до інтерфейсів робочої станції здійснюється після

персоніфікованої користувацької автентифікації за правилами, визначеними пунктами 5 та 6 цього розділу.

13. Робоча станція складу ІТС закріплюється за користувачем (користувачами), який є відповідальним за дотримання техніки безпеки, інструкції виробника або іншої експлуатаційної документації при використанні такої робочої станції.

Користувачам користувацького рівня забороняється самостійне встановлення ПЗ або внесення змін до вже встановлених компонентів ПЗ.

14. У випадку залишення без нагляду працюючої робочої станції в незамкнутому приміщенні (кімнаті, кабінеті) користувач повинен заблокувати доступ до робочої станції. Розблокування здійснюється через повторну процедуру авторизації за допомогою атрибутів ІБ.

У випадках присутності у приміщенні (кімнаті, кабінеті) третіх осіб користувач повинен дотримуватись на такій робочій станції принципу "чистого екрану".

15. Забороняється допуск до робочої станції осіб без дотримання процедур, визначених цим Регламентом.

16. Антивірусний захист ІТС повинен здійснюватися виключно засобами антивірусного захисту із системою централізованого керування, які за результатами державної експертизи мають чинні атестат відповідності або експертний висновок.

17. АВПЗ налаштовується виключно адміністраторами безпеки, зміна налаштувань здійснюється з використанням атрибутів ІБ. Забороняється експлуатація ІТС та відокремлених робочих станцій, без встановленого та налаштованого або з тимчасово відключеним АПВЗ.

18. У випадках виявлення АВПЗ шкідливих об'єктів або інших загроз користувачі повинні невідкладно повідомляти про це адміністраторів безпеки.

19. Не допускається використання в ІТС неперевірених або недозволених АПВЗ знімних зовнішніх носіїв інформації (за винятком випадків зчитування даних із засобів електронної ідентифікації особи).

Використання знімних зовнішніх носіїв інформації в ІТС здійснюється з обов'язковою реєстрацією їх ідентифікаційних даних ОС робочих станцій.

20. Електронне листування, пов'язане з виконанням службових обов'язків, повинне здійснюватися виключно з поштових доменів pfu.gov.ua та ca.pfu.gov.ua. Доступ до відповідних поштових ресурсів здійснюється за правилом, визначеним пунктом 5 цього розділу.

21. Не допускається відкривання вкладень електронних листів без перевірки їх вмісту АВПЗ, або перехід за гіперпосиланнями в електронних листах, отриманих від невідомих джерел.

22. Забороняється збереження атрибутів ІБ в кеші браузера.

IV. Організація доступу до інформації та програмного забезпечення в ІТС

1. Доступ до прикладних підсистем, програмного забезпечення, систем захисту ІТС, відокремлених робочих станцій здійснюється за допомогою створеного в підсистемі адміністрування прав доступу облікового запису користувача на підставі персональних автентифікаційних даних: логіна, пароля, кваліфікованого електронного підпису, сертифіката та особистого ключа CryptoAPI.

2. Обсяг доступу для оброблення інформації, зміни конфігурацій, налаштувань:

в прикладних підсистемах ІТС визначається набором ролей облікового запису користувача в кожній з прикладних підсистем ІТС;

в програмному забезпеченні та системах захисту ІТС, відокремлених робочих станцій визначається технічними умовами доступу користувача, передбаченими експлуатаційною документацією програмних чи технічних засобів.

Доступ користувачів розподіляється на такі рівні:

користувацький;

адміністративний.

3. Створення нового облікового запису користувача в прикладних підсистемах ІТС користувацького рівня здійснюється на підставі розпорядчого акта Фонду або ГУ про призначення працівника на посаду у Фонді або ГУ відповідно.

Створення облікового запису користувача в прикладних підсистемах ІТС адміністративного рівня, користувача програмного забезпечення, систем захисту ІТС, відокремлених робочих станцій користувацького та адміністративного рівнів, надання відповідних ролей та прав доступу здійснюється на підставі розпорядчого акта Фонду або ГУ, що визначає відповідне виконання обов'язків.

4. Обліковий запис може створюватись для вже призначених працівників в разі виникнення відповідних змін у програмному або технічному забезпеченні або зміни у посадових обов'язках працівника, у тому числі у разі виконання обов'язків тимчасово відсутніх працівників або за вакантною посадою.

У цьому випадку створення облікового запису, надання ролей та прав доступу, їх зміна здійснюється на підставі службової записки керівника самостійного структурного підрозділу Фонду або ГУ, погодженої відповідно

заступником Голови правління Фонду або заступником начальника ГУ згідно із розподілом обов'язків, не пізніше наступного робочого дня після отримання такої службової записки.

5. Блокування облікового запису користувача здійснюється:

не пізніше закінчення робочого часу дня звільнення працівника або втрати чинності акта Фонду чи ГУ, на підставі якого такий обліковий запис було створено;

невідкладно – при виявленні обставин компрометації облікового запису користувача;

в терміни, визначені в службовій записці, зазначеній у пункті 4 цього розділу.

6. При створенні облікового запису новий користувач під особистий підпис підлягає ознайомленню із режимом обробки інформації, вимоги щодо захисту якої встановлені законом, та забороною розголошувати інформацію з обмеженим доступом, отриману у зв'язку з виконанням службових обов'язків.

7. Користувачам забороняється розголошувати у будь-який спосіб дані про ІТС, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, крім випадків, передбачених законом. Така заборона чинна після припинення ними відповідної діяльності.

8. Створення та блокування користувачів, надання їм ролей та прав доступу, перевірка дій користувачів з програмним забезпеченням і системами захисту ІТС, на відокремлених робочих станціях покладається на підрозділ, до повноважень якого віднесено:

формування, ведення, адміністрування, організаційно-методичну підтримку, супровід та поточну експлуатацію ПЗ, прикладних підсистем ІТС, баз даних, що використовуються органами Фонду, комп'ютерного та мережевого обладнання;

забезпечення кіберзахисту та безпеки інформаційних технологій ІТС, захисту інформації в ІТС (далі – відповідальний підрозділ).

V. Організація захисту інформації в ІТС

1. Організаційне забезпечення завдань щодо супроводження КСЗІ в ІТС, здійснення контролю за її функціонуванням, а також заходи щодо експлуатації, обслуговування та підтримки працездатності КСЗІ, контролю за станом захищеності інформації в ІТС передбачають:

аналіз стану обробки інформації в ІТС з метою виявлення можливих загроз ІБ, формування моделі загроз, визначення заходів, спрямованих на реалізацію політики безпеки інформації, забезпечення функціонування ІТС;

організацію та координацію робіт, пов'язаних із захистом інформації в ІТС;

підтримку необхідного рівня захищеності інформації, ресурсів і технологій;

розроблення проєктів розпорядчих документів, згідно з якими реалізується захист інформації в ІТС;

організацію робіт зі створення (модернізації) і супроводження КСЗІ компонентів ІТС;

професійну підготовку і підвищення кваліфікації відповідальних осіб з питань захисту інформації;

формування у користувачів сприйняття необхідності виконання вимог нормативно-правових актів, нормативних і розпорядчих документів, що стосуються вимог захисту інформації.

2. Не пізніше 01 листопада відповідальним підрозділом Фонду Голові правління Фонду подається на затвердження план проведення робіт із захисту інформації в ІТС на наступний рік, який передбачає відповідний календарний графік заходів та відповідальних виконавців.

Не пізніше 10 робочих днів після затвердження план проведення робіт із захисту інформації в ІТС на відповідний рік надсилається ГУ для організації його виконання в межах компетенції.

На основі плану проведення робіт із захисту інформації в ІТС відповідальний підрозділ ГУ розробляє та подає на затвердження начальнику ГУ план проведення робіт із захисту інформації на вузлах ГУ на наступний рік.

3. План проведення робіт із захисту інформації має включати заходи щодо:

перевірки функціонування та налаштувань мережевого обладнання, модуля криптозахисту, серверного обладнання;

перевірки функціонування та налаштувань джерел безперебійного живлення ЛОМ та серверного обладнання;

перевірки функціонування та налаштувань політик безпеки ЛОМ;

перевірки вхідного та вихідного трафіку на робочих станціях та в ЛОМ на факти можливого віддаленого керування із-за меж контрольованої зони та наявності відповідного програмного забезпечення та/або налаштувань віддаленого доступу до файлів і додатків;

перевірки наявності службових носіїв інформації;

перевірки можливості запуску виконуваних файлів ".exe", ".bat", ".cmd", ".vbs", ".docm",".xlsm" на робочих станціях користувачів з директорій %APPDATA%, %TEMP%;

обстеження серверних приміщень щодо дотримання в них температурного режиму, наявності засобів протипожежного реагування;

ведення та підтримання в актуальному стані формулярів ОІД, документації щодо контрольованих зон ОІД;

здійснення контролю за інстальованим ПЗ на робочих станціях користувачів на відповідність встановленим вимогам КСЗІ;

перевірки стану захисних наклейок, пломб та інших засобів, що є індикаторами цілісності обладнання ЛОМ ІТС;

організації супроводження резервних копій баз даних, їх збереження.

4. Щопівроку, до 15 липня та 15 січня, відповідальним підрозділом ГУ на розгляд та затвердження начальнику ГУ подається звіт про виконання плану робіт із захисту інформації на вузлах ГУ, аналітична інформація про стан ІБ в ГУ, які після затвердження надсилаються до Фонду.

Узагальнений відповідальним підрозділом Фонду звіт про виконання плану робіт із захисту інформації в ІТС, аналітична інформація про стан ІБ в ІТС та пропозиції для подальшого удосконалення організації захисту інформації подаються на розгляд Голові правління Фонду до 25 липня та 25 січня.

5. При створенні КСЗІ або її модернізації необхідні заходи повинні включати:

проведення обстеження середовищ функціонування;

розробку технічного завдання на КСЗІ або доповнення до технічного завдання на КСЗІ;

модернізацію технічного проєкту КСЗІ (за необхідності);

модернізацію експлуатаційної документації КСЗІ (за необхідності);

проведення попередніх випробувань КСЗІ;

введення в експлуатацію КСЗІ.

6. КСЗІ ІТС в обов'язковому порядку має передбачати такі документи, як:

Модель загроз;

Модель порушника;

План захисту.

7. Введення в експлуатацію створеної або модернізованої КСЗІ здійснюється на підставі розпорядчого акта Фонду. Введення в експлуатацію КСЗІ вузлів ГУ здійснюється на підставі розпорядчого акта ГУ.

8. Не рідше двох разів на рік відповідальними підрозділами Фонду та ГУ здійснюються заходи для формування у користувачів сприйняття необхідності виконання вимог нормативно-правових актів, нормативних і розпорядчих документів, що стосуються сфери захисту інформації.

Роз'яснювальна робота з користувачами повинна включати, зокрема:

висвітлення основних положень Моделі загроз та Моделі порушника;

питання використання загальносистемного та прикладного ПЗ на робочих станціях;

питання використання ключів кваліфікованого електронного підпису у службовій діяльності.

9. Не рідше одного разу на рік за окремим графіком відповідальними підрозділами Фонду та ГУ здійснюється обстеження відповідності вимогам КСЗІ налаштування апаратного забезпечення ІТС та вузлів ГУ, операційних систем та робочих станцій. Результати обстеження оформлюються протоколами із зазначенням проведених змін у конфігурації та налаштуваннях.

10. Відповідальним підрозділом Фонду забезпечується комплекс заходів для безперервності дії КСЗІ ІТС, ЦОД1, ЦОД2, вебпорталу, Електронного реєстру листків непрацездатності, Контакт-центру Фонду, моніторингового центру, організаційно-технічного рішення АС оцифрування архівів пенсійних справ та зберігання електронних документів, відповідність яких підтверджується за результатами державної експертизи або чинним експертним висновком.

11. Завдання, функції, права та обов'язки щодо здійснення заходів стосовно кібербезпеки, кіберзахисту та безпеки інформаційних технологій ІТС, проведення організаційних та інженерно-технічних заходів із побудови КСЗІ визначаються в посадових інструкціях відповідних працівників.

VI. Регламент проведення робіт з ресурсами ІТС

1. Створення (модернізація) ПЗ має відповідати умовам технічних вимог на його створення (модернізацію), загальним вимогам до програмних продуктів, які закуповуються та створюються на замовлення державних органів, нормативно-правовій базі, яка регламентує діяльність у сфері пенсійного забезпечення та ведення обліку осіб, які підлягають загальнообов'язковому державному соціальному страхуванню.

2. Створене (модернізоване) ПЗ повинне відповідати вимогам функціональної придатності, ефективності роботи, сумісності, зручності використання, надійності, безпеки, зручності супроводу, а також оцінювання з позиції користувача.

3. Створене (модернізоване) програмне забезпечення до впровадження його в промислову експлуатацію підлягає випробуванню, за результатами якого складається відповідний акт.

4. Гарантійний строк на створене (модернізоване) прикладне ПЗ має становити не менше 12 місяців з дати його прийняття за актом приймання-передачі.

5. Регламентні роботи, в тому числі встановлення (оновлення) версій ПЗ, окремих компонентів програмно-апаратних і програмних засобів ІТС, що передбачає обмеження повнофункціональної доступності прикладних підсистем (окремої прикладної підсистеми) ІТС, здійснюється на підставі

службової записки заступника Голови правління Фонду з питань цифрового розвитку, цифрових трансформацій і цифровізації, погодженої Головою правління Фонду.

6. Проведення регламентних робіт на вузлах ГУ здійснюється за погодженням з начальником відповідного органу Фонду.

7. Проведення регламентних робіт з обслуговування програмно-апаратних і програмних засобів ІТС допускається у неробочий час.

VII. Адміністрування ресурсів ІТС

1. Адміністрування ресурсів ІТС, ПЗ та програмних комплексів, мережевих сервісів, серверів, мережі та комп'ютерного парку, баз даних, центрів обробки даних, сервісів АС, Інтернет-вузла, вебпорталу, антивірусного та мережевого захисту інформації та засобів безпеки, засобів електронного зв'язку, пристроїв інших електронних засобів комунікації здійснюється адміністраторами.

2. Залежно від функцій та обов'язків, адміністратори ІТС визначаються за такими категоріями:

адміністратори безпеки;
адміністратори БД та прикладного ПЗ;
адміністратори ЛОМ вузлів ІТС;
адміністратори окремої АС.

3. Залежно від функціональних напрямів та об'єктів адміністрування, завдань, прав і обов'язків адміністраторів, адміністратори розподіляються на:

адміністратор безпеки ІТС;
адміністратор БД та прикладного ПЗ ІТС;
адміністратор ЛОМ вузла ІТС;
адміністратор програмно-апаратного комплексу Контакт-центру Фонду;
адміністратор безпеки програмно-апаратного комплексу Контакт-центру Фонду;
адміністратор ЦОД1;
адміністратор безпеки ЦОД1;
адміністратор БД та прикладного ПЗ ЦОД1;
адміністратор ЦОД2;
адміністратор безпеки ЦОД2;
адміністратор БД та прикладного ПЗ ЦОД2;
адміністратор безпеки вебпорталу;
адміністратор БД вебпорталу;
адміністратор вебпорталу;
адміністратор системи вебпорталу.

4. Адміністратор безпеки:

1) створює облікові записи користувачів адміністративного рівня у прикладних підсистемах ІТС, користувачів програмного забезпечення, систем захисту ІТС, адміністраторів та користувачів окремої АС та відокремлених робочих станцій, надання відповідних ролей та прав доступу;

2) контролює дії користувачів з відповідними програмними та технічними засобами;

3) не рідше одного разу на місяць здійснює аналіз даних журналів роботи компонентів ІТС з метою виявлення можливих порушень вимог захисту інформації;

4) аналізує стан захищеності компонентів ІТС та окремих прикладних підсистем;

5) не рідше одного разу на квартал здійснює контрольні перевірки робочих станцій користувачів, серверів та засобів захисту компонентів ІТС з метою виявлення можливих обставин, що сприяють порушенню вимог захисту інформації;

6) контролює:

фізичне збереження засобів та обладнання захисту компонентів ІТС;

стан засобів та систем захисту компонентів ІТС, їхні параметри та конфігурацію;

стан захисних наклейок, пломб та інших засобів, що є індикаторами цілісності засобів та обладнання захисту компонентів ІТС;

правильність використання користувачами засобів захисту компонентів ІТС;

встановлення, використання, зберігання та розповсюдження в ІТС програмних засобів;

7) за необхідності проводить із користувачами роз'яснювальну роботу з питань дотримання вимог захисту інформації та ІБ;

8) повідомляє керівництво відповідального підрозділу про усі спроби порушення захисту ІТС;

9) не рідше одного разу на квартал надає керівництву відповідального підрозділу звітну та аналітичну інформацію про стан захищеності ІТС, виявлені випадки порушень встановлених вимог захисту інформації;

10) має право:

брати участь у контрольних заходах, що пов'язані з питаннями захищеності компонентів ІТС;

забороняти встановлення на серверах та робочих станціях нерегламентованого програмного та апаратного забезпечення;

ініціювати блокування облікового запису користувача, що здійснив несанкціонований доступ до ресурсів, які захищаються, чи порушив інші вимоги захисту інформації;

згідно з відповідною експлуатаційною документацією, документацією КСЗІ змінювати налаштування конфігураційних файлів ОС робочих станцій, серверів, СКБД та активного мережевого обладнання;

контролювати вміст журналів ОС робочих станцій, серверів, активного мережевого обладнання, засобів захисту, систем антивірусного захисту.

5. Адміністратор БД та прикладного ПЗ:

1) здійснює:

резервування БД, контроль за процесами резервування;

не рідше одного разу на місяць аналіз даних журналів роботи СКБД ІТС з метою виявлення можливих відмов, збоїв та помилок у ПЗ;

контрольні заходи з питань функціонування робочих станцій та тестування правильності функціонування засобів захисту СКБД з метою виявлення помилок і збоїв у програмному та апаратному забезпеченні;

регулярні оновлення компонентів СКБД та відповідних клієнтських модулів;

2) створює та блокує користувачів користувацького рівня, надає їм ролі та права доступу, контролює їх дії в прикладних підсистемах відповідно до вимог, визначених розділом ІІІ Регламенту;

3) повідомляє керівництво відповідального підрозділу про усі спроби порушення захисту СКБД, їх відмови та збої;

4) за необхідності проводить із користувачами роз'яснювальну роботу з питань правильного використання БД.

6. Адміністратор ЛОМ вузла ІТС:

1) здійснює:

контроль працездатності компонентів віддалених робочих станцій, компонентів та ЛОМ вузла ІТС в цілому;

контроль актуальності ПЗ та ОС на серверах, робочих станціях ЛОМ вузла ІТС та віддалених робочих станціях;

технічне обслуговування апаратного і програмного забезпечення ЛОМ вузла ІТС;

резервування елементів ЛОМ вузла ІТС та відновлення їх працездатності;

не рідше одного разу на місяць аналіз даних журналів роботи компонентів ЛОМ вузла ІТС з метою виявлення можливих порушень функціонування компонентів ЛОМ вузла ІТС;

налаштування апаратного і програмного забезпечення ЛОМ вузла ІТС;

2) контролює:

фізичне збереження засобів та обладнання ЛОМ вузла ІТС;

стан захисних наклейок, пломб та інших засобів, що є індикаторами цілісності обладнання ЛОМ вузла ІТС та віддалених робочих станцій;

правильність використання користувачами робочих станцій, інших компонентів ЛОМ вузла ІТС;

встановлення, використання, зберігання та розповсюдження у ЛОМ вузла ІТС та віддалених робочих станціях програмних засобів;

3) ініціює процес оновлення застарілого ПЗ та ОС ЛОМ вузла ІТС та віддалених робочих станцій;

4) повідомляє адміністратора безпеки та керівництво відповідального підрозділу про виявлені факти, що можуть створювати ризики порушення захисту інформації та ІБ ЛОМ вузла ІТС та віддалених робочих станцій;

5) має право:

брати участь у контрольних заходах з питань функціонування ЛОМ вузла ІТС;

забороняти встановлення на серверах, робочих станціях ЛОМ вузла ІТС та віддалених робочих станціях нерегламентованого програмного та апаратного забезпечення;

ініціювати блокування облікового запису користувача, що здійснив несанкціонований доступ до програмно-апаратних комплексів та програмних засобів, порушив інші вимоги захисту інформації, використовував компоненти ЛОМ вузла ІТС не за призначенням;

змінювати налаштування конфігураційних файлів ОС робочих станцій, серверів, СКБД та активного мережевого обладнання ЛОМ вузла ІТС;

контролювати вміст журналів ОС робочих станцій, серверів, активного мережевого обладнання ЛОМ вузла ІТС щодо випадків збоїв, помилок та відмов;

у разі необхідності проводити роз'яснювальну роботу із користувачами з питань використання компонентів ЛОМ вузла ІТС.

7. Адміністратор окремої АС:

1) контролює:

працездатність програмно-апаратного комплексу окремої АС;

фізичне збереження засобів та обладнання програмно-апаратного комплексу окремої АС;

стан захисних наклейок, пломб та інших засобів, що є індикаторами цілісності обладнання програмно-апаратного комплексу окремої АС;

правильність використання користувачами робочих станцій, інших компонентів програмно-апаратного комплексу окремої АС;

2) здійснює:

технічне обслуговування апаратного і системного забезпечення програмно-апаратного комплексу окремої АС;

резервування елементів програмно-апаратного комплексу окремої АС та відновлення їх працездатності;

не рідше одного разу на місяць аналіз даних журналів роботи компонентів програмно-апаратного комплексу окремої АС з метою виявлення можливих порушень функціонування компонентів програмно-апаратного комплексу окремої АС;

налаштування апаратного і програмного забезпечення програмно-апаратного комплексу окремої АС;

3) має право:

брати участь у контрольних заходах з питань функціонування програмно-апаратного комплексу окремої АС;

забороняти встановлення на серверах та робочих станціях програмно-апаратного комплексу окремої АС нерегламентованого програмного та апаратного забезпечення;

ініціювати блокування облікового запису користувача, що здійснив несанкціонований доступ до програмно-апаратних комплексів та програмних засобів, порушив інші вимоги захисту інформації, використовував компоненти програмно-апаратного комплексу окремої АС не за призначенням;

змінювати налаштування конфігураційних файлів ОС робочих станцій, серверів, СКБД та активного мережевого обладнання програмно-апаратного комплексу окремої АС;

контролювати вміст журналів ОС робочих станцій, серверів, активного мережевого обладнання програмно-апаратного комплексу окремої АС щодо випадків збоїв, помилок та відмов;

не допускати до роботи на робочих станціях та серверах програмно-апаратного комплексу окремої АС сторонніх осіб;

у разі необхідності проводити роз'яснювальну роботу із користувачами з питань використання компонентів програмно-апаратного комплексу окремої АС.

8. Адміністраторам забороняється:

розголошувати власні атрибути доступу до засобів ІТС або вводити їх у спосіб, що надає змогу ознайомитися з ними іншим особам;

фіксувати та зберігати облікові дані користувачів на знімних носіях та повідомляти їх іншим особам, ніж користувач;

фіксувати та зберігати вміст баз даних ІТС та файлів робочих станцій на непідконтрольних знімних носіях та передавати їх стороннім особам;

залишати свою робочу станцію та увімкнені незаблоковані технічні засоби ІТС без контролю;

надавати користувачам ролі та/або права доступу без визначених підстав;

використовувати технічні засоби ІТС не за призначенням;

застосовувати ПЗ ІТС, яке має ознаки неправильного функціонування;

несанкціоновано встановлювати, створювати, запускати на виконання на технічних засобах ІТС інше ПЗ, окрім того, що передбачено для функціонування ІТС;

самовільно змінювати конфігурацію мережі, технологій захисту інформації чи встановлювати нерегламентовані засоби захисту.

9. Налаштування, інсталяція та деінсталяція компонентів програмних та програмно-апаратних засобів ІТС згідно з експлуатаційною документацією та документацією КСЗІ здійснюється виключно відповідним адміністратором.

10. Для кожного із адміністраторів за відповідним напрямом та технологічним рівнем ІТС відповідальним підрозділом розробляється інструкція з адміністрування, яка затверджується Головою правління Фонду або начальником ГУ відповідно.

Ознайомлення адміністратора з інструкцією з адміністрування здійснюється засобами системи електронного документообігу з використанням кваліфікованого електронного підпису відповідної посадової особи, а у разі складення інструкції з адміністрування у паперовій формі – із проставленням на першому примірнику підпису адміністратора про ознайомлення.

11. Відповідальним підрозділом відповідно до затверджених інструкцій з адміністрування ведеться актуальний перелік з персональним складом основних та дублюючих адміністраторів за категоріями та напрямами.

VIII. Внутрішній контроль процесів в ІТС

1. Внутрішній контроль процесів в ІТС передбачає такі етапи:
планування та затвердження заходів контролю;
організація заходів контролю та моніторингу;
проведення та супроводження процедур контролю і моніторингу;
аналіз результатів;
звітування;
формування пропозицій для удосконалення.

2. Відповідно до цього Регламенту внутрішньому контролю підлягають організація та стан:

адміністрування, організаційно-методичної підтримки, супроводу та поточної експлуатації ПЗ, прикладних підсистем ІТС, БД, що використовуються органами Фонду, ЛОМ, ОС, комп'ютерного та мережевого обладнання;

забезпечення кіберзахисту та безпеки інформаційних технологій ІТС, захисту інформації в ІТС.

Аналізу стану внутрішнього контролю процесів в ІТС підлягають також результати контрольних заходів стосовно ІТС, проведених зовнішніми суб'єктами.

3. Щороку до 01 листопада відповідальним підрозділом Фонду на затвердження Голові правління Фонду подається план заходів щодо внутрішнього контролю процесів в ІТС на наступний рік, який не пізніше 10 робочих днів після затвердження надсилається ГУ для організації виконання в межах компетенції.

На основі плану заходів щодо внутрішнього контролю процесів в ІТС відповідальний підрозділ ГУ розробляє та подає на затвердження начальнику ГУ план заходів щодо внутрішнього контролю процесів на вузлах ГУ на відповідний рік.

4. Щопівроку відповідальний підрозділ ГУ подає на розгляд та затвердження начальнику ГУ аналітичний звіт про стан внутрішнього

контролю процесів на вузлах ГУ та після затвердження надсилає його до Фонду у строк до 15 липня та 15 січня.

Узагальнений відповідальним підрозділом Фонду аналітичний звіт про стан внутрішнього контролю процесів в ІТС та пропозиції для подальшого удосконалення його організації подаються на розгляд Голові правління Фонду до 25 липня та 25 січня.

5. Не рідше одного разу на рік за окремим графіком проводиться обстеження інфраструктури ІТС згідно з переліком питань, які передбачають:

загальні відомості (дані про особу, відповідальну за проведення обстеження);

відомості про кадрове забезпечення (дані про штатну та фактичну чисельність працівників відповідальних підрозділів відповідно Фонду та ГУ, в тому числі до повноважень яких належить адміністрування безпеки, адміністрування локальної обчислювальної мережі, адміністрування прикладних систем, здійснення заходів щодо кібербезпеки, кіберзахисту та безпеки інформаційних технологій ІТС, проведення організаційних та інженерно-технічних заходів із побудови КСЗІ);

відомості про апаратне забезпечення (дані про стан наявного апаратного забезпечення);

відомості про серверні приміщення (дані про стан серверних приміщень, в тому числі щодо обладнання їх засобами пожежогасіння, охоронною сигналізацією, системою оповіщення під час пожежі, наявності схем монтажу та розміщення обладнання, опису встановленого ПЗ та мережевих підключень, журналу відвідування);

відомості про підключення до мережі Інтернет;

відомості про програмне забезпечення (дані про операційні системи загального призначення, операційні системи комп'ютерних мереж, прикладне ПЗ);

відомості про адміністрування доступу до прикладних підсистем (дані про користувачів, в тому числі тих, які мають доступ щодо внесення або візування змін по кожному із прикладних ресурсів).

За результатами обстеження складається звіт, який подається на розгляд Голові правління Фонду.

6. Процедури виконання завдань моніторингу працездатності функціональних, прикладних та системних процесів в ІТС, стану інформаційних потоків, процесів керування обслуговуванням відвідувачів, аналітики відеоспостереження, виявлення, аналізу, реагування та попередження кіберінцидентів здійснюються моніторинговим центром згідно з Регламентом роботи моніторингового центру функціональних процесів та захисту даних інформаційно-телекомунікаційної системи Пенсійного фонду України, затвердженим наказом Пенсійного фонду України від 18 червня 2020 року № 48 (далі – регламент моніторингового центру).

7. Контрольні заходи щодо виконання регламентних робіт з ресурсами ІТС здійснюються відповідальними підрозділами.

IX. Порядок дій та інформування в аварійному режимі роботи ІТС або при настанні позаштатних ситуацій

1. Аварійна ситуація класифікується за такими ознаками, як вихід із ладу одного або декількох компонентів апаратного чи програмного забезпечення інфраструктури ІТС, що призвів до порушення роботи, цілісності, доступності прикладних підсистем (окремої прикладної підсистеми) ІТС, працездатності програмних та технічних засобів ІТС, прикладних серверів та сервісів, працездатності сервісних центрів та віддалених робочих місць.

Позаштатна ситуація класифікується за такими ознаками, як недоступність, обмеження доступності прикладних підсистем (окремої прикладної підсистеми) ІТС, працездатності програмних та технічних засобів ІТС, прикладних серверів та сервісів, вебпорталу, протягом 10 хвилини.

2. Повідомлення про аварійні та позаштатні ситуації надсилаються у такому порядку:

1) адміністратори ГУ інформують працівників відповідального підрозділу Фонду невідкладно;

2) моніторинговий центр інформує Фонд – у порядку, визначеному регламентом роботи моніторингового центру;

3) адміністратори Фонду інформують керівництво відповідального підрозділу Фонду у всіх випадках невідкладно;

4) керівництво відповідального підрозділу Фонду інформує керівництво Фонду невідкладно:

про настання аварійної ситуації;

у разі, якщо позаштатна ситуація може спричинити значні наслідки або недоступність, обмеження доступності прикладних підсистем (окремої прикладної підсистеми) ІТС, працездатності програмних та технічних засобів ІТС, прикладних серверів та сервісів, вебпорталу, становить більше 20 хвилини.

3. Повідомлення, передбачені пунктом 2 цього розділу, формуються для відповідного кореспондента засобами мобільного зв'язку (голосовий зв'язок, СМС-повідомлення, повідомлення через месенджери тощо).

4. По кожному факту настання аварійної ситуації для з'ясування причин та умов, що призвели до порушення штатного режиму функціонування ІТС, залежно від технологічного рівня ІТС, на підставі розпорядчого акта Фонду або ГУ відповідно утворюється комісія.

За результатами роботи комісії складається звіт про усунення наслідків інциденту і пропозиції щодо запобіжних заходів, необхідних для попередження порушення штатного режиму функціонування ІТС у майбутньому, який

подається на затвердження Голові правління Фонду або начальнику ГУ відповідно.

X. Документування подій

1. Дані про виявлені аварійні та позаштатні ситуації та вжиті заходи підлягають документуванню адміністратором безпеки.

2. Документуванню обов'язково підлягає така інформація:
дата та час виявлення аварійної або позаштатної ситуації;
короткий опис аварійної або позаштатної ситуації;
класифікація аварійної або позаштатної ситуації;
ступінь впливу аварійної або позаштатної ситуації;
здійснені дії для усунення або виправлення аварійної або позаштатної ситуації, упередження настання негативних наслідків.

3. Документування здійснюється в журналах за формою згідно з додатком (додається), крім випадків, передбачених пунктом 6 розділу VIII цього Регламенту, та реєстрації подій, що здійснюється вбудованими засобами ОС та ПЗ.

4. Журнали ведуться в електронній формі.

5. Контроль стану документування здійснюється керівником відповідального підрозділу не рідше одного разу на квартал.

В. о. директора Департаменту
з питань цифрового розвитку,
цифрових трансформацій
і цифровізації **Валентина БОРШОВСЬКА**

Додаток 1
до Регламенту роботи
інформаційно-телекомунікаційної
системи Пенсійного фонду
України

(пункт 2 розділу X)

Журнал

обліку аварійних або позаштатних ситуацій _____

№ з/п	Дата та час виявлення аварійної або позаштатної ситуації	Місце виявлення аварійної або позаштатної ситуації	ПІБ адміністратора безпеки	Короткий опис аварійної або позаштатної ситуації	Класифікація аварійної або позаштатної ситуації	Ступінь впливу аварійної або позаштатної ситуації па функціонування вузла ІТС	Здійснені дії для усунення або виправлення аварійної або позаштатної ситуації, упередження настання негативних наслідків	Дата та час передання даних про аварійну або позаштатну ситуацію на центральний рівень	ПІБ адресата інформації на центральному рівні	Рекомендації та/чи вчинені дії для усунення аварійної або позаштатної ситуації	Відмітка про контроль	Примітки
1	2	3	4	5	6	7	8	9	10	11	12	13