ЗАТВЕРДЖУЮ

Директор
ТОВ «Доктор Елекс»

_____ П.О. Коновалов
«__» _____ 2020 р.

ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА «МЕДИЧНА ІНФОРМАЦІЙНА СИСТЕМА «ДОКТОР ЕЛЕКС»

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ

Інструкція про порядок підключення технічних майданчиків закладів охорони здоров'я та аптечних закладів

UA.38582529.КСЗІ.00001.ІЗОЗ

2020

Інв. № орига. | Підп. та дата | Взам. інв. № | Інв. № дубл | Підп. та дата

ЗМІСТ

ТЕРМІНИ ТА ВИЗНАЧЕННЯ

В цьому документі використовуються терміни та визначення, визначені в:

– ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення;

– НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Інструкція про порядок підключення технічних майданчиків закладів охорони здоров'я та аптечних закладів до інформаційно-телекомунікаційної системи «Медична інформаційна система «Доктор Елекс» (далі – ІТС).

Інструкція розроблена відповідно до документу «План захисту інформації. UA.38582529.КСЗІ.00001.ПЗІ» в частині реалізації політики безпеки в ІТС і повинна розглядатись в сукупності усіх документів політики безпеки інформації, визначеної в зазначеному документі.

2. ПОРЯДОК РОЗГОРТАННЯ ТЕХНІЧНИХ МАЙДАНЧИКІВ ЗАКЛАДІВ ОХОРОНИ ЗДОРОВ'Я ТА АПТЕЧНИХ ЗАКЛАДІВ

Технічні майданчики закладів охорони здоров'я та аптечних закладів являють собою окремі робочі станції медичних працівників закладів охорони здоров'я та аптечних закладів (далі – працівники), які можуть бути об'єднані в локальні обчислювальні мережі та мають підключення до мережі Інтернет.

В якості робочих станцій працівників повинні використовуватись персональні електронні обчислювані машини (далі – ЕОМ), мобільні ЕОМ (ноутбуки), а також планшетні комп'ютери та смартфони за умови відповідності їх технічних характеристик вимогам до умов застосування прикладного програмного забезпечення «Медична інформаційна система «Доктор Елекс» (визначаються згідно з експлуатаційною документацією на прикладне програмне забезпечення «Медична інформаційна система «Доктор Елекс»). На робочих станціях працівників здійснюється лише обробка інформації, зберігання будь-яких даних на робочих станціях або інших засобах зберігання даних закладу охорони здоров'я чи аптечного закладу не допускається.

Підключення робочих станцій до ІТС «Медична інформаційна система «Доктор Елекс» та робота працівників здійснюється за умови виконання наступних заходів:

- наявність чинного договору (угоди) на право роботи в ІТС;
- використання на робочій станції ліцензійних засобів антивірусного захисту інформації, які встановлені та налаштовані в порядку, визначеному їх виробником;
- своєчасне оновлення баз антивірусних сигнатур засобів антивірусного

захисту інформації в порядку, визначеному їх виробником (не перевищує 1-2 дні);

- використання засобів розмежування доступу до робочої станції:
  - для персональних ЕОМ, мобільних ЕОМ (ноутбуків) – використання для кожного працівника, закріпленого за відповідною ЕОМ, окремого облікового запису, обов'язкова ідентифікація працівника за логіном/паролем, мінімальна довжина паролю 6 символів, в якості значень символів паролю обов'язково слід використовувати букви латинського алфавіту та цифри;
  - для планшетних комп'ютерів та смартфонів – обов'язкова ідентифікація працівника (за кодом доступу, графічним ключем, паролем доступу або іншим засобом ідентифікації, який підтримується відповідним пристроєм);
- обов'язкове перезавантаження операційної системи робочої станції після завершення сеансу роботи одного працівника перед початком сеансу роботи іншого (в разі закріплення за робочою станцією декількох працівників для персональних та мобільних ЕОМ);
- використання на робочій станції засобів кваліфікованого електронного підпису, які мають чинний позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації (відомості щодо порядку встановлення та налаштування надаються з боку ТОВ «Доктор Елекс»);
- використання на робочій станції засобів шифрування каналу зв'язку з серверним компонентом ІТС, які мають чинний позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації щодо можливості його використання для криптографічного захисту конфіденційної інформації (персональних даних фізичних осіб) (відомості щодо порядку встановлення та налаштування наведені в розділі 3 цього документу);
- використання ключових даних та кваліфікованих сертифікатів відкритих ключів, електронні довірчі послуги щодо обслуговування яких надаються кваліфікованими надавачами електронних довірчих послуг;
- забезпечення захисту робочої станції від несанкціонованого доступу до неї сторонніх осіб в процесі функціонування, в тому числі:
  - від перегляду інформації, що відображається на її пристрої відображення;
  - від перегляду даних автентифікації (паролів, кодів доступу, графічних ключей тощо), які вводяться працівником для отримання доступу до прикладного програмного забезпечення «Медична інформаційна система «Доктор Елекс»;
- заборона використання в веб-браузері, з використанням якого здійснюється доступ до прикладного програмного забезпечення «Медична інформаційна система «Доктор Елекс», куків (cookies) та інших механізмів збереження даних автентифікації працівників;
- заборона використання на робочій станції іншого програмного

забезпечення, яке не є необхідним для виконання функціональних обов'язків при роботі з прикладним програмним забезпеченням «Медична інформаційна система «Доктор Елекс»;

- забезпечення надійного зберігання носіїв особистих ключів в неробочий час із забезпеченням неможливості несанкціонованого доступу до них сторонніх осіб.

3. ПОРЯДОК ВСТАНОВЛЕННЯ ТА КОНФІГУРУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТЕХНІЧНИХ МАЙДАНЧИКІВ ЗАКЛАДІВ ОХОРОНИ ЗДОРОВ'Я ТА АПТЕЧНИХ ЗАКЛАДІВ

Обов'язковому встановленню та конфігуруванню на робочих станціях технічних майданчиків закладів охорони здоров'я та аптечних закладів незалежно від апаратної платформи (стаціонарні ЕОМ, мобільні ЕОМ (ноутбуки), планшетні комп'ютери та смартфони) підлягають:

- веб-браузер, необхідний для роботи з прикладним програмним забезпеченням «Медична інформаційна система «Доктор Елекс»;
- антивірусне програмне забезпечення;
- засіб криптографічного захисту інформації, призначений для забезпечення криптографічного захисту інформації, що передається між технічним майданчиком закладу охорони здоров'я чи аптечного закладу та центральним вузлом інформаційно-телекомунікаційної системи «Медична інформаційна система «Доктор Елекс».

Також може бути здійснено встановлення та конфігурування клієнтської частини прикладного програмного забезпечення «Медична інформаційна система «Доктор Елекс».

Встановлення та конфігурування наведеного програмного забезпечення здійснюється адміністратором технічного майданчику закладу охорони здоров'я чи аптечного закладу (далі – адміністратор).

Веб-браузер обирається виходячи з програмної та інформаційної сумісності із прикладним програмним забезпеченням «Медична інформаційна система «Доктор Елекс».

Веб-браузери мають мати версію виконання не нижче від наведених нижче:

- веб-браузер Firefox – версія 31 або вище;
- веб-браузер Chrome – версія 69 або вище;
- веб-браузер Opera – версія 58 або вище;
- веб-браузер Edge – версія 13 або вище;
- веб-браузер Internet Explorer – версія 11 або вище;
- веб-браузер Safari – версія 7 або вище.

Веб-браузер повинен забезпечити функціонування криптографічних бібліотек (java-скриптів), призначених для формування та перевірки кваліфікованого електронного підпису в прикладному програмному забезпеченні «Медична інформаційна система «Доктор Елекс» у випадках, передбачених Порядком функціонування електронної системи охорони здоров'я, затвердженим

постановою Кабінету Міністрів України від 25.04.2018 № 411. Необхідні відомості та рекомендації щодо веб-браузерів та порядку їх використання надаються за відповідним запитом власника технічного майданчика закладу охорони здоров'я чи аптечного закладу з боку відповідальних осіб ТОВ «Доктор Елекс».

Крім зазначених налаштувань адміністратором повинні бути встановлені наступні обмеження на роботу робочої станції користувачів:

- для персональних ЕОМ, мобільних ЕОМ (ноутбуків):
  - адміністратору повинен відповідати окремий обліковий запис в операційній системі; умовним найменуванням цього облікового запису може слугувати прізвище адміністратора;
  - обліковий запис адміністратора повинен входити до групи користувачів «Адміністратори» операційної системи;
  - кожному працівнику повинен відповідати окремий обліковий запис в операційній системі; умовним найменуванням цього облікового запису може слугувати прізвище працівника;
  - всі облікові записи працівників повинні входити до групи «Користувачі» операційної системи;
  - вбудований обліковий запис «Гість» операційної системи повинен бути заблокований;
  - всі облікові записи працівників не повинні мати можливості модифікації системних налаштувань операційної системи та встановлення будь-якого додаткового програмного забезпечення;
  - всім обліковим записам користувачів повинен бути наданий доступ лише до каталогів та файлів, які містять матеріали, необхідні для виконання посадових обов'язків;
  - вбудований міжмережевий екран операційної системи повинен бути ввімкнений та налаштований на пропускання інформаційних потоків лише прикладного програмного забезпечення та антивірусного програмного забезпечення;
- для планшетних комп'ютерів та смартфонів – обов'язкова ідентифікація працівника (за кодом доступу, графічним ключем, паролем доступу або іншим засобом ідентифікації, який підтримується відповідним пристроєм).

Антивірусне програмне забезпечення призначене для антивірусного захисту робочих станцій технічного майданчика закладу охорони здоров'я чи аптечного закладу. Встановлення та налаштування антивірусного програмного забезпечення повинно здійснюватись згідно вимог експлуатаційної документації на нього. При цьому повинні бути виконані заходи, наведені в розділі 7 цього документу.

Засіб криптографічного захисту інформації повинен мати чинний позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації щодо можливості його використання для криптографічного захисту конфіденційної інформації (персональних даних фізичних осіб).

В разі використання для роботи з ІТС веб-браузеру – до нього інтегрований відповідний засіб криптографічного захисту інформації. Встановлення, налаштування та експлуатація такого засобу криптографічного захисту інформації повинні здійснюватися відповідно до вимог документу «Програмний засіб шифрування даних з використанням протоколу захисту транспортного рівня TCP Transport Layer Security (TLS). Методика перевірки коректності функціонування клієнтської частини електронної системи охорони здоров'я», а також з урахуванням рекомендацій відповідальних осіб ТОВ «Доктор Елекс».

В разі використання для роботи з ІТС клієнтської частини прикладного програмного забезпечення «Медична інформаційна система «Доктор Елекс» – засіб криптографічного захисту інформації входить до її складу. Встановлення, налаштування та експлуатація такого засобу криптографічного захисту інформації повинні здійснюватися відповідно до вимог документів «Інструкція із забезпечення безпеки експлуатації. UA.36049014.00002-01 91 01», «Інструкція щодо порядку генерації ключових даних та поводження з ключовими документами. UA.36049014.00002-01 92 01», а також з урахуванням рекомендацій відповідальних осіб ТОВ «Доктор Елекс».

4. ПОРЯДОК РЕЄСТРАЦІЇ ОБЛІКОВИХ ЗАПИСІВ ПРАЦІВНИКІВ

Реєстрація та управління обліковими записами користувачів здійснюється на рівні центральної бази даних електронної системи охорони здоров'я керівником (власником) закладу охорони здоров'я та відповідним співробітником відділу кадрів та не входить до завдань ІТС.

Управління обліковими записами працівників аптеки та обліковими даними аптеки здійснюється на рівні центральної бази даних електронної системи охорони здоров'я керівником (власником) відповідної аптеки та не входить до завдань ІТС.

5. ОБОВ'ЯЗКИ ТА ВІДПОВІДАЛЬНІСТЬ

5.1. Обов'язки та відповідальність адміністраторів

При адмініструванні робочої станції технічного майданчика закладу охорони здоров'я чи аптечного закладу за призначенням адміністратор відповідає за:

- забезпечення безперебійної експлуатації та технічного супроводження програмного забезпечення та технічних засобів робочої станції;
- технічне обслуговування програмного забезпечення та технічних засобів робочої станції згідно з експлуатаційної документацією;
- усунення аварійних ситуацій в роботі програмного забезпечення та технічних засобів робочої станції;
- адміністрування засобів програмного забезпечення та технічних засобів робочої станції;
- проведення робіт з модернізації програмного забезпечення та технічних

засобів робочої станції;

- забезпечення ведення журналів аудиту подій, що реєструються засобами програмного забезпечення та технічних засобів робочої станції;
- забезпечення антивірусного захисту інформації та оновлення антивірусних баз робочої станції;
- проведення тестових перевірок програмного забезпечення та технічних засобів робочої станції з метою своєчасного виявлення та ліквідації несправностей;
- коректне застосування доступних механізмів захисту для реалізації часткових політик безпеки;
- виявлення і усунення порушень безпеки;
- використання доступних і надійних засобів аудиту для полегшення виявлення порушень безпеки;
- проведення своєчасних перевірок системних журналів та журналів обліку порушень безпеки;
- надання допомоги при визначенні джерела зловмисного програмного забезпечення, зони його розповсюдження та наступного видалення;
- надання/відміну прав і повноважень, налаштування робочих параметрів засобів захисту;
- оперативне припинення порушень безпеки, які виникають в процесі функціонування робочої станції;
- підтримку та захист програмного забезпечення і відповідних файлів на технічних засобах робочої станції, використовуючи доступні механізми і процедури.

При адмініструванні робочої станції технічного майданчика закладу охорони здоров'я чи аптечного закладу за призначенням адміністратор зобов'язаний:

- знати і виконувати вимоги цієї Інструкції, дотримуватися режиму безпеки в роботі;
- систематично підвищувати власний професійний рівень;
- своєчасно доповідати керівництву закладу охорони здоров'я про факти виявлення несправностей в роботі програмного забезпечення та технічних засобів робочої станції, готувати рекомендації та вживати заходів щодо їхнього усунення;
- забезпечувати організацію, повноту та якісне виконання наведених вище організаційно-технічних заходів;
- надавати консультації іншому персоналу щодо порядку роботи з технічними засобами та програмним забезпеченням робочої станції в частині, що його стосується;
- виключати можливість впливу на програмне забезпечення та технічні засоби робочої станції або на їх роботу інших осіб або програмно-технічних засобів;
- вживати коригувальних заходів у разі виявлення спроб несанкціонованого доступу до робочої станції, порушенні правил експлуатації засобів захисту інформації або інших дестабілізуючих факторів;

- забезпечувати спостереження (реєстрація, моніторинг та аудит подій) за функціонуванням робочої станції;

- приймати участь у проведенні заходів з модернізації, тестування, оперативного відновлення функціонування робочої станції після збоїв, відмов, аварій окремих її компонентів;

- проводити аналіз даних журналів аудиту подій, що реєструються засобами захисту інформації, з метою виявлення можливих порушень;

- готувати акти щодо виявлених порушень безпеки експлуатації робочої станції, готувати рекомендації щодо їхнього усунення.

При адмініструванні робочої станції технічного майданчика закладу охорони здоров'я чи аптечного закладу за призначенням адміністратору забороняється:

- передавати іншим особам закріплені за ним матеріали або зберігати їх таким чином, що до них можуть отримати несанкціонований доступ інші особи; проявляти бездіяльність або не повідомляти про факти псування або втрати закріплених за ним матеріалів;

- розголошувати власні паролі доступу до робочої станції або вводити їх у спосіб, що надає змогу ознайомитись з ними іншим особам;

- при зміні паролів доступу вводити у якості нових значень їхні попередні значення або тривіальні значення;

- застосовувати програмне забезпечення робочої станції, яке проявляє явні ознаки неправильного функціонування;

- використовувати технічні засоби робочої станції, які проявляють явні ознаки неправильного функціонування;

- несанкціоновано вносити зміни у програмне забезпечення робочої станції, крім випадків, передбачених експлуатаційною документацією;

- несанкціоновано встановлювати, створювати, запускати на виконання на технічних засобах робочої станції інше програмне забезпечення, окрім того, що передбачено для його функціонування;

- використовувати технічні засоби робочої станції не за призначенням;

- залишати без контролю увімкнені незаблоковані (засобами операційної системи) технічні засоби робочої станції після проходження автентифікації для керування ними або у режимі конфігурування;

- здійснювати несанкціоноване відкриття системних блоків технічних засобів робочої станції, корпусів мережевої апаратури, від'єднання та приєднання пристроїв до інтерфейсних з'єднувачів мережевої апаратури та технічних засобів.

5.2. Обов'язки та відповідальність працівників

При використанні робочої станції технічного майданчика закладу охорони здоров'я чи аптечного закладу за призначенням працівник відповідає за:

- експлуатацію власної робочої станції згідно функціонального призначення та прийнятої політики безпеки;

- своєчасне інформування адміністратора про всі випадки порушення працездатності ІТС та порушення безпеки інформації, що обробляється та

зберігається в ній.

При використанні робочої станції технічного майданчика закладу охорони здоров'я чи аптечного закладу за призначенням працівник зобов'язаний:

- знати і виконувати вимоги цієї Інструкції, дотримуватися режиму безпеки при експлуатації ІТС;
- виключати можливість впливу на програмне та апаратне забезпечення власної робочої станції або на її роботу інших осіб або програмно-технічних засобів;
- експлуатувати робочу станцію з урахуванням вимог, наведених в розділі 2 цього документу;
- експлуатувати прикладне програмне забезпечення «Медична інформаційна система «Доктор Елекс» у відповідності до вимог експлуатаційної документації на нього (надається з боку ТОВ «Доктор Елекс»);
- негайно інформувати відповідальних осіб ТОВ «Доктор Елекс» про факти компрометації (або підозру на компрометацію) даних автентифікації (паролів, кодів доступу, графічних ключей тощо) або особистого ключа кваліфікованого електронного підпису.

При використанні робочої станції технічного майданчика закладу охорони здоров'я чи аптечного закладу за призначенням працівнику забороняється:

- розголошувати дані автентифікації (паролі, кодів доступу, графічні ключі тощо) або вводити їх у спосіб, що надає змогу ознайомитись з ними іншим особам;
- експлуатувати робочу станцію з порушенням вимог, наведених в розділі 2 цього документу;
- при зміні паролів доступу вводити у якості нових значень їхні попередні значення або тривіальні значення;
- застосовувати програмне забезпечення, яке проявляє явні ознаки неправильного функціонування;
- встановлювати, створювати, запускати на виконання на робочій станції інше програмне забезпечення, окрім того, що передбачено для її функціонування;
- використовувати робочу станцію не за призначенням;
- залишати без контролю увімкнену незаблоковану робочу станцію після проходження ідентифікації.

6. ВИМОГИ ДО КОНТРОЛЮ ЗА ФУНКЦІОНУВАННЯМ ТЕХНІЧНИХ МАЙДАНЧИКІВ ЗАКЛАДІВ ОХОРОНИ ЗДОРОВ'Я ТА АПТЕЧНИХ ЗАКЛАДІВ

6.1. Загальні положення щодо контролю за функціонуванням технічних майданчиків закладів охорони здоров'я та аптечних закладів

На стадії експлуатації технічних майданчиків закладів охорони здоров'я та аптечних закладів контроль полягає в перевірці й аналізі функціонування їх технічних засобів з метою оцінки ефективності їх функціонування, а також у контролі за станом захисту інформації, що обробляється на них. Оцінка

ефективності технічних майданчиків закладів охорони здоров'я та аптечних закладів здійснюється адміністратором з метою визначення й удосконалення стану захисту інформації, виявлення та запобігання порушенням вимог безпеки інформації, що створює умови або реальну можливість порушення безпеки інформації.

Контроль за функціонуванням технічних майданчиків закладів охорони здоров'я та аптечних закладів включає:

– контроль за забезпеченням режиму безпеки під час обробки інформації на технічних майданчиках закладів охорони здоров'я та аптечних закладів;

– контроль виявлення інцидентів та подій безпеки.

Контроль за функціонуванням технічних майданчиків закладів охорони здоров'я та аптечних закладів здійснюється шляхом безпосереднього оперативного контролю під час обробки інформації на технічних майданчиках закладів охорони здоров'я та аптечних закладів.

Безпосередній оперативний контроль за станом захисту інформації на технічних майданчиках закладів охорони здоров'я та аптечних закладів здійснюється як у процесі повсякденної діяльності, виходячи із ситуації, що конкретно складається на тій або іншій дільниці роботи, так і в ході планових перевірок. У повсякденній діяльності організація оперативного контролю під час обробки інформації на технічних майданчиках закладів охорони здоров'я та аптечних закладів покладається на відповідальних осіб (адміністраторів).

Контрольно-інспекційні перевірки функціонування технічних майданчиків закладів охорони здоров'я та аптечних закладів включають планування та проведення перевірок стану захисту інформації на них, проведення аналізу та надання рекомендацій щодо вдосконалення заходів та засобів захисту.

В ІТС безпосередньому контролю підлягають:

– журнали операційних систем;

– програмне забезпечення антивірусного захисту;

– фізична цілісність та охорона (контролюється відповідно до встановлених правил доступу до приміщень в закладі охорони здоров'я).

Контроль може здійснюватися шляхом локального чи віддаленого перегляду журналів аудиту.

6.2. Порядок контролю журналів операційних систем

Метою контролю є попередження спроб підбору паролів та здійснення несанкціонованого доступу до інформаційних об'єктів, які підлягають захисту.

У журналах операційних систем контролю підлягають:

– повідомлення про невдалий вхід у систему;

– повідомлення про невдалі спроби доступу до файлів;

– повідомлення про невдалі спроби зміни налаштувань політики безпеки;

– помилки при запуску служб чи інших компонентів.

Контроль здійснюється шляхом перегляду журналу операційних систем.

При перегляді повідомлень про невдалий вхід у систему необхідно звертати

увагу на повідомлення про невдалий локальний вхід у систему, які повторюються 3 та більше разів підряд, що може свідчити про спроби підбору пароля.

При перегляді повідомлень про невдалі спроби доступу до файлів необхідно звертати увагу на процеси, які здійснюють ці спроби. Вказані процеси повинні бути ідентифіковані і перевірені на предмет зараження шкідливим програмним забезпеченням (далі – ПЗ). Повідомлення про невдалі спроби доступу до файлів можуть свідчити про спроби несанкціонованого втручання у роботу технічного майданчика закладу охорони здоров'я чи аптечного закладу. Повинні бути ідентифіковані джерела цих спроб і вжиті заходи для попередження несанкціонованого доступу (далі – НСД).

Обов'язковому контролю підлягають файли особистих ключів користувачів.

Крім того треба звертати увагу на загальний стан функціонування операційної системи, шляхом перегляду повідомлень про збої в службах ОС. Вказане може свідчити про можливість навмисних або ненавмисних деструктивних дій, які можуть вплинути на процеси обробки інформації.

Контроль журналів операційних систем проводиться не рідше разу на місяць.

6.3. Порядок контролю антивірусного програмного забезпечення

Метою контролю є мінімізація втрат, викликаних зараженням шкідливим ПЗ.

У антивірусному ПЗ контролю підлягають:

- повідомлення про виявлення вірусів;
- повідомлення про невдале лікування;
- кількість часу з моменту останнього оновлення;
- загальне функціонування усіх складових антивірусного ПЗ.

Контроль здійснюється переглядом журналу антивірусного ПЗ на конкретній РС шляхом перегляду зведених та статистичних даних, моніторингу подій.

У повідомленнях про виявлення вірусів необхідно звертати увагу на шляхи проникнення. Необхідно визначати і за можливістю перекривати найбільш імовірні шляхи проникнення шкідливого ПЗ до технічного майданчику та взагалі в інфраструктуру закладу охорони здоров'я.

У повідомленнях про невдале лікування необхідно визначати місця зберігання шкідливого програмного забезпечення і видаляти його вручну.

Кількість часу з моменту останнього оновлення визначається за датою останнього успішного оновлення. Якщо вірусні бази антивірусного ПЗ не були оновлені вчасно, то необхідно вжити заходів для встановлення причин відсутності оновлень і їх усунення.

Загальне функціонування усіх складових антивірусного ПЗ визначається відсутністю помилок у функціонуванні усіх компонентів ПЗ. У випадку виявлення помилок у функціонуванні компонентів антивірусного ПЗ необхідно вжити заходів для відновлення їх працездатності.

Контроль здійснюється шляхом перегляду журналу антивірусного ПЗ на конкретній РС, а також в центрі управління антивірусного ПЗ (за наявності).

Повідомлення про невдале лікування повинні перевірятися щоденно, усе інше – щотижня.

7. ВИМОГИ ДО АНТИВІРУСНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Джерелами загроз проникнення шкідливого ПЗ на компоненти технічних майданчиків закладів охорони здоров'я та аптечних закладів є:

- знімні / зовнішні носії даних (далі – ЗНД): флеш-носії, оптичні диски, накопичувачі на жорстких магнітних дисках (вінчестери) або SSD-накопичувачі;
- електронна пошта;
- веб-сторінки;
- зовнішні мережі загального користування;
- встановлене ПЗ.

7.1. Вимоги до складу та функцій антивірусного програмного забезпечення

В ІТС дозволяється використовувати тільки ліцензійні антивірусні засоби, що закуплені у розробників (постачальників) вказаних засобів.

Системні вимоги та характеристики послуг, які виконуються обраним антивірусним ПЗ повинні підходити під операційне та технічне забезпечення технічних майданчиків закладів охорони здоров'я та аптечних закладів, забезпечувати безперешкодне виконання всіх процесів технології обробки інформації технічних майданчиків закладів охорони здоров'я та аптечних закладів.

До складу антивірусного ПЗ повинні, щонайменш, входити модулі, наведені в табл. 7.1.

Таблиця 7.1

№	Модулі, що входять до складу антивірусного ПЗ	Призначення модулю
1	Захист файлової системи в реальному часі	Модуль здійснює аналіз файлів, до яких звертається користувач в процесі роботи
2	Модуль сканування складу веб-сторінок	Модуль здійснює аналіз складу веб-сторінок, до яких звертається користувач в процесі роботи
3	Модуль оновлень	Здійснює завантаження оновлень баз вірусних сигнатур із визначеного джерела та інтеграцію до антивірусного ПЗ в реальному часі
4	Антивірусний сканер за запитом	Здійснює повну перевірку файлової системи на наявність шкідливого ПЗ за запитом

Основними параметрами, які повинно виконувати антивірусне ПЗ є:

- можливість управління механізмами антивірусного ПЗ, в тому числі

оновлення антивірусних баз даних;

- механізми антивірусного ПЗ повинні функціонувати в режимі виявлення вірусів автоматично, тобто без втручання користувача;
- механізми антивірусного ПЗ повинні забезпечувати блокування проникнення комп'ютерних вірусів з зовнішніх носіїв інформації (дистрибутивів ПЗ, флеш накопичувачів, оптичних дисків, тощо);
- механізми антивірусного ПЗ повинні забезпечувати можливість лікування вірусів, що піддаються лікуванню, з занесенням інформації про наслідки лікування у відповідні протоколи комплексу засобів захисту для забезпечення моніторингу роботи;
- робота антивірусного ПЗ не повинна блокувати (ускладнювати) роботу ІТС;
- механізми антивірусного ПЗ повинні забезпечувати можливість надання файлів для автоматичного оновлення антивірусного ПЗ;
- у разі підозри на зараження інформації невідомим шкідливим ПЗ (комп'ютерними вірусами) антивірусне ПЗ повинно забезпечувати блокування доступу користувачів та процесів до такої інформації.

Антивірусним ПЗ повинні реалізуються такі функції:

- контроль власної цілісності;
- застосування евристичних методів захисту у процесі викриття шкідливого ПЗ;
- захист файлової системи;
- оновлення антивірусних баз.

Антивірусне ПЗ повинно містити модулі контролю цілісності, які не дозволяють у режимі реального часу інтегрувати у власний код інше ПЗ або шкідливий код. Це забезпечує захист від спроб зламу, обходу або вимкнення антивірусного захисту. У ході контролю цілісності виконується перевірка всіх компонентів системи, у т.ч. файлів та налаштувань, які повинні змінюватися під час функціонування антивірусного ПЗ. Захист від вимкнення антивірусного ПЗ реалізується за рахунок блокування можливості вимкнення служб та модулів, які відповідають за захист системи у режимі реального часу.

Застосування евристичних методів захисту дозволяє забезпечити захист від шкідливого ПЗ, опис якого ще відсутній у базі. Методи ґрунтуються на аналізі процесів запущених в операційній системі та дозволяють попередити користувача про можливу небезпеку та запобігти їй.

Евристичний аналіз ґрунтується на припущенні, що нові віруси часто виявляються схожі на вже відомі. Таке припущення виправдовується наявністю в антивірусних базах сигнатур для визначення не одного, а відразу декількох вірусів. Заснований на такому припущенні евристичний метод полягає в пошуку файлів, які не повністю, але дуже близько відповідають сигнатурам відомих вірусів. Позитивним ефектом від використання цього методу є можливість виявити нові віруси ще до того, як для них будуть виділені сигнатури.

Захист файлової системи базується на тому, що антивірусне ПЗ здійснює

антивірусну перевірку всіх файлів під час їх створення, запуску або модифікації. Реалізована можливість перевірки окремих файлів, каталогів, дисків (локальних, мережевих). Антивірусне ПЗ захищає файлові сховища в режимі реального часу, видаляючи віруси, троянські та інші шкідливі програми.

За замовчуванням антивірусне ПЗ перевіряє тільки нові або змінені файли, тобто файли, які були додані або змінені з часу останнього звернення до них. Процес перевірки файлу виконується за таким алгоритмом:

- звернення користувача або деякої програми до кожного файлу перехоплюється відповідним компонентом антивірусного ПЗ;
- антивірусне ПЗ перевіряє наявність інформації про перехоплений файл у антивірусних базах; на підставі отриманої інформації приймається рішення про необхідність перевірки файлу.

Спочатку файл аналізується на наявність шкідливого ПЗ. Розпізнавання шкідливих об'єктів здійснюється із використанням баз вірусів програми. Бази містять опис всіх відомих на даний момент шкідливих програм, загроз, мережевих атак і способів їх знешкодження.

У результаті аналізу можливі наступні варіанти поведінки антивірусного ПЗ: якщо у файлі виявлено шкідливий код, антивірусне ПЗ блокує файл і намагається його лікувати. У результаті успішного лікування файл стає доступним для роботи. Якщо лікування провести не вдалося, файл видаляється. При лікуванні та видалені файлу, його копія поміщається до резервного сховища.

Якщо у файлі виявлено код, схожий на шкідливий, але стовідсоткової гарантії цього немає, файл поміщається в спеціальне сховище – карантин. Пізніше можна спробувати вилікувати його з оновленими базами.

Якщо у файлі не виявлено шкідливого коду, він відразу ж стає доступним для роботи.

7.2. Порядок застосування антивірусного програмного забезпечення

Контроль всіх дисків і файлів на предмет виявлення можливого ураження шкідливим ПЗ (комп'ютерними вірусами) повинен проводитись в автоматичному режимі.

Обов'язковому антивірусному контролю підлягає будь-яка інформація (текстові файли будь-яких форматів, файли даних, файли що обробляються, тощо) на ЗНД (зовнішні жорсткі магнітні диски, оптичні носії інформації, флеш-накопичувачі тощо).

Також обов'язковому антивірусному контролю підлягає:

- інформація у разі її експорту або її архівації;
- інформація у разі її імпорту;
- прикладне програмне забезпечення, яке встановлюється.

При виникненні підозри наявності шкідливого ПЗ (нетипова робота ПЗ, поява графічних або звукових ефектів, спотворень даних, зникнення файлів, часта поява повідомлень про системні помилки тощо) повинно бути проведено позачерговий антивірусний контроль.

Щоденно з початку роботи під час завантаження / перезавантаження в

автоматичному режимі повинен проводитись антивірусний контроль всіх носіїв інформації та файлових систем. Крім того раз на тиждень повинна виконуватись повна антивірусна перевірка.

Будь-яка інформація (текстові файли будь-яких форматів, файли даних, файли що виконуються, інформація, що отримується та передається по телекомунікаційних каналах, а також інформація на ЗНД при імпорті підлягає обов'язковому антивірусному контролю.

Контроль вхідної інформації необхідно проводить безпосередньо в момент прийому, а також під час кожного звертання до цієї інформації.

Контроль вихідної інформації необхідно проводити безпосередньо перед архівуванням та відправкою (записом на ЗНД), а також в момент відправки.

7.3. Порядок оновлення антивірусного ПЗ

Оновлення антивірусних баз сигнатур антивірусного ПЗ, що має експертний висновок за результатами державної експертизи у сфері технічного захисту інформації, необхідно здійснювати відповідно до положень Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи у сфері технічного захисту інформації, затвердженого наказом Адміністрації Держспецзв'язку від 26.03.2007 № 45, зареєстрованого в Міністерстві юстиції України 10.04.2007 за № 320/13587.

Оновлення антивірусних баз сигнатур іншого антивірусного ПЗ необхідно здійснювати в порядку, визначеному його виробником.

Оновлення антивірусних баз сигнатур антивірусного ПЗ та його програмного забезпечення в ІТС здійснюється адміністратором.

7.4. Інсталяція та налаштування засобів антивірусного захисту

Інсталяція та налаштування антивірусного ПЗ здійснюється адміністратором.

Антивірусне ПЗ має бути інстальованим у відповідності до експлуатаційної документації на антивірусне ПЗ.

7.5. Контроль функціонування та аудит

Для забезпечення функціонування та здійснення аудиту антивірусного ПЗ адміністратор має вживати заходи, що наведені в табл. 7.2.

Таблиця 7.2

№	Заходи, що проводяться	Періодичність проведення
1	Перевірка факту здійснення щоденного оновлення антивірусного ПЗ	1 доба
2	Перевірка незмінності налаштувань антивірусного ПЗ	1 місяць
3	Повна перевірка файлової системи ЕОМ на наявність шкідливого ПЗ	1 місяць
4	Перегляд журналу подій антивірусного ПЗ	3 місяці

Умовами правильного функціонування антивірусного ПЗ є:

- запуск антивірусного ПЗ при старті операційної системи;
- функціонування всіх модулів антивірусного ПЗ у реальному часі;
- актуальна версія бази даних сигнатур вірусів;
- здійснення противірусних дій шляхом очищення/видалення інфікованих файлів.

Перевірка запуску антивірусного ПЗ здійснюється візуальним переглядом існування значка антивірусного ПЗ у системному лотку (tray) операційної системи. У випадку виникнення проблем з функціонуванням значок антивірусу буде мати відповідний вигляд. При виникненні даної ситуації адміністратор зобов'язаний з'ясувати причини виникнення проблем з антивірусним ПЗ й виконати дії з відновлення його нормального функціонування.

Функціонування модулів антивірусного ПЗ можливо перевірити по загальним критеріям стану захисту:

- модуль антивірусного захисту – включений;
- оновлення сигнатур вірусів актуальні – дата вірусної бази даних сигнатур не перевищує 1-2 днів.

У випадку відмінності даних параметрів від зазначених вище, адміністратор повинен провести аналіз налаштувань антивірусного ПЗ і виконати відповідні дії з усунення викритих недоліків.

7.6. Оновлення баз сигнатур вірусів антивірусного ПЗ

Оновлення баз сигнатур вірусів антивірусного ПЗ здійснюється в порядку, наведеному в п. 7.3 цього документу.

7.7. Відновлення працездатності після збоїв

Відновлення працездатності антивірусного ПЗ після збоїв здійснюється адміністратором.

Процедура відновлення працездатності здійснюється шляхом здійснення повторної інсталяції та/або повторного налаштування антивірусного ПЗ.

Після здійснення процедури відновлення слід перевірити:

- налаштування антивірусного ПЗ, а в разі необхідності здійснити повторне налаштування;
- належне функціонування антивірусного ПЗ;
- здійснити оновлення баз даних вірусних сигнатур антивірусного ПЗ (за необхідністю).

7.8. Дії при виявленні шкідливого ПЗ

7.8.1. Дії при підозрі на наявність шкідливого ПЗ

У разі виникнення підозри про наявність шкідливого ПЗ адміністратор повинен провести позачерговий вірусний контроль для визначення факту наявності або відсутності шкідливого ПЗ.

У разі виникнення підозри про наявність шкідливого ПЗ (нетипова робота

ПЗ, поява графічних або звукових ефектів, перекручування даних, зникнення файлів, часта поява повідомлень про системні помилки та ін.) працівник разом із адміністратором повинен провести позачерговий антивірусний контроль власної робочої станції для визначення ними факту наявності або відсутності комп'ютерного вірусу.

7.8.2. Дії при виявленні шкідливого ПЗ

У разі виявлення шкідливого ПЗ адміністратор зобов'язаний:

- провести очищення або знищення заражених файлів;
- в разі виявлення нового шкідливого ПЗ, який не підлягає очищенню антивірусного ПЗ, що використовуються, видалити заражений файл;
- провести позачерговий антивірусний контроль для визначення факту наявності або відсутності шкідливого ПЗ.

У разі виявлення заражених комп'ютерними вірусами файлів при проведенні антивірусної перевірки, працівники зобов'язані:

- зупинити обробку інформації на робочій станції;
- відключити робочу станцію від мережі;
- провести очищення або знищення заражених файлів; у разі неможливості очищення (знищення) заражених файлів – скласти службову записку керівнику закладу охорони здоров'я чи аптечного закладу, в якій необхідно вказати імовірне джерело зараженого файлу, тип зараженого файлу, характер інформації, що міститься в файлі, тип вірусу та антивірусні заходи, що проводились.

8. ПОРЯДОК ОРГАНІЗАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ТЕХНІЧНОГО МАЙДАНЧИКА ЗАКЛАДУ ОХОРОНИ ЗДОРОВ'Я ЧИ АПТЕЧНОГО ЗАКЛАДУ

При розгортанні технічного майданчика закладу охорони здоров'я чи аптечного закладу виготовляються копії, забезпечується надійне збереження наступних матеріалів та експлуатаційних документів, з якими забезпечується ознайомлення працівників:

- цей документ;
- експлуатаційна документація на прикладне програмне забезпечення «Медична інформаційна система «Доктор Елекс» (в частині, що містить опис роботи працівників);
- експлуатаційна документація на операційну систему та антивірусне ПЗ (допускається зберігати в електронному вигляді, визначеному виробником відповідного ПЗ);
- форми (шаблони) документів, які обробляються на технічному майданчику закладу охорони здоров'я;
- акт завершення робіт з розгортання технічного майданчика закладу охорони здоров'я;

- інформаційні матеріали (пам'ятки), що визначають контактну інформацію (посади, прізвища, ім'я, по батькові, телефони, електронні адреси тощо) відповідальних осіб ТОВ «Доктор Елекс», з якими взаємодіють адміністратор та працівники.

Наказом керівника закладу охорони здоров'я чи аптечного закладу призначаються адміністратори. З метою забезпечення безперебійного функціонування технічних майданчиків закладів охорони здоров'я та аптечних закладів можуть призначатись декілька (наприклад, основний та резервний) адміністратори.

На посаду адміністратора доцільно призначати осіб, які мають вищу технічну освіту, досвід роботи в галузі телекомунікацій та необхідний рівень кваліфікації щодо побудови та функціонування інформаційно-телекомунікаційних систем.

Особи, призначені на посади адміністраторів, інструктуються щодо суті роботи, яку будуть виконувати, та повинні бути ознайомлені із цією Інструкцією під підпис.

Звільнення або переміщення адміністраторів проводиться тільки після здавання за актом усіх документів та матеріалів, що значаться за ними, та ліквідації їх облікових записів в операційних системах робочих станцій технічних майданчиків закладів охорони здоров'я та аптечних закладів.

9. ПОРЯДОК ВВЕДЕННЯ В ДІЮ ТЕХНІЧНОГО МАЙДАНЧИКА ЗАКЛАДУ ОХОРОНИ ЗДОРОВ'Я ЧИ АПТЕЧНОГО ЗАКЛАДУ

9.1. Загальні положення щодо введення в дію технічного майданчика закладу охорони здоров'я чи аптечного закладу

Після розгортання апаратних засобів, встановлення та конфігурування системного та прикладного програмного забезпечення, виготовлення необхідних експлуатаційних документів проводяться заходи щодо перевірки відповідності технічного майданчика закладу охорони здоров'я чи аптечного закладу вимогам до захисту інформації та оформлюється відповідний акт завершення робіт з розгортання технічного майданчика закладу охорони здоров'я чи аптечного закладу.

Перевірка відповідності технічного майданчика закладу охорони здоров'я чи аптечного закладу вимогам повинна проводитись в порядку, наведеному в розділі 10 цього документу.

Перевірка відповідності технічного майданчика закладу охорони здоров'я чи аптечного закладу проводиться комісією, призначеною його керівником. До складу комісії обов'язково включається адміністратор та, щонайменш, один працівник. За результатами перевірки оформлюється акт завершення робіт розгортання технічного майданчика закладу охорони здоров'я (додаток 1 до цього документу).

Акт завершення робіт з розгортання технічного майданчика закладу охорони здоров'я чи аптечного закладу оформлюється в двох примірниках,

підписується всіма особами, які проводили перевірку, і затверджується керівником закладу охорони здоров'я чи аптечного закладу. Один примірник акту зберігається в цьому закладі, а другий надсилається до ТОВ «Доктор Елекс» та зберігається в цьому товаристві.

ТОВ «Доктор Елекс» здійснює підключення технічного майданчика закладу охорони здоров'я чи аптечного закладу до інформаційно-телекомунікаційної системи «Медична інформаційна система «Доктор Елекс» виключно за позитивними результатами розгортання технічного майданчика закладу охорони здоров'я чи аптечного закладу, наведеними в наданому акті завершення робіт з розгортання технічного майданчика закладу охорони здоров'я чи аптечного закладу, про що інформується заклад охорони здоров'я чи аптечний заклад.

9.2. Порядок та методи перевірки технічного майданчика закладу охорони здоров'я чи аптечного закладу

Перевірка складається з наступних окремих перевірок:

– перевірка складу апаратного та програмного забезпечення робочої станції;

– перевірка налаштувань комплексу засобів захисту від несанкціонованого доступу робочої станції;

– перевірка антивірусного програмного забезпечення;

– перевірка вимог до фізичного середовища робочої станції;

– перевірка вимог до користувачів робочої станції;

– перевірка вимог до організаційного забезпечення робочої станції.

9.2.1. Методика перевірки складу апаратного та програмного забезпечення робочої станції

Порядок проведення перевірки:

– перевірити склад апаратного та програмного забезпечення робочої станції на відповідність відомостям, наведеним в розділі 3 цього документу.

Очікуваний результат:

– склад апаратного та програмного забезпечення робочої станції відповідає відомостям, наведеним в розділі 3 цього документу.

Умови (критерії) прийняття рішення щодо відповідності об'єкту перевірки встановленим вимогам: позитивний висновок щодо відповідності складу апаратного та програмного забезпечення робочої станції робиться у випадку, якщо отримані результати відповідають очікуваному.

9.2.2. Перевірка налаштувань комплексу засобів захисту від несанкціонованого доступу робочої станції

Зауваження до порядку проведення перевірки:

Поділені відповідно до функціонального призначення, місця розміщення та виду представлення програмно-інформаційні ресурси технічного майданчика закладу охорони здоров'я, доступні його працівникам, наведені в табл. 9.1.

Таблиця 9.1

Об'єкт захисту	Умовне позначення
журнал реєстрації подій системного програмного забезпечення робочої станції в електронній формі	{LOG}
конфігураційні та системні об'єкти компонентів робочої станції, що визначають параметри конфігурації, функціонування та правила розмежування доступу	{CONFIG}
ключові дані працівників	{KEY}

На робочій станції виділені ролі працівників, наведені в табл. 9.2.

Таблиця 9.2

Суб'єкт доступу	Умовне позначення
адміністратор	[A_A]
працівник	[K_O]

На робочій станції повинні виконуватись правила розмежування доступу, наведені в табл. 9.3, 9.4.

Таблиця 9.3

Об'єкт доступу	[A_A]	[K_O]
{LOG}	+	
{CONFIG}	+	
{KEY}		+

Таблиця 9.4

Суб'єкт	Тип доступу			
	Читання	Модифікація	Створення	Видалення
[A_A]	{LOG} {CONFIG}	{CONFIG}	{LOG} {CONFIG}	{CONFIG}
[K_O]	{KEY}			{KEY}

Порядок проведення перевірки:

1. Здійснити ідентифікацію програмного забезпечення, наведеного в розділі 3 цього документу, та перевірити дотримання ліцензійних умов при його застосуванні за призначенням.

Очікуваний результат: програмне забезпечення, яке наведено в розділі 3 цього документу, використовується за призначенням із дотримання відповідних ліцензійних умов.

2. Перевірити відповідність діючих параметрів налаштування програмного забезпечення, наведеного в розділі 3 цього документу, та призначених атрибутів доступу значенням, наведеним у відповідній документації, зазначеній у розділах 3, 8 цього документу.

Очікуваний результат: налаштування програмного забезпечення, наведеного в розділі 3 цього документу, та призначені атрибути доступу

відповідають значенням, наведеним у відповідній документації, зазначеній у розділах 3, 8 цього документу.

3. Перевірити (шляхом ініціювання відповідних спроб доступу) можливість реєстрації засобами операційної системи та антивірусного ПЗ у відповідних журналах дій користувачів щодо доступу до засобів робочої станції та оброблюваної на ній інформації.

Очікуваний результат: засоби операційної системи та антивірусного ПЗ забезпечують реєстрацію дій користувачів щодо доступу до засобів робочої станції та оброблюваної у ній інформації.

4. Перевірити можливість проведення аналізу зареєстрованих даних.

Очікуваний результат: засоби операційної системи та антивірусного ПЗ забезпечують можливість проведення аналізу зареєстрованих даних адміністратором.

5. Перевірити використання встановленого програмного забезпечення щодо надання працівникам можливості виконувати свої службові обов'язки, згідно з прийнятою технологією роботи та з дотриманням встановлених вимог щодо захисту інформації

Очікуваний результат: наявна можливість використання встановленого програмного забезпечення при виконанні працівниками своїх службових обов'язків згідно з прийнятою технологією роботи та з дотриманням встановлених вимог щодо захисту інформації.

6. Шляхом ініціювання входу під обліковими записами адміністратора та працівників до операційної системи робочої станції з коректним та некоректним значеннями даних автентифікації перевірити працездатність механізмів ідентифікації та автентифікації.

Очікуваний результат: спроби входу під обліковими записами адміністратора та працівників з некоректним значенням даних автентифікації завершено невдало; спроби входу з коректним значенням даних автентифікації завершено вдало.

7. Під обліковим записом адміністратора на робочих станціях на платформі стаціонарних та мобільних ЕОМ перевірити:

- можливість створювати та видаляти облікові записи користувачів, управляти їх правами доступу, встановлювати паролі;
- можливість управляти налаштуваннями програмного та апаратного забезпечення робочої станції.

Перевірити, що жодний інший користувач не має зазначених прав.

Очікуваний результат: адміністратор має наведені можливості в операційній системі зазначених технічних засобів; жодний інший користувач не має зазначених прав.

8. Перевірити налаштування антивірусного ПЗ щодо повернення до антивірусних баз попередньої версії в разі невдалого завантаження оновлення.

Очікуваний результат: антивірусне ПЗ налаштоване на автоматичне повернення до антивірусних баз попередньої версії в разі невдалого завантаження відповідного оновлення.

9. Штатними засобами антивірусного ПЗ перевірити функціонування механізмів оновлення антивірусних баз.

Очікуваний результат: антивірусне ПЗ дозволяє здійснювати оновлення антивірусних баз; при цьому відсутня необхідність повторного інсталювання або переривання функцій захисту.

10. Під обліковим записом адміністратора на робочих станціях на платформі стаціонарних та мобільних ЕОМ перевірити повноваження користувачів щодо інсталювання програмного забезпечення.

Очікуваний результат: лише адміністратор має можливість інсталювання, видалення та модернізації програмного забезпечення на робочих станціях на платформі стаціонарних та мобільних ЕОМ.

11. Під обліковим записом адміністратора на робочих станціях на платформі стаціонарних та мобільних ЕОМ здійснити контроль працездатності системного програмного забезпечення (шляхом запуску відповідних системних утиліт).

Очікуваний результат: операційна система робочих станцій на платформі стаціонарних та мобільних ЕОМ забезпечує можливість самотестування системного та прикладного забезпечення робочої станції; для цього використовуються штатні засоби відповідного програмного та апаратного забезпечення.

12. Під обліковим записом адміністратора на робочих станціях на платформі стаціонарних та мобільних ЕОМ перевірити налаштування операційної системи та антивірусного ПЗ на реєстрацію подій, наведених в розділі 6 цього документу.

Очікуваний результат: операційна система та антивірусне ПЗ налаштовані на реєстрацію подій, наведених в розділі 6 цього документу.

13. Під обліковим записом адміністратора перевірити факт реєстрації на робочих станціях на платформі стаціонарних та мобільних ЕОМ в журналах реєстрації дій операційної системи та антивірусного ПЗ, які виконувались при проведенні перевірок за кроками 1 – 12 цієї перевірки.

Очікуваний результат: в журналах реєстрації відображені всі дії, які виконувались при проведенні перевірок за кроками 1 – 12 цієї перевірки.

14. Під обліковим записом адміністратора здійснити внесення будь-яких змін до файлів журналу реєстрації подій.

Очікуваний результат: після внесення змін до журналів реєстрації подій та наступній спробі їх перегляду видається повідомлення про пошкодження журналу реєстрації подій.

Умови (критерії) прийняття рішення щодо відповідності об'єкту перевірки встановленим вимогам: позитивний висновок щодо правильності налаштувань комплексу засобів захисту від несанкціонованого доступу робочої станції робиться у випадку, якщо отримані результати відповідають очікуваним.

9.2.3. Методика перевірки антивірусного ПЗ робочої станції

Порядок проведення перевірки:

– здійснити ідентифікацію антивірусного програмного забезпечення;

– здійснити перевірку коректності інсталювання та конфігурування антивірусного ПЗ: шляхом перевірки, аналізу і перегляду поточних налаштувань безпеки перевірити їх відповідність вимогам експлуатаційної документації на антивірусне програмне забезпечення;

– перевірити працездатність сканера файлової системи та коректність його функціонування; для цього використати тестовий архів із набором тестових вірусів, який доступний в мережі Інтернет за адресою https://spec-komp.com/download/parol111.zip (цей тестовий архів містить набір тестових вірусів, призначених для перевірки правильності функціонування антивірусного програмного забезпечення); тестовий архів послідовно скопіювати на жорсткий диск ЕОМ; здійснити запуск на виконання сканеру файлової системи та перевірити жорсткий диск ЕОМ, на якому розміщено тестовий файловий архів (перевірка проводиться лише для робочих станцій на платформі стаціонарних та мобільних ЕОМ);

– перевірити працездатність активних моніторів файлової системи; для цього використати тестовий архів із набором тестових вірусів; тестовий архів необхідно записати на жорсткий диск ЕОМ (перевірка проводиться лише для робочих станцій на платформі стаціонарних та мобільних ЕОМ);

– перевірити працездатність моніторів веб-трафіку; для цього спробувати завантажити тестовий вірус з мережі Інтернет за адресою http://www.rexswain.com/eicar.html.

Очікуваний результат:

– налаштування безпеки для антивірусного ПЗ відповідають вимогам експлуатаційної документації на нього;

– антивірусне програмне забезпечення налаштоване на постійне сканування об'єктів оперативної пам'яті, завантажувальних секторів, об'єктів файлової системи та веб-трафіку;

– в усіх випадках за результатами роботи засобів виявлення вірусів отримано повідомлення про виявлені віруси;

– антивірусні бази регулярно оновлюються;

– лише адміністратор може змінювати системні налаштування антивірусного програмного забезпечення.

Умови (критерії) прийняття рішення щодо відповідності об'єкту перевірки встановленим вимогам: позитивний висновок щодо відповідності робочої станції вимогам до антивірусного захисту інформації робиться у випадку, якщо отримані результати відповідають очікуваним.

9.2.4. Методика перевірки вимог до фізичного середовища

Перевірка проводиться лише для робочих станцій на платформі стаціонарних та мобільних ЕОМ.

Порядок проведення перевірки: перевірити умови розташування технічних засобів робочої станції.

Очікуваний результат: технічні засоби робочої станції розміщені таким

чином, що:

– приміщення, в яких вони розташовуються, обладнані механічним або електронним замком, ключі від якого знаходяться у відповідних працівників;

– ознайомлення сторонніми особами з інформацією з обмеженим доступом, що відображається на моніторах робочої станції, є неможливим;

– дотримані вимоги щодо встановлення відповідного обладнання та умови експлуатації, визначені його виробником.

Умови (критерії) прийняття рішення щодо відповідності об'єкту перевірки встановленим вимогам: позитивний висновок щодо відповідності робочої станції вимогам до фізичного середовища робиться у випадку, якщо отримані результати відповідають очікуваним.

9.2.5. Методика перевірки вимог до працівників робочої станції

Перевірка проводиться лише для робочих станцій на платформі стаціонарних та мобільних ЕОМ.

Порядок проведення перевірки: перевірити наявність облікових записів адміністратора та працівників;

Очікуваний результат: в операційній системі робочої станції наявні окремі облікові записи адміністратора та працівників.

Умови (критерії) прийняття рішення щодо відповідності об'єкту перевірки встановленим вимогам: позитивний висновок щодо відповідності робочої станції вимогам до користувачів робиться у випадку, якщо отримані результати відповідають очікуваним.

9.2.6. Методика перевірки вимог до організаційного забезпечення

Порядок проведення перевірки: перевірити склад документів, що використовуються для забезпечення діяльності технічного майданчика закладу охорони здоров'я.

Очікуваний результат: склад документів, що використовуються для забезпечення діяльності технічного майданчика закладу охорони здоров'я, відповідає вимогам розділу 8 цього документу.

Умови (критерії) прийняття рішення щодо відповідності об'єкту перевірки встановленим вимогам: позитивний висновок щодо відповідності робочої станції вимогам до організаційного забезпечення робиться у випадку, якщо отримані результати відповідають очікуваним.

10.ВИМОГИ ДО ЗМІСТУ ДОГОВОРУ (УГОДИ) НА ПРАВО РОБОТИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІЙ СИСТЕМІ

Договір (угода) на право роботи в ІТС укладається між власником ІТС (ТОВ «Доктор Елекс») та закладом охорони здоров'я чи аптечного закладу, працівники якого користуються її інформаційними послугами.

Договір (угода) на право роботи в ІТС повинна, окрім всього іншого, визначати:

- повноваження власника ІТС (ТОВ «Доктор Елекс») щодо надання доступу до ІТС та відповідного консультативно-методичного забезпечення з питань захисту інформації, що обробляється та зберігається в ІТС;

- обов'язки власника ІТС (ТОВ «Доктор Елекс») щодо забезпечення захисту інформації, що надається для зберігання до ІТС з боку працівників закладу охорони здоров'я чи аптечного закладу (як розпорядників персональних даних фізичних осіб), в порядку, визначеному законодавством;

- визначення обсягу інформаційних послуг ІТС, які доступні для використання працівниками закладу охорони здоров'я чи аптечного закладу;

- обов'язки закладу охорони здоров'я чи аптечного закладу щодо забезпечення виконання його працівниками правил щодо безпечного використання ІТС за призначенням.

Типові обов'язки власника ІТС (ТОВ «Доктор Елекс») визначаються згідно з наступним:

- надавати закладу охорони здоров'я чи аптечному закладу послуги, перелік яких визначений у додатках до договору (угоди), дотримуючись визначених договором (угодою) стандартів якості надання послуг;

- забезпечувати технічну підтримку та супроводження ІТС, на умовах, визначених договором (угодою);

- надавати закладу охорони здоров'я чи аптечному закладу консультації з питань використання ІТС, на умовах, визначених у договорі (угоді);

- при отриманні повідомлення закладу охорони здоров'я чи аптечного закладу про інциденти, усувати їх у погоджені сторонами строки;

- організовувати отримання електронних згод (в тому числі їх належне логування та збереження відповідних логів) на обробку персональних даних під час самостійної реєстрації кінцевих користувачів в ІТС шляхом проставлення відмітки про надання дозволу на обробку персональних даних;

- організовувати отримання згод на обробку персональних даних під час самостійного звернення кінцевих користувачів до call-центру власника ІТС у формі, що дає змогу зробити висновок про надання згоди за умови обов'язкового збереження інформації, що може підтвердити отримання такої згоди;

- здійснювати технічне адміністрування ІТС;

- забезпечувати захист даних, створених або внесених закладом охорони здоров'я чи аптечним закладом, від несанкціонованого використання, спотворення, знищення або зміни;

- не використовувати у власних цілях отриману в результаті надання послуг за договором (угодою) інформацію закладу охорони здоров'я чи аптечного закладу (дане положення не поширюється на конкретні дії власника ІТС з використання інформації кінцевого користувача – суб'єкта персональних даних, на підставі розпорядження (згоди) кінцевого користувача щодо інформації, а також інформації, володільцем якої є власник ІТС);

- на вимогу закладу охорони здоров'я чи аптечного закладу надавати звіт про надані послуги за допомогою електронної пошти;

- не розголошувати, не поширювати і не передавати персональні дані у

випадках, що не передбачені законом та/або без згоди закладу охорони здоров'я, аптечного закладу чи суб'єкта персональних даних;

- у разі розірвання договору (угоди), передати закладу охорони здоров'я, аптечному закладу або особі, яка буде ним визначена, структуровані дані, що були внесені до ІТС закладом охорони здоров'я чи аптечним закладом у порядку, визначеному договором (угодою).

Типові обов'язки закладу охорони здоров'я чи аптечного закладу визначаються згідно з наступним:

- негайно повідомляти власника ІТС у встановленому порядку про інциденти в роботі ІТС у порядку, встановленому договором (угодою);

- не використовувати ІТС в цілях, що суперечать чинному законодавству України, правам чи законним інтересам третіх осіб та/або умовам договору (угоди);

- зберігати у таємниці ідентифікатори доступу (власні та працівників) та пов'язані з наданням послуг дані, що призначені виключно для використання закладом охорони здоров'я чи аптечним закладом та їх працівниками (в т.ч. – слова-паролі, смс-коди та ін.);

- негайно змінювати ідентифікатори доступу та/або блокувати облікові записи у випадку виявлення несанкціонованого доступу, розголошення або підозри розголошення ідентифікаторів доступу, про що заклад охорони здоров'я чи аптечний заклад повідомляє власника ІТС у порядку, встановленому договором (угодою);

- не вчиняти дій (в тому числі, але не виключно: розсилка спаму, встановлення шкідливого програмного забезпечення, ботів, засобів підбору паролів, ddos атак тощо) результатом яких може бути порушення нормальної роботи ІТС як в цілому, так і окремих її частин;

- не вчиняти дій, результатом яких є усунення або зниження ефективності технічних засобів захисту ІТС;

- організовувати підписання та зберігання всіх необхідних документів (передбачених законодавством та/або договором (угодою)), при цьому зміст документів, шаблони яких передбачено договором (угодою), не може бути звужено;

- вносити до ІТС виключно повну, актуальну, достовірну, вичерпну інформацію (в тому числі інформацію про стан здоров'я пацієнтів, інші медичні дані, інформацію щодо графіку прийому лікарів, відвідування прийомів пацієнтами тощо);

- отримувати від кінцевих користувачів перед початком збору персональних даних згоди на обробку їх персональних даних у ІТС (за зразком, встановленим договором (угодою)), та зберігати їх протягом усього строку обробки персональних даних;

- на вимогу власника ІТС надавати підтвердження законності отримання переданих для обробки персональних даних протягом трьох робочих днів з моменту отримання такої вимоги;

- здійснити ознайомлення працівників закладу охорони здоров'я чи

аптечного закладу з вичерпною інформацію щодо заходів безпеки при використанні ІТС, з метою недопущення витоку конфіденційної інформації, в тому числі – ідентифікаторів доступу; забезпечити проставлення працівником особистого підпису на зобов'язанні користувача ІТС (за зразком, встановленим договором (угодою));

- надавати доступ до ІТС працівникам закладу охорони здоров'я чи аптечного закладу виключно після ознайомлення та підписання Зобов'язання користувача ІТС (за зразком встановленим договором (угодою));

- надавати доступ до ІТС працівникам закладу охорони здоров'я чи аптечного закладу тільки в тих випадках і в тій мірі, в якій це є необхідним для належного виконання ними трудових або договірних обов'язків; при цьому, рівень доступу таких працівників налаштовується уповноваженою особою закладу охорони здоров'я чи аптечного закладу безпосередньо в ІТС;

- забезпечити працівників закладу охорони здоров'я чи аптечного закладу безпечним кінцевим обладнанням та програмним забезпеченням (на якому оновлені до останньої доступної версії операційна система та браузер; здійснені налаштування адміністрування операційної системи, що не дозволяють встановлювати без дозволу адміністратора операційної системи іншого програмного забезпечення, що зокрема унеможливлює встановлення кейлогерів; встановлений і оновлений до останньої доступної версії антивірус тощо), для організації безпечного доступу до мережі Інтернет та безпечної передачі даних у локальній мережі закладу охорони здоров'я чи аптечного закладу.

Типовий порядок надання доступу закладу охорони здоров'я чи аптечному закладу та їх працівникам визначається згідно з наступним:

Сторони у 5-ти денний термін з моменту підписання договору (угоди(призначають відповідальних представників, які взаємодіють з усіх питань стосовно виконання договору (угоди), про що письмово повідомляють одна одну.

Для здійснення першого входу до ІТС уповноважені особи закладу охорони здоров'я чи аптечного закладу отримують одноразові ідентифікатори доступу до їх облікових записів та/або особистих кабінетів; одноразові ідентифікатори доступу мають бути обов'язково змінені під час першого входу.

Уповноважені особи закладу охорони здоров'я чи аптечного закладу отримують повний доступ до послуг, в тому числі можливість реєструвати в ІТС працівників закладу охорони здоров'я чи аптечного закладу, створювати їх облікові записи та/або особисті кабінети, дотримуючись інструкцій та вказівок, які надаються власником ІТС або отримані від працівників call-центру власника ІТС.

Після реєстрації, доступ до ІТС здійснюється за умови автентифікації користувача.

Працівники закладу охорони здоров'я чи аптечного закладу отримують доступ до визначеної в договорі (угоді) кількості облікових записів.

Використання одного облікового запису більш ніж одним працівником закладу охорони здоров'я чи аптечного закладу та/або передача ідентифікаторів доступу більш ніж одному працівнику закладу охорони здоров'я чи аптечного

закладу забороняється.

Заклад охорони здоров'я чи аптечний заклад не вправі за плату дозволяти третім особам здійснювати доступ до ІТС під власним обліковим записом та/або отримувати кінцевий результат від використання ІТС.

У будь-який момент уповноважені особи закладу охорони здоров'я чи аптечного закладу та зареєстровані працівники закладу охорони здоров'я чи аптечного закладу можуть змінити власні ідентифікатори доступу, за умови дотримання вимог, які встановлені власникам ІТС до складу ідентифікаторів доступу або відновити втрачені ідентифікатори доступу у порядку, вставленому власником ІТС в ІТС.

Заклад охорони здоров'я чи аптечний заклад зобов'язується забезпечити дотримання всіма працівниками, що отримали доступ до ІТС, наступних умов:

- працівник зберігає ідентифікатори доступу в таємниці, та не розголошує їх третім особам;
- працівник негайно доповідає уповноваженим особам закладу охорони здоров'я чи аптечного закладу та власника ІТС:
  а) про компрометацію облікового запису (розголошення ідентифікаторів доступу);
  б) про виникнення підозри або виявлення факту доступу до ІТС, отримання відомостей з неї третіми особами;
  в) про намагання сторонніх осіб у будь-який спосіб отримати інформацію щодо ідентифікаторів доступу до ІТС;
- працівник зобов'язаний після закінчення професійних, службових, договірних чи трудових відносин або при переведенні на іншу посаду, що не пов'язана з роботою в ІТС, повідомити про це уповноважених осіб закладу охорони здоров'я чи аптечного закладу;
- працівник зобов'язується не передавати право/можливість доступу до ІТС та отримання відомостей з неї третім особам;
- працівник зобов'язується не допускати третіх осіб до роботи з ІТС під власним обліковим записом;
- працівник зобов'язується не залишати пристрої, з яких проводився вхід у ІТС, без нагляду до моменту виходу з ІТС.

Типовий зміст *зобов'язання працівників закладів охорони здоров'я та аптечних закладів*, які користуються інформаційними послугами ІТС, наведений в додатку 2 до цього документу.

Додаток 1

ЗАТВЕРДЖУЮ
Керівник закладу охорони здоров'я
чи аптечного закладу

«___» _____ 20__ року

АКТ
завершення робіт з розгортання технічного майданчика

_____
(найменування закладу охорони здоров'я чи аптечного закладу)

м. _____ «___» _____ 20__ року

1. Загальні відомості

Власник технічного майданчика закладу охорони здоров'я закладів охорони здоров'я чи аптечного закладу (далі – технічний майданчик): _____ (фізична адреса: _____).

Робочі станції технічного майданчика розташовані в будівлях за адресою: _____.

Ступінь обмеження доступу до інформації, яка обробляється в МІС, – конфіденційна інформація (персональні дані фізичних осіб), відкрита інформація.

Кількість користувачів МІС – не обмежується.

Підставою для розгортання технічного майданчика є договір між ТОВ «Доктор Елекс» та _____ № _____ від __.__.20__ року.

Технічний майданчик технічного майданчика призначений для організації доступу до інформаційно-телекомунікаційної системи «Медична інформаційна система «Доктор Елекс» (далі – ІТС), яка має комплексну систему захисту інформації з підтвердженою відповідністю (атестат відповідності № _____ від __.__.20__ року).

Технічний майданчик розгорнутий в порядку, визначеному в документі «Інструкція про порядок підключення технічних майданчиків закладів охорони здоров'я та аптечних закладів. UA.38582529.КСЗІ.00001.ІЗОЗ».

2. Нормативні документи та нормативно-правові акти, вимоги яких ураховувались при розгортанні технічного майданчика

- Закон України «Про інформацію»;
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;
- Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету міністрів України № 373 від 29.03.2006 (зі змінами);
- Типовий порядок обробки персональних даних, затверджений наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-

14;

- Порядок функціонування електронної системи охорони здоров'я, затверджений постановою Кабінету Міністрів України від 25.04.2018 № 411;

- Загальні технічні вимоги до медичних та фармацевтичних (аптечних) інформаційних систем для підключення до інформаційно-телекомунікаційної системи «Центральна база даних електронної системи охорони здоров'я» (в частині захисту інформації). UA.41848148.КСЗІ.00001.ЗТВ;

- Технічні вимоги до електронної медичної інформаційної системи для її підключення до центральної бази даних електронної системи охорони здоров'я, затверджені наказом Національної служби здоров'я України від 06.02.2019 № 28;

- Постанова Кабінету Міністрів України від 03.03.2020 № 193 «Про реалізацію експериментального проекту щодо забезпечення можливості використання удосконалених електронних підписів і печаток, які базуються на кваліфікованих сертифікатах відкритих ключів».

- Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 № 93, зареєстроване в Міністерстві юстиції України 16.07.2007 за № 820/ 14087;

- Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141, зареєстроване в Міністерстві юстиції України 30.07.2007 р. за № 862/14129;

- ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення;

- ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт;

- НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;

- НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі;

- НД ТЗІ 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці;

- НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу;

- НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу;

- НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі;

- НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

3. Склад документів, які були використані під час проведення робіт з розгортання технічного майданчика

- наказ про призначення відповідальних осіб (адміністраторів) № _____ від __.__.20__;
- наказ про проведення перевірки технічного майданчика закладу охорони здоров'я вимоги до захисту інформації від несанкціонованого доступу № _____ від __.__.20__;
- «Інструкція про порядок підключення технічних майданчиків закладів охорони здоров'я та аптечних закладів. UA.38582529.КСЗІ.00001.ІЗОЗ»;
- атестат відповідності комплексної системи захисту інформації інформаційно-телекомунікаційної системи «Медична інформаційна система «Доктор Елекс» № _____ від __.__.20__ року із відповідним експертним висновком.

4. Результати робіт з розгортання технічного майданчика

4.1. Розгортання технічного майданчика проводилось у порядку, визначеному в документі «Інструкція про порядок підключення технічних майданчиків закладів охорони здоров'я та аптечних закладів. UA.38582529.КСЗІ.00001.ІЗОЗ».

4.2. Наказом № _____ від __.__.20__ призначено особу, відповідальну за захист інформації на технічному майданчику (далі – відповідальна особа), та покладено на відповідальну особу виконання обов'язків адміністратора згідно з розділом 5 документу «Інструкція про порядок підключення технічних майданчиків закладів охорони здоров'я та аптечних закладів. UA.38582529.КСЗІ.00001.ІЗОЗ».

4.3. Відповідальною особою у відповідності до положень розділу 2 документу «Інструкція про порядок підключення технічних майданчиків закладів охорони здоров'я та аптечних закладів. UA.38582529.КСЗІ.00001.ІЗОЗ» проведено розгортання технічного майданчика та зареєстровано в ІТС ролі медичних працівників в такому обсязі:

- лікар – ___;
- адміністратор – ___;
- працівник аптеки – ___;
- пацієнт – ___.

4.4. Комісією, створеною наказом № _____ від __.__.20__, після завершення робіт з розгортання технічного майданчика, у відповідності до розділу 9 документу «Інструкція про порядок підключення технічних майданчиків закладів охорони здоров'я та аптечних закладів. UA.38582529.КСЗІ.00001.ІЗОЗ» проведено перевірку технічного майданчика вимогам до захисту інформації, результати яких викладено нижче.

За результатами проведеної перевірки встановлено, що технічний майданчик відповідає вимогам до фізичного середовища, а саме розміщення його компонентів виконується, виходячи з:

- унеможливлення ознайомлення сторонніми особами з інформацією, що відображається на відображуючих пристроях робочих станцій;

- унеможливлення неконтрольованого несанкціонованого доступу сторонніх осіб до робочих станцій;

- технічних характеристик обладнання і вимог щодо його встановлення та умов експлуатації, визначених їх виробником.

4.5. За результатами проведеної перевірки встановлено, що технічний майданчик відповідає вимогам до захисту інформації від несанкціонованого доступу (далі – НСД), а саме:

- до складу комплексу засобів захисту (далі – КЗЗ) технічного майданчика входять:
  - операційна система (далі – ОС) _____;
  - антивірусне програмне забезпечення _____;
  - засіб криптографічного захисту інформації _____, який має чинний позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації № _____ від __.__.20__ щодо можливості застосування для криптографічного захисту конфіденційної інформації (персональних даних фізичних осіб);
- на робочих станціях, що використовуються у складі технічного майданчика, наявні встановлені наведені вище засоби КЗЗ;

- у засобах КЗЗ зареєстровано облікові записи адміністраторів та працівників закладу охорони здоров'я чи аптечних закладів (далі – працівники) та призначено їх атрибути доступу у відповідності до вимог розділу 4 документу «Інструкція про порядок підключення технічних майданчиків закладів охорони здоров'я та аптечних закладів. UA.38582529.КСЗІ.00001.ІЗОЗ»;

- діючі параметри налагодження КЗЗ та встановлені атрибути доступу відповідають значенням, наведеним в розділі 3 документу «Інструкція про порядок підключення технічних майданчиків закладів охорони здоров'я та аптечних закладів. UA.38582529.КСЗІ.00001.ІЗОЗ»;

- засоби КЗЗ забезпечують реєстрацію дій користувачів щодо доступу до ІТС та оброблюваної у ній інформації з обмеженим доступом;

- засоби КЗЗ забезпечують можливість проведення аналізу зареєстрованих даних уповноваженим адміністратором.

4.6. За результатами проведеної перевірки встановлено, що технічний майданчик відповідає вимогам до антивірусного захисту інформації, а саме:

- на робочих станціях, що використовуються у складі технічного майданчика, наявні встановлені засоби антивірусного захисту _____;

- діючі параметри налагодження антивірусних засобів та використовуваний порядок оновлення антивірусних баз відповідають вимогам, наведеним в розділі 7 документу «Інструкція про порядок підключення технічних майданчиків закладів охорони здоров'я та аптечних закладів. UA.38582529.КСЗІ.00001.ІЗОЗ».

4.7. За результатами проведеної перевірки встановлено, що технічний майданчик із встановленими засобами КЗЗ є працездатним, а саме забезпечується

можливість використання користувачами встановленого програмного забезпечення для обробки інформації, що потребує захисту, згідно з призначеними атрибутами доступу, та обміну цією інформацією з ІТС.

4.8. За результатами проведеної перевірки встановлено, що технічний майданчик відповідає вимогам до належного рівня підготовленості персоналу та впровадження інших організаційних заходів захисту, а саме:

- у відповідальної особи наявні документальні підтвердження ознайомлення працівників з документом «Інструкція про порядок підключення технічних майданчиків закладів охорони здоров'я та аптечних закладів. UA.38582529.КСЗІ.00001.ІЗОЗ»;

- адміністратор та працівники знають основні положення документу «Інструкція про порядок підключення технічних майданчиків закладів охорони здоров'я та аптечних закладів. UA.38582529.КСЗІ.00001.ІЗОЗ» у частині, що їх стосується;

- адміністратор та працівники знають порядок своїх дій на всіх етапах робіт щодо оброблення інформації, яка потребує захисту.

Висновки

У результаті проведення робіт з розгортання технічного майданчику забезпечено виконання вимог щодо захисту інформації, які встановлені в документі «Інструкція про порядок підключення технічних майданчиків закладів охорони здоров'я та аптечних закладів. UA.38582529.КСЗІ.00001.ІЗОЗ».

На підставі результатів перевірки, викладених в розділі 4 цього акту, технічний майданчик визнаний таким, що забезпечує захист оброблюваної інформації відповідно до вимог нормативних документів з технічного захисту інформації в обсязі функцій, наведених в експертному висновку на комплексну систему захисту інформації інформаційно-телекомунікаційної системи «Медична інформаційна система «Доктор Елекс» (додаток до атестату відповідності № _____ від __.__.20__ року).

Технічний майданчик визнаний готовим до підключення до ІТС.

Керівник закладу охорони здоров'я чи аптечного закладу, адміністратор та працівники з вимогами статті 9 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» ознайомлені.

Голова комісії _____ (підпис) _____ (ініціали, прізвище)

Члени комісії _____ (підпис) _____ (ініціали, прізвище)

_____ (підпис) _____ (ініціали, прізвище)

Додаток 2

Типовий зміст зобов'язання працівників закладів охорони здоров'я та аптечних закладів, які користуються інформаційними послугами ІТС (зобов'язання користувачів ІТС)

Я, _____, що проживає за адресою: _____

паспорт ____ № _____, виданий _____

«____» _____ року, на період співпраці з _____

_____

(далі – Заклад охорони здоров'я чи Аптечний заклад) та після її закінчення, зобов'язуюся:

- зберігати ідентифікатори доступу до інформаційно-телекомунікаційної системи «Медична інформаційна система «Доктор Елекс» (далі – прикладне програмне забезпечення «Медична інформаційна система «Доктор Елекс»), в тому числі власні логін та пароль, в таємниці та не розголошувати їх третім особам, в тому числі іншим співробітникам Закладу охорони здоров'я чи Аптечного закладу;
- докладати всіх можливих зусиль для недопущення розголошення власних ідентифікаторів доступу та інформації з обмеженим доступом, в тому числі конфіденційної інформації, комерційної таємниці, персональних даних кінцевих користувачів прикладного програмного забезпечення «Медична інформаційна система «Доктор Елекс»;
- не передавати право/можливість доступу до прикладного програмного забезпечення «Медична інформаційна система «Доктор Елекс» та отримання відомостей з неї третім особам;
- не допускати третіх осіб до роботи з прикладним програмним забезпеченням «Медична інформаційна система «Доктор Елекс» під власним обліковим записом;
- не залишати пристрої, з яких відбувався вхід в прикладне програмне забезпечення «Медична інформаційна система «Доктор Елекс», без нагляду до моменту виходу з прикладного програмного забезпечення «Медична інформаційна система «Доктор Елекс»;
- використовувати для доступу до прикладного програмного забезпечення «Медична інформаційна система «Доктор Елекс» виключно безпечне обладнання (тобто таке, на якому оновлені до останньої доступної версії операційна система та браузер; здійснені налаштування адміністрування операційної системи, що не дозволяють встановлювати без дозволу адміністратора операційної системи іншого програмного забезпечення, що зокрема унеможливлює встановлення кейлогерів; встановлений і оновлений до останньої доступної версії антивірус тощо);
- використовувати для введення ідентифікаторів доступу до прикладного програмного забезпечення «Медична інформаційна система «Доктор Елекс»

виключно екранну клавіатуру;

- негайно доповідати уповноваженим особам Закладу охорони здоров'я чи Аптечного закладу та ТОВ «Доктор Елекс» про:

а) компрометацію облікового запису (розголошення ідентифікаторів доступу);

б) виникнення підозри або виявлення факту доступу до прикладного програмного забезпечення «Медична інформаційна система «Доктор Елекс», отримання відомостей з неї третіми особами;

в) намагання сторонніх осіб у будь-який спосіб отримати інформацію щодо моїх ідентифікаторів доступу до прикладного програмного забезпечення «Медична інформаційна система «Доктор Елекс»;

- негайно змінювати ідентифікатори доступу та/або блокувати обліковий запис у випадку розголошення або підозри розголошення ідентифікаторів доступу;

- після закінчення професійних, службових, договірних чи трудових відносин, при переведенні на іншу посаду, що не пов'язана з роботою в прикладному програмному забезпеченні «Медична інформаційна система «Доктор Елекс», після припинення іншої співпраці, повідомити про це уповноважених осіб Закладу охорони здоров'я чи Аптечного закладу та ТОВ «Доктор Елекс»;

- дотримуватись правил зміни та відновлення паролю, а також вимог до складу паролю, вставлених у прикладному програмному забезпеченні «Медична інформаційна система «Доктор Елекс»;

- зберігати носій електронного підпису (особистого ключа), який використовується для роботи у прикладному програмному забезпеченні «Медична інформаційна система «Доктор Елекс» (в тому числі для підписання медичних документів), у недоступному для третіх осіб місці;

- негайно повідомляти Заклад охорони здоров'я чи Аптечний заклад, ТОВ «Доктор Елекс» та кваліфікованого надавача електронних довірчих послуг, який видав відповідний особистий ключ про його компрометацію, тобто будь-яку подію та/або дію, що призвела або може призвести до несанкціонованого використання особистого ключа;

- не використовувати прикладне програмне забезпечення «Медична інформаційна система «Доктор Елекс» в цілях, що суперечать чинному законодавству України або правам чи законним інтересам третіх осіб;

- вносити до прикладного програмного забезпечення «Медична інформаційна система «Доктор Елекс» виключно повну, правдиву, вичерпну та актуальну інформацію (в тому числі інформацію про стан здоров'я пацієнтів, інші медичні дані, інформацію щодо графіку прийому лікарів, відвідування прийомів пацієнтами та тощо).

Я погоджуюсь, що ТОВ «Доктор Елекс» має право:

- відмовити мені у наданні ідентифікаторів доступу до прикладного програмного забезпечення «Медична інформаційна система «Доктор Елекс» у разі

виникнення об'єктивних сумнівів у можливості збереження в таємниці ідентифікаторів доступу;

- в разі необхідності, з метою уникнення розголошення інформації з обмеженим доступом, в тому числі – конфіденційної інформації, комерційної таємниці, персональних даних користувачів прикладного програмного забезпечення «Медична інформаційна система «Доктор Елекс», в односторонньому порядку обмежити або заблокувати мій доступ до прикладного програмного забезпечення «Медична інформаційна система «Доктор Елекс» та вимагати усунення порушень.

Я підтверджую:

- інформація, що вноситься мною в прикладне програмне забезпечення «Медична інформаційна система «Доктор Елекс» (в тому числі про стан здоров'я пацієнтів, інші медичні дані) є повною, актуальною, правдивою, вичерпною та не порушує чинного законодавства України;

- взяття на себе зобов'язання зі збереження у таємниці ідентифікаторів доступу до прикладного програмного забезпечення «Медична інформаційна система «Доктор Елекс»;

- прийняття мною адекватних заходів для збереження ідентифікаторів доступу в таємниці;

- розуміння наслідків порушення цього зобов'язання, результатом якого стало розголошення інформації з обмеженим доступом (в тому числі конфіденційної інформації, комерційної таємниці, персональних даних користувачів прикладного програмного забезпечення «Медична інформаційна система «Доктор Елекс»), а також будь-яких незаконних дій відносно інформації, внесеної в прикладне програмне забезпечення «Медична інформаційна система «Доктор Елекс» (таких як знищення персональних даних, зміна персональних даних чи іншої інформації, в тому числі тимчасова, тощо); такими наслідками є можливість притягнення до дисциплінарної, адміністративної чи кримінальної відповідальності згідно з вимогами законодавства України, а також відшкодування шкоди, завданої подібними діями.