ПОГОДЖЕНО
Перший заступник Голови
Державної служби
спеціального зв'язку
та захисту інформації України

О.М. Чаузов
«28» 11 2019 р.

ЗАТВЕРДЖУЮ
В.о. генерального директора
ДП «Електронне здоров'я»

А.В. Сучик
«__» _____ 20__ р.

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

2019

ЗМІСТ

1. Загальна інформація

Цей документ відображає загальні технічні вимоги до електронних медичних та фармацевтичних (аптечних) інформаційних систем, які будуть підключатися до інформаційно-телекомунікаційної системи «Центральна база даних електронної системи охорони здоров'я» (далі – ІТС ЦБД), а також призначений для виконання при забезпеченні заходів з побудови комплексних систем захисту інформації таких систем (зокрема - у частині передпроектних робіт, розробки технічного завдання, проектування, побудови, випробувань та дослідної експлуатації комплексної системи захисту інформації, а також проходження державної експертизи в сфері технічного захисту інформації).

Цей документ розроблений державним підприємством «Електронне здоров'я», яке відповідно до Порядку функціонування електронної системи охорони здоров'я, затвердженого постановою Кабінету Міністрів України від 25.04.2018 № 411, виконує функції адміністратора ІТС ЦБД та вживає заходів до захисту інформації, що міститься в ЦБД, відповідно до вимог законодавства.

При розробці цього документу враховані:

- вимоги законодавства з питань захисту інформації;
- нормативних документів системи технічного захисту інформації з питань створення комплексних систем захисту інформації;
- роз'яснення Держспецзв'язку, як державного органу, який призначений для формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації;
- модель загроз безпеки інформації, що обробляється та зберігається в ІТС ЦБД, та модель порушників безпеки для цієї інформації, які були визначені на етапі побудови комплексної системи захисту інформації в ІТС ЦБД.

Посилання на нормативні документи:

- 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 від 29.03.06 № 373;
- Порядок функціонування електронної системи охорони здоров'я, затверджений постановою Кабінету Міністрів України від 25.04.2018 № 411;
- Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 16.05.2007 № 93 (зі змінами);
- НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу;
- НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі;
- ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення;
- ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

2. Опис та призначення ІТС ЦБД

ІТС ЦБД призначена для централізованого збереження та обробки відомостей у центральній базі даних електронної системи охорони здоров'я, а також забезпечення можливості створення, перегляду, обміну інформацією та документами між реєстрами, ведення яких забезпечується з її використанням, та зовнішніми інформаційно-телекомунікаційними системами (медичними та фармацевтичними (аптечними) інформаційними системами) в порядку, визначеному Порядком функціонування електронної системи охорони здоров'я, затвердженому постановою Кабінету Міністрів України від 25.04.2018 № 411, та наданню інших сервісів, передбачених чинним законодавством.

Характеристики інформації, що обробляється та зберігається в ІТС ЦБД:

- технологічна інформація (налаштування програмного та апаратного забезпечення ІТС, налаштування безпеки програмного та апаратного забезпечення ІТС, паролі та логіни користувачів ІТС та дані їх облікових записів, журнали реєстрації тощо), технологічна інформація є інформацією з обмеженим доступом (конфіденційною інформацією), яка доступна тільки адміністраторам ІТС ЦБД згідно з їхніми службовими обов'язками; до цієї інформації висуваються підвищені вимоги щодо забезпечення її конфіденційності, цілісності та доступності;
- відкрита інформація (інформація, що містить загальнодоступні дані щодо закладів охорони здоров'я (аптечні заклади) та його працівників); до цієї інформації висуваються підвищені вимоги щодо забезпечення її цілісності та доступності
- персональні дані пацієнтів, конфіденційна інформація, що містить, а також ключові дані обслуговуючого персоналу ІТС; до цієї інформації висуваються підвищені вимоги щодо забезпечення її конфіденційності, цілісності та доступності.

3. Загальні вимоги до електронних медичних та фармацевтичних (аптечних) інформаційних систем, що підключаються до ІТС ЦБД

При підключенні та інформаційній взаємодії електронних медичних та/або фармацевтичних (аптечних) інформаційних систем (далі – МІС) із ІТС ЦБД повинен забезпечуватись захист інформації від несанкціонованого та неконтрольованого ознайомлення (в тому числі при передачі через незахищене середовище), модифікації, знищення, копіювання, поширення, а також забезпечення постійної доступності зазначеної інформації для авторизованих користувачів та забезпечення спостережності за їх функціонуванням.

З урахуванням наведених відомостей:

- ДП «Електронне здоров'я» розробляє та узгоджує загальні правила політики безпеки, що діють в межах МІС;

- технічне завдання на КСЗІ МІС повинно бути погоджене із ДП «Електронне здоров'я» та Адміністрацією Державної служби спеціального зв'язку та захисту інформації;
- підключення МІС до ІТС ЦБД, обмін та обробка даними з нею повинна бути можливою лише за умови підтвердження відповідності у встановленому порядку створеної в ній комплексної системи захисту інформації.

МІС має виконувати мінімальні вимоги щодо кіберзахисту своєї ІТС, а саме:

1) необхідність регулярного встановлення оновлень загального програмного забезпечення (операційних систем, систем керування базами даних, програмних бібліотек тощо);

2) необхідність контролю цілісності та автентичності оновлень програмного забезпечення (як системного прикладного забезпечення (далі – ПЗ), так і прикладного ПЗ МІС) з урахуванням особливостей побудови та функціонування відповідного програмного забезпечення;

3) необхідність забезпечення мережевого захисту МІС, щонайменше, в такому обсязі:

- фільтрація та аналіз мережевого трафіку за протоколами, портами і IP-адресами відправника й одержувача;
- маскування топології і мережевих адрес технічних засобів МІС від публічного перегляду;
- контроль інформаційних потоків з метою виявлення спроб мережевих вторгнень та несанкціонованого доступу до мережевих ресурсів МІС, виявлення і протидія мережевим атакам і несанкціонованій мережевій активності, забезпечення реєстрації, попередження та протидії таким спробам;
- протоколювання (реєстрація) подій, що мають відношення до мережевої безпеки.

Рекомендовано встановити необхідність процедур тестування безпеки прикладного ПЗ МІС, які повинні виконуватись перед оновленням прикладного ПЗ МІС на серверах МІС. Методи тестування безпеки прикладного ПЗ МІС повинні обиратись розробником виходячи з технології розробки прикладного ПЗ МІС (використання статичних аналізаторів коду, ручне тестування за OWASP Testing Guide, автоматизоване сканування вразливостей або ін.) з урахуванням особливостей побудови та функціонування відповідного програмного забезпечення.

Комплекс засобів захисту МІС має забезпечувати захист даних, зокрема, забезпечувати їх конфіденційність, цілісність, доступність та розмежування доступу до них.

Для підключення до ІТС ЦБД, виконання функцій формування / перевіряння кваліфікованого електронного підпису, для взаємодії з кінцевими користувачами в складі МІС мають використовуватись засоби криптографічного захисту інформації, які мають чинний позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації щодо можливості їх використання для

криптографічного захисту конфіденційної інформації (персональних даних фізичних осіб).

МІС має відповідати вимогам Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», Правилам забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затвердженим Постановою Кабінету Міністрів України від 29.03.06 № 373, та інших нормативно-правових актів, що регулюють питання захисту інформації з обмеженим доступом в інформаційно-телекомунікаційних системах, а також забезпечувати обробку інформації в порядку, визначеному в Порядку функціонування електронної системи охорони здоров'я, затвердженому постановою Кабінету Міністрів України від 25.04.2018 № 411.

МІС має підтримувати протоколи інформаційної взаємодії (прикладні програмні інтерфейси) з ІТС ЦБД згідно відповідних технічних вимог (онлайн-ресурс «eHealth API», доступний за посиланням https://uaehealthapi.docs.apiary.io/ #introduction/contribution-guidelines).

За необхідності МІС має забезпечувати надання відповідних рекомендацій кінцевим користувачам щодо забезпечення безпеки даних, що обробляються та зберігаються в їх інформаційних системах (в тому числі, розгорнутих з використанням організаційно-технічних рішень на розгортання типових складових компонент КСЗІ).

МІС повинна реалізовувати такі **основні функції захисту:**

- забезпечення стійкості МІС в цілому до відмов та унеможливлення втрати інформації;
- забезпечення періодичного резервного копіювання баз даних МІС;
- розмежування доступу користувачів МІС до інформації, що обробляється та зберігається в ній, відповідно до їх повноважень згідно технологічного процесу обробки інформації;
- забезпечення однозначної ідентифікації та автентифікації користувачів МІС;
- забезпечення ведення журналів реєстрації подій;
- забезпечення захисту організаційними заходами від несанкціонованого доступу до інформації при її обробці засобами МІС;
- контроль за проходженням на мережевому рівні тільки дозволених інформаційних потоків з боку телекомунікаційних мереж до МІС, а також в зворотному напрямку (щонайменш, на рівнях L3, L4 моделі Open Systems Interconnections, OSI);
- забезпечення реєстрації подій, пов'язаних з отриманням користувачами доступу до ресурсів МІС (проходження/непроходження автентифікації), зміни настроювань програмного забезпечення, серверів та комутаційного обладнання;
- наявність засобів перегляду та аналізу подій (логування);
- наявність засобів для резервування конфігураційних файлів та критично важливих для функціонування обладнання МІС системних файлів (створення образів дисків, резервування операційних систем серверів та

комутаційного обладнання) з метою їх наступного швидкого відновлення в разі збоїв;

- забезпечення конфіденційності та цілісності інформації з обмеженим доступом, що передається каналами зв'язку через незахищене середовище;
- формування та перевірку кваліфікованого електронного підпису на інформаційних об'єктах в МІС її користувачами відповідно до їх повноважень згідно технологічного процесу обробки інформації;
- забезпечення антивірусного захисту (забезпечення захисту від внесення в МІС шкідливого програмного коду (вірусів, троянських програм та ін.), перевірку на наявність шкідливого програмного коду всіх вкладень що завантажуються користувачами до МІС та у разі ураження вкладень шкідливим програмним кодом, блокувати завантаження для запобігання використанню МІС у протиправних і злочинних цілях, блокування завантаження виконуваних файлів та скриптів до МІС тощо).

4. Вимоги до функціонування електронних медичних та фармацевтичних (аптечних) інформаційних систем, що підключаються до ІТС ЦБД

4.1 Захист від несанкціонованого доступу

Для захисту інформації, що передається між МІС та ІТС ЦБД, повинен використовуватись програмний засіб шифрування даних з використанням протоколу захисту транспортного рівня TCP Transport Layer Security (TLS), який призначений для забезпечення криптографічного захисту даних, що передаються з використанням протоколу захисту транспортного рівня TCP Transport Layer Security (TLS) або інші засоби криптографічного захисту інформації, що мають чинні позитивні експертні висновки за результатами державної експертизи в сфері криптографічного захисту інформації щодо можливості його використання для криптографічного захисту конфіденційної інформації (персональних даних фізичних осіб) або інші засоби криптографічного захисту інформації. Рішення щодо використання конкретних засобів криптографічного захисту інформації для захисту інформації, що передається між МІС та ІТС ЦБД, приймається ДП «Електронне здоров'я».

Для формування / перевіряння кваліфікованого електронного підпису та для обміну даними з кінцевими користувачами (закладами охорони здоров'я, аптечними закладами тощо) через незахищене середовище в складі МІС повинні використовуватись засоби криптографічного захисту інформації, які мають чинний позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації щодо можливості їх використання для криптографічного захисту конфіденційної інформації (персональних даних фізичних осіб).

Комплекс засобів захисту МІС повинен забезпечувати виконання таких функцій захисту інформації від несанкціонованого доступу:

- розмежування доступу до інформації, що обробляється та зберігається в МІС (шляхом реалізації функціональних послуг безпеки «Адміністративна конфіденційність», щонайменше, на рівні КА-2 та «Адміністративна цілісність», щонайменше, на рівні ЦА-1, див. п. 4.1.1, 4.1.3 цього документу);

- забезпечення конфіденційності та цілісності інформації при її передачі через незахищене середовище, підтвердження автентичності сторін обміну такою інформацією (шляхом реалізації функціональних послуг безпеки «Конфіденційність при обміні», щонайменше, на рівні КВ-1, «Цілісність при обміні», щонайменше, на рівні ЦВ-1 та «Ідентифікація та автентифікація при обміні», щонайменше, на рівні НВ-1 див. п. 4.1.2, 4.1.5, 4.1.14 цього документу);
- відкат (відмову) операцій оновлення системного програмного забезпечення технічних засобів МІС та їх технологічної конфігураційної інформації (шляхом реалізації функціональної послуги безпеки «Відкат», щонайменше, на рівні ЦО-1, див. п. 4.1.4 цього документу);
- забезпечення стійкості до відмов технічних засобів МІС (шляхом реалізації функціональної послуги безпеки «Стійкість до відмов», щонайменше, на рівні ДС-1, див. п. 4.1.6 цього документу);
- оновлення апаратного та програмного забезпечення технічних засобів МІС та відновлення її працездатності в разі збоїв в роботі (шляхом реалізації функціональних послуг безпеки «Гаряча заміна», щонайменше, на рівні ДЗ-1 та «Відновлення після збоїв», щонайменше, на рівні ДВ-1, див. п. 4.1.7, 4.1.8 цього документу);
- ведення журналів реєстрації подій (шляхом реалізації функціональної послуги безпеки «Реєстрація», щонайменше, на рівні НР-2, див. п. 4.1.9 цього документу);
- забезпечення ідентифікації та автентифікації користувачів МІС (шляхом реалізації функціональної послуги безпеки «Ідентифікація та автентифікація», щонайменше, на рівні НИ-1, див. п. 4.1.10 цього документу);
- забезпечення виділення адміністративних ролей користувачів, які керують функціонуванням МІС та відповідають за забезпечення безпеки інформації в ній (шляхом реалізації функціональної послуги безпеки «Розподіл обов'язків», щонайменше, на рівні НО-2 з урахуванням приміток, наведених в п. 4.1.11 цього документу);
- забезпечення цілісності засобів захисту інформації МІС та контроль за їх функціонуванням (шляхом реалізації функціональних послуг безпеки «Цілісність комплексу засобів захисту», щонайменше, на рівні НЦ-1 та «Самотестування», щонайменше, на рівні НТ-2, див. п. 4.1.12, 4.1.13 цього документу);
- забезпечення ідентифікації та автентифікації посадових осіб закладів охорони здоров'я, які здійснюють формування (завантаження) даних до МІС (шляхом реалізації функціональної послуги безпеки «Автентифікація відправника», щонайменше, на рівні НА-2 з урахуванням приміток, наведених в п. 4.1.15 цього документу).

Політика безпеки інформації, яка реалізується кожною наведеною функціональною послугою безпеки, повинна визначатись згідно НД ТЗІ 2.5-004-99 з урахуванням наведених нижче положень. Наведені положення визначають мінімальний обов'язковий набір правил політики безпеки інформації, що реалізуються відповідною функціональною послугою безпеки, та визначають лише ті вимоги, які уточнюють (конкретизують) або підсилюють

відповідні специфікації, визначені в НД ТЗІ 2.5-004-99. Решта специфікацій відповідних функціональних послуг безпеки, не визначені в цьому документі, повинні відповідати вимогам НД ТЗІ 2.5-004-99.

Власником (адміністратором) МІС при побудові комплексної системи захисту інформації в МІС наведені нижче правила політики безпеки інформації для кожної функціональної послуги можуть бути підвищені, виходячи з особливостей побудови та функціонування конкретної інформаційної системи, а також можуть бути запропонована реалізація інших (додаткових або таких, що мають більш високий рівень реалізації) функціональних послуг безпеки.

4.1.1 Вимоги до реалізації функціональної послуги безпеки «Адміністративна конфіденційність» рівня КА-2

Політика послуги повинна стосуватись наступної інформації, що обробляється та зберігається в МІС:

- інформація, що містить персональні дані пацієнтів;
- ключові дані обслуговуючого персоналу МІС;
- технологічна конфігураційна інформація апаратного та програмного забезпечення технічних засобів МІС (системного, прикладного та антивірусного програмного забезпечення, систем управління базами даних, засобів криптографічного захисту інформації, комутаційного обладнання (в тому числі активного мережевого обладнання) тощо).

Управління доступом до інформації, що містить персональні дані пацієнтів, повинно здійснюватися уповноваженою посадовою особою закладу охорони здоров'я (аптечного закладу), якій надано відповідні повноваження щодо управління правами доступу працівників відповідного закладу, або адміністратором МІС шляхом призначення працівника закладу охорони здоров'я (аптечного закладу) на відповідну роль в прикладному програмному забезпеченні МІС. Для управління правами доступу МІС повинна підтримувати відповідні облікові записи користувачів, які не використовуються працівниками закладів при виконанні інших, не пов'язаних з управлінням правами доступу, покладених на них функціональних обов'язків.

Управління доступом до ключових даних працівників закладів охорони здоров'я (аптечних закладів) повинно здійснюватися власником відповідних ключових даних особисто.

Управління доступом до технологічної конфігураційної інформації апаратного та програмного забезпечення технічних засобів МІС повинно здійснюватися адміністраторами МІС.

Працівники закладу охорони здоров'я (аптечного закладу) повинні отримувати доступ (в частині читання / перегляду) до інформації, що містить персональні дані пацієнтів лише в обсязі, необхідному для виконання покладених функціональних обов'язків з урахуванням вимог Порядку функціонування електронної системи охорони здоров'я, затвердженого постановою Кабінету Міністрів України від 25.04.2018 № 411.

Доступ до технологічної конфігураційної інформації апаратного та програмного забезпечення технічних засобів МІС (в частині читання / перегляду) повинні мати лише адміністратори МІС.

Правила розмежування доступу та порядок управління доступом до інформації, що обробляється та зберігається в МІС, повинні бути документовані.

4.1.2 Вимоги до реалізації функціональної послуги безпеки «Конфіденційність при обміні» рівня КВ-1

Політика послуги повинна стосуватись обміну конфіденційною інформацією, що містить персональні дані пацієнтів та технологічну конфігураційну інформацію апаратного та програмного забезпечення технічних засобів МІС та яка передається між МІС та:

- ІТС ЦБД;
- кінцевими користувачами (працівниками закладу охорони здоров'я та / або аптечного закладу, в разі, якщо доступ зазначених користувачів до МІС здійснюється з територіально віддалених технічних майданчиків цих закладів)
- адміністраторами МІС (в разі, якщо адміністратори МІС здійснюють віддалене адміністрування програмного та апаратного забезпечення МІС з територіально віддалених технічних майданчиків).

Для криптографічного захисту такої інформації повинні використовуватись засоби криптографічного захисту інформації, які забезпечують шифрування відповідних даних та мають сертифікат відповідності або чинний позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації щодо можливості їх використання для криптографічного захисту конфіденційної інформації.

Управління налаштуваннями засобів криптографічного захисту інформації МІС повинно здійснюватися адміністраторами МІС.

Правила забезпечення криптографічного захисту та порядок управління налаштуваннями засобів криптографічного захисту інформації МІС повинні бути документовані.

4.1.3 Вимоги до реалізації функціональної послуги безпеки «Адміністративна цілісність» рівня ЦА-1

Політика послуги повинна стосуватись наступної інформації, що обробляється та зберігається в МІС:

- відкрита загальнодоступна інформація;
- інформація, що містить персональні дані пацієнтів;
- ключові дані обслуговуючого персоналу МІС;
- технологічна конфігураційна інформація апаратного та програмного забезпечення технічних засобів МІС (системного, прикладного та антивірусного програмного забезпечення, систем управління базами даних, засобів криптографічного захисту інформації, комутаційного обладнання (в тому числі активного мережевого обладнання) тощо).

Управління доступом до інформації, що містить персональні дані пацієнтів, повинно здійснюватися уповноваженою посадовою особою закладу охорони здоров'я (аптечного закладу), якій надано відповідні повноваження щодо управління правами доступу працівників відповідного закладу, або

адміністратором МІС шляхом призначення працівника закладу охорони здоров'я (аптечного закладу) на відповідну роль в прикладному програмному забезпеченні МІС. Для управління правами доступу МІС повинна підтримувати відповідні облікові записи користувачів, які не використовуються працівниками закладів при виконанні інших, не пов'язаних з управлінням правами доступу, покладених на них функціональних обов'язків.

Управління доступом до ключових даних працівників закладів охорони здоров'я (аптечних закладів) повинно здійснюватися власником відповідних ключових даних особисто.

Управління доступом до технологічної конфігураційної інформації апаратного та програмного забезпечення технічних засобів МІС повинно здійснюватися адміністраторами МІС.

Працівники закладу охорони здоров'я (аптечного закладу) повинні отримувати доступ (в частині модифікації, створення та видалення) до інформації, що містить персональних даних пацієнтів лише в обсязі, необхідному для виконання покладених функціональних обов'язків з урахуванням вимог Порядку функціонування електронної системи охорони здоров'я, затвердженого постановою Кабінету Міністрів України від 25.04.2018 № 411.

Доступ до технологічної конфігураційної інформації апаратного та програмного забезпечення технічних засобів МІС (в частині модифікації, створення та видалення) повинні мати лише адміністратори МІС.

Правила розмежування доступу та порядок управління доступом до інформації, що обробляється та зберігається в МІС, повинні бути документовані.

4.1.4 Вимоги до реалізації функціональної послуги безпеки «Відкат» рівня ЦО-1

Політика послуги повинна відноситися, щонайменш, до системного програмного забезпечення МІС та забезпечувати за необхідності відкат (відмову) операцій щодо оновлення системного програмного забезпечення її технічних засобів (наприклад, при втраті зв'язку з відповідними серверами оновлення його виробника) та відповідними змінами в технологічній конфігураційній інформації такого програмного забезпечення для повернення системного програмного забезпечення технічних засобів МІС до попереднього захищеного працездатного стану.

Відкат (відмова) наведених операцій повинні здійснюватися адміністраторами МІС.

Правила проведення відкату (відмови) наведених операцій повинні бути документовані.

4.1.5 Вимоги до реалізації функціональної послуги безпеки «Цілісність при обміні» рівня ЦВ-1

Політика послуги повинна стосуватись обміну всією інформацією, яка передається між МІС та:

- ІТС ЦБД;

- кінцевими користувачами (працівниками закладу охорони здоров'я та / або аптечного закладу, в разі, якщо доступ зазначених користувачів до МІС здійснюється з територіально віддалених технічних майданчиків цих закладів)
- адміністраторами МІС (в разі, якщо адміністратори МІС здійснюють віддалене адміністрування програмного та апаратного забезпечення МІС з територіально віддалених технічних майданчиків).

Для криптографічного захисту такої інформації повинні використовуватись засоби криптографічного захисту інформації, які забезпечують контроль цілісності (з використанням засобів формування та перевірки імітовставки та/або кваліфікованого електронного підпису) відповідних даних та мають сертифікат відповідності або чинний позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації щодо можливості їх використання для криптографічного захисту конфіденційної інформації.

Управління налаштуваннями засобів криптографічного захисту інформації МІС повинно здійснюватися адміністраторами МІС.

Правила забезпечення криптографічного захисту та порядок управління налаштуваннями засобів криптографічного захисту інформації МІС повинні бути документовані.

4.1.6 Вимоги до реалізації функціональної послуги безпеки «Стійкість до відмов» рівня ДС-1

Власником МІС повинен бути проведений аналіз можливих загроз до стійкості функціонування інформаційної системи та її доступності, а також запропоновані заходи щодо забезпечення її працездатності при успішній реалізації зазначених загроз. Як приклади зазначених заходів можуть бути розглянуті:

- резервування електроживлення (за рахунок використання джерел безперебійного живлення);
- резервування засобів зберігання та обробки даних (за рахунок використання відповідних дублюючих (резервних) компонентів);
- резервування каналів зв'язку (за рахунок використання резервованих каналів зв'язку).

Порядок дій користувачів МІС при настанні таких відмов повинні бути документовані.

4.1.7 Вимоги до реалізації функціональної послуги безпеки «Гаряча заміна» рівня ДЗ-1

Політика послуги повинна забезпечувати можливість оновлення апаратного та програмного забезпечення технічних засобів МІС, що забезпечує покращення її експлуатаційних характеристик та не призводить до необхідності проведення додаткової державної експертизи комплексної системи захисту інформації МІС в сфері технічного захисту інформації. Обов'язковому оновленню підлягає програмне забезпечення засобів антивірусного захисту та їх бази антивірусних сигнатур.

Модернізація повинна проводитись адміністраторами МІС.

Обсяг можливих змін в апаратному та програмному забезпеченні технічних засобів МІС, повноваження та обов'язки адміністраторів МІС щодо проведення модернізації та порядок проведення модернізації повинні бути документовані.

4.1.8 Вимоги до реалізації функціональної послуги безпеки «Відновлення після збоїв» рівня ДВ-1

Політика послуги повинна забезпечувати можливість повернення МІС до попереднього захищеного стану та відновлення її працездатності після настання збоїв в роботі програмного або апаратного забезпечення її технічних засобів, що призвели до припинення функціонування або втрати інформації, що обробляється та зберігається в МІС. З цією метою повинно забезпечуватись періодичне резервне копіювання інформації, що обробляється та зберігається в МІС.

Відновлення працездатності повинно здійснюватися адміністраторами МІС.

Процедури відновлення працездатності МІС, повноваження та обов'язки адміністраторів МІС щодо відновлення працездатності МІС та інформації, що обробляється та зберігається в ній, повинні бути документовані.

4.1.9 Вимоги до реалізації функціональної послуги безпеки «Реєстрація» рівня НР-2

Політика послуги повинна відноситись до всіх користувачів ІТС та забезпечувати можливість ведення журналів реєстрації подій, в яких загальному випадку повинні реєструватись, щонайменше, наступні типи подій:

- вхід / вихід користувачів до системного та прикладного програмного забезпечення технічних засобів МІС;
- доступ до інформації, що обробляється та зберігається в МІС, та дії з нею;
- здійснення резервного копіювання та відновлення інформації, що обробляється та зберігається в МІС;
- управління обліковими записами користувачів в системному та прикладному програмному забезпеченні технічних засобів МІС;
- управління правами доступу користувачів;
- порушення цілісності системного та прикладного програмного забезпечення, а також порушення працездатності комутаційного обладнання МІС.

Повинно забезпечуватись ведення журналів реєстрації подій, щонайменше, засобами:

- системного та прикладного програмного забезпечення технічних засобів МІС;
- антивірусного програмного забезпечення;
- комутаційного обладнання.

Перегляд та аналіз журналів реєстрації подій повинні здійснювати лише адміністратори МІС.

Процедури контролю за станом функціонування МІС з використанням журналів реєстрації подій, повноваження та обов'язки адміністраторів МІС щодо проведення цих заходів повинні бути документовані.

4.1.10 Вимоги до реалізації функціональної послуги безпеки «Ідентифікація та автентифікація» рівня НИ-1

Політика послуги повинна забезпечувати можливість ідентифікації та автентифікації всіх користувачів МІС, які отримують доступ до її інформаційних ресурсів. В разі виділення в МІС користувачів мережі Інтернет, які отримують доступ до МІС лише для перегляду загальнодоступної відкритої інформації, вимоги до їх ідентифікації та автентифікації не висуваються.

Ідентифікація та автентифікація користувачів МІС повинна здійснюватися, щонайменше, за їх ідентифікатором, отриманим від зовнішніх (по відношенню до МІС) сервісів авторизації користувачів, наприклад:

- інформаційно-телекомунікаційної системи «Центральна база даних електронної системи охорони здоров'я»;
- інформаційно-аналітичної платформи електронної верифікації та моніторингу.

За необхідності власником МІС можуть бути запроваджені механізми ідентифікації та автентифікації користувачів з використанням власних засобів системного та прикладного програмного забезпечення технічних засобів МІС (реалізація функціональної послуги безпеки на рівні НИ-2), а також механізми багатофакторної автентифікації (реалізація функціональної послуги безпеки на рівні НИ-3).

Управління даними облікових записів адміністраторів МІС повинно здійснюватися ними особисто, а управління даними облікових записів кінцевих користувачів уповноваженою посадовою особою закладу охорони здоров'я (аптечного закладу) або адміністраторами МІС.

4.1.11 Вимоги до реалізації функціональної послуги безпеки «Розподіл обов'язків» рівня НО-2

Політика послуги повинна визначати, щонайменше, дві адміністративні ролі користувачів та ролі кінцевих користувачів.

Як приклади адміністративних ролей користувачів можуть бути розглянуті системний адміністратор та адміністратор безпеки.

Так для адміністраторів повинна забезпечуватись можливість виконання, щонайменше, наступних операцій:

- управління технологічною конфігураційною інформацією апаратного та програмного забезпечення технічних засобів МІС;
- управління обліковими записами користувачів МІС та їх правами доступу до інформації, що обробляється та зберігається в МІС;
- проведення відкату (відмови) операцій щодо оновлення системного програмного забезпечення технічних засобів МІС та відповідними змінами в технологічній конфігураційній інформації такого програмного забезпечення;
- проведення заходів з модернізації (оновлення) апаратного та програмного забезпечення технічних засобів МІС;

- проведення заходів з резервного копіювання інформації, що обробляється та зберігається в МІС, відновлення працездатності МІС;
- перегляд журналів реєстрації подій, що ведуться в МІС;
- контроль цілісності та працездатності апаратного та програмного забезпечення технічних засобів МІС;
- проведення антивірусних перевірок в МІС та контроль за станом антивірусного захисту.

Розподіл наведених обов'язків між адміністративними ролями користувачів визначається власником МІС виходячи з особливостей побудови та функціонування відповідної інформаційної системи. За обґрунтованим рішенням власника МІС, виходячи з особливостей функціонування конкретної інформаційної системи та її організаційного забезпечення, з урахуванням можливих ризиків щодо поєднання адміністративних обов'язків посадових осіб, які керують функціонуванням МІС та відповідають за забезпечення безпеки інформації в ній, послуга «Розподіл обов'язків (НО)» може бути реалізована на рівні НО-1. Таке обґрунтування наводиться у відповідному технічному завданні на створення комплексної системи захисту інформації, яке розробляється, погоджується та затверджується з урахуванням вимог розділу 3 цього документу.

Як приклади ролей кінцевих користувачів можуть бути наведені наступні:
- керівник (власник, головний лікар) закладу охорони здоров'я;
- реєстратор (працівник реєстратури закладу охорони здоров'я);
- лікар закладу охорони здоров'я;
- керівник підрозділу обліку кадрів закладу охорони здоров'я;
- керівник (власник) аптечного закладу;
- фармацевт (працівник аптечного закладу).

При визначенні конкретного переліку ролей кінцевих користувачів та їх прав доступу до інформації, що обробляється та зберігається в МІС, необхідно керуватись положеннями документації щодо інтеграції та забезпечення інформаційної взаємодії з інформаційно-телекомунікаційною системою «Центральна база даних електронної системи охорони здоров'я».

Обов'язки адміністраторів МІС повинні бути покладені на відповідних посадових осіб наказом (розпорядженням) власника МІС, керівника закладу охорони здоров'я або аптечного закладу, в залежності від особливостей побудови та функціонування конкретної інформаційної системи.

4.1.12 Вимоги до реалізації функціональної послуги безпеки «Цілісність комплексу засобів захисту» рівня НЦ-1

Політика послуги повинна забезпечувати контроль цілісності, щонайменше, таких засобів захисту інформації, що входять до складу комплексу засобів захисту МІС:
- платформи віртуалізації (в разі використання);
- системного програмного забезпечення;
- прикладного програмного забезпечення (в тому числі систем керування базами даних);
- антивірусного програмного забезпечення;

- засобів криптографічного захисту інформації;
- комутаційного обладнання (в тому числі міжмережевого екрану).

Адміністратори МІС повинні мати повноваження щодо контролю цілісності наведених засобів захисту інформації та здійснення за необхідності їх відновлення.

Процедури контролю та відновлення цілісності, повноваження та обов'язки адміністраторів МІС щодо проведення зазначених операцій повинні бути документовані.

4.1.13 Вимоги до реалізації функціональної послуги безпеки «Самотестування» рівня НТ-1

Політика послуги повинна забезпечувати можливість самотестування щонайменше, таких засобів захисту інформації, що входять до складу комплексу засобів захисту МІС:

- платформи віртуалізації (в разі використання);
- системного програмного забезпечення;
- прикладного програмного забезпечення (в тому числі систем керування базами даних);
- антивірусного програмного забезпечення;
- засобів криптографічного захисту інформації;
- комутаційного обладнання (в тому числі міжмережевого екрану).

Адміністратори МІС повинні мати можливість запуску процедур самотестування наведених засобів захисту інформації.

Процедури проведення самотестування засобів захисту інформації МІС, повноваження та обов'язки адміністраторів МІС щодо проведення зазначених операцій повинні бути документовані.

4.1.14 Вимоги до реалізації функціональної послуги безпеки «Ідентифікація та автентифікація при обміні» рівня НВ-1

Політика послуги повинна забезпечувати автентифікацію засобів захисту інформації, що використовуються в складі МІС та використовуються для встановлення режиму захищеного обміну даними між МІС та:

- ІТС ЦБД;
- кінцевими користувачами (працівниками закладу охорони здоров'я та / або аптечного закладу, в разі, якщо доступ зазначених користувачів до МІС здійснюється з територіально віддалених технічних майданчиків цих закладів)
- адміністраторами МІС (в разі, якщо адміністратори МІС здійснюють віддалене адміністрування програмного та апаратного забезпечення МІС з територіально віддалених технічних майданчиків).

Для автентифікації повинні використовуватись засоби криптографічного захисту інформації, які забезпечують автентифікацію (перевірку справжності) сторін обміну даними та встановлення захищеного каналу зв'язку між ними та мають сертифікат відповідності або чинний позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації щодо можливості їх використання для криптографічного захисту конфіденційної інформації.

Управління налаштуваннями засобів криптографічного захисту інформації МІС повинно здійснюватися адміністраторами МІС.

Правила забезпечення криптографічного захисту та порядок управління налаштуваннями засобів криптографічного захисту інформації МІС повинні бути документовані.

4.1.15 Вимоги до реалізації функціональної послуги безпеки «Автентифікація відправника» рівня НА-2

Політика послуги повинна забезпечувати можливість проведення автентифікації, щонайменше, медичних працівників закладів охорони здоров'я, які здійснюють формування наборів медичних даних (медична картка пацієнта, декларація про вибір лікаря, який надає первинну медичну допомогу, рецепти, направлення, медичні записи тощо) в МІС. Автентифікація лікаря закладу охорони здоров'я повинна здійснюватися за його кваліфікованим електронним підписом, яким засвідчуються наведені вище набори медичних даних.

Конкретний перелік наборів медичних даних, які засвідчуються кваліфікованим електронним підписом, визначається власником МІС в залежності від особливостей її побудови та функціонування.

Для накладання кваліфікованого електронного підпису використовується особистий ключ медичного працівника закладу охорони здоров'я – формувача (відправника) відповідних даних; для перевірки кваліфікованого електронного підпису використовується його кваліфікований сертифікат відкритого ключа, створений відповідним кваліфікованим надавачем електронних довірчих послуг.

Надання послуг з кваліфікованого електронного підпису та обслуговування сертифікатів відкритих ключів, які використовуються для забезпечення функціонування МІС, повинно здійснюватися кваліфікованим відповідно до законодавства України надавачем електронних довірчих послуг.

Для автентифікації повинні використовуватись засоби криптографічного захисту інформації, які забезпечують перевірку справжності відправника (з використанням засобів формування та перевірки кваліфікованого електронного підпису) та мають сертифікат відповідності або чинний позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації щодо можливості їх використання для криптографічного захисту конфіденційної інформації.

Функціональні послуги безпеки, специфікації яких наведені в п. 4.1.1 – 4.1.15 цього документу, за сукупністю формують наступний мінімальний функціональний профіль захищеності, який має реалізуватись комплексом засобів захисту МІС {КА-2, КВ-1, ЦА-1, ЦО-1, ЦВ-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НИ-1, НО-2, НЦ-1, НТ-1, НВ-1, НА-2}.

4.2 Використання засобів антивірусного захисту

На всіх ЕОМ, включених до складу МІС, повинні бути встановлені засоби антивірусного захисту.

На ЕОМ, на яких здійснюється завантаження файлів кінцевими користувачами (працівниками закладів охорони здоров'я, аптечних закладів тощо), повинні бути встановлені засоби антивірусного захисту, які повинні виконувати антивірусне сканування кожного завантаженого файлу перед тим, як надати будь-якому іншому користувачу доступ до цього файлу або завантажити його до електронної системи охорони здоров'я.

Програмне забезпечення засобів антивірусного захисту та їх бази антивірусних сигнатур повинні регулярно оновлюватися. Оновлення повинно здійснюватися в автоматичному або ручному режимі централізовано. Внесення оновлень програмного забезпечення засобів антивірусного захисту та їх баз антивірусних сигнатур до МІС повинно виконуватись у встановленому виробником засобів антивірусного захисту порядку з урахуванням Порядку оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації, затвердженого наказом Адміністрації Держспецзв'язку № 45 від 26.03.2007.

4.3 Використання засобів криптографічного захисту

Засоби криптографічного захисту інформації, у тому числі засоби кваліфікованого електронного підпису, що використовуються при функціонуванні МІС, повинні мати чинні сертифікати відповідності або позитивні експертні висновки за результатами державної експертизи у сфері криптографічного захисту інформації щодо можливості їх використання для криптографічного захисту конфіденційної інформації (персональних даних фізичних осіб).

«ПОГОДЖЕНО»
Представники ТОВ «ДОЛЯ І КО. ЛТД»
(організатора державної експертизи комплексної системи захисту інформації ІТС ЦБД в сфері технічного захисту інформації)

Менеджер систем інформаційної безпеки А.Л. Волошин

Начальник відділу інформаційної безпеки Ю.В. Сергієнко