ЗАТВЕРДЖЕНО
Наказ Міністерства охорони здоров’я України
_____ № _____

План захисту інформації в інформаційно-комунікаційних системах забезпечення функціонування інформаційних систем, електронної пошти та вебсайтів Міністерства охорони здоров’я України

І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1. План захисту інформації в інформаційно-комунікаційних системах забезпечення функціонування інформаційних систем, електронної пошти та вебсайтів Міністерства охорони здоров’я України (далі – План захисту) є базовим документом, згідно з яким здійснюється захист інформації на всіх етапах життєвого циклу інформаційно-комунікаційних системах забезпечення функціонування інформаційних систем, електронної пошти та вебсайтів Міністерства охорони здоров’я України, як функціональних підсистем галузевої інформаційно-комунікаційної системи Міністерства охорони здоров’я України «HealthNet» (далі – ГІКС).

2. Вимоги цього документу розповсюджуються на всіх посадових осіб, які здійснюють обробку інформації в ГІКС.

3. План захисту повинен регулярно переглядатися та за необхідності змінюватись. Зміни та доповнення до Плану захисту інформації затверджуються на тому ж рівні та в тому ж порядку, що і основний документ.

ІІ. НОРМАТИВНІ ПОСИЛАННЯ

1. У цьому документі наведено посилання на такі нормативні документи:

Закон України «Про захист інформації в інформаційно-комунікаційних системах».

Закон України «Про інформацію».

Правила забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджені постановою Кабінету Міністрів України від 29.03.2006 № 373.

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.

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

НД ТЗІ 1.1-003-99 Термінологія в галузі 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 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 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

ІІІ. ЗАВДАННЯ ЗАХИСТУ ІНФОРМАЦІЇ В ГІКС

1. Основною метою Плану захисту є захист Міністерства охорони здоров'я України від можливого нанесення матеріального, морального або іншого збитку внаслідок випадкового або навмисного несанкціонованого втручання в процес функціонування ГІКС або несанкціонованого доступу до інформації і її незаконного використання.

2. Завданнями захисту інформації в ГІКС є:

– забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється в ГІКС;

– забезпечення однозначної ідентифікації та автентифікації користувачів ГІКС;

– забезпечення розмежування доступу зареєстрованих користувачів до функцій та об'єктів, що містять інформацію, яка підлягає захисту, у відповідності до Політики інформаційної безпеки МОЗ (далі – Політика безпеки);

– забезпечення доступності сервісів ГІКС;

– захист від мережевих атак;

– забезпечення спостережності за діями користувачів та персоналу, реєстрації подій, які мають відношення до безпеки інформації та їх періодичний аудит адміністратором безпеки.

3. Вирішення завдань захисту інформації в ГІКС досягається:

– регламентацією процесів обробки даних користувачами, на основі затверджених керівництвом МОЗ організаційно-розпорядчих документів з питань інформаційної безпеки;

– виконанням вимог організаційно-розпорядчих документів з питань інформаційної безпеки в МОЗ;

– призначенням і підготовкою посадових осіб (співробітників), відповідальних за інформаційну безпеку в МОЗ;

– наділенням кожного користувача ГІКС мінімально необхідними для виконання ними своїх функціональних обов'язків повноваженнями щодо доступу до ресурсів ГІКС;

– чітким знанням і дотриманням всіма співробітниками, що експлуатують і обслуговують апаратні та програмні засоби ГІКС, встановлених вимог з питань інформаційної безпеки;

– персональною відповідальністю кожного з персоналу ГІКС за свої дії;

– обліком всіх ресурсів ГІКС (інформації, програмне забезпечення (далі – ПЗ), компонентів ГІКС тощо);

– застосуванням заходів забезпечення фізичної цілісності технічних засобів та безперервною підтримкою необхідного рівня захищеності компонентів ГІКС;

– застосуванням фізичних і технічних (програмно-апаратних) засобів захисту ресурсів ГІКС та безперервною адміністративною підтримкою їх використання;

– проведенням роботи з персоналом (підбір, роз'яснення, навчання тощо) і ефективним контролем за дотриманням користувачами ГІКС вимог з інформаційної безпеки;

– проведенням постійного аналізу ефективності та достатності вжитих заходів і застосовуваних засобів захисту інформації, розробкою та реалізацією пропозицій з вдосконалення системи захисту ГІКС.

IV. ОСНОВНІ ПОЛОЖЕННЯ ПОЛІТИКИ БЕЗПЕКИ ІНФОРМАЦІЇ В ГІКС

1. Організаційні і технічні заходи щодо захисту інформації в ГІКС повинні проводитися у відповідності з вимогами чинного законодавства, чинних нормативно-правових актів Адміністрації Держспецзв'язку, а також нормативних і організаційно-розпорядчих документів МОЗ та ДП «Електронне здоров'я» з питань інформаційної безпеки.

2. Для всіх ресурсів ГІКС повинен бути визначений необхідний рівень захищеності. Ресурси ГІКС, які потребують захисту (інформація, ПЗ, компоненти ГІКС і т.п.), підлягають обліку.

3. Для користувачів ГІКС повинні бути розроблені необхідні інструкції, які включають вимоги з інформаційної безпеки.

4. Всі користувачі ГІКС повинні бути ознайомлені з політикою безпеки інформації в частині, що їх стосується, повинні знати і неухильно виконувати

посадові інструкції, документи комплексної системи захисту інформації (далі – КСЗІ), МОЗ та ДП «Електронне здоров'я» з питань інформаційної безпеки. Доведення вимог до осіб, допущених до обробки інформації, що захищається, повинно здійснюватися начальниками підрозділів під розпис.

5. Користувачі ГІКС повинні нести персональну відповідальність за порушення встановленого порядку автоматизованої обробки інформації, правил зберігання, використання і передачі ресурсів системи, які знаходяться в їх розпорядженні та потребують захисту. Кожний співробітник (при прийомі допуску до роботи з ресурсами ГІКС, що захищаються) повинен підписувати угоду (зобов'язання) про дотримання і відповідальність за порушення встановлених вимог із збереження інформації з обмеженим доступом, а також правил роботи з інформацією в ГІКС. Будь-яке грубе порушення порядку і правил роботи в ГІКС її користувачами повинно розслідуватися. До порушників повинні застосовуватися адекватні дії. Міра відповідальності персоналу за дії, які порушують встановлені правила забезпечення захищеної автоматизованої обробки інформації, визначаються завданим збитком, наявністю злого наміру і інших факторів керівництвом МОЗ відповідно до вимог розпорядчих та нормативних документів МОЗ та законодавства України.

6. Допуск користувачів ГІКС до роботи з нею, а також доступ до її ресурсів повинен бути регламентований. Будь-які зміни складу і повноважень користувачів ГІКС повинні здійснюватися встановленим порядком адміністратором безпеки.

7. Кожному користувачу ГІКС повинні надаватися мінімально необхідні права і повноваження щодо доступу до інформаційних ресурсів ГІКС для виконання функціональних обов'язків. Жоден користувач не повинен володіти всією повнотою повноважень щодо одноосібного безконтрольного знищення, зміни або створення інформаційних ресурсів в ГІКС. Керівники підрозділів зобов'язані своєчасно надавати заявки на надання своїм співробітникам або позбавлення (у разі звільнення, переведення, хвороби і т.п.) співробітників відповідних прав доступу і повноважень щодо роботи з інформаційними ресурсами ГІКС.

8. Апаратно-програмна конфігурація ГІКС повинна відповідати складу покладених на користувачів ГІКС функціональних обов'язків та функцій ГІКС. Непотрібні для роботи програмні засоби ГІКС повинні бути вилучені.

9. Всі зміни в конфігурації технічних і програмних засобів ГІКС повинні здійснюватися системним адміністратором згідно з Порядоком модернізації та оновлення компонентів ГІКС.

10. В ГІКС повинні встановлюватися і використовуватися тільки отримані у встановленому в МОЗ порядку програмні засоби. Використання програмного забезпечення, яке не поставлене на облік встановленим порядком, заборонено.

11. Експлуатація ГІКС повинна здійснюватися в приміщеннях, обладнаних замками і постійно знаходитися під охороною або спостереженням, що виключає можливість безконтрольного проникнення в приміщення сторонніх осіб і забезпечує фізичне збереження ресурсів, що захищаються (ПЕОМ, документів, реквізитів доступу і т.п.).

12. Розробка задач ПЗ, проведення випробувань розробленого або придбаного ПЗ, передача ПЗ в експлуатацію повинні здійснюватися відповідно до затвердженого порядку розробки, проведення випробувань і передачі ПЗ в експлуатацію.

13. Повинно бути забезпечено реєстрацію щонайменше таких класів подій компонентами ГІКС:

– доступ до об’єктів захисту ГІКС;

– реєстрація подій, пов’язаних зі зміною прав доступу до об’єктів захисту ГІКС;

– внесення змін до таблиць бази даних (додавання/зміна/видалення записів в таблицях бази даних);

– здійснення резервного копіювання технологічної інформації компонентів ГІКС, віртуальних машин ГІКС, баз даних та їх відновлення з резервних копій;

– вхід/вихід користувачів в/із ГІКС (ім’я користувача, дата, час). Мають реєструватися невдалі спроби входу користувача в систему та перевищення граничної кількості спроб введення пароля;

– створення/модифікація/видалення користувачів в ГІКС (ім’я користувача, дата, час);

– зміна паролю користувача (ім’я користувача, дата, час);

– реєстрація подій, пов’язаних зі зміною конфігураційних налаштувань компонентів системи;

– порушення цілісності криптографічних засобів захисту (далі – КЗЗ).

14. В ГІКС повинні бути встановлені засоби антивірусного захисту, які мають забезпечувати захист її ресурсів від комп’ютерних вірусів та зловмисних програм, у фоновому режимі або за запитом відповідного адміністратора.

15. Забороняється використовувати в ГІКС будь-які зовнішні носії даних без попередньої перевірки на віруси.

16. Оновлення антивірусного ПЗ та антивірусних баз повинно здійснюватися системним адміністратором.

V. ПОЛОЖЕННЯ ПРО ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ СИСТЕМІ

1. Для забезпечення безпеки інформації під час її обробки в ГІКС, створюється КСЗІ, яка представляє собою сукупність організаційних та інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації. Захист інформації повинен забезпечуватися на всіх технологічних етапах її обробки і в усіх режимах функціонування ГІКС.

2. Для здійснення захисту інформації на всіх стадіях життєвого циклу ГІКС система захисту інформації повинна передбачати застосування наступних заходів із захисту інформації:

– організаційно-правові заходи, які реалізуються поза обчислювальною системою ГІКС;

– інженерно-технічні заходи, що реалізуються поза обчислювальною системою ГІКС;

– програмно-апаратні та програмні засоби захисту від несанкціонованого доступу до інформації, яка обробляється та зберігається в ГІКС.

3. КСЗІ ГІКС повинна забезпечувати виконання таких основних функцій:

– реалізацію заданої в ГІКС політики безпеки інформації;

– забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється в ГІКС;

– забезпечення однозначної ідентифікації та автентифікації користувачів ГІКС;

– забезпечення розмежування доступу зареєстрованих користувачів до функцій та об’єктів, що містять інформацію, яка підлягає захисту, у відповідності до прийнятої політики безпеки;

– забезпечення доступності сервісів ГІКС;

– захист від вірусів та зловмисного ПЗ;

– забезпечення спостережності за діями користувачів та персоналу, реєстрації подій, які мають відношення до безпеки інформації та їх періодичний аудит адміністратором безпеки.

4. Організація робіт зі створення та супроводження КСЗІ, управління засобами захисту інформації, контроль за дотриманням положень політики безпеки здійснюється відповідним підрозділом – службою захисту інформації.

5. Політика безпеки визначає ресурси, що потребують захисту, враховує основні загрози для інформації і моделі порушників, впроваджені технології оброблення інформації і вимоги до захисту інформації від загроз.

6. КСЗІ повинна підтримувати визначену політику безпеки – множину правил, які при наявній класифікації суб'єктів доступу та об'єктів захисту використовуються для визначення можливості надання дозволу на доступ конкретного суб'єкта до конкретного об'єкта, надання та зміни повноважень, моніторингу всіх подій, які впливають на безпеку, та їх реєстрації.

7. Політика безпеки, яка реалізується КСЗІ ГІКС для захисту від потенційних внутрішніх та зовнішніх загроз, повинна поширюватись на всі об'єкти захисту ГІКС та всі ролі користувачів.

8. КСЗІ повинна мати атестат відповідності щодо її відповідності вимогам ТЗ на створення КСЗІ та НД ТЗІ 2.5-004-99.

9. Робота ГІКС в штатних режимах повинна бути можливою лише при функціонуючій КСЗІ. У разі відмови КСЗІ (окремого її модуля, компонента) повинен передбачатись режим аварійного блокування роботи ГІКС чи окремого її компонента.

10. Суб'єкт оперативного інформування – посадова особа, яка отримує сповіщення про події.

11. КСЗІ повинна вести облік і здійснювати реєстрацію подій, які пов'язані з безпосереднім доступом (спробами доступу) до інформації, здійснювати контроль за такими подіями та забезпечувати захист реєстраційної інформації від несанкціонованої модифікації, руйнування або знищення. Обсяг реєстраційної інформації повинен бути достатнім для встановлення причин та джерела виникнення зареєстрованої події.

12. КСЗІ повинна унеможливлювати несанкціоноване або неконтрольоване використання ресурсів ГІКС з боку її користувачів.

13. Критичні з точки зору безпеки компоненти КСЗІ повинні резервуватися, з тим щоб їх відмова не призводила до переривання процесу надання послуг користувачам.

14. Приміщення, де розміщуються компоненти ГІКС, повинні бути розміщені в межах контрольованої території, що має перепускний та внутрішній режими, які відповідають режимним вимогам чинних нормативних та розпорядчих документів МОЗ та ДП «Електронне здоров'я».

15. Контроль за доступом до приміщень, де розміщуються компоненти ГІКС, носії з копіями даних та програмного забезпечення ГІКС повинен забезпечуватись на всіх етапах їх життєвого циклу. Порядок доступу до таких приміщень із визначенням категорій користувачів, які мають право це здійснювати, визначається службою захисту інформації і затверджується керівництвом МОЗ та ДП «Електронне здоров'я».

16. Всі користувачі ГІКС повинні мати належний рівень кваліфікації і володіти навичками для виконання робіт відповідно до покладених на них завдань. Вони повинні мати дозвіл керівництва МОЗ (або інших осіб, визначених керівництвом МОЗ) на доступ до інформації, що обробляється в ГІКС, згідно зі своїми службовими обов'язками.

VI. ПРИНЦИПИ УПРАВЛІННЯ ДОСТУПОМ КОРИСТУВАЧІВ ДО ІНФОРМАЦІЇ

1. Відповідно до призначення ГІКС виділяються такі групи користувачів:

– користувачі зі складу обслуговуючого персоналу, які забезпечують роботу ГІКС– системний адміністратор, адміністратор безпеки;

– користувачі ГІКС: системні адміністратори прикладних інформаційних систем, модератори веб-сайтів, зовнішні незареєстровані користувачі електронної пошти МОЗ.

2. В ГІКС повинно бути реалізоване адміністративне управління доступом.

3. Всі спроби будь-якого суб'єкта отримати доступ до будь-якого об'єкту ГІКС повинні оброблятися засобами ПЗ компонентів ГІКС, які повинні порівнювати інформацію безпеки суб'єкта-користувача з інформацією безпеки списку контролю доступу об'єкту і дозволяти або заборонити доступ відповідно політиці безпеки.

4. Дозволи користувачам на виконання будь-яких дій з ресурсами ГІКС повинні регулюватися привілеями і правами доступу. Привілеї регулюють права користувача на виконання системних операцій. Права доступу визначають правомірність виконання користувачем конкретних дій з ресурсами (файлами, об'єктами баз даних тощо).

5. Управління привілеями та правами доступу користувачів (груп користувачів) до об'єктів захисту повинно здійснюватися адміністратором безпеки.

6. Всі користувачі ГІКС повинні мати право запускати програмне забезпечення, але не змінювати його та його налаштування.

7. Дозволи на доступ користувачів до ресурсів ГІКС повинні надаватися тільки до даних, що ними використовуються або обробляються.

8. Для надання однакових прав і привілеїв доступу до ресурсів ГІКС відразу декільком користувачам, останні можуть бути організаційно об’єднані в групи.

VII. ОПИС ОСНОВНИХ АТРИБУТІВ ДОСТУПУ КОРИСТУВАЧІВ, ПРОЦЕСІВ І ПАСИВНИХ ОБ’ЄКТІВ

1. Основними атрибутами доступу користувачів, що використовуються для проведення ідентифікації, автентифікації та авторизації засобами КЗЗ, є:

– логін;

– пароль.

2. Атрибутами інформаційних об’єктів, що використовуються для розмежування доступу, є:

– для об’єктів баз даних: найменування таблиці (стовпців таблиці) бази даних, список доступу до об’єкта бази даних (таблиці бази даних);

– для файлів: найменування та розширення файлу, атрибути доступу (читання, модифікація, знищення).

3. Атрибутами процесів є:

– назва виконуваного програмного модуля;

– ідентифікатор процесу в операційній системі.

VIII. ПРАВИЛА АДМІНІСТРУВАННЯ ОБЛІКОВИХ ЗАПИСІВ КОРИСТУВАЧІВ ГІКС

1. Адміністрування облікових записів.

При створенні (модифікації) облікових записів користувачів адміністратор безпеки повинен керуватися такими рекомендаціями:

до імен користувачів:

– облікові імена користувачів повинні бути унікальними;

– імена користувачів можуть містити до 20 будь-яких символів, окрім службових, на верхньому або нижньому регістрах;

до паролів користувачів:

– пароль повинен містити не менше 8 символів;

– термін дії пароля для облікового запису кожного користувача повинен встановлюватися не більше 90 діб;

– для захисту від повторного використовування можуть зберігатися не більше п’яти паролів, використаних раніше;

– паролі повинні бути конфіденційними і видаватися користувачам захищеним від перегляду сторонніми особами шляхом.

2. Адміністрування груп

При створенні (модифікації) груп користувачів адміністратор повинен керуватися наступними параметрами щодо визначення членства користувачів в групі:

– приналежністю до одного рівня користувачів;
– виконуваними посадовими обов'язками;
– складом та варіантом функціональних задач в ГІКС;
– функціями, які виконуються при вирішенні, як окремої задачі, так і всієї сукупності задач.

IX. ПОЛІТИКА РЕЄСТРАЦІЇ ПОДІЙ В ГІКС

1. Компонентами ГІКС повинні реєструватися такі події:

– доступ до об'єктів захисту ГІКС;
– внесення змін до таблиць бази даних (додавання/зміна/видалення записів в таблицях бази даних);
– здійснення резервного копіювання технологічної інформації компонентів ГІКС, віртуальних машин ГІКС, баз даних та їх відновлення з резервних копій;
– реєстрація подій, пов'язаних зі зміною прав доступу до об'єктів захисту ГІКС;
– вхід/вихід користувачів в/із ГІКС (ім'я користувача, дата, час). Мають реєструватися невдалі спроби входу користувача в систему та перевищення граничної кількості спроб введення пароля;
– створення/модифікація/видалення користувачів в ГІКС (ім'я користувача, дата, час);
– зміна паролю користувача (ім'я користувача, дата, час);
– реєстрація подій, пов'язаних зі зміною конфігураційних налаштувань компонентів системи;
– порушення цілісності КЗЗ.

Журнали реєстрації повинні містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події.

Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і об'єкта, що мали відношення до кожної зареєстрованої події.

2. Реєстрація подій, пов'язаних з безпекою інформації, в ГІКС повинна здійснюватися службами реєстрації кожного з компонентів ГІКС в журналах реєстрації подій кожного з компонентів. Адміністратор безпеки, під час налаштування політики реєстрації подій кожного з компонентів ГІКС, повинен

зафіксувати, чи повний перелік зазначених подій та їх параметрів реєструє компонент чи якусь з подій чи параметр він не вміє фіксувати.

Адміністратори повинні мати засоби перегляду журналів подій, що ведуться компонентами ГІКС. Налаштовувати політику реєстрації подій в компонентах ГІКС та видаляти журнали реєстрації подій повинен мати право тільки системний адміністратор.

X. ВІДПОВІДАЛЬНІСТЬ ЗА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ СИСТЕМІ

1. Служба захисту інформації (далі – СЗІ) в ГІКС при забезпеченні безпеки інформації, що циркулює в ГІКС, відповідає за організацію наступних заходів:

– проведення ефективного управління ризиками (ідентифікацію цінностей, які підлягають захисту, визначення вразливих ресурсів, аналізу ризику, їх використання і реалізації рентабельних засобів захисту);

– визначення та формування ефективної політики безпеки;

– своєчасне інформування співробітників щодо заходів політики безпеки;

– здійснення програми навчання основам безпеки для користувачів, яка гарантує знання ними діючих політик безпеки та правил роботи в ГІКС;

– своєчасне інформування адміністраторів про зміни в статусі будь-якого користувача ГІКС;

– впровадження і реалізацію затвердженої політики безпеки, оперативне управління і підтримку реалізованих заходів захисту;

– коректне застосування доступних механізмів захисту для реалізації часткових політик безпеки;

– інформування керівництва про працездатність існуючих політик безпеки та підготовку технічних пропозицій, які могли б підвищити її ефективність;

– захищеність середовища ГІКС і інтерфейсів з іншими інформаційними системами і зовнішніми мережами;

– виявлення і прийняття участі в усуненні порушень безпеки;

– використання доступних і надійних засобів аудиту для полегшення виявлення порушень безпеки;

– проведення періодичних перевірок системних журналів та журналів обліку порушень безпеки;

– коректне застосування прав та повноважень користувачами;

– розробку відповідних процедур та інструкцій щодо запобігання, виявлення та видалення несанкціонованого (зловмисного) програмного забезпечення;

– розробку процедур інформування користувачів про виявлені порушення безпеки;

– надання допомоги при визначенні джерела зловмисного програмного забезпечення, зони його розповсюдження та наступного видалення;

– надання користувачам доступу до необхідних даних, програм, функцій та ресурсів ГІКС;

– надання/відміна прав і повноважень, налаштування робочих параметрів засобів захисту;

– контроль за всіма пов’язаними із захистом подіями і за розслідуванням будь-яких реальних або підозрюваних порушень;

– оперативне припинення порушень безпеки, які виникають в окремих компонентах ГІКС в процесі її функціонування;

– присвоєння ідентифікаційних атрибутів кожному користувачу;

– своєчасне інформування керівництва про всі виявлені випадки порушення безпеки інформації;

– захищеність середовища ГІКС і інтерфейсів з іншими інформаційними системами і зовнішніми мережами;

– організацію належного функціонування пакетів антивірусних програм в ГІКС;

– коректне застосування своїх прав та повноважень.

2. Персонал ГІКС відповідає за:

– розуміння та дотримання відповідних законодавчих актів України, нормативних документів, політик безпеки та пов’язаних з ними процедур, прийнятих в ГІКС;

– правильне використання доступних механізмів безпеки для захисту критичної інформації та ресурсів ГІКС;

– правильне використання апаратно-програмних компонентів ГІКС відповідно до діючої політики безпеки;

– надання допомоги іншим користувачам у використанні механізмів захисту належним чином;

– своєчасне інформування адміністратора безпеки про будь-яку підозру щодо порушення політики безпеки;

– знання та використання відповідних політик та процедур для запобігання, виявлення та видалення зловмисного програмного забезпечення;

– знання та правильне виконання процедур щодо забезпечення безперервної роботи і відновлення при потенційних інцидентах.

3. Особи, винні в порушенні порядку та правил захисту оброблюваної в ГІКС інформації, несуть дисциплінарну, адміністративну, кримінальну або матеріальну відповідальність відповідно до чинного законодавства України та нормативних і розпорядчих документів МОЗ та ДП «Електронне здоров’я».

XI. ПОРЯДОК ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В ІКС

1. Забезпечення безпеки інформації в ГІКС здійснюється поетапно.

1 етап – визначення та аналіз загроз;

2 етап – розробка системи захисту інформації;

3 етап – контроль функціонування та управління системою захисту інформації.

2. На першому етапі здійснюється обстеження ГІКС. В процесі обстеження необхідно здійснити аналіз об'єктів захисту (ідентифікацію активів) і умов функціонування ГІКС, аналіз загроз та їх наслідків (оцінка ризиків), визначення слабкості в захисті. Повинні бути визначені загрози, вірогідності їх реалізації та величини можливого збитку. Оцінка ризику здійснюється на підставі аналізу загроз, існуючих в системі вразливостей, ефективності вже реалізованих заходів захисту ресурсів ГІКС. Величина ризику може бути визначена в грошовому вимірі або у вигляді формальної оцінки (високий, низький і т.п.). За наслідками обстеження складається акт обстеження, розробляється модель загроз інформації в ГІКС та формується політика безпеки інформації.

3. На другому етапі на підставі проведеного аналізу ризиків та сформульованої політики безпеки здійснюється вибір функціонального профілю захищеності ГІКС від несанкціонованого доступу. Функціональний профіль захищеності інформації в ГІКС визначається відповідно НД ТЗІ 2.5-005-99 на підставі класу ГІКС.

Для реалізації функціонального профілю захищеності ГІКС здійснюється вибір ефективних і економічних захисних заходів та механізмів і розробляється план захисту інформації в ГІКС та техноробочий проект, які визначають послідовність і зміст етапів робіт по впровадженню і експлуатації КСЗІ. В доповненні до комплексу програмно-технічних способів захисту інформації визначаються організаційні, фізичні і інші заходи захисту, які реалізуються поза ГІКС. До складу КСЗІ повинні включатися захисні заходи і механізми, реалізація яких дозволила б понизити рівень остаточного ризику до допустимого рівня. Вартість заходів щодо захисту інформації в ГІКС повинна бути адекватна величині можливого збитку.

4. В процесі виконання робіт здійснюється реалізація і перевірка вибраних заходів і механізмів захисту.

5. Третій етап реалізується на стадії експлуатації ГІКС і полягає в аналізі функціонування КСЗІ з метою оцінки її ефективності і розробки додаткових (уточнюючих) вимог для доробки при зміні початкових умов (характеристик обчислювальної системи, оброблюваної інформації, фізичного середовища, персоналу, призначення ГІКС, політики безпеки і т.п.). Процес управління КСЗІ (управління ризиками) повинен підтримуватися протягом всього життєвого циклу ГІКС.

6. Реалізація функцій та задач КСЗІ повинна забезпечуватися комплексним використанням методів і засобів криптографічного та технічного захисту інформації.

XII. ПОРЯДОК РЕАГУВАННЯ НА ПОРУШЕННЯ БЕЗПЕКИ

1. При виявлені порушень встановлених політикою правил безпеки інформації необхідно:

– негайно зупинити процес, в ході якого встановлено порушення безпеки (обробка, передача інформації і т.п.);

– в ручному або автоматичному режимі доповісти про факт порушення адміністратору безпеки (якщо порушення виявлено не адміністратором безпеки), керівнику підрозділу, де мав місце факт порушення, та керівництву ДП «Електронне здоров'я».

2. За фактом порушення безпеки повинно проводитися адміністративне розслідування комісією, яка призначається керівництвом ДП «Електронне здоров'я». Результати розслідування оформляються актом із підписами членів комісії. Акт затверджує керівництво ДП «Електронне здоров'я».

3. Керівник підрозділу, в якому мало місце порушення безпеки, разом с СЗІ розробляє порядок, терміни і заходи щодо усунення виявлених недоліків або порушень безпеки та затверджує їх у керівництва ДП «Електронне здоров'я».

4. Залежно від характеру порушень (навмисні або випадкові), їх ваги (нанесеною збитку) приймаються відповідні заходи реагування. До осіб, які винні в порушенні безпеки, повинні застосовуватися заходи дисциплінарної, адміністративної, кримінальної або матеріальної відповідальності відповідно до чинного законодавства України. Відповідальність за порушення безпеки користувачами ГІКС і застосування відповідних заходів дії повинні бути регламентовані окремими положеннями, затвердженими за встановленим порядком.

XIII. ОРГАНІЗАЦІЯ НАВЧАННЯ ТА ПЕРЕПІДГОТОВКИ КОРИСТУВАЧІВ

1. Затверджена політика безпеки в ГІКС, а також способи і засоби захисту, повинні доводитися до відома всіх користувачів ГІКС з використанням різних форм навчання (наприклад лекції, семінари, інструктажі, самостійна робота згідно завдань керівників функціональних підрозділів, які погоджені з СЗІ).

2. Поглиблене навчання та перепідготовка користувачів повинна проводитися на:

– курсах, які організовуються ДП «Електронне здоров'я» та МОЗ, як самостійно так і спільно з підприємствами-розробниками прикладного програмного забезпечення і апаратно-програмних засобів захисту та/або підприємствами, які проводять спеціалізовані навчальні курси;

– базі вищих навчальних закладів, організацій, установ та підприємств, які здійснюють підготовку фахівців в області безпеки інформації.

Користувачі по завершенню різних форм навчання і перепідготовки повинні одержувати відповідні свідоцтва, якщо такі передбачені.

XIV. ПОРЯДОК ПРОВЕДЕННЯ КОНТРОЛЮ ЗА ФУНКЦІОНУВАННЯМ ПРОГРАМНИХ ТА ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ ІКС ТА АНАЛІЗУ ДАНИХ АУДИТУ

1. Контроль за функціонуванням програмних та програмно-апаратних засобів ІКС, здійснюється з метою забезпечення дотримання вимог політики безпеки інформації впровадженої в КСЗІ ІКС та дотримання встановленого порядку оброблення інформації.

2. Контроль за функціонуванням програмних та програмно-апаратних засобів ІКС здійснюється шляхом:

– перевірки цілісності та працездатності програмних та програмно-апаратних засобів ІКС;

– контролю дотримання прийнятої політики безпеки при реєстрації облікових записів користувачів і призначення їм атрибутів доступу;

– контролю дотримання прийнятої політики безпеки при наданні користувачам прав доступу до інформаційних ресурсів;

– здійснення вибіркового контролю за діями користувачів;

– контролю настроювань та аналізу зареєстрованої інформації щодо функціонування програмно-апаратних засобів ІКС.

3. Перевірка цілісності та працездатності програмних та програмно-апаратних засобів ІКС має здійснюватися:

– у випадку отримання повідомлень про збої у роботі компоненту ІКС;

– після завершення будь-яких робіт із відновлення працездатності або модернізації програмних та програмно-апаратних засобів ІКС;

– після виконання переінсталяції ПЗ компонента ІКС за будь-яких причин;

– періодично (не рідше ніж один раз на місяць).

4. Перевірка цілісності та працездатності програмних та програмно-апаратних засобів ІКС, має здійснюватися системним адміністратором із

залученням адміністратора безпеки згідно з вимогами документації виробника на ці засоби.

5. Контроль дотримання політики безпеки має здійснюватися шляхом:

– перевірки настроювань компонентів ІКС на відповідність встановленій політики безпеки;

– аналізу зареєстрованих за певний час журналів реєстрації подій з метою виявлення порушень прийнятої політики безпеки.

6. Контроль настроювань параметрів безпеки компонентів ІКС має здійснюватися періодично або у випадку нештатних ситуацій адміністратором безпеки із залученням системного адміністратора згідно з вимогами експлуатаційної документації на ці засоби.

Аналіз журналів реєстрації подій компонентів ІКС має здійснюватися адміністратором безпеки згідно з вимогами експлуатаційної документації на ці засоби.

При здійсненні аналізу особлива увага має приділятися подіям про:

– факти входу/виходу або спроби входу/виходу до/із ОС або іншого ПЗ, яке потребує автентифікації користувачів;

– факти реєстрації та видалення або спроби реєстрації та видалення облікових записів користувачів ІКС;

– факти зміни даних ідентифікації та автентифікації користувачів;

– спроби порушення встановленої політики безпеки;

– факти зміни даних ідентифікації та автентифікації;

– факти порушення цілісності компонентів ІКС;

– факти порушення працездатності компонентів ІКС;

– факти перезавантаження, вимикання обладнання ІКС та інші системні події.

XV. КАЛЕНДАРНИЙ ПЛАН РОБІТ ІЗ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ СИСТЕМІ

1. Етапи життєвого циклу.

1.1. План робіт передбачає запровадження заходів захисту на всіх етапах життєвого циклу ІКС. Визначено такі етапи життєвого циклу ІКС:

– створення ІКС (включаючи створення КСЗІ) та налагодження ІКС та КСЗІ;

– попередні випробування та дослідна експлуатація КСЗІ ІКС;

– державна експертиза КСЗІ ІКС;

– експлуатація ІКС (включаючи обробку інформації, профілактику, ремонт, модернізацію ІКС або КСЗІ тощо);

– виведення ІКС з експлуатації.

1.2. Відповідальним за організацію робіт щодо захисту інформації в ІКС на всіх етапах її життєвого циклу є керівник СЗІ.

2. Створення КСЗІ

2.1. Створення КСЗІ передбачає:

– розробку та впровадження необхідних заходів та засобів захисту відповідно до вимог ТЗ на КСЗІ та документації КСЗІ;

– проведення попередніх випробувань КСЗІ.

2.2. Після закінчення робіт щодо створення КСЗІ та перевірки відповідності КСЗІ вимогам технічного завдання на її розробку та НД ТЗІ проводяться попередні випробування КСЗІ.

3. Попередні випробування та дослідна експлуатація

3.1. Попередні випробування КСЗІ проводяться комісією, яка призначається керівництвом ДП «Електронне здоров’я» відповідно до затвердженої встановленим порядком програми випробувань.

3.2. Випробування проводяться з використанням умовної інформації.

3.3. За результатами попередніх випробувань складається акт, у якому зазначаються результати випробувань і робиться висновок про можливість впровадження ІКС (та КСЗІ) у дослідну експлуатацію.

3.4. ІКС вводиться у дослідну експлуатацію наказом керівництва ДП «Електронне здоров’я» на підставі протоколу попередніх випробувань.

3.5. Призначаються особи, відповідальні за експлуатацію ІКС.

3.6. Наказом керівництва ДП «Електронне здоров’я» призначаються адміністратори ІКС.

3.7. Дослідна експлуатація проводиться з використанням умовної інформації. Під час дослідної експлуатації:

– відпрацьовуються технології щодо обробки інформації, обігу носіїв інформації, надання доступу користувачів до ресурсів ІКС, розмежування доступу та контролю за діями користувачів;

– співробітники, які відповідають за захист інформації, та користувачі ІКС набувають практичних навичок;

– здійснюється (за необхідності) доопрацювання програмного забезпечення, додаткове налагодження засобів захисту від НСД, доопрацювання інструкцій та інших документів, які входять до складу КСЗІ.

3.8. Після завершення дослідної експлуатації складається акт, у якому зазначаються результати дослідної експлуатації і робиться висновок про можливість подання КСЗІ для проведення державної експертизи.

4. Порядок проведення державної експертизи

Державна експертиза КСЗІ ІКС здійснюється організатором експертизи відповідно до Положення про державну експертизу в сфері технічного захисту інформації, затвердженого Адміністрації Державної служби спеціального зв'язку та захисту інформації від 16.05.2007 № 93.

5. Експлуатація

5.1. ІКС вводиться у промислову експлуатацію наказом керівництва ДП «Електронне здоров'я» на підставі атестату відповідності, отриманого від Адміністрації Держспецзв'язку України.

5.2. Підтримання КСЗІ в робочому стані в процесі промислової експлуатації досягається шляхом:

- повсякденного контролю за виконанням вимог цього документу;
- постійного контролю за працездатністю комплексу засобів захисту інформації від НСД.

5.3. Доступ користувачів до роботи в ІКС надається керівництвом МОЗ та ДП «Електронне здоров'я» (або інших осіб, визначених керівництвом МОЗ та ДП «Електронне здоров'я») в обсязі, мінімально необхідному для виконання співробітниками покладених на них функціональних обов'язків.

5.4. Користувачі несуть відповідальність за дотримання ними встановлених правил обробки інформації під час роботи в ІКС.

5.5. Порядок обробки інформації регламентується інструкціями та іншими документами, перелік яких наведено в розділі 2 даного документу.

6. Модернізація

6.1. Порядок дій за необхідності модернізації ГІКС визначається Порядоком модернізації та оновлення компонентів ГІКС.

7. Виведення з експлуатації

7.1. Порядок виведення ІКС з експлуатації розробляється після прийняття рішення про припинення її експлуатації.

7.2. У загальному випадку порядок виведення ІКС з експлуатації повинен передбачати:

– призначення відповідального за виведення ІКС з експлуатації;

– розроблення порядку видалення інформації з носіїв, які можуть використовуватися пізніше для оброблення відкритої інформації (в інших інформаційно-комунікаційних системах);

– розроблення порядку переносу інформації у інші інформаційно-комунікаційні системи (за необхідності).

XVI. СИСТЕМА ДОКУМЕНТІВ ІЗ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ СИСТЕМІ

1. Порядок обробки та захисту інформації в ІКС регламентується нормативними документами, зазначеними в розділі 3, та такими документами:

– експлуатаційна та проєктна документація КСЗІ;

– документи МОЗ та ДП «Електронне здоров'я» з питань захисту інформації, інформаційної безпеки та функціонування ІКС.

– розпорядження, накази, посадові функціональні обов'язки, інструкції обслуговуючого персоналу та інші організаційно-розпорядчі документи МОЗ та ДП «Електронне здоров'я»;

– документація на компоненти ІКС, які поставляються їх виробниками.

2. У разі потреби розробляються інші документи із забезпечення захисту інформації.

XVII. ПОРЯДОК ДІЙ КОРИСТУВАЧІВ У РАЗІ ВІДМОВИ АБО ЗБОЇВ КОМПОНЕНТІВ ІКС

1. У випадку виникнення нештатних ситуацій системний адміністратор зобов'язаний негайно повідомляти начальника СЗІ та інформувати адміністратора безпеки про всі виявлені збої у роботі програмно-апаратних засобів ІКС.

2. У випадку підтвердження факту виникнення нештатної ситуації, яка не дозволяє продовжувати нормальну роботу програмно-апаратних засобів ІКС, системним адміністратором має бути здійснено аналіз нештатної ситуації, зокрема:

– визначення причини виникнення нештатної ситуації та її можливі наслідки;

– визначення переліку заходів щодо відновлення працездатності програмно-апаратних засобів ІКС та ліквідації наслідків виникнення нештатної ситуації;

– формулювання пропозицій щодо недопущення виникнення аналогічної ситуації у подальшому.

3. Про результати здійсненого аналізу нештатної ситуації та запропоновані заходи має бути у письмовому вигляді повідомлено начальника СЗІ.

4. Заходи щодо відновлення працездатності програмно-апаратних засобів ІКС та ліквідації наслідків виникнення нештатної ситуації мають здійснюватися згідно з порядком, визначеним у розділі 22 цього документу.

5. Результати проведених робіт з ліквідації наслідків виникнення нештатної ситуації в КСЗІ ІКС мають бути зафіксовані у Формулярі ІКС.

XVIII. ПОРЯДОК ПРОВЕДЕННЯ ВІДНОВЛЮВАЛЬНИХ РОБІТ ТА ЗАМІНИ ПРОГРАМНИХ ТА ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ ІКС

1. У разі виходу з ладу програмно-апаратних засобів ІКС для відновлення їх нормального функціонування мають бути проведені ремонтні роботи або заміна.

2. Усі ремонтні роботи повинні здійснюватися системним адміністратором або під його наглядом.

3. Контроль за виконанням ремонтних робіт має здійснюватися адміністратором безпеки.

4. У разі необхідності, до проведення ремонтних робіт можуть залучатися співробітники інших організацій, які мають необхідний рівень кваліфікації та дозвіл на виконання певних видів робіт.

5. У разі втрати працездатності ПЗ, здійснюється відновлення їх працездатності шляхом використання резервних копій конфігурацій, віртуальних машин, баз даних.

6. Відновлення працездатності ПЗ має здійснюватися із використанням штатних засобів обладнання та ПЗ КСЗІ ІКС, згідно з вимогами документації виробника.

7. В разі неможливості відновлення працездатності ПЗ за рахунок використання штатних засобів обладнання та ПЗ КСЗІ ІКС, може здійснюватися повторна інсталяція та налаштування згідно з вимогами проєктної документації на КСЗІ ІКС або відновлення з резервних копій.

8. Відновлення віртуальної машини, ПЗ та/або технологічної інформації з резервної копії здійснюється у випадку виникнення нештатних ситуацій (вихід з ладу обладнання, збої у електроживленні, наслідки дій комп'ютерних вірусів або некваліфікованих дій адміністраторів ІКС тощо), у результаті чого працездатність ПЗ була втрачена.

9. Відновлення віртуальних машин, технологічної інформації, баз даних з резервних копій здійснюється системним адміністратором після проведення робіт з усунення причин виникнення нештатних ситуацій.

10. Відновлення віртуальних машин, технологічної інформації, баз даних з резервних копій виконується за допомогою штатних механізмів компонентів КЗЗ КСЗІ ІКС.

11. У разі втрати працездатності апаратних засобів ІКС, здійснюється їх заміна.

12. Результати проведених робіт мають бути зафіксовані у Формулярі ГІКС.

XIX. ПОРЯДОК ПРОВЕДЕННЯ РЕЗЕРВУВАННЯ ДАНИХ ІКС

1. З метою забезпечення сталого функціонування та працездатності програмно-апаратних компонентів ІКС та оперативного відновлення їх функціонування після час аварій та збоїв має проводитись періодичне резервування технологічної інформації компонентів ІКС, віртуальних машин серверів, баз даних.

2. Створення резервних копій має виконуватися системним адміністратором періодично, але не рідше одного разу на тиждень, шляхом створення резервних копій технологічної інформації компонентів ІКС, віртуальних машин серверів, баз даних.

3. Відповідальність за збереження резервних копій покладається на системного адміністратора.

XX. ПОРЯДОК ПЕРЕГЛЯДУ ПЛАНУ ЗАХИСТУ

1. План захисту підлягає частковому перегляду в наступних випадках:

– при зміні конфігурації, додаванні або вилученні програмних і технічних засобів в ІКС, що не змінює технологію обробки інформації;

– при зміні конфігурації і налаштувань технічних засобів захисту, що використовуються в ІКС;

– при зміні складу і обов’язків користувачів і обслуговуючого персоналу ІКС і співробітників, що відповідають за інформаційну безпеку.

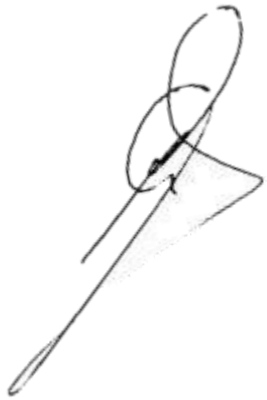
2. Профілактичний перегляд плану захисту проводиться не рідше 1 разу на рік і має на меті перевірку відповідності визначених даним планом заходів реальним умовам застосування ІКС і поточним вимогам до її захисту.

3. План захисту підлягає повному перегляду у разі зміни технології обробки інформації або використанні нових технічних засобів захисту.

4. У разі часткового перегляду можуть бути додані, вилучені або змінені вимоги плану захисту з обов’язковою вказівкою в листі реєстрації змін даних про те, хто, коли, з якою метою, які зміни вніс і хто санкціонував ці зміни.

5. Зміни, що вносяться в план, не повинні суперечити іншим положенням плану захисту і повинні бути перевірені на коректність та повноту.

6. Будь-який перегляд плану захисту повинен здійснюватися з обов’язковою участю представників СЗІ.

Директор Департаменту цифрових трансформацій в охороні здоров'я  **Олена САВІЧЕВА**