Інформаційна безпека
Шаблон політики



Розроблено в рамках проекту HRS (Health Reform Support).

Інструкція з користування

Наданий шаблон політики інформаційної безпеки закладу охорони здоров'я (ЗОЗ) вимагає заповнення деяких положень, щоб забезпечити відповідність стосовно наявних бізнес процесів, фізичного, інформаційного середовища та середовища користувачів. Після заповнення важливо, щоб розроблена відповідно даного шаблону Політика інформаційної безпеки (ПІБ) була затверджена вищім керівництвом ЗОЗ та доведена до усіх співробітників і відповідно виконувався, як зазначено. Можливо внесення інших корегувань, якщо це необхідно, виходячи з потреб вашого навколишнього та інформаційного середовища, а також змін у вимогах регулюючих органів, що опікуються кібербезпекою об'єктів критичної інфраструктури України.

Елементи, виділені червоним в межах шаблону обов'язкові до заповнення, виділені жовтим бажано коригувати відповідно до особливостей фізичного, інформаційного середовища та середовища користувачів ЗОЗ.

Номер	Назва	Опис
1	Назва ЗОЗ	Назва закладу охорони здоров'я
2	Дата останньої редакції	Остання дата перегляду Політики інформаційної безпеки.
3	Власник документа	Керівник ЗОЗ, який затверджує ПІБ
4	Дата затвердження	Дата затвердження ПІБ
5	Дата набрання чинності	Дата набрання чинності ПІБ
6	Назва підрозділів	Назва організаційних та штатних підрозділів ЗОЗ до яких застосовуються конкретні частини ПІБ
7	Зовнішні організації	Зовнішні установи або організації, які мають повноваження впливати та контролювати реалізацію ПІБ (СБУ, ДССЗЗУ, НКЦК РНБОУ тощо)
8	Відповідальний за інформаційну безпеку	Вказати прізвище та ім'я, номер телефону, адресу електронної пошти особи, призначеної відповідальною за інформаційну безпеку.
9	Команда реагування на інциденти ІБ	Вказати ПІБ осіб, які призначені у команду реагування на інциденти ІБ
10	Постачальники послуг	Назва юридичних осіб, які надають послуги ЗОЗ (МІС, інтернет-провайдери тощо)

Номер	Назва	Опис
11	Час блокування екрану	Час між моментом, коли користувач залишає комп'ютер незаблокованим, до автоматичного блокування екрану. Цей час потрібно визначити та налаштувати на робочих станціях ЗОЗ.
12	Електронний зв'язок, електронна пошта, користування Інтернетом	Визначити допустимі у ЗОЗ засоби електронної комунікації, електронної пошти та ресурсів Інтернету для користування з службових питань.
13	Аудит ідентифікаторів входу	Вкажіть, як часто перевіряються ідентифікатори користувачів. Сюди входять мережеві та облікові записи користувачів.
14	Блокування користувача	Вкажіть, скільки невдалих спроб входу в систему має користувач до блокування його облікового запису.
15	Довжина пароля	Вкажіть мінімальну довжину пароля для доступу до робочої станції.
16	Зміна пароля	Вкажіть, скільки днів діє пароль перш ніж його необхідно змінити.
17	Повторне використання пароля	Вкажіть, скільки попередніх паролів не можна використовувати.
18	Антивірусне програмне забезпечення	Вкажіть назву антивірусного програмного забезпечення, що використовується у ЗОЗ
19	Виробник Антивірусного ПЗ	Вкажіть назву компанії виробника, яка здійснює підтримку та оновлення антивірусного ПЗ.
20	Оновлення антивірусу	Вкажіть, з якою періодичністю заплановано виконувати оновлення антивірусного ПЗ.
21	Система фізичної безпеки	Вкажіть яким чином забезпечується фізична безпека та захист ЗОЗ у неробочий час.
22	Час роботи	Вкажіть час роботи ЗОЗ
23	Безпечні двері	Вкажіть, як контролюється доступ до захищених ділянок ЗОЗ

Номер	Назва	Опис
24	Детектори руху	Вкажіть, чи використовуються датчики/детектори руху.
25	Датчики скла	Вкажіть, чи використовуються датчики розбиття скла.
26	Камери відеоспостереження	Вкажіть, чи використовуються камери відеоспостереження.
27	Зміна пароля	Вкажіть, за скільки днів починає надходити попередження про необхідність зміни пароля.
28	Надане обладнання	Перерахуйте все обладнання, яке надається працівникам ЗОЗ, які працюють як на робочому місці так і віддалено.
29	Віддалене блокування екрана	Час з моменту коли користувач залишає комп'ютер незаблокованим до автоматичного блокування екрану для працівників, які працюють віддалено.
30	Збереження записів	Вкажіть, як довго зберігаються документи, пов'язані з використанням та розкриттям інформації, повідомленням про практику конфіденційності, скаргами тощо.
31	Різне	Зазначте іншу інформацію, яка може бути важливою для забезпечення інформаційної безпеки ЗОЗ
32	Контактний номер телефону	Вкажіть номер технічної підтримки або сервіс-деску

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

НАЗВА ЗОЗ

ДАТА ОСТАНЬОЇ РЕДАКЦІЇ

ДАТА

ДОКУМЕНТ ЗАТВЕРДЖЕНО

Прізвище ім’я та по батькові керівника ЗОЗ

Підпис

ЗМІСТ

1 Введення 8
1.1 Загальні положення 8
1.2 Глосарій 8
1.3 Застосовані положення 11
1.4 Відповідальний за інформаційну безпеку 11
1.5 Робоча група з інформаційної безпеки 14
2 Обов'язки персоналу 15
2.1 Вимоги до персоналу 15
2.2 Заборонена діяльність 16
2.3 Користування Інтернетом та електронною поштою 17
2.4 Доступ до Інтернету 18
2.5 Повідомлення про несправності 19
2.6 Повідомлення про інциденти безпеки 20
2.7 Передача конфіденційної інформації 20
2.8 Передача даних та програмного забезпечення 21
2.9 Шифрування електронної пошти та даних 21
3 Управління доступом 23
3.1 Загальні положення 23
3.2 Ролі щодо контролю доступу 23
3.3 Ідентифікація користувачів 24
3.4 Правила встановлення та поводження з паролями 24
3.5 Угода про конфіденційність 24
3.6 Контроль доступу 24
3.7 Припинення прав доступу 26
3.8 Припинення дії облікового запису користувача 26
3.9 Заходи безпеки екстреного доступу до захищеної медичної інформації 27
3.10 Заходи безпеки з обмеження доступу до персональних даних 28
3.11 Заходи безпеки з обмеження фізичного доступу 29
3.12 Відповідальність 29
4 Підключення до мережі 30
4.1 З'єднання та підключення 30
4.2 Телекомунікаційне обладнання 30

4.3 Постійні з'єднання 31
4.4 Договір на телекомунікаційні послуги 31
4.5 Брандмауер 32
5 Антивірусний захист 33
5.1 Загальні положення 33
5.2 Ролі та відповідальність 34
5.3 Вимоги до антивірусного ПЗ та роботи користувачів 34
5.4 Порядок встановлення та використання 35
5.5 Виявлення та усунення загроз 36
5.6 Відповідальність 36
6 Криптографічний захист 38
6.1 Загальні положення 38
6.2 Мета використання 39
6.3 Порядок застосування 39
6.4 Використання інфраструктури відкритих ключів 40
6.5 Використання WinZip 43
6.6 Протокол передачі файлів sFTP 43
6.7 Веб-інтерфейс рівня захищених сокетів (SSL/TLS) 43
6.8 Використання SSH 44
6.9 Шифрування носіїв і файлових систем 44
6.10 Шифрування інформації з обмеженим доступом для сервісів хмарних обчислень 45
6.11 Аудит використання ключів 45
6.12 Відповідальність 45
7 Фізична безпека 46
8 Дистанційна робота 48
8.1 Загальні вимоги 48
8.2 Необхідне обладнання 48
8.3 Захист апаратного забезпечення 49
8.4 Безпека даних 49
8.5 Утилізація паперових документів та зовнішніх носіїв 50
9 Політика чистого столу/чистого екрану 51
9.1 Загальні положення 51
9.2 Вимоги 51
9.3 Відповідальність 52

10 Утилізація зовнішніх носіїв та комп’ютерів 53
10.1 Утилізація зовнішніх носіїв 53
10.2 Утилізація комп’ютерів 53
10.3 Використання надлишкового обладнання 53
11 Управління змінами 54
12 Моніторинг стану інформаційної безпеки 55
13 Аудит інформаційної безпеки 56
14 Цілісність даних пацієнтів 58
15 Плани резервного копіювання та аварійного відновлення 59
15.1 План резервного копіювання 59
15.2 План аварійного відновлення 60
16 Обізнаність та навчання з питань безпеки 61
17 Управління ризиками 63
18 Відповідальність за порушення 66
19 Перевірка кандидатів 69
20 Політика управління інцидентами ІБ 70
20.1 Загальні положення 70
20.2 Терміни 70
20.3 Управління інцидентами 71
20.4 Обов’язки та відповідальність 74
Додаток 1 – Форма запиту на доступ 76
Додаток 2 – Угода про конфіденційність 77
Додаток 3 – Затверджене програмне забезпечення 78
Додаток 4 – Затверджені постачальники 79
Додаток 5 – Журнал реєстрації інцидентів ІБ 80
Додаток 6 – Згода на перевірку кандидата 81
Додаток 7 – Журнал управління змінами 82

Назва ЗОЗ[1] **Політика інформаційної безпеки**	
Назва: ВВЕДЕННЯ	**п 1.1 – 1.5**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Інформаційна безпека ЗОЗ 2 категорії**

1. ВВЕДЕННЯ

1.1. Загальні положення

Ця політика інформаційної безпеки визначає основні засади забезпечення належного рівня інформаційної безпеки Назва ЗОЗ, далі – Політика або скорочено ПІБ. ПІБ служить центральним програмним документом з інформаційної безпеки, з яким повинні бути ознайомлені всі працівники ЗОЗ, підрядники (постачальники послуг), і визначає дії, застереження, заборони, яких повинні дотримуватися всі користувачі інформаційних та цифрових активів ЗОЗ. Політика роздруковується та затверджується керівником ЗОЗ та зберігається у відповідального за інформаційну безпеку ЗОЗ. Уразі неможливості призначити окремого відповідального за інформаційну безпеку із-за обмеженості людського ресурсу закладу, функцію відповідального за інформаційну безпеку виконує головний лікар (ГЛ) закладу.

Належний рівень інформаційної безпеки, це такий стан фізичного, інформаційного середовища та середовища користувачів інформаційних та цифрових активів Назва ЗОЗ, який гарантує конфіденційність, доступність, цілісність інформації ЗОЗ та зпостережність і контрольованість систем/підсистем, в яких ця інформація циркулює.

Належний рівень інформаційної безпеки досягається за рахунок вмілого застосування комплексу програмних/технічних засобів та організаційних заходів, спрямованих на забезпечення захищеності даних від зловмисного використання.

Вимоги та обмеження ПІБ, застосовуються до мережевої інфраструктури, баз даних, носіїв інформації, засобів шифрування, друкованих документів, мульті-медіа файлів, засобів бездротового зв'язку, телекомунікаційних систем, аудіо повідомлень та будь-яких інших засобів, що використовуються для передачі, обробки та зберігання інформації у всіх апаратних, програмних та інших інформаційних та цифрових системах ЗОЗ. Цієї політики повинні дотримуватися всі штатні та тимчасові працівники в усіх місцях (на робочому місці, в будівлі ЗОЗ чи працюючи віддалено), а також підрядники – постачальники послуг, які працюють з ЗОЗ.

1.2. Глосарій

1.2.1. Загальні терміни та абревіатури, які використовуються в цьому документі.

Актив – матеріальні та нематеріальні об’єкти або інформація, що мають цінність для ЗОЗ.

Брандмауер – спеціальне обладнання або програмне забезпечення, що працює на комп'ютері, яке дозволяє або відмовляє в проходженні трафіку через нього, на основі набору правил.

ВІБ – відповідальний за інформаційну безпеку, призначена особа, яка відповідає за впровадження та дотримання Політики інформаційної безпеки в закладі охорони здоров’я. Уразі неможливості призначити окремого відповідального за інформаційну безпеку, його функцію виконує головний лікар.

Вірус – шкідливе програмне забезпечення, здатне відтворювати сама себе і зазвичай здатне завдати великої шкоди файлам або іншим програмам на комп'ютері, який воно атакує.

ГЛ – головний лікар.

Доступність інформації – властивість, яка гарантує те, що забезпечується своєчасний доступ авторизованих осіб та процесів до інформації, а також відсутні простої в процесі її обробки, тобто коли інформація знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і у той час, коли вона йому необхідна. У випадку втрати інформації існує можливість своєчасного її відновлення.

ЗОЗ – заклад охорони здоров’я.

Зовнішні носії інформації – компакт-диски, DVD-диски, дискети, флешки, USB, флеш-накопичувачі, касети та інші.

ІБ - Інформаційна безпека, це процес, який забезпечує збереження визначених Політикою безпеки властивостей інформації та спрямований на запобігання несанкціонованим діям в інформаційній системі, що включає сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи інформаційної системи.

ІС – Інформаційна система, організаційно-технічна система, у якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

ІТ – Інформаційна технологія.

Керівник– керівник закладу охорони здоров’я.

Конфіденційність інформації – властивість, яка гарантує те, що доступ до інформації можуть одержати тільки авторизовані особи або процеси.

Користувач - Будь-яка особа зі складу персоналу ЗОЗ, уповноважена на доступ до певного інформаційного ресурсу.

Користувачі з можливостями запиту (лише для читання) – особи, яким на основі прав доступу заборонено додавати, видаляти або змінювати записи в базі даних та інших доступних їм масивах інформації. Їх системний доступ обмежується лише зчитуванням інформації.

Користувачі з можливостями редагування/оновлення – особи, яким дозволено на основі прав доступу додавати, видаляти або змінювати записи в базах даних та інших масивах інформації ЗОЗ.

Локальна мережа – комп'ютерна мережа ЗОЗ.

ПІБ – Політика інформаційної безпеки, це центральний, програмний документ, який визначає основні засади забезпечення належного рівня інформаційної безпеки закладу охорони здоров'я.

Персонал – всі працівники ЗОЗ, які використовують інформаційні ресурси закладу, комп'ютерне, телекомунікаційне і офісне обладнання відповідно до своїх посадових обов'язків.

ПК – персональний комп'ютер.

Привілейовані користувачі – системні адміністратори та інші особи, які конкретно ідентифіковані та мають санкціонований керівництвом доступ до певних баз даних та масивів інформації.

РГІБ – робоча група з інформаційної безпеки, колективний керівний орган системи управління інформаційною безпекою ЗОЗ.

Спостережність системи - властивість, що дозволяє фіксувати діяльність користувачів і процесів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки або забезпечення відповідальності за певні дії.

СУІБ - Система управління інформаційною безпекою, це комплекс організаційних, програмних, технічних і фізичних заходів, спрямованих на управління ризиками, що пов'язані з використанням у ЗОЗ інформації та інформаційних технологій.

Третя сторона – фізична чи юридична особа, яка перебуває у будь-яких договірних відносинах з ЗОЗ та є стороною таких відносин.

Цілісність інформації – властивість, яка гарантує те, що інформація не містить помилок, є актуальною, вичерпною, будь-які зміни інформації здійснюються авторизованими особами чи процесами.

Шифрування – процес перетворення інформації, використовуючи алгоритм, щоб зробити її нечитабельною для будь-кого, крім тих, хто має авторизовану «потребу знати».

VLAN – Віртуальна локальна мережа – локальна мережа, яка використовується для сегментації мережевого трафіку з метою адміністрування та безпеки.

VPN – Віртуальна приватна мережа – забезпечує безпечну передачу даних та доступ через загальнодоступні мережі.

1.2.2. Інші терміни, що вживаються у цій Політиці, застосовуються в значеннях, визначених чинним законодавством України.

1.3. Застосовані положення

Нижче наведено перелік нормативних та регулюючих законів, актів, стандартів на основі яких розроблено цей документ.

1. Закон України «Про основні засади забезпечення кібербезпеки України»;
2. Закон України «Про інформацію»;
3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;
4. Закон України «Про електронні документи та електронний документообіг»;
5. Постанова КМУ №518 від 19.06.2019 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»;
6. ISO/IEC27000:2019 - Інформаційні технології - Методи і засоби забезпечення безпеки - Системи управління інформаційною безпекою - Загальні відомості і словник;
7. ISO/IEC 27001:2013 - Інформаційні технології - Методи захисту - Системи управління інформаційною безпекою – Вимоги;
8. ISO/IEC 27002:2013/COR 2:2015 - Інформаційні технології - Методи захисту - Звід рекомендованих правил для управління інформаційною безпекою;
9. ISO/IEC 27003:2017 - Інформаційні технології - Методи безпеки - Системи управління інформаційною безпекою – Керівництво;
10. ISO/IEC 27004:2016 - Інформаційні технології - Методи безпеки - Управління інформаційною безпекою - Моніторинг, вимір, аналіз і оцінка;
11. ISO/IEC 27005:2018 - Інформаційні технології - Методи безпеки - Управління ризиками інформаційної безпеки;

12. ISO/IEC 15408-1:2009 - Загальні критерії оцінки захищеності інформаційних технологій;

13. ISO/IEC TS 27008:2019 - Методи безпеки - Вказівки для оцінки засобів контролю інформаційної безпеки;

14. ISO 27032 – Інформаційні технології. Методи захисту;

15. ISO 27035 – Управління інцидентами.

1.4. Відповідальний за інформаційну безпеку

Відповідальний за інформаційну безпеку (ВІБ) закладу охорони здоров'я - призначена особа зі складу персоналу закладу, який/яка відповідає за дотримання належного рівня інформаційної безпеки ЗОЗ, контролює всю поточну діяльність, пов'язану з розробкою, впровадженням та підтримкою політики інформаційної безпеки закладу, зберігає актуальний затверджений примірник ПІБ у себе на робочому місці та при необхідності надає до нього доступ. Чинним ВІБ є:

ІПІБ –електронна адреса та номер телефону[8]

Відповідальний за захист інформації забезпечує захист інформаційних систем закладу охорони здоров'я від несанкціонованого доступу та дій, направлених на відмову в обслуговуванні, порушення цілісності та неспростовності інформації відповідно до вимог Політики інформаційної безпеки.

Відповідальний за захист інформації підпорядковується ГЕНЕРАЛЬНОМУ ДИРЕКТОРУ (ДИРЕКТОРУ) / НАЧАЛЬНИКУ (ЗАВІДУВАЧУ) ЗАКЛАДУ ОХОРОНИ ЗДОРОВ'Я.

1.4.1. Завдання та обов'язки

Здійснює координацію працівників закладу та інформаційних систем, що забезпечують безпеку закладу відповідно до Політики інформаційної безпеки. Розроблює заходи й плани забезпечення інформаційної безпеки та розвитку систем з інформаційної безпеки. Розроблює або приймає участь у розробленні документів щодо інформаційної безпеки. Контролює виконання заходів щодо забезпечення інформаційної безпеки на всіх стадіях життєвого циклу інформаційних систем закладу. Розслідує інциденти інформаційної безпеки. Спільно з іншими спеціалістами приймає участь у відновленні функціонування інформаційних систем закладу після збоїв у роботі внаслідок інцидентів інформаційної безпеки. Розроблює та здійснює програми з метою моніторингу, аудиту, навчання та впровадження новітніх технологій у систему інформаційної безпеки закладу. Контролює стан дотримання секретності розміщення устаткування системи з інформаційної безпеки. Аналізує інформацію про стан інформаційної безпеки закладу в цілому та за окремими напрямами роботи. Готує матеріали з інформаційної безпеки для керівників і працівників, які зайняті забезпеченням інформаційної безпеки підприємства. Контролює інформаційні матеріали з метою перевірки правильності їх відображення та для подальшого використання в засобах масової інформації. Забезпечує контакти з відповідними підрозділами міністерств, відомств, інших органів

державної виконавчої влади щодо обміну інформаційними матеріалами в межах наданих йому повноважень і законодавства України. Контролює надходження засобам масової інформації матеріалів про діяльність закладу з метою недопущення витоку секретної інформації. Проводить переговори з представниками газет, журналів, радіо, телебачення, спортивних і культурних організацій у разі виникнення загроз витоку інформації щодо інформаційної безпеки закладу. Здійснює заходи щодо забезпечення законності та дисципліни у службовій діяльності працівників, їх особистої безпеки під час виконання обов'язків пов'язаних із забезпеченням належного функціонування системи інформаційної безпеки, організовує взаємодію з правоохоронними органами в разі витоку секретної інформації з закладу. Здійснює співробітництво з відповідними службами інших установ та підприємств. Бере участь у плануванні розвитку трудового колективу, вирішенні спірних питань і конфліктів, залучає до їх вирішення відповідних консультантів і експертів (правових, технічних, фінансових). Приймає рішення щодо раціонального використання наданих коштів для забезпечення належного функціонування системи інформаційної безпеки закладу.

1.4.2. Повинен знати

Конституцію України, законодавчі акти, що стосуються охоронної діяльності та інформаційної безпеки; інші нормативно-правові акти, що регламентують питання організації та здійснення охорони органів державної влади та місцевого самоврядування України, інших підприємств, установ, організацій незалежно від форм їх власності та осіб, які є об'єктами охорони; положення відповідних відомчих наказів, розпоряджень та інструкцій з охоронної діяльності, основи організації інформаційної безпеки; профіль, спеціалізацію й особливості функціонування системи з інформаційної безпеки; основи менеджменту, комерційної діяльності; основи організації праці й управління; основи фінансово-господарчої діяльності та маркетингу; методи прогнозування та моделювання систем з охоронної діяльності, формування конкурентоспроможних охоронних послуг, порядок ціноутворення, способи та методи співпраці із засобами масової інформації, іншими юридичними та приватними особами; методи вивчення й аналізу інформаційних джерел; порядок розроблення планів і програм організаційно-господарської діяльності; порядок укладання господарських та інших договорів, припинення договірних відносин і ведення претензійної роботи; методи вивчення умов праці на робочих місцях; систему стандартів безпеки праці, захисту працівників від протиправних дій під час виконання службових обов'язків; норми та правила охорони праці та протипожежної безпеки; основні принципи роботи з комп'ютером та відповідні програмні засоби; державну та одну з міжнародних мов.

1.4.3. Права

Має право брати участь у стратегічному керівництві з питань інформаційної безпеки закладу та бути залученим до визначення напрямів розвитку інформаційної безпеки закладу. Контролювати відповідність заходів інформаційної безпеки актуальним потребам бізнес-процесів закладу. Контролювати впровадження заходів інформаційної безпеки в закладі.

1.4.4. Кваліфікаційні вимоги

Повна вища освіта відповідного напряму підготовки за освітньо-кваліфікаційним рівнем магістра, спеціаліста. Підвищення кваліфікації у сфері охоронної діяльності та менеджменту. Стаж роботи за фахом на керівних посадах – не менше 2 років.

1.4.5. Відповідальність

Забороняється мати повноваження з розроблення, впровадження, супроводження (адміністрування) та експлуатації інформаційних систем закладу, крім тих, що використовуються для забезпечення безпеки інформації.

Забороняється бути власником інформаційних систем закладу, які безпосередньо забезпечують автоматизацію бізнес-діяльності закладу.

Несе відповідальність за:

- Якість і своєчасність виконання обов'язків, визначених цією посадовою інструкцією.
- Дотримання правил внутрішнього трудового розпорядку закладу.
- Дотримання норм і вимог з охорони праці, протипожежної безпеки та виробничої санітарії.

Несе дисциплінарну та матеріальну відповідальність відповідно до чинного законодавства. За здійснення в процесі виконання своїх посадових обов'язків вчинків, які містять склад злочину, несе відповідальність згідно норм законодавства України.

1.5. Робоча група з інформаційної безпеки

Робоча група з інформаційної безпеки закладу, це колективний керівний орган з управління системою інформаційної безпеки Назва ЗОЗ.

Всі члени робочої групи з інформаційної безпеки (РГІБ), визначені в рамках цієї політики, призначаються керівником ЗОЗ. Термін повноважень членів РГІБ складає один рік та може бути продовжений відповідним рішенням керівника ЗОЗ. Рекомендується до РГІБ включати керівника, головного лікаря (ГЛ), відповідального за інформаційну безпеку (ІБ) та відповідального за підтримку ІТ-інфраструктури ЗОЗ. Чинними членами РГІБ є:

Посада – ПІБ

Посада – ПІБ

Посада – ПІБ

Посада – ПІБ

Посада – ПІБ

РГІБ збирається щоквартально, або частіше за потреби, щоб обговорити питання інформаційної безпеки та розглянути проблеми, які виникли протягом кварталу. РГІБ визначає та затверджує програму щорічного навчання персоналу з інформаційної безпеки, та переглядає/оновлює політику інформаційної безпеки, якщо це необхідно.

РГІБ вирішує нагальні питання інформаційної безпеки в міру їх виникнення, а також приймає та схвалює необхідні заходи безпеки, які повинні бути вжиті. Відповідальність РГІБ полягає в тому, щоб визначити ризики інформаційної безпеки та вчасно вжити необхідних заходів з мінімізації чи усунення.

РГІБ контролює ведення журналу подій інформаційної безпеки. Ведення цього журналу здійснюється на постійній основі. До журналу вносяться дата події, дії, вжиті для вирішення події, а також рекомендації щодо подальших дій персоналу, якщо це доречно. Цей журнал розглядається РГІБ під час щоквартальних засідань.

Відповідальний за ІБ забезпечує ведення журналу подій інформаційної безпеки, а також напрацьовує на його основі та подає на розгляд РГІБ пропозиції з підвищення рівня ІБ, покращення захисту інформації та активів ЗОЗ.

Назва ЗОЗ **Політика інформаційної безпеки**	
Назва: ОБОВ'ЯЗКИ ПЕРСОНАЛУ	**п 2.1 -2.9**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Інформаційна безпека, людські ресурси** **ЗОЗ 2 категорії**

2. ОБОВ’ЯЗКИ ПЕРСОНАЛУ

2.1. Вимоги до персоналу

Першою лінією захисту в системі управління інформаційною безпекою є персонал або користувачі. Користувачі несуть відповідальність за безпеку всіх даних, які можуть надходити до них у будь-якому форматі.

Для ідентифікації персоналу запроваджуються ідентифікуючі беджі, які персонал повинен носити на собі та які легко переглядати іншім. Це допоможе підтримувати фізичну безпеку закладу та активів ЗОЗ. Підрядникам, представники третьої сторони, які також можуть знаходитися в будівлі ЗОЗ, надаються беджі іншого ніж у персоналу кольору. Пацієнти та інші відвідувачі, які можуть перебувати в ЗОЗ, не повинні мати беджів та не можуть знаходитися у службових приміщеннях та приміщеннях з обмеженим доступом.

Обов'язком всього персоналу закладу є вжиття необхідних заходів для забезпечення фізичної безпеки активів ЗОЗ. Якщо будь хто з персоналу бачить невстановлену особу в службовому приміщені чи приміщені з обмеженим доступом, він/вона повинен вжити всіх можливих

заходів для виведення такої особи із зазначеного приміщення та проінформувати про такий випадок ВІБ або охорону ЗОЗ при наявності служби охорони. Усі відвідувачі закладу повинні заходити до ЗОЗ через стійку реєстрації та знаходитись тільки в тих приміщеннях, які дозволені для перебування відвідувачів.

Захист робочих станцій. Всі робочі станції (ПК), які знаходяться в закладі не повинні залишати ЗОЗ без відповідного дозволу керівника чи ВІБ. Всім новим користувачам надається перший інструктаж на робочому місці щодо правил використання та зберігання робочих станцій закладу. Більшість ПК ЗОЗ містять конфіденційні дані медичного, кадрового чи фінансового характеру, тому слід дотримуватися максимальної обережності, щоб ці дані не були скомпрометовані. При використані робочих станцій за межами ЗОЗ користувач повинен вжити всіх можливих заходів із забезпечення безпечного зберігання та використання ПК, інформації та програмного забезпечення, що на ньому знаходяться.

На робочих станціях, серверному та іншому цифровому медичному обладнанні дозволено використання тільки ліцензійного програмного забезпечення та/або спеціального програмного забезпечення, яке надається авторизованим виробником разом з апаратним забезпеченням.

ПК без нагляду – робочі станції, які залишаються без нагляду повинні бути заблоковані користувачем при виході з робочої зони (робочого місця). Це правило нагадується усьому персоналу під час навчань з інформаційної безпеки. Також на робочих станціях повинно застосовуватись налаштування автоматичного блокування екрана після десяти (10) хвилин бездіяльності. Персоналу заборонено відключати чи змінювати це налаштування без відповідного дозволу ВІБ.

Робочі станції, ноутбуки, телефоні апарати інше цифрове обладнання, яке знаходиться в зоні дозволеної для знаходження відвідувачів, повинні бути облаштовані спеціальними замками та дротом прикріплення для фіксації та унеможливлення їх виносу з місця розташування.

Домашнє використання ПК. Дозволяється підключати до локальної мережі ЗОЗ тільки таке комп'ютерне обладнання та програмне забезпечення, яке дозволено використовувати. На ПК, що дистанційно підключається до локальної мережі ЗОЗ може бути встановлено лише програмне забезпечення, схвалене для використання. Персональні комп'ютери, що надаються для дистанційної роботи, повинні використовуватися виключно в службових цілях. Персонал і підрядники повинні бути ознайомлені і розуміти перелік заборонених видів діяльності, який викладений у п.2.2. нижче. Самовільне переналаштування або зміни конфігурації не допускаються на комп'ютерах, що використовуються для дистанційної роботи персоналом.

Збереження права власності - Усі програмні засоби та документація, що встановлюється на робочих станціях або надаються персоналу чи підрядниками для забезпечення діяльності ЗОЗ, є власністю закладу, якщо це не передбачено іншим договором. Виключенням можуть бути випадки використання на робочих станціях програмного забезпечення придбаного за власний кошт працівником закладу.

2.2. Заборонена діяльність

Персоналу забороняється здійснювати наступні дії. Перелік не є вичерпним. На інші заборонені види діяльності є посилання в інших місцях цього документа.

- Дії що призводять до збою інформаційної системи. Навмисні дії що призводять до збою інформаційної системи категорично заборонені. Користувачі можуть не усвідомлювати, що вони спричинили збій системи, але якщо буде виявлено, що збій стався в результаті дії користувача, повторні дії користувача, що призводять до збою інформаційної системи можуть розглядатися як навмисний вчинок.
- Спроба несанкціонованого доступу до інформаційного ресурсу або спроба обійти функцію безпеки. Це включає в себе запуск програм для злому паролів або програм для сканування локальної мережі з метою виявлення вразливостей, а також спроби обійти заборону на доступ до інформаційних ресурсів.
- Завантаження або спроба завантаження комп'ютерних вірусів, троянів, шпигунських програм або інших видів шкідливого програмного забезпечення в інформаційну систему. Винятком може бути перевірка стійкості системи уповноваженим персоналом або представниками третьої сторони, що авторизовано перевіряє СУІБ.
- Несанкціонований перегляд інформації. Умисний, несанкціонований доступ або перегляд інформації, до якої не надавалися права на доступ чи перегляд відповідно до правила «надання мінімально необхідного доступу» для виконання службових завдань. Цілеспрямована спроба перегляду або доступу до інформації, до якої не було надано доступу за визначеною в ПІБ процедурою, суворо заборонено.
- Використання особистого або недозволеного програмного забезпечення на робочих станціях. Використання особистого або недозволеного програмного забезпечення на робочих станціях ЗОЗ заборонено. Все програмне забезпечення, встановлене на робочих станціях, має бути затверджене та дозволене до використання.
- Використання неліцензійного програмного забезпечення. Все програмне забезпечення, яке встановлене на робочих станціях повинно бути ліцензійним та/або дозволеним до використання.
- Використовувати дозволене програмне забезпечення не належним чином. Порушувати або намагатися порушити умови використання або ліцензійну угоду будь-якого програмного продукту, що дозволено до використання на робочих станціях, суворо заборонено.
- Використовувати інформаційні системи не належним чином. Брати участь у будь-якій діяльності з будь-якою метою, яка є незаконною або суперечить чинній політиці інформаційної безпеки, суворо заборонено.

2.3. Користування Інтернетом та електронною поштою

Електронні засоби комунікації та Інтернет є дієвими інструментами підвищення продуктивності, Ділове використання електронних комунікацій заохочується. Однак усі системи електронного зв'язку та всі повідомлення, що генеруються на обладнанні, що належить Назва ЗОЗ, або обробляються на пристроях, що належать закладу, вважаються власністю Назва ЗОЗ, а не власністю окремих користувачів. Отже, ця політика поширюється на весь персонал і підрядників (третю сторону) та охоплює всі електронні комунікації, включаючи, але не обмежуючись ними, телефони, електронну пошту, голосову пошту, обмін миттєвими повідомленнями, Інтернет, факс, персональні комп'ютери та сервери.

Надані персоналу інформаційні ресурси, такі як робочі станції або ноутбуки, комп'ютерні системи, мережі, електронна пошта, програмне забезпечення, а також доступ до Інтернет, призначені для використання в ділових цілях. Однак особисте використання допустимо до тих пір, поки це:

- не відволікає від виконання роботи або функціональних обов'язків,
- не зменшує продуктивність персоналу,
- не перешкоджає діяльності закладу,
- не порушує нічого з наступного:

1) Незаконна діяльність - використання інформаційних ресурсів Назва ЗОЗ для досягання незаконних цілей або для здійснення правопорушень, суворо заборонено.
2) Порушення авторських прав – це включає скачування, тиражування та використання піратського програмного забезпечення, музики, книг, відео та аудіо файлів, а також незаконне дублювання та/або розповсюдження інформації та іншої інтелектуальної власності, яка перебуває під авторським правом.
3) Комерційне використання – використання інформаційних ресурсів Назва ЗОЗ для отримання особистої вигоди суворо заборонено.
4) Політична діяльність – Вся політична діяльність суворо заборонена в приміщеннях та з використанням інформаційних ресурсів Назва ЗОЗ. Заклад заохочує своїх працівників голосувати та активно брати участь у виборчому процесі, але ці заходи не повинні виконуватися з використанням активів та ресурсів Назва ЗОЗ.
5) Переслідування та дискримінація - забороняється використання комп'ютерів, електронної пошти, голосової пошти, обміну миттєвими повідомленнями, текстових повідомлень та Інтернету способами, які є образливими для інших або шкідливими та аморальними. Наприклад, показ або передача зображень, повідомлень і відео сексуального характеру суворо заборонені. Інші приклади неправильного використання включають, але не обмежуються ними, етнічні образи, расові коментарі, або все, що може бути розтлумачено як переслідування, дискримінація, зневажливе ставлення, вираз погроз або прояв неповаги до інших.
6) Небажана електронна пошта - усі повідомлення зроблені з використанням ІТ-ресурсів Назва ЗОЗ повинні бути адресними та доцільними. Розповсюдження «небажаної» пошти, наприклад, листів щастя, реклами або несанкціонованих клопотань, забороняється. Якщо користувачі отримали будь-яке з перерахованого вище повідомлень, необхідно їх видалити та нікому не пересилати.

Заклад зберігає за собою право здійснювати моніторинг змісту будь-якого електронного повідомлення та комунікації, що генерується або передається з використанням інформаційних активів Назва ЗОЗ. Це робиться з метою належного обслуговування та захисту інформаційно-телекомунікаційного обладнання, мереж та ефективного використання наявних ресурсів. Моніторинг може здійснюватися постійно або час від часу. Для цього можуть застосовуватися різні методи моніторингу. Наприклад, для аудиту або аналізу витрат на зв'язок, можуть відстежуватися набрані номери зі службових телефонів, тривалість дзвінків, кількість дзвінків на/з конкретного телефону, час доби і т.д. Інші приклади, коли електронні комунікації можуть контролюватися, включають, але не обмежуються, дослідженнями та тестуваннями спрямованими на оптимізацію ІТ-ресурсів, усунення технічних проблем та виявлення закономірностей зловживань або незаконної діяльності.

Заклад залишає за собою право на власний розсуд переглядати файли або електронні повідомлення будь-якого працівника в обсязі, необхідному для забезпечення ефективного використання всіх службових електронних носіїв і засобів комунікації відповідно до всіх чинних законів і нормативних актів, а також цієї Політики інформаційної безпеки.

2.4 Доступ до Інтернет

Доступ в Інтернет надається тільки тим співробітникам, хто його потребує для виконання службових обов'язків. Доступ до Інтернет це ресурс, за який Назва ЗОЗ витрачає кошти тому його використання потребує виконання наступних вимог. Персонал, що має доступ до Інтернету, не повинен використовувати цей доступ для розваг, прослуховування музики чи радіо, прослуховування онлайн аудіо книг та перегляду фільмів та інших медійних файлів тощо. Забороняється використовувати доступ до Інтернет для особистої комерційної діяльності чи вирішення своїх побутових питань. Треба розуміти, що використання цього ресурсу не цільовим шляхом збільшую витрати закладу, а також створює додаткові загрози інформаційної безпеки.

Персонал повинен розуміти, що індивідуальне використання Інтернету контролюється, і якщо виявиться, що співробітник витрачає надмірну кількість часу, витрачає великі обсяги трафіку для особистого чи нецільового користування, або відвідує ресурси, які небезпечні з точки зору забезпечення інформаційної безпеки, то до нього/неї будуть вжиті дисциплінарні заходи.

Ресурси які заборонено відвідувати, такі як ігрові інтернет-сайти, торенти, файлообмінники, порносайти, чати та онлайн програми для обміну музикою, тощо, автоматично блокуються. Перелік заборонених ресурсів постійно контролюється і оновлюється в міру необхідності. Будь-який співробітник, який цілеспрямовано, неодноразово буде намагатися відвідати заборонені ресурси в Інтернет, буде притягнутий до дисциплінарної відповідальності і може бути звільнений.

В закладі здійснюються спеціальні запобіжні заходи для блокування зовнішнього доступу через Інтернет до інформаційних ресурсів закладу, не призначених для публічного доступу, а також для захисту конфіденційної інформації ЗОЗ при її передачі через Інтернет.

Відповідальний за інформаційну безпеку контролює виконання заходів із безпечного використання Інтернету, а саме:

- контролює щоб доступ до Інтернет з робочих місць здійснювався через встановлені точки доступу до Інтернет;
- контролює, щоб тільки публічна та відкрита інформація про ЗОЗ була доступна в Інтернете;
- контролює, щоб користувачі не мали прав встановлювати або завантажувати будь-яке програмне забезпечення (додатки, медіа файли, заставки тощо) з Інтернет. Якщо у користувачів є потреба в додатковому програмному забезпеченні, користувач повинен отримати дозвіл;
- використання Інтернету повинно узгоджуватися з комерційною діяльністю закладу. Мережа може бути використана для продажи послуг, однак використання мережі на робочому місці для отримання особистого прибутку заборонено;
- конфіденційні або персональні дані, включаючи номери кредитних карток, номери телефонів, паролі для входу в систему та інші дані, які можуть бути використані для

доступу до конфіденційної або персональної інформації повинні передаватися через Інтернет у зашифрованому виді.
- використання програмного забезпечення для шифрування та ключів шифрування повинно контролюватися відповідальним за ІБ. Самостійне використання шифрувального програмного забезпечення та ключів шифрування, без погодження з відповідальним за ІБ, заборонено, і може призвести до дисциплінарного покарання.

2.5. Повідомлення про несправності

Користувач повинні інформувати IT підрозділ про випадки, коли програмне забезпечення робочої станції не функціонує належним чином. Несправне програмне забезпечення становить ризик для інформаційної безпеки. Якщо користувач, або керівник користувача, підозрює зараження робочої станції вірусом, слід негайно вжити наступних заходів:

- припинити використання комп'ютера;
- не запускати на виконання ніяких команд, включаючи команду збереження даних;
- не закривати жодного з вікон або програм комп'ютера;
- не вимикати комп'ютер або периферійний пристрій на самому екрані;
- по можливості фізично відключити комп'ютер від мереж живлення та локальної мережі;
- повідомити про ураження робочої станції IT-підрозділ та відповідального за ІБ, вказавши ознаки незвичайної поведінки комп'ютера (блокування екрану, виникнення несподіваного доступ до системного диска, незвичайна реакція на команди тощо) і час, коли це було вперше помічено;
- повідомити про будь-які зміни у використанні апаратного чи програмного забезпечення, які передували несправності;
- не намагатися самостійно видалити підозрілий файл!

Відповідальний з ІБ повинен вжити заходи для усуненням несправності, а також повідомити керівнику закладу про результати цих дій з рекомендаціями щодо подальших кроків для запобігання подібних випадків у майбутньому.

2.6. Повідомлення про інциденти безпеки

Весь персонал, який є користувачами інформаційних ресурсів закладу або підрядники, які мають доступ до цифрових активів Назва ЗОЗ зобов'язані повідомляти відповідального з ІБ про виявлені інциденти інформаційної безпеки. Користувач - це будь-яка особа, уповноважена на доступ до інформаційного ресурсу закладу. Користувачі несуть відповідальність за повсякденну практичну безпеку ресурсу, яким вони користуються. Користувачі повинні повідомляти про всі інциденти безпеки або порушення політики безпеки негайно своєму безпосередньому керівнику або відповідальному з інформаційної безпеки. При неможливості негайного повідомлення про інцидент безпеки вищевказаним особам, користувач повинен без зволікань проінформувати про інцидент будь-якого члена Робочої групи з інформаційної безпеки закладу, які вказані вище в цьому документі.

Реагування на повідомлення про інциденти інформаційної безпеки повинно бути якомога швидким. Кожен член Робочої групи з інформаційної безпеки повинен негайно вжити заходи відповідно до Плану реагування на інцидент інформаційної безпеки. Кожен інцидент повинен бути проаналізованим, щоб визначити, чи потрібно внесення необхідних змін в

існуючу систему управління інформаційною безпекою Назва ЗОЗ. Усі виявлені інциденти реєструються в журналі інцидентів інформаційної безпеки. Обов'язком відповідального за ІБ є організація та проведення навчання, щодо будь-яких змін у плані реагування на інциденти, які були зроблені в результаті розслідування інциденту.

Внутрішні порушення інформаційної безпеки повинні оперативно розслідуватися. У разі підозри на порушення законодавства, відповідальний з ІБ повинен звернутися до правоохоронних органів.

2.7 Передача конфіденційної інформації

Передача конфіденційної інформації може здійснюватися за допомогою засобів електронного зв’язку, на цифрових носіях чи у паперовому виді. Конфіденційна інформація передається від однієї особи іншій під час ведення службових справ. Особа, яка отримала конфіденційну інформацію повинна забезпечити її зберігання відповідно до умов, встановлених особою, що надала таку інформацію. Весь персонал повинен розуміти про чутливий характер медичних та персональних даних, що отримує заклад в ході свого функціонування, і утримуватись від розголошення таких даних. Будь-яке цілеспрямоване оприлюднення конфіденційних даних, до яких працівник має доступ, є порушенням, яке призведе до покарання, а також може призвести до судового позову стосовно порушника.

2.8. Передача даних та програмного забезпечення

Власне програмне забезпечення, яке не дозволене до використання в закладі не може використовуватися на робочих станціях чи комп'ютерах або в локальній мережі Назва ЗОЗ. Якщо існує потреба в конкретному програмному забезпеченні, потрібно надати запит на дозвіл своєму безпосередньому керівнику. Користувачі не повинні використовувати програмне забезпечення, що встановлене на робочих станціях, або на особистих комп'ютерах чи комп'ютерному обладнанні при дистанційній роботі без відповідного дозволу.

Дані, що є власністю закладу включаючи інформацію про пацієнтів, інформацію про ІТ-системи, фінансову інформацію або дані про людські ресурси, не повинні розміщуватися на будь-якому комп'ютері, який не є власністю ЗОЗ, без письмової згоди відповідного керівника. ЗОЗ повинен захищати всі дані та програмне забезпечення, які йому належать, тому повинен контролювати системи, в яких такі дані містяться. У випадку, якщо відповідний керівник отримає від персоналу запит на переміщення даних з робочої станції на особистий ПК, керівник повинен визначитися чи є в цьому службова потреба та уразі прийняття рішення на дозвіл переміщення, повідомити відповідального з інформаційної безпеки про таку передачу даних.

Треба розуміти, що заклад обмежений у можливостях захисту даних на персональних ПК тому дозвіл на переміщення треба надавити у разі гострої службової необхідності. Заклад не може бути впевнений у засобах, які можуть бути застосовані для захисту конфіденційної чи чутливої інформації на персональних ПК, звідси необхідність цього обмеження.

2.9. Шифрування електронної пошти та даних

Для забезпечення конфіденціальної та захисту конфіденційної інформації при передачі в мережі Інтернет дозволяється використання відповідного програмного забезпечення (наприклад програми WinZip), яке дозволяє персоналу обмінюватися електронною поштою з віддаленими користувачами, які теж мають відповідне програмне забезпечення для шифрування/дешифрування. Обидва користувачі обмінюються таємними паролями (у випадку використання WinZip) або відкритими ключами, які можуть бути використані для дешифрування повідомлення. Співробітник, який бажає використати відповідне програмне забезпечення повинен звернутися до відповідального за ІБ для отримання дозволу на використання відповідного програмного забезпечення.

При передачі конфіденційної інформації електронною поштою та розумінні, що є ризик потрапляння такої інформації до сторонніх осіб чи отримання доступу до неї сторонніми особами необхідно застосовувати програмне забезпечення шифрування/дешифрування (наприклад WinZip).

Вся персональна інформація та дані яка зберігаються на робочих станціях ЗОЗ повинні бути в зашифрованому вигляді. До такої інформації відноситься будь-яка інформація, яка може бути використана для ідентифікації особи, а саме:

- Імена та прізвища
- Адреси
- Дані геолокації
- Всі елементи дат, безпосередньо пов'язаних з особою (Дати народження, шлюбу, смерті і т.п.)
- Телефонні номери
- Факсимільні номери
- Номери водійських прав
- Адреси електронної пошти
- Номери соціального та медичного страхування
- Персональні медичні дані (картка пацієнта, історія хвороби, листи непрацездатності тощо)
- Номери рахунків, номери сертифікатів/ліцензій
- Ідентифікатори транспортних засобів та серійні номери
- Ідентифікатори пристроїв і серійні номери
- URL-адреси та IP-адреси
- Біометричні ідентифікатори
- Фотографічні зображення обличчя.

Назва ЗОЗ **Політика інформаційної безпеки**	
Назва: УПРАВЛІННЯ ДОСТУПОМ	**П 3.1 – 3.12**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Інформаційна безпека ЗОЗ 2 категорії**

3. УПРАВЛІННЯ ДОСТУПОМ

3.1. Загальні положення

Мета цієї політики полягає в тому, щоб забезпечити контроль доступу до інформації та пристроїв, а також гарантувати наявність процедур для забезпечення надійного захисту інформації. Захист інформації з обмеженим доступом і зокрема захист персональних даних є пріоритетною ціллю.

3.2. Ролі щодо контролю доступу

Керівник закладу - визначає цю політику.

Відповідальний за інформаційну безпеку - координує цю політику.

Персонал - виконує цю політику, згідно посадових обов’язків.

3.3. Ідентифікація користувачів

Кожний користувач повинен мати унікальний обліковий запис (логін) та пароль для входу. Система контролю доступу повинна ідентифікувати кожного користувача шляхом створення і

використання унікального облікового запису користувача та запобігати доступу та використанню інформаційних ресурсів закладу неавторизованим користувачем. Вимоги безпеки для ідентифікації користувача включають:

- кожному користувачеві присвоюється унікальний обліковий запис;
- користувачі несуть відповідальність за використання та неправомірне використання свого індивідуального облікового запису користувача.

Усі облікові записи користувачів перевіряються щонайменше раз на рік і всі неактивні облікові записи користувача и блокуються. Відділ кадрів ЗОЗ сповіщає відповідального за ІБ або відповідного фахівця ІТ-відділу про звільнення працівника або припинення співробітництва з персоналом підрядника. При отримані такого сповіщення неактивні облікові записи блокуються.

Обліковий запис блокується після максимум трьох (3) невдалих спроб входу в систему. Для відновлення доступу в цьому випадку потрібне залучення Адміністратора.

Користувачі, яким необхідно отримати доступ до систем або мереж ЗОЗ, повинні заповнити відповідну Форму Доступу (Додаток 1). Ця форма повинна бути підписана безпосереднім керівником та погоджена керівником ЗОЗ або відповідальним за інформаційну безпеку.

3.4. Правила встановлення і поводження з паролями

Ідентифікатори користувачів і паролі потрібні для того, щоб отримати доступ до мереж і робочих станцій. До всіх паролів застосовується встановлена цім документом Парольна політика, для забезпечення стійкості паролів. Це означає, що всі паролі повинні відповідати вимогам, які призначені для того, щоб пароль було важко підібрати чи зламати. Користувачі зобов'язані створювати та користуватися паролями, щоб отримати доступ до відповідних мереж, ІТ-ресурсів чи робочої станції. При призначені паролю користувачеві буде автоматично запропоновано вручну призначити пароль, відповідно до таких вимог:

Довжина пароля – Пароль повинен складатися з мінімуму восьми (8) символів.

Вимоги до складу - Пароль повинен містити комбінацію символів латинського алфавіту верхнього та нижнього регістру, числових символів та спеціальних символів.

Частота зміни – Пароль повинен бути змінений кожні 30 днів. Скомпрометований пароль повинен бути змінений негайно.

Повторне використання - Попередні шість (6) паролі не можуть бути використані повторно.

Обмеження на обмін паролями - Паролі не повинні передаватися іншим працівникам, записуватися на папері або зберігатися на робочій станції і повинні зберігатися у таємниці.

Обмеження на відображення та зберігання паролів - Паролі маскуються на екрані робочої станції при введені, не друкуються і не включаються до електроних журналів чи звітів. Паролі зберігаються у зашифрованому виді.

3.5. Угода про конфіденційність

Користувачі інформаційних ресурсів Закладу при працевлаштуванні підписують угоду про конфіденційність (Додаток 2). Угода повинна містити наступне твердження:

Я розумію, що будь-яке несанкціоноване використання або розголошення конфіденційної інформації, може призвести до покарання, відповідно до чинного законодавства та політики інформаційної безпеки. Мої зобов'язання щодо нерозголошення конфіденційної інформації, залишаються чинними безстроково.

Тимчасово влаштовані працівники та підрядники, які не підписували угоди про конфіденційність, підписують такий документ при отримані доступу до інформаційних ресурсів ЗОЗ.

3.6. Контроль доступу

Інформаційні ресурси закладу захищаються за рахунок використання системи контролю доступу. Система контролю доступу включає внутрішні засоби захисту (паролі, шифрування, таблиці контролю доступу, налаштування інтерфейсів користувача тощо), так і зовнішні (пристрої захисту портів, брандмауери, автентифікацію на основі хоста тощо).

Правила доступу до ресурсів встановлюються власником ресурсу. Доступ надається тільки шляхом заповнення форми запиту на доступ (Додаток 1). Ця форма затверджується керівником чи відповідальним з ІБ.

При надані доступу використовується принцип мінімально необхідного доступу до ресурсу користувача для виконання ним функціональних завдань. Доступ користувача до відповідного ресурсу відбувається тільки після затвердження форми запиту на доступ керівником або головним лікарем та тільки до того ресурсу до якого був наданий запит на допуск.

В закладі можуть використовуватись випливаючи на екрані робочих станцій електронні попередження про несанкціоноване використання ресурсу та про відповідальність порушника.

При використанні програмного забезпечення управління безпекою кінцевих пристроїв повинна підтримуватися онлайн авторизація при використані додатків. Кожне підключення підлягає процесу авторизації (введенню логіна та пароля).

Для систем, що містять обмежену та персональну ідентифікаційну інформацію (PII), встановлено правило на передумові "Усе взагалі заборонено, доки явно не дозволено" та розроблено матрицю контролю доступу для фіксації санкціонованого доступу на основі ролей користувачів. Для визначення зв'язку між правами доступу та ролями, індивідуально для кожної ролі надається доступ лише до інформації, необхідної для виконання завдань, а фізичний доступ надано лише до засобів оброблення інформації (IT-обладнання, прикладних програм, процедур, кімнат), потрібних для виконання завдання/роботи/ролі. Матриця контролю доступу переглядається і оновлюється власником не рідше ніж один раз на рік.

Привілейовані та технічні записи мають відповідального співробітника згідно з виконуваними ним функціями та роллю. Події доступу з використанням звичайних, привілейованих та технічних записів логуються технічними засобами і відображаються у належним чином захищеному реєстрі подій. Керівники власників звичайних, технічних та привілейованих облікових записів гарантують дотримання принципу "необхідно знати" при наданні прав доступу та періодично переглядають відповідність наданих прав доступу фактичному використанню облікового запису. Облікові дані для будь-яких облікових записів

захищені від компрометації, не зберігаються у вигляді відкритого тексту, та не є частиною вихідного коду програмного забезпечення. При створенні технічних облікових записів, перевіряється виконання вимоги що ці записи не повинні бути доступні для інтерактивного доступу користувачів, щоб не допустити зловживання. Керівники відповідають за належне адміністрування засобів контролю управлінням привілейованим доступом.

Звичайні користувачі не мають привілейованих прав доступу.

За кожним технічним обліковим записом закріплений його власник.

Дані користувача для входу в систему передаються користувачу особисто або виключно з використанням безпечних каналів зв'язку, ці дані ніколи не записуються на носії та не передаються третім особам. Архівація записів усіх значущих подій, пов’язаних з використанням та управлінням ідентифікацією користувачів і таємною інформацією автентифікації забезпечується технічними засобами.

Після успішного входу, користувачі гарантують, що обладнання не залишається без їх нагляду, а активні сеанси припиняються або блокуються, коли це необхідно. Користувач виходить з системи одразу, як припиняє в ній роботу.

Надані користувачу права доступу, відповідність наданого обсягу прав поточній ролі користувача, займаній ним посаді та виконуваній конкретним співробітником роботі перевіряється керівником не рідше ніж один раз на рік. При перегляді прав доступу, беруться до уваги всі облікові записи, як звичайні, так привілейовані і технічні облікові записи. Для привілейованих і технічних облікових записів перевіряється відповідність наданих прав доступу фактичному використанню облікового запису.

3.7. Припинення права доступу

Якщо працівник змінює посаду його безпосередній керівник ініціює перегляд прав доступу та заповнює Форму запиту на доступ (Додаток 1). У Формі вказується дата набрання чинності зміни посади та назва посади, щоб ІТ-відділ міг змінити права доступ відповідно до принципу мінімально необхідного доступу до ресурсів. Протягом обмеженого періоду працівнику, який змінює посаду, можуть зберігатися попередні права доступу, а також додаватися нові права доступу, необхідні для виконання нових посадових обов'язків.

Перегляд прав доступу персоналу повинен проводитися не рідше ніж один раз на рік. Відповідальний за інформаційну безпеку повинен сприяти перегляду прав доступу користувачів, щоб переконатися, що весь персонал має мінімально необхідні права доступ для ефективного виконання своїх робочих функцій. Виявлені в ході перегляду надлишкові права доступу припиняються.

3.8. Припинення дії облікового запису користувача

При звільненні працівника, його безпосередній керівник повинен завчасно ініціювати процедуру припинення доступу, вказавши «Видалити доступ» у Формі запиту на доступ (Додаток 1) та дату останнього робочого дня працівника, щоб його обліковий запис користувача міг бути налаштований на закінчення терміну дії у день звільнення. Безпосередній керівник контролює своєчасну здачу працівником, що звільняється відповідних

пристрої доступу, які йому/їй надавалися. Обліковий запис та доступ працівника блокується по завершені останнього робочого дня.

Не рідше одного разу на рік, відповідальний з інформаційної безпеки повинен ініціювати перегляд списку активних облікових записів користувачів для оцінки прав доступу відповідно до принципу надання мінімально необхідного доступу до IT-ресурсів для виконання функціональних завдань. Керівники відділів закладу повинні переглянути списки доступу стосовно своїх підлеглих та протягом п'яти (5) робочих днів надати уточнюючи дані щодо прав доступу. Якщо буде виявлені надлишкові права доступу вони повинні бути припинені. Про необхідність припинення надлишкових прав доступу або блокуванні активних акаунтів звільнених працівників керівники відділів закладу без зволікань повідомляють IT-відділ та надає оновлену Форму запиту на доступ (Додаток 1).

3.9. Заходи з безпеки екстреного доступу до електронної захищеної медичної інформації

Заклад забезпечує для медпрацівника гарантований терміновий засіб доступу до електронної захищеної медичної інформації у разі екстреної необхідності.

Рішення екстреного доступу використовується лише тоді, коли звичайні процеси виявляються недостатніми для своєчасного надання медичної допомоги і дозволяються в наступних ситуаціях, які можуть виникнути при наданні невідкладної медичної допомоги пацієнту:

- Медпрацівник забув свої ім’я користувача/пароль;
- Пароль медпрацівника заблокований;
- Медпрацівник не має облікового запису користувача;
- Збій центральної системи автентифікації;
- Несправність зчитувача смарт-карти або біометричних даних;
- Невідкладна медична ситуація змушує особу виконувати роль, у якій він/вона не має достатніх прав доступу до необхідної електронної захищеної медичної інформації.

Відповідальний з інформаційної безпеки розробляє, документує, впроваджує та перевіряє процедури екстреного доступу, які використовуються у випадку надзвичайної ситуації, яка вимагає екстреного доступу до електронної захищеної медичної інформації. Для кожної системи, яка містить електронну захищену медичну інформацію розроблена чітко визначена та зрозуміла процедура надання термінового доступу за допомогою альтернативних та/або ручних методів в екстрених випадках. Всі облікові записи для екстреного доступу та процедури розподілу доступу для них задокументовані та протестовані.

Доступ до таємних даних автентифікації, такі як логін та пароль, для використання надзвичайних облікових записів, створених заздалегідь, надаються на таких носіях, як друкована сторінка, картка з магнітною смугою, смарт-картка або жетон в залежності від способу автентифікації для конкретної системи.

Носій з таємними даними автентифікації зберігається в запечатаному конверті у сейфі старшої медсестри. Отримання носія вимагає надання ідентифікації за допомогою

посвідчення особи, яка отримує носій та реєстрації факту отримання носія в журналі реєстрації з метою гарантування принципу 4-х очей та неспростовності події.

Всі факти використання носія, перевіряються відповідальним з інформаційної безпеки. Під час перевірки, робиться огляд виконаної діяльності, включаючи отримані дані або дані, до яких був доступ. Отримані фактичні дані та контрольні журнали звіряються, щоб пересвідчитися в їх відповідності. Якщо це необхідно, відповідальний з інформаційної безпеки робить відповідні записи з розкриття інформації. Для запобігання повторному використанню, коли пароль відомий, екстрені облікові записи невідворотно блокуються. Відповідальний з інформаційної безпеки визначає ефективність процедури екстреного доступі, і за необхідності корегує її.

Неприйнятне використання екстреного доступу фіксується як інцидент інформаційної безпеки, відносно якого вживаються відповідні заходи реагування на інциденти.

Відповідальний з інформаційної безпеки щорічно проводить перевірку і навчання персоналу, щоб переконатися, що процедура екстреного доступу залишається актуальною.

3.10. Заходи безпеки з обмеження доступу до персональних даних

В закладі встановлено процес класифікації персональних даних. Персональні дані збираються лише на основі особистої згоди, або якщо це визначено чинним законодавством, і лише з метою та в обсязі, як це зазначено у згоді чи визначено законодавством. Персональні дані обробляються та зберігаються не довше, ніж це необхідно для досягнення цілей, для яких вони були зібрані. Персональні дані можуть передаватися третім особам лише за наявності дозволу чи відповідно до вимог законодавства. Зібрані персональні дані захищаються від несанкціонованого доступу відповідно до вимог чинного законодавства та кращих галузевих практик.

Встановлені та виконуються наступні процедури:

- отримання згоди фізичних осіб на збір персональних даних;
- надання доступу до персональних даних;
- обробки та зберігання персональних даних;
- безпечної передачі персональних даних третім особам;
- деперсоналізації персональних даних;
- безпечного видалення персональних даних;
- обробки запитів та претензій від осіб щодо обробки їхніх персональних даних, експорту даних;
- повідомлення про інциденти несанкціонованого доступу чи цілісності персональних даних.

Доступ до персональних даних надається обмеженій групі осіб. Доступ налаштований таким чином, щоб заборонити експорт даних за межі захищеної системи чи сервісу. Доступ до персональних даних надається на підставі службових обов'язків в частині медичного обслуговування пацієнтів. Експорт масиву персональних даних здійснюється у виняткових випадках через формальне затвердження з боку керівництва.

Опис переміщення персональних даних в IT-середовищі, місця зберігання персональних даних та перелік усіх процесів та процедур, пов'язаних із збиранням та обробкою персональних даних задокументовано та оновлюється після змін в інформаційних системах, в процесах та процедурах чи у законодавстві щодо захисту персональних даних.

Процес затвердження надання доступу до інформаційних систем включає перевірку відповідності вимогам політики захисту персональних даних пацієнтів.

Місця зберігання персональних даних, включно з персональними медичними даними зведено до абсолютно необхідного мінімуму, для того, щоб скоротити взаємодію таких даних із кіберзагрозами. IT-процеси та IT-архітектура переглядається та вдосконалюється регулярно з метою покращення захисту персональних даних.

Кількість працівників, яким надається доступ до персональних даних обмежена до мінімально необхідної з урахуванням необхідності забезпечити надання доступу для осіб, які будуть заміняти колег у разі відсутності для забезпечення неперервності процесів закладу.

Передача персональних даних включно з персональними медичними даними третій стороні заборонена, окрім випадків, коли це дозволено згодою пацієнта чи передбачено законодавством. Для всіх процесів, що включають доступ третьої сторони до персональних даних визначено ролі та обов'язки володільця та розпорядника даних.

Одразу після досягнення мети обробки персональних даних, вони деперсоналізуються чи безпечно видаляються, включно з персональними медичними даними. В іншому випадку, отримується нова згода пацієнта на обробку його персональних даних. Видалення персональних даних здійснюється безпечно і невідворотно, відповідно до кращих галузевих практик.

3.11. Заходи безпеки з обмеження фізичного доступу

Заходи безпеки з обмеження фізичного доступу визначені в розділі "ФІЗИЧНА БЕЗПЕКА" Політики інформаційної безпеки.

3.12. Відповідальність

Вимоги цієї політики поширюються на весь персонал закладу. Усі працівники закладу мають бути ознайомлені із її вимогами. Відповідальність за порушення визначена у відповідному розділі затвердженої Політики інформаційної безпеки Назва ЗОЗ.

Назва ЗОЗ[1] **Політика інформаційної безпеки**	
Назва: ПІДКЛЮЧЕННЯ ДО МЕРЕЖІ	**П 4.1 – 4.5**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Інформаційна безпека ЗОЗ 2 категорії**

4. ПІДКЛЮЧЕННЯ ДО МЕРЕЖІ

4.1. З’єднання та підключення

Доступ до інформаційних ресурсів закладу через модеми, інші комунікаційні пристрої або відповідне програмне забезпечення підлягає авторизації та автентифікації системою контролю доступу. Зовнішній виклик чи комутація на внутрішній номер (кінцевий пристрій) без проходження через систему контролю доступу заборонений.

Системи, що дозволяють проходження зовнішнього виклику на кінцевий пристрій, в тому числі сервер повинні гарантувати додаткову безпеку на рівні операційної системи та додатків. Такі системи повинні також мати можливість контролювати рівень активності, щоб гарантувати, що використання кінцевих пристроїв відбувається належним чином та з виконанням заходів безпеки.

Права доступу до з'єднання через комутатори надаються тільки на вимогу керівника відділу з поданням Форми доступу (Додаток 1) та затверджуються керівником закладу чи відповідальним з ІБ.

Підключення до зовнішніх мереж відбувається через інтернет-провайдера. Якщо користувач має конкретну потребу зв'язатися із зовнішнім комп'ютером або мережею через прямий канал зв’язку він повинен отримати дозвіл від керівника закладу або відповідального з ІБ. При

прийняті позитивного рішення відповідальний з інформаційної безпеки повинен вжити необхідних заходів із забезпечення належного рівня безпеки нового каналу зв’язку.

4.2. Телекомунікаційне обладнання

До телекомунікаційного обладнання та засобів відноситься наступне:

- телефонні лінії та обладнання
- факсимільні лінії та обладнання
- телефоні навушники та гарнітура
- телефони типу програмного забезпечення, встановлені на робочих станціях
- службові мобільні телефони
- програмне забезпечення для маршрутизації викликів
- обладнання для адміністрування телефонної системи
- мережеві лінії
- міжміські лінії
- місцеві телефонні лінії.

Цей перелік не є вичерпним.

4.3. Постійні з’єднання

Забезпечення безпеки телекомунікаційних з’єднань є дуже важливим завданням. Інформаційна безпека закладу може бути поставлена під загрозу, якщо не забезпечити безпечне користування засобами зв’язку. Необхідно забезпечити аналіз ризиків при підключені до зовнішніх мереж та регулярно аналізувати ризики постійно діючих каналів з’єднання. Аналіз ризиків повинен враховувати тип необхідного доступу, цінність інформації що передається, заходи безпеки, що застосовуються третьою стороною, а також наслідки для системи управління безпекою закладу. Відповідальний за інформаційну безпеку повинен бути залучені до процесів проектування та затвердження каналів підключення до зовнішніх мереж, а також укладення договорів з третьою стороною на отримання послуг з телекомунікаційного забезпечення закладу.

4.4. Договір на телекомунікаційні послуги

При укладанні договору на отримання телекомунікаційних послуг закладом необхідно враховувати наступні вимоги до постачальника таких послуг:

- відповідні розділи політики інформаційної безпеки надавача послуг були переглянуті та приведені у відповідність з вимогами політики інформаційної безпеки закладу;
- відповідні вимоги враховані та застосовуються;
- проведена оцінка ризиків пов’язаних з виконанням додаткових зобов'язань надавача послуг;
- включене право на аудит виконання договірних зобов’язань;
- домовленість стосовно повідомлення про інциденти інформаційної безпеки включені в угоду;
- наданий опис кожної послуги, яка буде доступна;

- доступ до ресурсів закладу надавачем послуг повинен бути лише на мінімально необхідному рівні, достатньому для виконання договірних зобов'язань;
- детальний список користувачів з боку надавача послуг, які будуть мати доступ до мережі закладу, повинен бути доступний для аудиту;
- дата і час, коли послуга повинна бути доступна, завчасно узгоджені;
- процедури щодо захисту інформаційних ресурсів узгоджені заздалегідь, а спосіб аудиту затверджений обома сторонами;
- спосіб моніторингу і припинення доступу користувачів визначений;
- обмеження на копіювання та розкриття інформації включені;
- обов'язки щодо встановлення та технічного обслуговування апаратного та програмного забезпечення зрозумілі та заздалегідь узгоджені;
- заходи щодо забезпечення повернення або знищення програмного забезпечення та інформації після закінчення дії договору визначені та прописані;
- заходи фізичного захисту, при необхідності, також включені в угоду;
- спосіб надання доступу та авторизація користувачів, повинен бути встановлений до того, як користувачам буде наданий доступ;
- створені механізми для забезпечення дотримання заходів безпеки сторонами угоди;
- детальний перелік заходів безпеки, які будуть вжиті сторонами угоди, повинен бути розглянутий та погоджений до укладення угоди.

4.5. Брандмауер

Налаштування брандмауера повинно контролюватися відповідальним з ІБ. Якщо брандмауер знаходиться та налаштовується стороною, яка надає ІТ-послуги закладу то ця сторона повинна надати повну інформацію про актуальні налаштування брандмауера відповідальному за інформаційну безпеку та активно співпрацювати з ним/нею у питаннях подальшого його використання та змін налаштувань.

Назва ЗОЗ **Політика інформаційної безпеки**	
Назва: Антивірусний захист	П 5.1. – 5.6.
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Інформаційна безпека ЗОЗ 2 категорії**

5. АНТИВІРУСНИЙ ЗАХИСТ

5.1. Загальні положення

Політика забезпечення антивірусного захисту в Назва ЗОЗ (далі – Політика АЗ) встановлює загальні вимоги та порядок забезпечення антивірусного захисту інформаційних ресурсів та цифрових активів. Метою політики є мінімізація та/або запобігання негативних наслідків, які можуть виникнути в результаті зловмисних дій за допомогою шкідливого програмного забезпечення.

Вимоги, що містяться в Політиці АЗ, є загальними для всього серверного обладнання і робочих станцій в Назва ЗОЗ і носять обов'язковий характер до виконання і дотримання усім персоналом.

Цілями Політики АЗ є:

1. Підтримання інформаційної безпеки Назва ЗОЗ на належному рівні.
2. Відповідність вимогам нормативно-правових актів України в області інформаційної безпеки, міжнародних стандартів в області ІБ та Політики інформаційної безпеки Назва ЗОЗ.
3. Захисту інформаційних активів Назва ЗОЗ від порушень конфіденційності, цілісності та доступності.

Основними **завданнями** Політики АЗ є:

- Визначення принципів та вимог щодо антивірусного захисту Назва ЗОЗ;
- Захист інформаційних активів Назва ЗОЗ;
- Мінімізація ризиків;

- Попередження і унеможливлення вірусних атак;
- Забезпечення надання медичних послуг та надійної роботи Назва ЗОЗ .

До використання в Назва ЗОЗ допускаються лише Назва антивірусного програмного забезпечення (ПЗ), централізовано закуплене у Назва виробника антивірусного ПЗ.

У разі необхідності використання інших антивірусних засобів, необхідно отримати дозвіл на використання у відповідального за інформаційну безпеку (ІБ) закладу.

Дія Політики АЗ поширюється на всі інформаційні ресурси та системи Назва ЗОЗ.

5.2. Ролі та відповідальність

З метою належного виконання Політики АЗ у Назва ЗОЗ встановлюються наступні функціональні ролі та відповідальність:

1. Системний адміністратор - посадова особа, що здійснює підтримку та супроводження засобів системи антивірусного захисту в прикінцевому обладнанні, мережі та інформаційних системах Назва ЗОЗ згідно з вимогами чинної Політики АЗ;
2. Відповідальний за ІБ – контролює та наглядає за дотриманням вимог з антивірусного захисту, які визначені у Політиці АЗ;
3. Керівник закладу - узгоджує права доступу користувачів та приймає рішення на закупівлю антивірусного ПЗ;
4. Персонал:
    - Має знати та виконувати вимоги цієї Політики АЗ та Політики інформаційної безпеки Назва ЗОЗ;
    - Повинен сприяти попередженню, виявленню та розслідуванню інцидентів інформаційної безпеки;
    - Повинен вживати всі можливі заходи безпеки з метою запобігання чи зменшення втрат і збитків Назва ЗОЗ;
    - Відповідає за виконання вимог цієї Політики АЗ на робочому місці.

5.3. Вимоги до антивірусного ПЗ та роботи користувачів

1. До застосування в Назва ЗОЗ дозволене тільки ліцензійне програмне забезпечення - Назва антивірусного програмного забезпечення.
2. Засоби антивірусного захисту мають забезпечувати захист робочих станцій та серверів під управлінням ОС Windows;
3. Система антивірусного захисту Назва ЗОЗ повинна надавати можливість віддаленого централізованого керування та обслуговування, зокрема:
    - встановлення та видалення антивірусного ПЗ та його компонентів;
    - налаштування параметрів антивірусного ПЗ та його компонентів;
    - контроль дотримання налаштувань антивірусного ПЗ користувачами;
    - централізоване створення та віддалений запуск завдань антивірусного захисту, в тому числі перевірка жорстких дисків, переносних носіїв інформації тощо;

- встановлення ліцензійних ключів та контроль дотримання умов ліцензійної угоди;
- автоматичне оновлення антивірусних баз даних та модулів антивірусного ПЗ;
- централізований збір, реєстрація та інформування системного адміністратора щодо подій та інцидентів безпеки, зафіксованих антивірусним ПЗ.

4. Оновлення баз даних антивірусного ПЗ у інформаційних системах закладу повинно відбуватися щоденно в автоматичному режимі.
5. Для робочих станцій, які не підключені до мережі, оновлення антивірусних баз даних повинно проводитися не рідше одного разу на тиждень.
6. Поширення оновлень антивірусних баз даних для інформаційних систем, під'єднаних до мережі, повинно проводитися централізовано через відповідний сервер антивірусного захисту, а для робочих станцій, не під'єднаних до мережі — за допомогою зовнішніх носіїв.
7. Клієнтські антивіруси повинні регулярно, щоденно перевіряти наявність останніх оновлень антивірусних баз та компонентів на сервері оновлень, та встановлювати їх, якщо такі наявні.
8. У антивірусного ПЗ мають бути наступні функціональні можливості:
   - пошук вірусів в пам'яті ПК та на підключених до нього носіях;
   - ідентифікація шкідливого ПЗ;
   - видалення шкідливого ПЗ;
   - видалення/ізоляція інфікованих файлів якщо їх лікування в даний момент не можливе;
   - оповіщення про виявлені загрози користувача та системного адміністратора;
   - автоматичне журналювання подій;
   - захист від зміни конфігурації чи видалення антивірусного ПЗ будь-ким окрім системного адміністратора.
9. Користувачі **не повинні** мати права:
   - змінювати настройки антивірусного ПЗ;
   - відключати антивірусні програмні засоби;
   - видаляти антивірусні програмні засоби.

5.4. Порядок встановлення та використання

1. Антивірусне програмне забезпечення встановлюється на ПК та серверах для забезпечення захисту від вірусних атак та перевірки на наявність вірусних програм у отриманих файлах, у тому числі по електронній пошті та на зовнішніх носіях інформації.
2. Антивірусне програмне забезпечення встановлюється при підготовці робочої станції при первинній настройці та/або при переустановленні операційної системи;
3. Антивірусне ПЗ має бути встановлене та регулярно оновлюватися на всіх робочих станціях, серверному обладнанні. Робочі станції та серверне обладнання без встановленого антивірусного ПЗ не повинні використовуватись. В разі виявлення робочих станцій без встановлених засобів антивірусного захисту необхідно негайно їх встановити і провести повне сканування на предмет наявності шкідливого ПЗ.

4. При інсталяції антивірусного ПЗ використовується стандартна конфігурація яку встановлює системний адміністратор при створенні інсталяційних пакетів. Дана конфігурація має передбачати регулярне оновлення баз та періодичне сканування системи на наявність шкідливого ПЗ.
5. Перевірка робочих станцій має відбуватися за наступним розкладом:
    - проактивний захист – включений постійно;
    - повна перевірка – раз в 2 тижні;
    - швидка перевірка – при ввімкненні ПК та при оновленні вірусних баз (перевірка оперативної пам'яті та завантажувальних секторів);
    - перевірка за вимогою - в будь який час.
6. Користувачі робочих станцій зобов'язані:
    - контролювати працездатність антивірусного програмного забезпечення на своїй робочій станції та повідомляти системного адміністратора про вихід із ладу антивірусного програмного забезпечення;
    - виконувати антивірусну перевірку всіх файлів, які надходять електронними каналами (електронна пошта, Інтернет тощо), та на зовнішніх носіях (дисках, флеш-накопичувачах тощо);
    - вчасно повідомляти системному адміністратору про підозрілі та незвичні події у роботі операційної системи;
    - сприяти діям системного адміністратора та відповідального за ІБ з локалізації (зупинки поширення) та ліквідації (видалення, усунення) ураження шкідливим ПЗ, якщо таке відбулося;
7. Користувачам забороняється:
    - блокувати оновлення антивірусних баз даних;
    - відкривати прикріплені файли електронних листів, отриманих з невідомих або недостовірних джерел;
    - завантажувати файли з невідомих або підозрілих веб-сайтів;
    - приносити та/або використовувати змінні носії інформації, які не пройшли антивірусну перевірку та не належать Назва ЗОЗ;
    - завантажувати програми, які надійшли невідомим шляхом або які не відносяться до програм, що використовуються в повсякденній роботі та дозволені до використання;
    - відкривати документи сумнівного характеру та виконувати макроси, які містяться в документах.

5.5. Виявлення та усунення загроз

Всі події, що пов'язані з роботою антивірусного ПЗ, мають протоколюватися. Копія журналів (протоколів) має зберігатися на окремому ПК (сервері). Термін зберігання журналів в оперативному доступі не менш ніж 3 місяці, в архіві – не менше одного року.

Негайне інформування системним адміністратором відповідального за ІБ відбувається в наступних випадках:

- виявлення шкідливого ПЗ;
- виявлення мережевих атак;

- помилка оновлення антивірусних баз;
- помилка ініціалізації модулів захисту.

5.6. Відповідальність

Відповідальність за організацію введення в дію та контроль виконання Політики АЗ, своєчасного внесення змін до даної Політики покладається на відповідального за ІБ Назва ЗОЗ.

Відповідальність за забезпечення всіх необхідних ресурсів для виконання Політики АЗ несе керівник Назва ЗОЗ.

Відповідальність за виконання вимог Політики АЗ покладається на увесь персонал Назва ЗОЗ.

Увесь без винятку персонал несе персональну відповідальність за дотримання чинної Політики антивірусного захисту відповідно до встановленої відповідальності за порушення Політики інформаційної безпеки Назва ЗОЗ.

Назва ЗОЗ **Політика інформаційної безпеки**	
Назва: КРИПТОГРАФІЧНИЙ ЗАХИСТ	**П 6.1 – 6.12.**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Інформаційна безпека ЗОЗ 1 категорії**

6. КРИПТОГРАФІЧНИЙ ЗАХИСТ

6.1 Загальні положення

Мета політики криптографічного захисту – гарантувати відповідне та ефективне використання криптографії для захисту конфіденційності, автентичності, цілісності та/або неспростовності інформації. Захист інформації з обмеженим доступом і зокрема захист персональних даних є пріоритетною ціллю.

Криптографічний захист інформації за допомогою шифрування даних є найефективнішим засобом забезпечення безпеки даних Назва ЗОЗ. Завдяки шифруванню, інформація що зберігається чи передається стає нечитабельною для будь-кого, крім тих, хто має авторизовану «потребу знати». Щоб отримати доступ до зашифрованої інформації, необхідно мати доступ до секретного ключа або паролю, що дозволяє його розшифрувати.

Назва ЗОЗ використовує наступні засоби криптографічного захисту:

- кваліфікований електронний підпис;
- шифрування файлів та електронної пошти;
- захист портів мережевого обладнання;
- захист онлайн ресурсів;
- програму–архіватор WinZip;
- протокол sFTP для передачі файлів;
- веб-інтерфейс рівня захищених сокетів (SSL/TLS);
- використання SSH;
- шифрування носіїв і файлових систем;
- шифрування інформації з обмеженим доступом для сервісів хмарних обчислень.

Криптографічний захист інформації, що передається, обробляється та зберігається в медичних інформаційних системах (МІС) забезпечується провайдером МІС. Назва ЗОЗ використовує засоби криптографічного захисту інформації, що надає назва провайдера МІС для роботи з Назва медичної інформаційної системи.

На електронні документи та інформацію, що вносяться до МІС, накладається кваліфікований електронний підпис автора документу, з урахуванням вимог, передбачених порядком роботи з Назва медичної інформаційної системи.

6.2. Мета використання

Криптографічний захист інформації використовується для захисту конфіденційної та медичної інформації Назва ЗОЗ. Конфіденційні дані та файли, що містять конфіденційну інформацію, при передачі через мережу загального користування чи Інтернет підлягають шифруванню.

Конфіденційна інформація, що обробляється, передається чи зберігається в МІС захищається за допомогою засобів криптографічного захисту провайдера МІС.

6.3. Порядок застосування

Класифікація інформації відповідно до закону наведена нижче:

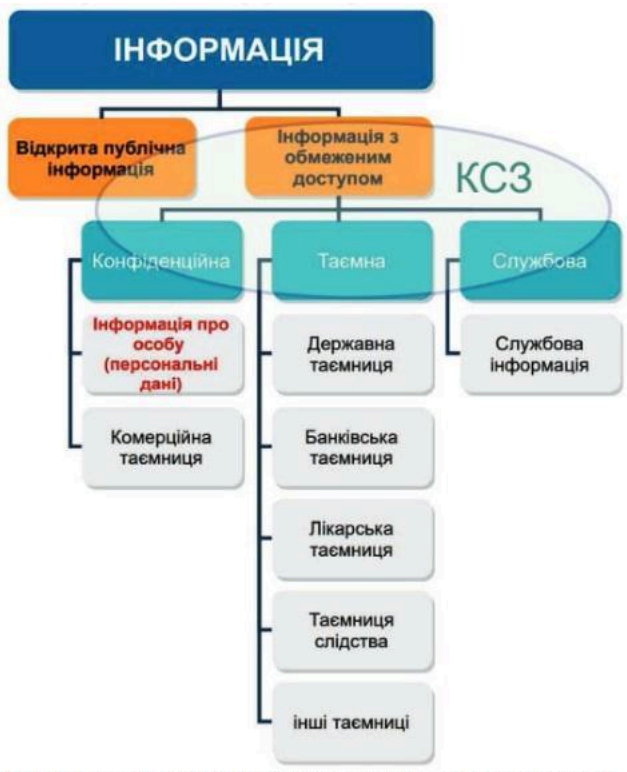


Рис. 1. Класифікація інформації відповідно до Закону України

Відповідно до ст. 8 ЗАКОНУ УКРАЇНИ "Про захист інформації в інформаційно-комунікаційних системах", державні інформаційні ресурси або інформація з

обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю.

Заклади охорони здоров'я, які знаходяться в державній власності, є операторами інформації, що становить державну таємницю, службової інформації (наприклад, наведеної в Переліку відомостей, що містять службову інформацію, розпорядником якої є Міністерство охорони здоров'я України), створеної на замовлення державних органів або інформації, яка є власністю держави або обробляють таємну інформацію, яка не становить державної таємниці, та конфіденційну інформацію в державних органах, органах місцевого самоврядування, на підприємствах, в установах та організаціях, які належать до сфери їх управління, підпадають під обмеження відповідних законів та нормативно-правових актів.

Перелік таких обмежень включає, але не вичерпується наступним:

- Для криптографічного захисту інформації, що становить державну таємницю, та службової інформації, створеної на замовлення державних органів або яка є власністю держави, використовуються криптосистеми і засоби криптографічного захисту, допущені до експлуатації. Зазначені криптосистеми і засоби перебувають у державній власності. Засоби криптографічного захисту службової інформації та криптосистеми з відповідного дозволу можуть перебувати і в недержавній власності.
- Для захисту таємної інформації, що не становить державної таємниці, та конфіденційної інформації в державних органах, органах місцевого самоврядування, на підприємствах, в установах та організаціях, які належать до сфери їх управління, військових формуваннях, які створені відповідно до закону, можуть застосовуватися засоби КЗІ, призначені для криптографічного захисту службової інформації та/або інформації, що становить державну таємницю, які мають чинне свідоцтво про допуск до експлуатації.

У разі необхідності передачі зашифрованих даних між закладом та сторонньою організацією розробляється та запроваджується взаємна процедура обміну та безпечного управління ключами/паролями шифрування.

Ключ шифрування визначає особливість перетворення простого тексту у зашифрований, або навпаки під час дешифрування (розшифрування).

Правила поводження з ключами шифрування, а саме створення, встановлення, видалення та контроль використання, для кожного криптографічного засобу, що застосовується в Назва ЗОЗ, визначаються відповідальним за інформаційну безпеку.

Заклад може використовувати декілька методів безпечної передачі даних за допомогою криптографічного захисту.

6.4. Використання інфраструктури відкритих ключів

6.4.1 Кваліфікований електронний підпис

Електронний цифровий підпис призначений для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів. Кваліфікований

електронний підпис (КЕП) – це удосконалений електронний підпис, який використовується фізичними та юридичними особами – суб'єктами електронного документообігу для ідентифікації підписувача та підтвердження цілісності даних в електронній формі, створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа. КЕП накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. КЕП робить електронний документ оригіналом і гарантує його достовірність. Кваліфікована електронна довірча послуга створення, перевірки та підтвердження кваліфікованого електронного підпису чи печатки надається кваліфікованим постачальником електронних довірчих послуг. Захищений носій особистих ключів – це пристрій для безпечного зберігання ключів кваліфікованого електронного підпису. Таким засобом може бути токен, мережевий крипто модуль, MobileID або смарт-картка. Відповідно до Постанови № 749 КМУ, для інформаційного обміну державні органи і підприємства державної форми власності повинні використовувати ключі лише на захищених носіях. Відповідно до Постанови № 193 КМУ, інші категорії користувачів – приватний сектор – повинні використовувати ключі лише на захищених носіях. Захищений носій – це засіб криптографічного захисту, який має експертний висновок ДССЗЗІ, що підтверджує наявність у засобі правильно реалізованих криптографічних алгоритмів шифрування. Передавання захищеного носія особистих ключів іншим особам та/або неавторизоване використання захищеного носія особистих ключів не допускається.

Порядок використання КЕП і захищених носіїв для роботи з системою електронного документообігу визначається вимогами вживаної у закладі МІС та погоджено з керівником і відповідальним за інформаційну безпеку.

6.4.2 Шифрування файлів та електронної пошти

Заклад може використовувати інфраструктуру відкритих ключів для шифрування файлів та електронної пошти. Файл або повідомлення електронної пошти шифрується відправником за допомогою відкритого ключа отримувача та розшифровується за допомогою особистого ключа отримувача. Послуга створення, перевірки та підтвердження ключів і відповідних сертифікатів надається постачальником довірчих послуг. Приватні ключі та/або сертифікати випускаються, доставляються, зберігаються та відкликаються постачальником довірчих послуг відповідно до умов обслуговування. Режим доставки, збереження і використання приватних ключів та/або сертифікатів гарантує, що доступ до ключа та/або сертифіката з приватним ключем обмежується особою, яка використовує цей ключ. Відповідальний за інформаційну безпеку веде облік всіх приватних ключів та/або сертифікатів, вживаних в закладі. Всі приватні ключі та/або сертифікати, строк дії яких закінчився, невідворотно видаляються. Передавання особистих ключів або сертифікатів іншим особам та/або їх неавторизоване використання не допускається. Порядок шифрування файлів та електронної пошти повинен бути погоджений з керівником та відповідальним за інформаційну безпеку.

6.4.3 Захист портів мережевого обладнання

Заклад може використовувати інфраструктуру відкритих ключів для контролю доступу до портів мережевого обладнання з використанням методів розширеної автентифікації (802.1x) за допомогою цифрових сертифікатів, які встановлюються на серверне та/або клієнтське обладнання. При використанні цієї технології, клієнтське обладнання, яке діє в недовіреному

середовищі або в такому, де є підвищений ризик компрометації, для запобігання такої компрометації, може запитувати попередню автентифікацію сервера за допомогою його цифрового сертифіката перед тим, як надсилати свої дані автентифікації. В свою чергу, сервер, пересвідчується в тім, що клієнтське обладнання має право доступу до мережевих портів шляхом перевірки клієнтських автентикаційних даних, які можуть надаватися у вигляді цифрового сертифікату. Створення, перевірка, підтвердження, доставка, інсталяція, відзив та видалення ключів і відповідних сертифікатів надається постачальником відповідних IT-послуг відповідно до умов обслуговування. При створенні приватного ключа або сертифіката для обладнання, строк дії такого ключа встановлюється відповідно до потреб закладу, але не більше ніж 2 роки. Режим встановлення, збереження і використання сертифікатів для авторизованого обладнання гарантує, що доступ до ключа та/або сертифіката з приватним ключем обмежується обладнанням, яке використовує цей сертифікат. Порядок авторизації обладнання визначено в Політиці контролю доступу.

6.4.4 Захист онлайн ресурсів

Заклад може використовувати інфраструктуру відкритих ключів для захисту онлайн ресурсів шляхом використання цифрових сертифікатів для своїх веб-серверів. Послуга створення, перевірки та підтвердження відповідних сертифікатів надається постачальником довірчих послуг. Сертифікати випускаються, доставляються та відкликаються постачальником довірчих послуг відповідно до умов обслуговування. Режим доставки, збереження і використання сертифікатів гарантує, що доступ до сертифіката з приватним ключем обмежується особою, яка авторизована для виконання операцій з цим сертифікатом відповідно до Політики контролю доступу. Відповідальний за інформаційну безпеку веде облік всіх сертифікатів, вживаних в закладі. Всі сертифікати, строк дії яких закінчився, невідворотно видаляються.

Якщо заклад уповноважив свій підрозділ (IT відділ) на виконання функцій постачальника довірчих послуг, який створює і обслуговує власний Центр сертифікації (CA) і відповідну інфраструктуру відкритих ключів (PKI), такий підрозділ гарантує наступне:

1. Якщо генерується пара відкритий/приватний ключ, то ключ генерується із надійного джерела випадковості та зазвичай має бути згенерований кінцевою сутністю, яка його використовуватиме.
2. Якщо приватний ключ потрібно згенерувати поза кінцевою сутністю, то він зашифрований під час передачі та в спокої. Доступ до ключа відстежується, автентифікується та авторизується, розроблена надійна процедура реєстрації сертифіката.
3. Після створення приватного ключа він надійно захищається, щоб він міг використовуватися лише тією особою/сутністю, яку цей ключ представляє.
4. Приватна частина ключа завжди зберігається в безпеці, тоді як публічну частину можна розповсюджувати іншим користувачам системи. Якщо приватний ключ потрапив до рук зловмисника, той міг використати його, видавати себе за користувача та отримати доступ до системи, тобто такий ключ є скомпрометованим і має бути відкликаним.

5. Приватний ключ Центра сертифікації зберігається в апаратному захисті, наприклад апаратному модулі безпеки (HSM). Це забезпечує надійне зберігання, захищене від злому.
6. Приватний ключ для кінцевої сутності може зберігатися в чіпі Trusted Platform Module (TPM) або USB-токені безпеки, стійкому до втручання. Якщо метод захисту на основі апаратного забезпечення недоступний або недоцільне, використовується захищене сховище приватних ключів клієнтської операційної системи.
7. При розміщенні в хмарі, використовуються надані постачальником хмарні сховища ключів з підтвердженою відповідністю. Лише при цій умові, приватний ключ може зберігатися в апаратному сховищі ключів у хмарі.
8. Тип і використання ключа визначатимуть, чи потрібно йому залишати пристрій для резервного копіювання. Це рішення має бути засноване на оцінці ризику, з урахуванням вимог до доступності та труднощів відновлення ключа в сценарії аварійного відновлення.
9. Кореневий ключ Центру сертифікації завжди має надійну резервну копію, щоб ключ можна було відновити у разі збою системи. Якщо ключ потрібно експортувати, його шифрують як під час передавання, так і під час зберігання. Ключ зашифрований у спосіб, який захищає його, але дозволяє його розшифрувати після інциденту.
10. Ключ, який використовується для сертифіката кінцевої сутності, наприклад ключ пристрою кінцевого користувача, може не потребувати резервного копіювання. Цей тип ключа має легко відновлюватися, і відповідний сертифікат можна буде видати знову.
11. Для ключів, які створює власний CA, встановлюється мінімальна довжина:
    - для алгоритмів шифрування RSA та Diffie–Hellman – 2048 біт;
    - для алгоритмів AES та ECC – 256 біт.

6.5. Використання WinZip

Програмне забезпечення WinZip дозволяє обмінюватися зашифрованими файлами за допомогою електронної пошти або месенжджерів з віддаленими користувачами, які мають таке саме програмне забезпечення. Обидва користувачі обмінюються одноразовим паролем, який використовується як для шифрування, так і для дешифрування/розшифрування кожного повідомлення. Пароль передається отримувачу альтернативним засобом зв'язку, таким як смс, інший мессенджер або телефоном. Повторне використання паролів забороняється. Працівник, який має потребу у передачі конфіденційної інформації віддаленому користувачу через Інтернет може запросити дозвіл на використання програми WinZip у відповідального з інформаційної безпеки. При цьому відповідальний з ІБ повинен також отримати пароль до зашифрованого архіву для перевірки інформації, що підлягає передачі чи отримується.

6.6. Протокол передачі файлів sFTP

Користувач може передати файли зі своєї робочої станції на захищені sFTP-сайти за допомогою відповідних заходів безпеки. sFTP (Secure File Transfer Protocol) це стандартний мережевий протокол прикладного рівня призначений для захищеного пересилання файлів між клієнтом та сервером в комп'ютерній мережі. Клієнт та сервер створюють окремі канали для передачі даних та обміну командами. Автентифікація клієнтів можлива із використанням

логіну та паролю або приватного ключа користувача. При створенні приватного ключа користувача, строк дії такого ключа встановлюється відповідно до потреб закладу, але не більше ніж один рік. Доступ до ключа обмежується особою, яка використовує цей ключ. Відповідальний за інформаційну безпеку веде облік всіх приватних ключів sFTP, вживаних в закладі. Всі приватні ключі, строк дії яких закінчився, невідворотно видаляються відповідальним за інформаційну безпеку. Порядок sFTP-передачі файлів повинен бути погоджений з керівником та відповідальним за інформаційну безпеку.

6.7. Веб-інтерфейс рівня захищених сокетів (SSL/TLS)

Для передачі конфіденційної інформації через веб-інтерфейс, використовуються протоколи SSL/TLS (англ. Secure Sockets Layer та Transport Layer Security) — криптографічні протоколи, які забезпечують встановлення безпечного з'єднання між клієнтом і веб-сервером. Ці протоколи забезпечують конфіденційність обміну даними між клієнтом і сервером. Використання захисту веб-інтерфейсу за допомогою протоколів SSL/TLS відбувається автоматично при роботі з онлайн-ресурсами, які підтримують цю технологію та надають веб-переглядачу відвідувача відповідного інтернет ресурсу свій SSL/TLS сертифікат, підписаний цифровим підписом визнаного довірчого центру сертифікації. Веб-адреси таких ресурсів починаються з «https://». Встановлення SSL/TLS для довірчих центрів сертифікації на робочі комп’ютери користувачів погоджується з відповідальним за інформаційну безпеку.

6.8. Використання SSH

Заклад може використовувати Secure Shell, SSH (англ. Secure SHell — «безпечна оболонка») — мережевий протокол рівня застосунків, що дозволяє проводити віддалене управління комп'ютером і тунелювання TCP-з'єднань (наприклад, для передачі файлів). З метою протидії підбору слабких паролів, автентифікація клієнтів із використанням логіну та паролю адміністративно заборонена і доступна тільки автентифікація клієнтів із використанням приватного ключа користувача. При створенні приватного ключа користувача, строк дії такого ключа встановлюється відповідно до потреб закладу, але не більше ніж один рік. Доступ до ключа обмежується особою, яка використовує цей ключ. Відповідальний за інформаційну безпеку веде облік всіх приватних ключів SSH, вживаних в закладі. Всі приватні ключі, строк дії яких закінчився, невідворотно видаляються. Порядок авторизації для використання SSH визначено в Політиці контролю доступу.

6.9. Шифрування носіїв і файлових систем

Для всіх засобів оброблення інформації з обмеженим доступом виконується шифрування носіїв на рівні блочних пристроїв або їх файлових систем з використанням симетричних алгоритмів шифрування з мінімальною довжиною ключа 256 біт. Доступ до ключа шифрування носіїв або їх файлових систем для відповідних засобів оброблення інформації з обмеженим доступом захищено адміністративним та користувацьким паролями. Адміністративний пароль використовується для адміністрування пристрою і надається особі з повноваженнями адміністратора. Користувацький пароль відомий тільки користувачу відповідного пристрою. Передача користувацького паролю доступу до файлової системи третім особам не допускається. При зміні користувача пристрою, адміністратор видаляє

пароль попереднього користувача і створює новий користувацький пароль доступу до файлової системи.

Якщо операційна система дозволяє виконати повне шифрування файлової системи (per-drive), то перевага надається саме такому засобу з урахуванням поточних вразливостей і відповідних ризиків конкретної імплементації (наприклад Windows EFS, BitLocker).

Де можливо, для зберігання і обробки приватного ключа шифрування використовується вбудований TPM-модуль.

Збереження, обробка, транспортування інформації з обмеженим доступом на носіях з незашифрованою файловою системою не допускається.

Порядок авторизації доступу до адміністративного та користувацького паролю носія із зашифрованою файловою системою, визначено в Політиці контролю доступу.

6.10 Шифрування інформації з обмеженим доступом для сервісів хмарних обчислень

Персональна ідентифікаційна інформація (PII) та інша інформація з обмеженим доступом, що передається загальнодоступними мережами передачі даних, зашифрована до її передачі та зберігається у хмарі в зашифрованому вигляді.

Процесор персональної ідентифікаційної інформації (PII) публічної хмари надав споживачеві сервісів хмарних обчислень повну інформацію про обставини, за яких для захисту оброблюваних ним PII використовуються засоби криптографічного захисту інформації. Від процесора PII публічної хмари отримана інформація про будь-які можливості, що надаються їм, і які здатні допомогти споживачеві служб хмарних обчислень у застосуванні його власного криптографічного захисту. На підставі отриманої інформації, була проведена оцінка ризиків та обрані і задокументовані засоби шифрування з підтвердженим рівнем відповідності.

6.11. Аудит використання ключів

Один раз на рік, відповідальний за інформаційну безпеку, перевіряє відповідність фактичної кількості ключів та сертифікатів, місць установки та зберігання даним, зазначеним в реєстрах ключів. Про всі невідповідності зазначається в звіті. Невідповідності звіту розглядаються як інциденти інформаційної безпеки.

6.12. Відповідальність

Персонал несе персональну відповідальність за дотримання чинної Політики криптографічного захисту відповідно до встановленої відповідальності за порушення Політики інформаційної безпеки Назва ЗОЗ.

Відповідальність за організацію та контроль дотримання Політики криптографічного захисту у Назва ЗОЗ покладається на відповідального за інформаційну безпеку.

У разі виникнення інциденту, пов'язаного з криптографічним захистом інформації, його вирішенням повинен займатися відповідальний за інформаційну безпеку закладу.

Назва ЗОЗ **Політика інформаційної безпеки**	
Назва: ФІЗИЧНА БЕЗПЕКА	**Розділ 7**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Фізична безпека ЗОЗ 2 категорії**

7. ФІЗИЧНА БЕЗПЕКА

Забезпечення фізичної безпеки персоналу полягає у створені безпечних умов на робочому місці та одночасним забезпеченням безпечного зберігання активів закладу. Будівля (комплекс будівель) закладу є дещо унікальним місцем з точки зору прав власності на будівлю або умов договору оренди, території навколо, шляхів під'їзду/виїзду, зовнішнього огородження, входів у приміщення, вимог до пожежної безпеки, систем електроживлення, забезпечення безпечного використання цифрових активів та контролю серверної кімнати. Необхідно постійно покращувати та модернізувати систему забезпечення фізичної безпеки для підвищення захисту своїх активів та медичної інформації. Наступний перелік визначає заходи, які запроваджені для забезпечення фізичної безпеки закладу.

Опис будівлі, місця розташування, прилеглої території, огородежння, квадратний метраж, система безперебійного живлення, захисту від несанкціонованого проникнення, система відеоспостереження, охорона сигналізація та система пожежної безпеки.

- Вхід до будівлі в неробочий час зачинений та контролюється охоронною сигналізацією. Спроба входу без введення коду безпеки для зняття з охоронної сигналізації призводить до негайного повідомлення до охоронної служби.
- Тільки конкретним працівникам закладу видається код безпеки для входу. Розголошення коду безпеки не працівникам категорично заборонено.

- Код безпеки змінюється на періодичній основі, змінений код відповідні працівники отримують через сповіщення на робочу електрону пошту. Код безпеки обов'язково змінюються при звільненні працівника, який мав доступ до нього.
- Вхідні двері в зону прийому пацієнтів та відвідувачів завжди замикаються у неробочий час і відмикаються у робочі години закладу. Біля вхідних дверей облаштована зона рецепції.
- Зона рецепції працює з 8:00 до 17:00.
- Будь-яка невизнана особа, яка перебуває в службових приміщеннях закладу повинна негайно виводитись з службової зони персоналом, що її побачив, та супроводжуватись до зони рецепції.
- Робочі станції, ноутбуки, телефоні апарати інше цифрове обладнання, яке знаходиться в зоні дозволеної для знаходження відвідувачів, повинні бути облаштовані спеціальними замками та дротом для фіксації до встановленого місця розташування, що унеможливлює їх винос або переміщення від встановленого місця розташування.
- До приміщення де знаходиться серверне обладнання вхід заблокований кодовим замком. Тільки обмежене коло посадових осіб мають право доступу до серверного приміщення. Код кодового замку змінюється періодично.
- В приміщені з серверним обладнанням ведеться цілодобове відеоспостереження, воно обладнане автоматизованою системою протипожежного захисту;
- Серверне та мережеве обладнання забезпечене основним та резервним безперебійним живленням.
- На першому поверсі будівлі є датчики детектування руху, які активуються в неробочий час.
- Всі зовнішні вікна будівлі мають датчики розбиття скла, які, якщо скло вікон буде розбите, призведуть до негайного повідомлення до охоронної служби.
- Будівля обладнана камерами відеоспостереження на всіх входах та виходах до будівлі. Всі, особи, які заходять/виходять до/з будівлі фіксуються за принципом 24/7, тобто 24 години на добу 365 днів на рік.
- Протипожежний захист будівлі встановлено відповідно до вимог ДСНС України.

Заклад обладнаний системою безперебійного живлення та дизель-генератором.

Назва ЗОЗ	Політика інформаційної безпеки
Назва: ДИСТАНЦІЙНА РОБОТА	**П 8.1 – 8.5**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Інформаційна безпека ЗОЗ 2 категорії**

8. ДИСТАНЦІЙНА РОБОТА

В закладі дозволяється та використовується дистанційна робота персоналу при певних, визначених керівництвом обставинах. Вимоги, щодо організації дистанційної роботи застосовуються до всіх працівників і підрядників, які працюють поза межами будівлі (комплексу будівель) закладу.

Хоча дистанційна робота може бути перевагою як для користувачів, так і для організації в цілому, вона представляє нові ризики інформаційної безпеки. Персонал, що працює дистанційно повинен бути захищеним від небезпеки атак шкідливим програмним забезпеченням та несанкціонованого витоку даних з пристроїв, що знаходяться за межами периметру безпеки закладу.

8.1. Загальні вимоги

Користувачі, що працюють віддалено, зобов'язані дотримуватися всіх правил закладу, які встановлені для персоналу та підрядників, а саме:
Потрібно знати: Користувачі, що працюють віддалено мають доступ тільки до тих ресурсів та інформації, які потрібні для виконання функціональних завдань.
Використання пароля: Користувачі, що працюють віддалено повинні дотримуватись вимог щодо встановлення та зміни паролів. Окрім того, вони не розголошують свій пароль і не

залишають записів щодо паролю там, де такий запис може побачити член сім'ї або стороння особа.

Навчання: персонал, який працює віддалено, повинен проходити ті самі навчання з інформаційної безпеки, що і персонал що працює на робочих місцях.

Специфічні вимоги: до персоналу, що працює віддалено, можуть бути застосовані додаткові вимоги, які пов'язані зі специфікою виконання функціональних завдань дистанційно.

8.2. Необхідне обладнання

Працівники, допущені до дистанційної роботи, повинні розуміти, що заклад не наддасть все обладнання, необхідне для забезпечення належного захисту інформації, до якої працівник має доступ; однак є певний перелік обладнання який заклад повинен надати:

Заклад надає:

- робочий комп'ютер (ноутбук) зі встановленим антивірусним ПЗ та програмним забезпеченням шифрування даних;
- VPN канал доступу;
- принтер;
- зовнішній носій для резервного копіювання;
- службовий мобільний телефон.

Працівник повинен забезпечити самостійно:

- широкосмуговий канал доступу до Інтернет;
- подрібнювач паперу або можливість іншим способом знищувати паперові носії;
- відокремлене від членів родини робоче місце;
- шафа, що зачиняється або сейф для захисту та зберігання робочого комп'ютера та робочих документів.

8.3. Захист апаратного забезпечення

Захист від вірусів**:** Користувач, що працює дистанційно, повинен постійно використовувати та оновлювати захист комп'ютера від вірусів та іншого шкідливого програмного забезпечення. Антивірусне програмне забезпечення встановлене на комп'ютерах закладу і налаштоване на періодичне оновлення. Заборонено працювати без оновленого антивірусного програмного забезпечення.

Використання VPN та брандмауера**:** При дистанційному підключені повинен використовуватись канал зв'язку, який вимагає використання VPN та брандмауера. При відключені VPN та/або брандмауера дистанційну роботу потрібно зупинити.

Шафа або сейф: Використовуйте шафу, що замикається або сейф для безпечного зберігання комп'ютеру та інших пристроїв наданих закладом для дистанційної роботи.

Захист ПК: персональний комп'ютер, що використовується для дистанційної роботи, повинен бути облаштований спеціальним замком для захисту від крадіжки.

Блокування екранів**:** Незалежно від місця розташування, завжди блокуйте екран, перш ніж відійти від робочої станції. Дані на екрані можуть містити конфіденційну інформацію.

Переконайтеся, що функцію автоматичного блокування настроєно на автоматичне ввімкнення після 10 хвилин бездіяльності.

8.4. Безпека даних

Резервне копіювання даних**:** Встановлена процедура резервного копіювання, яка шифрує дані, та переміщує їх на зовнішній носій. Для резервного копіювання використовується тільки встановлена процедура. Створювати самостійно інші процедури резервного копіювання даних заборонено. Якщо неможливо дотримуватись встановленої процедури резервного копіювання: не має відповідного програмного забезпечення та/або зовнішнього носія, треба звернутися до IT-підрозділу закладу. При гострій необхідності та неможливості звернутися до IT-підрозділу (наприклад під час відрядження) дозволено використовувати наявні засоби шифрування (архіватор-шифрувальник WinZip) та доступний зовнішній носій. Причому, безпечному зберіганню зовнішнього носія з резервною копією даних треба приділити значну увагу.

Передача даних**:** Передача даних до закладу вимагає використання затвердженого VPN-з'єднання для забезпечення конфіденційності та цілісності даних, що передаються. Не дозволено обходити встановлену процедуру, а також створювати власний метод передачі даних до закладу.

Доступ до зовнішніх систем (хмар): Якщо є потреба у доступі до зовнішньої IT-системи, необхідно зв'язатися зі своїм безпосереднім керівником або відповідальним за інформаційну безпеку. Вони визначать безпечний метод доступу до потрібної зовнішньої системи.

Доступ до інформації що знаходиться в медичних інформаційних системах потребує використання каналу VPN-з'єднання.

Електронна пошта: Не дозволено передавати будь-яку конфіденційну інформацію та персональні дані (перелік визначений у п.2.9 цього документу) електронною поштою, якщо вона не зашифрована. При гострій необхідності треба звернутися до свого безпосереднього керівника або відповідального за інформаційну безпеку. Вони визначать безпечний метод передачі конфіденційної інформації та персональних даних електронною поштою.

Підключення через публічний WiFi: необхідно дотримуватися надзвичайної обережності при підключенні до IT-систем закладу через публічну точку доступу до Інтернет. Хоча заклад застосовує системи безпеки для захисту даних проте заклад не може забезпечити захист даних у мережевому обладнанні, що знаходиться поза межами закладу.

Захистить дані, якими ви володієте: Потрібно отримувати доступ лише до тієї інформації, яка потрібна для виконання робочого завдання. Регулярно переглядайте дані, які ви зберегли, щоб переконатися, що масив даних, який зберігається знаходиться на мінімально необхідному рівні, а застарілі дані та версії файлів видалені. Зберігайте електронні дані тільки в зашифрованому виді. Якщо на ноутбуку не встановлено відповідне ПЗ для шифрування треба звернутися до IT-підрозділу.

Друковані звіти або робочі документи: Ніколи не залишайте паперові документи на робочому столі коли ви залишаєте робоче місце. Всі паперові документи повинні зберігатися у замкненій шафі або сейфі.

Введення даних у відкритому місці: Не виконуйте робочі завдання, які вимагають використання конфіденційної інформації або персональних даних у громадських місцях.

Надсилання даних за межі закладу**:** Вся передача даних за межі закладу повинна бути пов'язана з виконанням вимог договорів та дотримуватися вимог угод про конфіденційність і нерозголошення конфіденційної інформації. При необхідності передачі інформації стороннім організаціям з якими не укладено договорів та угод на обмін інформацією необхідно отримати письмову згоду безпосереднього керівника.

8.5. Утилізація паперових та зовнішніх носіїв

Паперові документи: Всі паперові документи, які містять конфіденційну інформацію, перед утилізацією потрібно подрібнити. Заборонено викидання не подрібнених паперових документів. Інший спосіб утилізації - такі документи палити. Персонал, який працює дистанційно повинен мати або подрібнювач паперу або можливість палити паперові документи.

Зовнішні носії: Всі зовнішні носії надані закладом для забезпечення дистанційної роботи повинні бути повернуті до закладу для утилізації.

Назва Закладу **Політика інформаційної безпеки**	
Назва: ПОЛІТИКА ЧИСТОГО СТОЛУ/ЕКРАНУ	**П. 9.1. – 9.3.**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Інформаційна безпека ЗОЗ 2 категорії**

9. ПОЛІТИКА ЧИСТОГО СТОЛУ/ЕКРАНУ

9.1. Загальні положення

Одним із засобів контролю за забезпечення інформаційної безпеки є політика чистого столу та чистого екрану, яка знижує ризик несанкціонованого доступу, втрату та пошкодження інформації протягом робочого часу та після його закінчення. Політика чистого столу та чистого екрану визначає методи, пов'язані із забезпеченням того, щоб конфіденційна інформація, як у цифровому, так і у паперовому/фізичному форматі, та активи (наприклад, робочі станції, ноутбуки, стаціонарні телефонні апарати, смартфони, цифрове медичне обладнання та інші) не залишаються без захисту, коли вони не використовуються, чи коли персонал залишає свої робочі місця на короткий час або наприкінці дня. Дотримання

політики чистого столу/екрану всього без винятку персоналу дозволить суттєво убезпечити Назва ЗОЗ від витоку конфіденційної інформації.

Метою впровадження політики чистого столу та чистого екрану в Назва ЗОЗ є:

- запобігання витоку/втраті конфіденційних даних закладу;
- дотримання правил кібергігієни та розвитку кіберкультури, щодо безпечного та належного поводження з конфіденційною інформацією та її носіями;
- створення та підтримання позитивного іміджу закладу серед пацієнтів.

9.2. Вимоги

Увесь персонал закладу повинен дотримуватись наступних правил:

- зберігати власні паролі в таємниці, не розголошувати та нікому не повідомляти їх;
- закривати активні сеанси після завершення роботи, якщо їх не можна захистити відповідним блокуючим механізмом, наприклад блокуванням екрану;
- встановити час автоматичного блокування екрану робочої станції 10 хвилин;
- по завершенні сеансу виходити із IT-систем та баз даних, до яких протягом сеансу був отриманий доступ (серверів, додатків, VPN – каналів тощо);
- забороняється вести запис паролів (наприклад, на папері, у програмному файлі або в кишеньковому пристрої), за винятком тих випадків, коли запис може зберігатися безпечно, а метод зберігання був затверджений відповідальним за ІБ;
- матеріальні носії конфіденційної інформації повинні замикатися в сейфі або шафі після завершення роботи з ними;
- робочі станції, комп'ютери та засоби зв’язку повинні бути залишені у стані виконаного виходу із системи/вимкнені коли вони перебувають без нагляду;
- цифрове медичне обладнання, що не використовується повинно бути вимкнене або переведене у безпечний режим;
- документи, які містять конфіденційну інформацію, повинні забиратися виконавцем з принтерів негайно;
- наприкінці робочого дня/зміни увесь персонал повинен упорядкувати своє робоче місце та прибрати всі робочі документи в сейф або шафу, що замикається;
- для утилізації конфіденційних документів слід використовувати знищувачі/подрібнювачі паперу;
- після закінчення робочого дня та у разі тривалої відсутності на робочому місці необхідно замикати на замок усі шафи та сейфи де зберігається конфіденційна інформація та робочі документи.

9.3. Відповідальність

Вимоги цієї політики поширюються на весь персонал закладу. Усі працівники закладу мають бути ознайомлені із її вимогами. Відповідальність за порушення визначена у відповідному розділі затвердженої Політики інформаційної безпеки Назва ЗОЗ.

Назва Закладу **Політика інформаційної безпеки**	
Назва: УТИЛІЗАЦІЯ ЗОВНІШНІХ НОСІЇВ ТА КОМП'ЮТЕРІВ	**П 10.1 – 10.3**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Інформаційна безпека ЗОЗ 2 категорії**

10. УТИЛІЗАЦІЯ ЗОВНІШНІХ НОСІЇВ ТА КОМП'ЮТЕРІВ

10.1. Утилізація зовнішніх носіїв

Вважається, що всі зовнішні носії, які використовувались персоналом містять конфіденційну та/або медичну інформацію. Відповідно застаріли або зіпсовані зовнішні носії, подальша експлуатація яких вже неможлива, повинні бути утилізовані методом, який гарантує, що не буде втрати даних і що конфіденційність і безпека цих даних не будуть порушені.

Необхідно дотримуватися наступних кроків:

- персонал, який використовує зовнішні носії, зобов'язаний визначити застаріли чи зіпсовані зразків для утилізації;
- заборонено самостійне викидання або утилізація зовнішніх носіїв;
- всі застаріли чи зіпсовані зразки передаються для знищення до відповідального з ІБ.

Відповідальний з ІБ забезпечує знищення зовнішніх носіїв, що підлягають утилізації.

10.2. Утилізація комп'ютерного обладнання

Комп’ютерне обладнання, в тому числі медичне, яке підлягає утилізації, проходить відповідну процедуру, яка складається з видалення усіх даних, затирання усіх міток та конфігурацій та повернення до заводських налаштувань. Відповідальний з інформаційної безпеки забезпечує утилізацію комп’ютерного обладнання відповідно до встановленої процедури.

10.3. Використання надлишкового обладнання

Оскільки старе комп'ютерне обладнання поступово замінюється більш сучасними цифровими системами, воно підлягає інвентаризації та зберіганню. Старе комп'ютерне обладнання може бути використане:

- для запасних частин,
- для аварійної заміни,
- для тестування нового програмного забезпечення,
- для створення та зберігання резервних копій для іншого виробничого обладнання,
- для використання персоналом за межами закладу, в тому числі для забезпечення дистанційної роботи.

Назва ЗОЗ **Політика інформаційної безпеки**	
Назва: УПРАВЛІННЯ ЗМІНАМИ	**Р 11**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Інформаційна безпека ЗОЗ 2 категорії**

11. УПРАВЛІННЯ ЗМІНАМИ

Для того, щоб відстежувати та управляти змінами в мережах, IT-системах та на робочих станціях, включаючи встановлення та налаштування нового програмного забезпечення та виправлення вразливостей програмного забезпечення в інформаційних системах, які містять конфіденційну та медичну інформацію, запроваджена процедура управління змінами, яка полягає в наступному:

Процедура

1. IT-підрозділ або інший призначений працівник, який здійснює оновлення, встановлення, переналаштовує або іншим чином вносить зміни у мережеве та комп’ютерне обладнання, повинен ретельно реєструвати всі зміни в журналі управління змінами.

2. IT-підрозділ або працівник, який впроваджує зміну, забезпечує створення всіх необхідних резервних копій програмного забезпечення та даних.

3. Працівник, який впроваджує зміну, також повинен бути ознайомлений з процесом повернення до попередніх налаштувань у тому випадку, якщо зміна викликає збоїв в мережі чи системах і потребує видалення.

В закладі дозволене до використання тільки ліцензійне програмне забезпечення, та дозволене програмне забезпечення (Додаток 3). Оновлення ліцензійного та дозволеного програмного забезпечення проводиться відповідно до рекомендацій розробників цього ПЗ. Персонал повинен здійснювати оновлення програмного забезпечення невідкладно, по мірі отримання/можливості доступу до оновленої версії ПЗ.

Назва ЗОЗ **Політика інформаційної безпеки**	
Назва: Моніторінг стану інформаційної безпеки	**Р 12**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Інформаційна безпека ЗОЗ 3 категорії**

12. МОНІТОРІНГ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В закладі запроваджені апаратні, програмні та процедурні механізми, які фіксують та відстежують стан інформаційних та медичних систем, що містять конфіденційну та персональну інформацію. Моніторинг стану інформаційної безпеки - це відповідні технологічні та процесуальні дії, які спрямовані на відстеження і фіксацію комп'ютерної та мережевої діяльності з метою визначення, чи сталося порушення інформаційної безпеки. Моніторинг передбачає відстеження та фіксацію зареєстрованих комп'ютерних подій, які стосуються стану операційних систем, програмного забезпечення або діяльності користувачів.

В закладі проводиться моніторинг діяльності користувачів з метою запобігання технологічних збоїв та виявлення потенційних ризиків та вразливостей системи інформаційної безпеки. Відповідно до виявлених збоїв, ризиків та вразливостей в закладі розробляються та запроваджуються відповідні адміністративні, фізичні та технічні заходи забезпечення інформаційної безпеки відповідно до вимог чинного законодавства у сфері кіберзахисту. Процедура моніторингу полягає у наступному:

1. Весь персонал та керівництво ознайомлене з чинною політикою інформаційної безпеки та дотримується її положень при виконанні службових обов’язків.

2. IT-підрозділ, або системний адміністратор забезпечують моніторинг та обробку журналів подій на всіх комп'ютерних та цифрових медичних системах, що містять та/або обробляють чи зберігають конфіденційну інформацію та персональні дані. Моніторинг, як мінімум, повинен включати: визначення ідентифікатора користувача, час і дату входу, а також обсяг та характер даних, до яких був отриманий доступ або спроба доступу. Моніторингова інформація (логі) повинна зберігатися на окремому комп'ютері, з метою мінімізації можливості доступу до цієї інформації не авторизованих осіб.

В закладі використовуються відповідні мережеві та хост-системи виявлення вторгнень. Відповідальний з інформаційної безпеки організовує та забезпечує встановлення, обслуговування та оновлення таких систем.

Назва ЗОЗ **Політика інформаційної безпеки**	
Назва: Аудит інформаційної безпеки	**Р 13**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Інформаційна безпека ЗОЗ 2 категорії**

13. АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В закладі періодично, раз на рік, проводиться аудит стану інформаційної безпеки, який включає, але не обмежується такими заходами як, перевірка облікових записів користувачів та прав доступ до IT- систем та мереж, доступ до файлів, перегляд та аналіз інцидентів безпеки, перегляд журналів моніторингу тощо. Аудит може проводитись як відповідним персоналом закладу так і зовнішніми аудиторами. Мета проведення аудиту – мінімізація порушень безпеки та забезпечення інформаційної безпеки закладу на належному рівні. У разі неможливості проведення аудиту стану інформаційної безпеки власними силами та засобами, заклад звертається до авторизованих зовнішніх аудиторів. Процедура аудиту передбачає:

1. Ознайомлення аудиторів з політикою інформаційної безпеки, іншою документацією стосовно ІБ, зокрема планом реагування на інциденти інформаційної безпеки, тощо.

2. IT-підрозділ та/або системний адміністратор несуть відповідальність за проведення періодичних оглядів діяльності інформаційних та мережевих систем та повинні мати відповідні технічні навички щодо безпечного застосування операційних систем, програмного забезпечення, додатків, баз даних, мережевого та медичного обладнання. IT-підрозділ та/або системний адміністратор надає доступ аудиторам до відповідних даних.

3. Відповідальний за ІБ повинен розробити формат звіту щодо результатів аудиту стану інформаційної безпеки та план усунення виявлених недоліків при необхідності. У такому звіті повинні бути вказані: хто проводив аудит, дата і час виконання, а також висновки, щодо стану інформаційної безпеки закладу, виявлені недоліки та вразливості (ризики). До звіту можуть додаватися рекомендації аудиторів щодо підвищення рівня ІБ закладу, усунення вразливостей та мінімізації ризиків.

4. Аудит стану ІБ проводиться щорічно але може проводитися позапланова, якщо є підстави підозрювати порушення, які можуть призвести до тяжких наслідків. При проведенні перегляду журналів подій аудитори повинні перевірити наступне:

- логі подій - стосується вдалих/невдалих спроб входу, при цьому особлива увага приділяється саме невдалим спробам входу, блокуванням облікових записів та несанкціонованим спробам доступу;

- доступ до файлів – вдалі/невдалі спроби доступу до файлів, особлива увага невдалим спробам доступу, несанкціонованому доступу і несанкціонованим спробам створення, зміни або видалення файлів;

- інциденти безпеки – перевіряються записи з журналу виявлення інцидентів безпеки та журналів моніторингу стану систем на предмет аномальних чи підозрілих дій або подій зі шкідливою логікою (наприклад, дій вірусів, хробаків, шкідливих експлойтів), відмовою в обслуговуванні або спробами сканування, тощо;

- облікові записи користувачів – перегляд облікових записів користувачів у всіх системах з метою переконатися, що користувачі не мають надлишкових прав доступу до інформаційних системах, та надлишкових прав поводження з інформацією.

Усі важливі висновки повинні бути відображені у звіті щодо аудиту стану інформаційної безпеки закладу. Особи що проводили аудит передають звіт та перелік рекомендованих заходів відповідальному з інформаційної безпеки для ознайомлення та вживання відповідних заходів. Відповідальний з ІБ при отримані звіту повинен невідкладно вжити всіх належних заходів з приведення стану ІБ до відповідного рівня та усунення виявлених недоліків.

Назва Закладу **Політика інформаційної безпеки**	
Назва: ЦІЛІСНІСТЬ ДАНИХ ПАЦІЄНТІВ	**Р 14**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Інформаційна безпека ЗОЗ 2 категорії**

14. ЦІЛІСНІСТЬ ДАНИХ ПАЦІЄНТІВ

Заклад впроваджує та підтримує відповідні організаційні та технологічні заходи для підтвердження того, що медичні дані пацієнтів інша конфіденційна інформація стосовно пацієнтів не були змінені або знищені несанкціонованим чином. Метою таких дій є забезпечення цілісності даних пацієнтів.

Заклад підтримує впровадження автоматизованих систем та програмного забезпечення, в тому числі з використанням штучного інтелекту, для автоматичної перевірки наявності людських помилок при обробці даних пацієнтів.

Заклад застосовує відповідні мережеві та хост-систем виявлення вторгнень. Відповідальний за ІБ організовує встановлення, контролює обслуговування та оновлення таких систем.

Збереження цілісності даних пацієнтів, що знаходяться в медичних інформаційних системах забезпечується провайдерами таких систем.

Щоб забезпечити цілісність даних при передачі персоналом закладу застосовується шифрування даних що передаються. Також для забезпечення цілісності даних пацієнтів використовується шифрування при зберіганні таких даних.

Заклад забезпечує перевірку можливого дублювання даних у своїх комп'ютерних системах та мережах, щоб запобігти поганій інтеграції даних між різними комп'ютерними системами.

Для запобігання збою ІТ-систем, які можуть призвести до порушення цілісності даних, заклад забезпечує перевірку своїх інформаційні системи на точність і функціональність, перш ніж

почне їх використовувати. IT-системи та мережеве обладнання проходить оновлення при випуску виробниками виправлень та оновлених версій програмного та апаратного забезпечення, які усувають виявлені помилки та недоліки.

Заклад встановлює та регулярно оновлює антивірусне програмне забезпечення на всіх робочих станціях та серверах, щоб своєчасно виявити та запобігти зміні або знищенню даних шкідливим програмним забезпеченням.

Назва Закладу **Політика інформаційної безпеки**	
Назва: ПЛАНИ РЕЗЕРВНОГО КОПІЮВАННЯ ТА АВАРІЙНОГО ВІДНОВЛЕННЯ	**П 15.1 – 15.2**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Інформаційна безпека ЗОЗ 2 категорії**

15. ПЛАНИ РЕЗЕРВНОГО КОПІЮВАННЯ ТА АВАРІЙНОГО ВІДНОВЛЕННЯ

В закладі впроваджені заходи та процедури реагування на надзвичайні події, які можуть завдати шкоди IT-системам та мережам, а також інформації. Для цього розроблений План аварійного відновлення та План резервного копіювання. Заклад переодично (один раз на рік) переглядає цій план з метою аналізу його ефективності та оцінки ризиків для внесення відповідних корегувань.

15.1. План резервного копіювання

Відповідальний з ІБ забезпечує розробку та впровадження плану резервного копіювання даних для створення та підтримки точних копій операційних систем, програмного забезпечення, баз даних, іншої інформації та даних закладу. План передбачає заходи з резервного копіювання даних, зберігання та відновлення даних з резервних копій. Також План повинен передбачати наступні положення:

1. На завершення кожного робочого дня, з понеділка по п'ятницю, додаткова резервна копія всіх серверів, що містять критично важливі дані, повинна бути згенеровано та перенесено до системи зберігання резервного копіювання. У суботу тижнева резервна копія всіх серверів, що містять критично важливі дані, повинна бути створена та

перенесена до системи зберігання резервного копіювання. Щотижневі резервні копії зберігаються у захищеному відокремленому від локальної мережі середовищі в зашифрованому виді. Місячна резервна копія створюється в останню суботу поточного місяця та зберігається на зовнішньому носії у зашифрованому виді. Резервні носії, які більше не експлуатуються, утилізуються відповідно до процедури «Утилізація зовнішніх носіїв».

2. Відповідальний за ІБ стежить за зберіганням і своєчасним видаленням резервних копій і забезпечує дотримання всіх належних заходів контролю доступу.
3. Відповідальний за інформаційну безпеку забезпечує щорічне тестування процедури резервного копіювання, щоб переконатися, що резервні копії створені та доступні. Таке тестування документується відповідальним за ІБ та при необхідності надає пропозиції про необхідність вдосконалення процедур резервного копіювання.

15.2. План аварійного відновлення

Відповідальний за ІБ розробляє та регулярно оновлює План аварійного відновлення з метою своєчасного відновлення та/або запобігання будь-яких втрат даних, систем, необхідних для надання медичної допомоги пацієнтам та забезпечення неперервності критично важливих процесів функціонування закладу. План аварійного відновлення має достатній рівень деталізації та необхідні пояснення, для того, щоб він міг бути виконаний персоналом заходу в разі надзвичайної події. Цій план повинен мати резервну копію, яка зберігається на іншому захищеному майданчику разом з місячною резервною копією критично важливих даних закладу.

План аварійного відновлення повинен містити наступне:

1. Порядок створення та оновлення копій документів щодо результатів інвентаризації інформаційних активів та конфігурації мереж;
2. Паперову копію Плану резервного копіювання;
3. Паперові копії бланків та документів, необхідних для функціонування закладу, здійснення медичної допомоги та фінансових розрахунків;
4. Список групи реагування у надзвичайних ситуаціях, члени якої несуть відповідальність за:

- визначення впливу надзвичайної ситуації на заклад;
- визначення безпечного місця розташування закладу;
- порядок відновлення втрачених даних;
- порядок використання аварійних систем протягом часу коли основні інформаційні системи недоступні;
- необхідні заходи для відновлення функціонування закладу.

5. Процедуру реагування на втрату електронних даних, включає, але не обмежуючись, пошуком і завантаженням даних з найбільш актуальної резервної копії.
6. Номери телефонів та/або адреси електронної пошти всіх осіб, з якими потрібно зв'язатися у разі надзвичайної ситуації, у тому числі: членів групи реагування; осіб, які відповідають за зберігання та відновлення резервних даних; постачальників інформаційних систем, а також інший персонал.
7. Група реагування повинна збиратися щорічно, щоб:

- переглянути План аварійного відновлення;
- запланувати проведення навчань стосовно дій у надзвичайних ситуаціях та оцінити результати таких навчань;
- переглянути паперові версії Плану резервного копіювання та Плану аварійного відновлення та зробити у них відповідні зміни.

Відповідальний за ІБ веде протокол засідань групи реагування та надає пропозиції щодо внесення змін до планів резервного копіювання та аварійного відновлення відповідно до результатів аналізу ризиків інформаційної безпеки.

Назва Закладу[1] **Політика інформаційної безпеки**	
Назва: Обізнаність та навчання з питань безпеки	**Р 16**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Інформаційна безпека ЗОЗ 2 категорії**

16. ОБІЗНАНІСТЬ ТА НАВЧАННЯ З ПИТАНЬ БЕЗПЕКИ

Для підвищення обізнаності стосовно питань інформаційної безпеки весь персонал закладу, включаючи керівництво, повинен регулярно проходити відповідні навчання. Навчання з ІБ для всього персоналу проводиться раз на три місяці, або позапланово при необхідності.

Навчальна програма з інформаційної безпеки
Відповідальний за інформаційну безпеку організовує та проводить навчання з інформаційної безпеки. Він/вона здійснює первинний інструктаж для нових працівників, щорічний інструктажі для всього персоналу, а також планові заняття стосовно Політики інформаційної безпеки та актуальних загроз. Для проведення навчань, відповідальний з ІБ може залучати інших працівників та сторонніх експертів, в тому числі виробників ІТ-систем та розробників програмного забезпечення. Відвідування та/або участь у такому навчанні є обов'язковим для всього персоналу. Відповідальний за інформаційну безпеку веде відповідну документацію про всі навчальні заходи.

Відповідальний з ІБ, при необхідності, може організовувати позапланові навчання при змінах у апаратному або програмному забезпечені, збільшені загроз, внесені змін у політику інформаційної безпеки, за результатами аудиту, тощо.

Пам’ятка з інформаційної безпеки
Відповідальний за ІБ розробляє пам’ятку з інформаційної безпеки, до якої включає правила кібергігієни та правила чистого столу. Пам’ятка містить актуальну інформацію стосовно безпеки паролів, шкідливого програмного забезпечення, ідентифікації та реагування на інциденти, а також контролю доступу. Відповідальний за ІБ забезпечує доведення пам’ятки з інформаційної безпеки до всього персоналу. Окрім того він/вона може поширювати

спеціальні повідомлення до персоналу стосовно нових загроз, небезпеки, вразливостей та необхідних заходах інформаційної безпеки.

Захист від шкідливого програмного забезпечення

У рамках вищезазначеної навчальної програми з безпеки відповідальний за ІБ проводить навчання щодо запобігання ураження та протидії шкідливому програмному забезпеченню. Таке навчання повинно включати в себе наступне:

- Вказівки щодо поводження з підозрілим вкладенням електронної пошти, електронними листами від незнайомих відправників і шахрайських повідомлень;
- Важливості оновлення антивірусного програмного забезпечення та правил перевірки робочої станції або інших пристроїв на встановлення актуального антивірусного захисту;
- Про небезпеку завантаження файлів з невідомих або підозрілих джерел;
- Про ознаки небезпечного шкідливого програмного забезпечення, яке може обійти антивірусний захист або загроз «нульового дня»;
- Важливість регулярного резервного копіювання критично важливих даних і зберігання даних в безпечному місці;
- Дотримання правил антивірусного захисту при дистанційній роботі;
- Про шкоду, яку можуть заподіяти віруси, трояни, хробаки та інше шкідливе програмне забезпечення
- Правила дій, якщо виявлено шкідливе програмне забезпечення на робочій станції

Дотримання парольної політики

У рамках вищезазначеної навчальної програми з безпеки та нагадувань про безпеку персоналу відповідальний за ІБ проводить навчання щодо дотримання парольної політики. Таке навчання стосується правил призначення та зміни паролів, а саме:

- Необхідність зміни паролів кожні 30 днів.
- Користувач не може повторно використовувати останні 6 паролів.
- Паролі повинні містити не менше восьми символів і містити літери латинського алфавіту (верхнього регістру), малі та великі літери, цифри та спеціальні символи.
- Заборону вживання прізвищ, імен, дат днів народження або номерів телефонів для призначених паролів.
- Негайній зміні паролю при його компрометації або розголошені.
- Заборону передачі паролів іншим працівникам та стороннім особам, включаючи членів родини
- Заборону на запис паролів на папері, у робочому блокноті та іншому незахищеному місті біля робочої станції.
- Заборону на завантаження, онлайн використання чи входу до стороннього програмного забезпечення та/або входу до інтернет-сайтів з автоматичним завантаженням паролів під час наступного доступу до цих ресурсів.
- Будь-який працівник, якому відповідальний з ІБ доручив змінити свій пароль, тому що призначений пароль не відповідав вищезазначеним стандартам, повинен зробити це негайно.

Назва ЗОЗ **Політика інформаційної безпеки**	
Назва: УПРАВЛІННЯ РИЗИКАМИ	**Р 17**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Інформаційна безпека ЗОЗ 2 категорії**

17. УПРАВЛІННЯ РИЗИКАМИ

Для забезпечення інформаційної безпеки заклад проводить точну та ретельну оцінку потенційних ризиків та вразливостей стосовно конфіденційності, цілісності та доступності даних, що зберігаються, обробляються та передаються інформаційними системами та мережами закладу.

Заклад проводити точний і ретельний аналіз ризиків, результат цього аналізу служить основою для організації зусиль із забезпечення інформаційної безпеки закладу на належному рівні. Заклад проводить повторну оцінку ризиків безпеки та оцінку ефективності заходів безпеки, якщо це необхідно при змінах у штатній структурі, створені нових процесів чи розвитку технологій.

Процедура

ВІБ організовує та координує аналіз та оцінку ризиків. Для цього він/вона залучає відповідних осіб з персоналу закладу та/або зовнішніх експертів. Аналіз ризиків повинен відбуватися таким чином:

1. Проводиться інвентаризація та аналіз наявних інформаційних системи.

- Оновлюється або здійснюється інвентаризації інформаційних систем: складається перелік всього інформаційного обладнання (наприклад, мережевих пристроїв, робочих станцій, принтерів, сканерів, мобільних пристроїв) і програмного забезпечення (наприклад, операційних систем, додатків, іншого програмного забезпечення та інтерфейсів); в переліку вказується: назва інформаційної системи, дата придбання, місцезнаходження, постачальник, ліцензії, графік технічного обслуговування та функції; здійснюється оновлення або розробка мережевої архітектури.
- Оновлюється або розробляється макет об'єкта, що показує розташування обладнання всіх інформаційних систем, джерел живлення, телефонних роз'ємів; та іншого

телекомунікаційного обладнання, мережевих точок доступу, схеми пожежної та охоронної сигналізації та обладнання, а також місця зберігання небезпечних матеріалів;

- для кожного елементу макету об’єкта ідентифікується відповідальний (авторизований користувач), вказується його посада та спосіб отримання дозволу на авторизоване користування;
- Для кожної інформаційної системи вказується:

  - пов’язані дані, про які зазначається, чи створені дані закладом або отримані від третьої сторони. Якщо дані отримані від третьої сторони, зазначається спосіб отримання;
  - чи зберігаються дані тільки всередині організації або передаються третій стороні. Якщо дані передаються третій стороні, визначають цю сторону, а також мету і спосіб передачі;
  - критичність інформаційної системи для закладу та пов'язаних з нею даних. Критичність визначають як високу, середню або низьку. Критичність - це ступінь впливу на діяльність закладу інформаційної системи, уразі якщо пов'язані з нею дані стануть недоступними протягом певного періоду часу;
  - визначена чутливість даних як висока, середня або низька. Чутливість - це характер даних пов’язаний з оцінкою шкоди, яка може виникнути в результаті порушення конфіденційності даних.
  - визначені засоби контролю безпеки для кожного ідентифікованого програмного забезпечення, що застосовується в інформаційних системах, із зазначенням процедури контролю та засобів контролю.

- При оцінці загроз конфіденційності, цілісності та доступності даних, які створених, отримані, зберігаються, передаються чи обробляються закладом звертається увага на таке:

  - загрози пошкодження даних навколишнім середовищем, наприклад, землетрусом, повінню, штормом, тощо.
  - Загрози надзвичайних ситуацій - пошкодження пожежею, аварією електромережі, припиненням отримання комунальних послуг, тощо.
  - Людські загрози, а саме:
    - ненавмисні дії, наприклад, помилки при введені даних, використання несправного програмного забезпечення, нездатність оновити програмне забезпечення, відсутність належних фінансових та людських ресурсів для підтримки необхідних засобів контролю безпеки
    - неналежна діяльність, наприклад, неналежна поведінка, зловживання привілеями чи правами, марнотратство, переслідування особистої користі
    - зловмисні дії, наприклад шахрайство, крадіжки, вандалізм, диверсії,
    - зовнішні атаки, наприклад, хакерські атаки, сканування, геополітичні ризики.

2. Виявляються вразливості інформаційних систем. Вразливість - це недолік або слабкість у процедурах безпеки, розробці, впровадженні або контролі за

використанням ІС, які можуть бути випадково спровоковані або навмисно використані, що призведе до несанкціонованого доступу, модифікації даних, відмові в обслуговуванні або відмові від ідентифікації (неможливості ідентифікувати джерело зловмисних дій і притягнути якусь особу до відповідальності за ці дії). Для виконання цього завдання проводиться аналіз стосовно використання та застосування стандартів інформаційної безпеки до конкретних ІС і визначається ймовірність інциденту безпеки через вразливість інформаційної системи. Ймовірність інциденту безпеки визначається як.

- «Дуже ймовірно» - такий, що має дуже високі шанси на виникнення.
- «Ймовірно» - такий, що має значний шанс на виникнення.
- «Мало ймовірно» - незначний шанс на виникнення.

3. Одночасно визначається рівень критичності для вразливості інформаційної системи, як

   «Високий» - такий, що має катастрофічний вплив на медичну практику, призведе до втрати чи компрометації значної кількості медичних записів.
   «Середній» - такий, що має значний вплив на медичну практику, може призвести до втрати або компрометації даних
   «Низький» - визначається як незначний вплив, включаючи незначну втрату або компрометацію деяких медичних записів.

4. Визначається показник ризику для кожної вразливості шляхом компіляції оцінок ймовірності та критичності. Ризики з більш високим показником ймовірності та критичності вимагають більшої уваги.

5. Визначаються відповідні заходи безпеки для усунення або мінімізації ризиків. Основні зусилля зосереджуються на усунені вразливостей з високими показниками ризику. Ризики які неможливо усунути чи мінімізувати приймаються. Це означає, що керівництво йде на такий ризик та усвідомлює наслідки.

6. Розробляється або уточняється політика інформаційної безпеки та здійснюються конкретні критично важливих заходів безпеки (наприклад закупівля відповідної системи інформаційної безпеки), а саме:

   - визначається термін реалізації;
   - визначити витрати на такий захід та джерело фінансування;
   - призначається відповідальна особа;
   - визначається порядок здійснення заходу;
   - термін завершення;
   - робиться попередня оцінка ефективності заходу, яка після його здійснення уточняється.

7. Відповідальний за ІБ здійснює оцінку ефективності заходу стосовно усунення чи мінімізації ризику та при необхідності забезпечує здійснення повторної оцінки, яка включає:

   - Огляди, інтерв'ю користувачів з метою аналізу ефективності заходу, перегляд процедур, планів та політики інформаційної безпеки, аналіз інцидентів безпеки, уточнення програми навчань з ІБ, тощо.

- Для здійснення оцінки відповідальний може залучати відповідних працівників закладу та/або зовнішніх експертів при необхідності.

Назва Закладу	**Політика інформаційної безпеки**
Назва: Відповідальність за порушення Порушення безпеки та дисциплінарне стягнення	**Р 18**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Інформаційна безпека ЗОЗ 2 категорії**

18. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ

Персонал та керівництво закладу повинні постійно захищати конфіденційність, цілісність та доступність інформації та забезпечувати підтримку інформаційної безпеки закладу на належному рівні. При порушенні чинного законодавства та політики інформаційної безпеки настає відповідальність за порушення.

До конфіденційної інформації закладу відноситься:

- захищена медична інформація – індивідуальна інформація про стан здоров'я пацієнтів, яка знаходиться в будь-якій формі будь то електронна, паперова або усна;
- електронна захищена медична інформація - індивідуальна інформація про стан здоров'я пацієнтів, яка знаходиться в електронному форматі;
- інформація про медичний персонал - будь-яка інформація, пов'язана з наймам та/або працевлаштуванням будь-якої фізичної особи, яка є або була працевлаштована в закладі.
- дані про заробітну плату персоналу;
- фінансові/бухгалтерські записи - будь-які записи, пов'язані з бухгалтерською або фінансовою звітністю закладу;
- інша конфіденційна інформація – будь-яка інша інформація, яка має конфіденційний характер або вважається конфіденційною відповідно до чинних угод та договорів.

Терміни доступність, цілісність та конфіденційність вживаються відповідно до визначень, що наведені у п. 1.2. цієї політики.

Перелік порушень та відповідальність за них

Нижче перераховані види порушень, які вимагають застосування покарань. Вони діляться на три рівня перший (1), другий (2) і третій (3) в залежності від серйозності порушення та їх наслідків.

Рівень	Опис порушення
Перший рівень порушень (1)	• Доступ до інформації, яка не потрібна для виконання службових обов’язків; • передача іншій особі персонального логіну та паролю та/або надання спільного доступу до робочої станції, авторизованого доступу; • залишення працюючого комп'ютера з доступом до конфіденційної інформації

Рівень	Опис порушення
	без нагляду; • розкриття конфіденційної інформації стороннім особам; • копіювання конфіденційної інформації без дозволу; • зміна конфіденційної інформації без дозволу; • обговорення конфіденційної інформації в публічному місці, де стороні особи мають можливість підслуховувати розмову; • обговорення конфіденційної інформації з неуповноваженою особою; • відмова від співпраці з відповідальним за ІБ та невиконання його вказівок щодо дотримання політики інформаційної безпеки.
Другий рівень порушень (2)	• Здійснення порушення першого рівня вдруге (не обов'язково має бути тим самим порушенням); • несанкціоноване використання або розголошення конфіденційної інформації; • отримання доступу під логіном та паролем іншої людини; • невиконання/відмова у виконанні вказівок щодо виправлення ситуації.
Третій рівень порушень (3)	• Здійснення порушення першого рівня втретє (не обов'язково має бути тим самим порушенням); • здійснення порушення другого рівня вдруге (не обов'язково має бути тим самим порушенням); • отримання конфіденційної інформації під вигаданими приводами; • використання та/або розкриття конфіденційної інформації з метою отримання особистої вигоди або здійснення зловмисних дій.

Дисциплінарні стягнення

У тому випадку, якщо працівник здійснив будь-яке з наведених вищі порушень до нього застосовуються наступні заходи дисциплінарного впливу чи покарання.

Рівень порушення	Дисциплінарні стягнення
Перший рівень порушень (1)	• Усна або письмова догана

Рівень порушення	Дисциплінарні стягнення
	• або пониження прав доступу • або направлення на додаткове заняття з інформаційної безпеки • або проходження додаткового інструктажу з інформаційної безпеки
Другий рівень порушень (2)	• Строга догана із занесенням в особову справу • або тимчасове відсторонення від виконання службових обов'язків; • або пониження прав доступу до рівня, що призводить до пониження у посаді чи рівні кваліфікації; • або призначення проходження позапланового навчання (курсу навчань) в неробочій час;
Третій рівень порушень (3)	• Припинення трудової діяльності або розірвання контракту; • та/або накладання штрафу для компенсації нанесених збитків; • та/або кримінальне покарання відповідно до чинного законодавства.

Дисциплінарні покарання носять виховуючи характер та застосовуються відповідно до певних обставин здійснення порушень. Керівництво закладу проводить консультації з відділом кадрів перед вжиттям відповідних заходів. У відповідних випадках накладаються більш м'які дисциплінарні покарання, якщо порушник усвідомлює неправильність вчинку та налаштований скорегувати поведінку.

Накладання сурової догани повинно бути попередньо обговорено керівництвом з відділом кадрів.

Винятки

В залежності від тяжкості наслідків порушення, будь-які окремі порушення першого та другого рівня можуть призвести до припинення трудової діяльності або розривання контракту з порушником.

Визнання відповідальності за порушення

Я, нижче підписаний працівник або підрядник, цим підтверджую отримання та ознайомлення з інформацією Назва закладу[1] стосовно відповідальності за порушення інформаційної безпеки.

Дата _____

_____ Підпис співробітника/підрядника

Назва Закладу безпеки	**Політика інформаційної**
Назва: ПЕРЕВІРКА КАНДИДАТІВ	**Р 19**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Інформаційна безпека ЗОЗ 2 категорії**

19. ПЕРЕВІРКА КАНДИДАТІВ

Заклад проводить довідкові перевірки кандидатів перед працевлаштуванням. Від кандидата завчасно отримується згода на проведення такої перевірки. Кандидат, який відмовляється від такої перевірки, перестає бути кандидатом та його вивчення кадровим відділом припиняється.

Відділ кадрів збирає інформацію про репутацію кандидата, особисті характеристики або спосіб життя. Ця інформація може бути зібрана в Інтернеті, включаючи сайти соціальних мереж, через публічні чи освітні записи або через співбесіди з попередніми роботодавцями, партнерами, особами, що можуть надати рекомендаційні листи або будь кім іншим.

Тип інформації, яка буде зібрана закладом під час перевірки біографічних даних, може включати, але не обмежуватися наступною інформацією:

- довідка про непритягувана до кримінальної відповідальності;
- диплом про освіту (включаючи середній бал);
- історію працевлаштування, здібності та причини припинення трудових відносин;
- сертифікати, дипломи про закінчення закладів навчання, курсів, тощо;
- кредитна історія;
- реєстр рішень цивільних судів;
- записи у відкритих реєстрах стосовно володіння рухомим та нерухомим майном;
- професійні або особисті довідки;
- резюме кандидата.

Ця інформація також може бути додатково переглянута під час здійснення працівником порушення або його/її перепризначення на посаду з розширенням прав доступу.
Повідомлення про судимість не обов'язково дискваліфікує кандидата на працевлаштування. При прийняті рішення враховується характер і серйозність правопорушення, дата правопорушення, обставини та можливі ризики для закладу при працевлаштуванні такого кандидата.

Заклад має право відкликати пропозицію про працевлаштування, або звільнити працівника при виявлені свідомого надання неправдивої інформації стосовно себе.

Звіти про перевірку біографічних даних зберігається, як конфіденційна інформація відділом кадрів.

Назва Закладу	**Політика інформаційної безпеки**
Назва: Реагування на інцидент	**П. 20.1. – 20.4.**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Інформаційна безпека ЗОЗ 2 категорії**

20. ПОЛІТИКА УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

20.1. Загальні положення

Цілями Політики управління інцидентами ІБ є:

- відновлення нормальної роботи комп'ютерної та обчислювальної техніки, інших ІТ-систем у найкоротші терміни;
- зведення до мінімуму впливу інцидентів ІБ на роботу Назва ЗОЗ;
- забезпечення виявлення та фіксації всіх інцидентів ІБ;
- залучення всіх необхідних сил та засобів для реагування на інциденти ІБ;
- здійснення необхідних заходів для запобігання або зменшення кількості інцидентів ІБ в подальшому.

Задачами Політики управління інцидентами ІБ є:

- оперативний моніторинг стану інформаційної безпеки Назва ЗОЗ;
- виявлення, облік, реагування, розслідування та аналіз інцидентів ІБ;
- інформування керівництва та зацікавлених сторін про стан ІБ.

20.2. Терміни

Подія – будь-яка подія, що спостерігається в системі або мережі закладу.

Інцидент інформаційної безпеки (інцидент ІБ) **–** це поодинока подія, або ряд небажаних та непередбачених подій інформаційної безпеки (ІБ), через які існує ймовірність компрометації інформації закладу та загрози інформаційній безпеці Назва ЗОЗ. До інцидентів ІБ відносяться:

- технічний збій та відмови в обслуговуванні комп'ютерної та обчислювальної техніки, інших ІТ-систем;

- порушення конфіденційності та цілісності інформації та/або несанкціонована зміна інформації,
- недотримання вимог інформаційної безпеки (порушення Політики інформаційної безпеки Назва ЗОЗ);
- зовнішні або внутрішні зловмисні дії пов'язані з незаконним моніторингом інформаційних систем, завантаженням/сприянням у проникненні до комп'ютерної мережі та ІТ-систем закладу шкідливого програмного забезпечення тощо;
- порушення Політики доступу до інформаційних систем (наприклад передача іншій особі або розголошення особистого паролю);
- спроби отримати несанкціонований доступ до ІТ-систем або даних;
- несанкціоноване використання ІТ-систем або комп'ютерів;
- вимагання викупу через крадіжку та/або шифруванням ІТ-систем або корпоративних даних;
- втрата конфіденційної інформації.

Оповіщення - повідомлення про те, що подія або послідовність подій може бути інцидентом ІБ. Оповіщення можуть надходити з багатьох джерел, таких як засоби безпеки, персонал, пацієнти, підрядники та канали розвідки загроз.

Робоча група реагування на кіберінциденти – тимчасово створена або постійно діюча робоча група відповідальних осіб, створена зі складу існуючих організаційних підрозділів закладу, яка щонайменша включає представників підрозділів відповідальних за інформаційні технології та інформаційну/кібер безпеку. Робоча група може залучати зовнішніх експертів за потреби.

20.3. Управління інцидентами ІБ

Управління інцидентами ІБ в Назва ЗОЗ складається з наступних заходів:

- Підготовка до інцидентів ІБ;
- Виявлення та повідомлення про інцидент ІБ;
- Реагування на інцидент ІБ;
- Розслідування та звітування про інцидент ІБ;
- Повідомлення про інцидент ІБ постраждалих та всіх зацікавлених сторін;
- Профілактика інцидентів ІБ.

20.3.1. Підготовка до інцидентів ІБ

1. Керівник закладу створює Робочу групу реагування на кіберінциденти.
2. Відповідальний за ІБ готує План реагування на інциденти ІБ.
3. В закладі проводяться тренінги та навчання персоналу з реагування на інциденти інформаційної безпеки.
4. При необхідності розробляються інструкції щодо реагування на інциденти ІБ.

,

20.3.2. Виявлення та повідомлення про інциденти ІБ

1. Будь-який працівник, якому стало відомо про порушення політик інформаційної безпеки або про інцидент ІБ негайно повідомляє про це свого безпосереднього керівника та/або відповідального за ІБ.
2. При наявності сервіс-деск (ІТ-відділу) працівник, якому стало відомо про порушення політик інформаційної безпеки або про інцидент ІБ, невідкладно повідомляє про такий інцидент ІТ-відділ встановленим в Назва ЗОЗ порядком. ІТ-відділ фіксує інцидент в електронному журналі подій ІБ.
3. Повідомлення повинно відбуватися негайно після виявлення можливого порушення або до закінчення зміни, якщо інші обов'язки заважають зробити це негайно.
4. Безпосередній керівник або відповідальний за ІБ перевіряє обставини можливого порушення та невідкладно вживає можливі заходи реагування на порушення, а також доповідає про порушення керівнику закладу. Якщо у закладі відсутній ІТ-відділ, відповідальний за ІБ вносить інформацію про інцидент у Журналі подій ІБ.
5. Для негайного повідомлення про порушення персонал може зателефонувати відповідальному за інформаційну безпеку за номером телефону _____-_____.

20.3.3. Реагування на інциденти ІБ

Відповідальний за інформаційну безпеку при отримані повідомлення про порушення Політики інформаційної безпеки Назва ЗОЗ або інцидент ІБ організовує роботу Робочої групи реагування на кіберінциденти, яка здійснює наступні заходи:

1. Аналізує інцидент ІБ з метою визначення його типу та масштабу.

2. Локалізує інцидент ІБ з метою зменшення шкоди від нього. До локалізації входять наступні дії:

- відключення систем,
- від’єднання систем від мережі,
- блокування певних портів, протоколів, служб, функцій,
- блокування доступу до скомпрометованих систем,
- перевірка коду у «пісочницях», зовнішніх носіїв інформації на локалізованих комп’ютерах тощо.

3. Усуває причини та наслідки інциденту ІБ, а також здійснює заходи зі зменшення ризиків повторного виникнення схожих загроз. Робоча група реагування на кіберінциденти визначає дії, необхідні для усунення інцидентів різних типів. Дії з усунення інцидентів включають, серед іншого:

- ідентифікацію та обробку усіх експлуатованих вразливостей;
- видалення шкідливого програмного забезпечення та інших компонентів кібератаки;

- безперервний аналіз дій для ідентифікації всіх вражених хостів/кінцевого обладнання та завершення дій з локалізації та усунення всіх заражених/вражених систем.

4. Здійснює заходи з відновлення, які складаються з наступних кроків:

- відновлення заражених/вражених систем;
- підтвердження нормального функціонування цих систем;
- впровадження додаткового моніторингу для відслідковування пов’язаних активностей.

20.3.4. Розслідування та звітування

1. При розслідуванні інциденту ІБ Робоча група реагування на кіберінциденти розглядає обставини, причини та наслідки інциденту ІБ та оцінює ризики інформаційної безпеки, які пов’язані з інцидентом. При цьому розглядаються наступні фактори, але не обмежуються ними:
    - характер цифрового активу, який постраждав в наслідок інциденту та його важливість для функціонування закладу;
    - необхідні заходи та засоби для відновлення функціонування;
    - договірні зобов'язання, які можуть бути не виконані, порушені;
    - ризики крадіжки особистих даних або втрати інформації в наслідок її псування, затирання чи шифрування, можливості щодо відновлення якомога актуальнішої версії резервного копіювання;
    - ризик заподіяння фізичної шкоди, якщо втрата даних ставить під загрозу життя людини;
    - ризик заподіяння шкоди репутації закладу;
    - обсяги (масив) втраченої, вкраденої чи зіпсованої інформації та кількість постраждалих осіб.

2. Звіт про інцидент ІБ формується після завершення усіх дій з його розслідування. Цей крок передбачає документування важливої інформації про інцидент ІБ та про результати реагування. Звіт про інцидент ІБ може включати:

- опис інциденту, яким чином було виявлено та повідомлено про інцидент;
- висновки щодо того, як стався інцидент;
- перелік дій, вжитих для реагування на інцидент;
- Рекомендації щодо зниження кіберризиків у майбутньому.

20.3.5. Повідомлення про інциденти ІБ

1. За рішенням керівника заклад повідомляє правоохоронні орган (CERT-UA, кіберполіцію) про інцидент безпеки та його ознаки.
2. Про всі інциденти ІБ, які були повідомлені правоохоронним органам заклад доповідає до Центрального апарату Міністерства охорони здоров’я України встановленим МОЗ України порядком.

3. Відповідно до чинного законодавства заклад повідомляє постраждалим особам про виток їх персональних даних та медичної інформації.
4. Постраждалі особи повинні бути повідомлені не пізніше двох місяців після відбуття інциденту ІБ. Повідомлення повинні містити наступну інформацію:
    - що сталося;
    - яка сама персональна та медична інформація стосовно постраждалої особи вкрадена (скомпрометована) чи зіпсована;
    - рекомендації, що постраждалій особі бажано зробити;
    - інформація про дії закладу для запобігання подібних інцидентів у майбутньому;
    - контактна інформація.

    Повідомлення надсилається на електронну пошту постраждалої особи або інший електронний акаунт.
5. Якщо заклад повідомив про інцидент правоохоронні органи то інформування постраждалих осіб відбувається тільки після дозволу правоохоронців, щоб не перешкоджати кримінальному розслідуванню.
6. Непряме сповіщення, таке як публікація інформації на веб-сайті або сторінці закладу у соціальних мережах, може відбутися коли кількість постраждалих значна, перевищує 500 осіб.
7. Використання декількох методів оповіщення в певних випадках може виявитися найбільш ефективним підходом.

20.3.6. Профілактика

1. Враховуючи виявлені недоліки, команда з реагування на інциденти та інші зацікавлені сторони можуть сформувати рекомендації для усунення вразливостей та ризиків.
2. При необхідності може проводитися аудит безпеки фізичних, організаційних і технологічних заходів, також може проводитись перегляд політики інформаційної безпеки.
3. Для підготовки рекомендацій та аналізу причин інциденту ІБ при необхідності можуть залучатися зовнішні експерти.
4. Результати розслідування інциденту ІБ доповідаються керівнику закладу разом з рекомендаціями, щодо запобігання подібних інцидентів у майбутньому.
5. За результатами складається план заходів з усунення недоліків, виявлених в ході розслідування інциденту, якщо це доречно.

20.4. Обов’язки та відповідальність

4.1. Керівник закладу несе повну відповідальність за захист даних та підтримку належного рівня інформаційної безпеки закладу. Він/вона організовує роботу Робочої групи реагування на кіберінциденти та при необхідності долучається до її роботи при розслідуванні інцидентів ІБ.

4.2. Відповідальний за ІБ закладу розробляє та періодично (щорічно або за результатами розслідування інцидентів ІБ при необхідності) оновлює План реагування на інциденти ІБ та організовує тренування з реагування на кіберінциденти. Він/вона несе загальну відповідальність за виконання технічних аспектів реагування на інциденти та відповідає за управління Робочою групою реагування на кіберінциденти, управління персоналом,

прийняття основних рішень в процесі реагування, коли це необхідно. Крім того, відповідальний за ІБ відіграє важливу роль у ескалації інцидентів до рівня зацікавлених сторін, здійснює взаємодію з відповідними державними органами, доносить керівництву закладу необхідну інформацію та координує рішення управлінського рівня.

4.3. Члени Робочої групи реагування на інциденти ІБ здійснюють безпосереднє реагування на інцидент ІБ, долучаються до розслідування та підготовки звіту про інцидент ІБ.

4.4. Начальник відділу ІТ відповідає за надання розгорнутої та повної інформації про інцидент членам Робочої групи з реагування на кіберінциденти та іншим зацікавленим особам, а також за виконання безпосередній технічних дій в інформаційних системах задіяних в реагуванні на інцидент ІБ, згідно затвердженого Плану реагування на інциденти ІБ.

4.5. Юридичний відділ дає рекомендації щодо відповідності законодавчим вимогам, наприклад, щодо безпеки персональних даних, повідомлення про інциденти ІБ всіх зацікавлених сторін тощо.

4.6. Підрозділ управління персоналом відповідає за внутрішню комунікацію для персоналу закладу стосовно інцидентів ІБ та координує відповідні внутрішні комунікації в закладі.

4.7. Увесь персонал повинен невідкладно інформувати про виявлені інциденти ІБ, дотримуватись вимог чинної Політики, а також вказівок відповідального за ІБ при реагуванні на інциденти ІБ та усунені їх наслідків.

4.8. Керівництво та всі працівники закладу, які порушують Політику інформаційної безпеки несуть дисциплінарну та/чи адміністративну відповідальність, яка встановлена відповідним розділом Політики інформаційної безпеки Назва ЗОЗ. При порушені вимог чинного законодавства персонал та керівництво закладу несуть адміністративну та/чи кримінальну відповідальність.

ДОДАТОК 1

ФОРМА ЗАПИТУ НА ДОСТУП

(запит працівника чи підрядника на доступ до інформаційних ресурсів)

ПІБ_____

Посада _____

Дата початку доступу _____

Режим доступу (цілодобовий чи у певні робочі години) _____

Дата та час припинення доступу_____

Перелік ресурсів до яких надається доступ з вказанням прав доступу (читання, редагування, здачі під охорону сигналізацію, відвідування у вихідні дні тощо)

1. Електронна пошта _____
2. Електронні реєстри_____
3. ІТ-системи, мережі_____
4. Програмне забезпечення, додатки_____
5. Віддалений доступ _____
6. Службовий телефон _____
7. Доступ до будівлі _____

Погодження безпосереднього керівника _____

Погодження відповідального за ІБ _____

ДОДАТОК 2

Згода про нерозголошення

ВІДПОВІДАЛЬНІСТЬ ЗА РОЗГОЛОШЕННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Я розумію і погоджуюся зберігати, захищати та не розголошувати конфіденційну інформацію Назва ЗОЗ. Крім того, я розумію, що будь-яке несанкціоноване використання або розголошення інформації закладу , може призвести до дисциплінарної, адміністративної чи кримінальної відповідальності відповідно до політики інформаційної безпеки Назва ЗОЗ та чинного законодавства.

_____ _____

Дата Підпис

_____ _____

Дата Підпис відповідального за ІБ

ДОДАТОК 3

ЗАТВЕРДЖЕНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Нижче наведений перелік затверджено для використання програмного забезпечення, яке повинно бути встановлене на робочих станціях та використовуватись персоналом для роботи. Використання не затвердженого програмного забезпечення на робочих станціях заборонено.

ПЗ	Версія	Затверджено	Дата	Опис/Коментарі

ДОДАТОК 4

ЗАТВЕРДЖЕНІ ПОСТАЧАЛЬНИКИ

Постачальник	Основний контакт	Основний номер	Товар/Послуга	Опис/Коментарі

ДОДАТОК 5

ЖУРНАЛ РЕГІСТРАЦІЇ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

№	Назва події	Дата. Час	Ознаки/ індикатори	Вжиті заходи/ реагування	Рекомендації/ коментарі

ДОДАТОК 6

ЗГОДА НА ПЕРЕВІРКУ КАНДИДАТА

Я, _____, даю свою згоду Назва ЗОЗ на перевірку моєї біографічної і особистої інформації. Я розумію, що за результатами цієї перевірки мені можуть не запропонувати працевлаштування в Назва ЗОЗ.

Дата __

Підпис заявника _____

ДОДАТОК 7

ЖУРНАЛ УПРАВЛІННЯ ЗМІНАМИ

Дата	Назва ПЗ/АЗ	Опис зміни	Створена РЗ до зміни	Зміна запроваджена з (дата, час)	Отриман і відгуки/ скарги	Вжиті заходи	Коментарі

Прим. ПЗ – програмне забезпечення;

АЗ – апаратне забезпечення;

РК - резервна копія.