Назва ЗОЗ **Політика Управління Ризиками Інформаційної Безпеки**	
Назва: УПРАВЛІННЯ РИЗИКАМИ	**ЗОЗ 1, 2 категорії**
Дата затвердження: Дата[4]	**Огляд: Щорічний**
Дата набрання чинності: Дата[5]	**Затверджено: ПІБ Назва ЗОЗ**

ПОЛІТИКА УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗАКЛАДУ ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ

ЗМІСТ **стр.**

1. ВСТУП

1.1. Управлінню ризиками необхідно приділяти підвищену увагу з боку керівництва закладу охорони здоров'я. Управління ризиками відноситься до управління надзвичайними подіями, які не завжди можна передбачити заздалегідь, але у разі настання такі події призводять до негативних наслідків. У зв'язку з цим дуже важливо мати стале управління персоналом та активами за допомогою імплементації ризик-орієнтовного підходу управління, а також запровадити ефективні механізми управління ризиками.

1.2. Управління ризиками інформаційної безпеки здійснюється відповідно до вимог чинного законодавства України, а саме:

- Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518;
- вимог ДСТУ ISO/IEC 27001:2015 «Інформаційні технології Методи захисту. Системи управління інформаційною безпекою. Вимоги" (далі – ДСТУ ISO/IEC 27001:2015);
- вимог ДСТУ ISO/IEC 27002:2015 "Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки" (далі – ДСТУ ISO/IEC 27002:2015);
- вимог ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT) Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (далі ДСТУ ISO/IEC 27005:2019);
- з урахуванням інших міжнародних стандартів з питань інформаційної безпеки, загальноприйнятих у міжнародній практиці принципів забезпечення інформаційної безпеки і кіберзахисту.

1.3. Для управління ризиками 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 та здійснює управління виявленими ризиками інформаційної безпеки.

1.4. Заклад проводить точний і ретельний аналіз існуючих та перспективних ризиків інформаційної безпеки, результат цього аналізу відображається на Карті ризиків та служить основою для розробки Плану обробки ризиків, а також організації зусиль із забезпечення інформаційної безпеки закладу на належному рівні.

1.5. Заклад проводить повторну оцінку ризиків інформаційної безпеки та оцінку ефективності заходів безпеки раз на рік або позапланово, якщо це необхідно при змінах у штатній структурі, створені нових процесів чи розвитку технологій.

2. ВИЗНАЧЕННЯ

Актив - матеріальні та нематеріальні об'єкти або інформація, що мають цінність для ЗОЗ. **Інформаційний актив** – це інформаційні та цифрові системи або інформація (дані), що мають цінність для ЗОЗ.

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 ЗОЗ.

Вразливість ІС - це недолік або слабкість у процедурах безпеки, розробці, впровадженні або контролі за використанням інформаційних систем, 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).

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.

Запобігання ризику - це прийняття рішення не вести певну діяльність чи змінити умови її ведення, щоб уникнути ризику, асоційованого з цією діяльністю. Це рішення може бути прийняте у разі високих ризиків або перевищення вартості впровадження заходів захисту над очікуваними перевагами.

Збереження ризику означає, що за результатами оцінки впливу цього ризику прийнято рішення, що подальші дії з його обробки не потрібні, тобто оцінка рівня очікуваного ризику відповідає критерію прийняття ризику.

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.

Модифікацій ризику - це управління ризиком шляхом застосування або зміни заходів захисту, що призводить до оцінки залишкового ризику як прийнятного. При модифікації ризиків вибираються виправдані та релевантні заходи захисту, які відповідають вимогам, визначеним на етапах оцінки та обробки ризиків.

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

Передача ризику – передача функції управління ризиком третій стороні, яка зможе керувати ним найефективніше. На підставі оцінки ризиків приймається рішення про передачу певних ризиків, наприклад, шляхом страхування кібер-ризиків.

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

Прийняття ризику передбачає оцінку залишкового ризику як прийнятного. Однак слід враховувати, що в деяких випадках вартість усунення або модифікації ризику перевищує вартість наслідків реалізації ризику, що може призвести до прийняття ризиків, які не відповідають прийнятному рівню. В даному випадку керівництво усвідомлює негативні наслідки реалізації ризику та свідомо йде на такий ризик.

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.

3. ВІДПОВІДАЛЬНІСТЬ

3.1. Відповідальний за інформаційну безпеку Закладу організовує та координує аналіз та оцінку ризиків. Для цього він/вона залучає відповідних осіб з персоналу закладу та/або зовнішніх експертів.
3.2. Відповідальний за інформаційну безпеку проводить інвентаризацію та аналіз наявних інформаційних активів. Визначає можливі вразливості цих активів та оцінює пов'язані з цими вразливостями загрози та ризики. На основі цієї оцінки розробляє Карту ризиків.
3.3. Відповідальний за інформаційну безпеку закладу на основі Карти ризиків розробляє План оброблення ризиків та затверджує його у керівника Закладу.
3.4. Керівник Закладу здійснює загальне управління політикою щодо управління ризиками, затверджує План оброблення ризиків та приймає управлінські рішення щодо модифікації, обробки, збереження, запобігання, передачі та прийняття ризиків.
3.5. Працівники Закладу, які відповідають за збереження інформаційних активів допомагають відповідальному за інформаційну безпеку провести інвентаризацію інформаційних активів, визначитися з їх вразливостями та пов'язаними загрозами, а також скласти Карту ризиків Закладу.
3.6. Увесь персонал Закладу долучається до процесу управління ризиками з метою запобігання та мінімізації ризиків та їх наслідків.

4. ПРОЦЕДУРА УПРАВЛІННЯ РИЗИКАМИ

Відповідно до стандарту ДСТУ ISO/IEC 27005:2019 процедура управління ризиками є безперервним та повторювальним процесом (Див. Схему 1), який складається з наступних заходів:

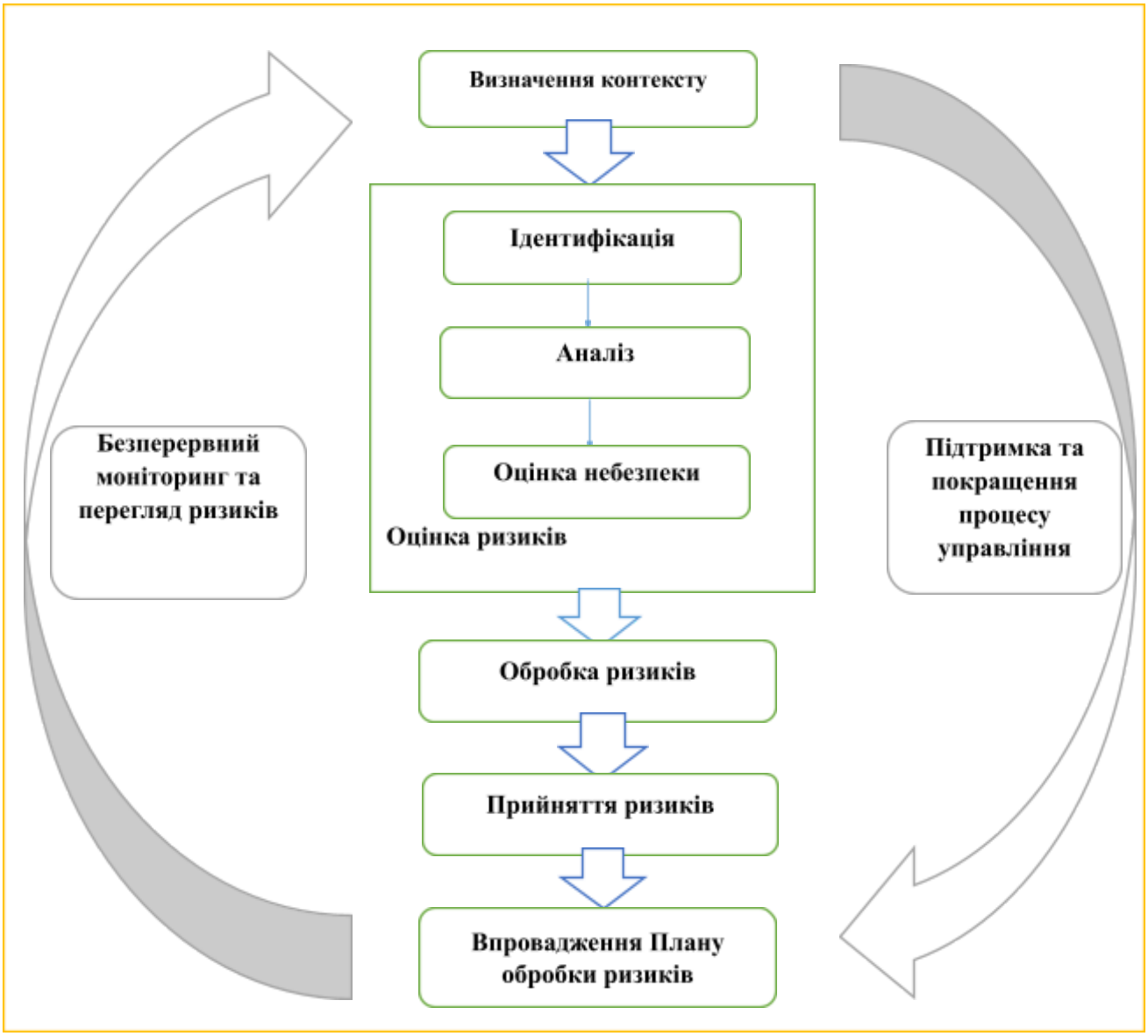

Схема 1. Процедура управління ризиками.

- **Визначення контексту** передбачає встановлення підходу до управління ризиками, а саме: визначення середовища в якому функціонує заклад та притаманні цьому середовищу ризики; які критерії оцінки ризиків застосовувати; які критерії прийняття ризиків; які правила управління та обробки ризиків.
- **Оцінка ризиків,** яка в свою чергу складається:
    - **Ідентифікація ризиків** (інвентаризація активів, ідентифікація загроз, ідентифікація наявних заходів захисту, визначення вразливостей, виявлення наслідків реалізації загроз порушення конфіденційності/цілісності/доступності інформаційних активів);

    - **Аналіз ризиків.** Проводиться з різною глибиною, залежно від критичності активів, кількості відомих уразливостей, а також з урахуванням інцидентів, що відбулися раніше. При первинному аналізі ризиків застосовуємо якісний аналіз для виділення високо пріоритетних ризиків. При вторинному аналізі ризиків застосовуємо кількісний аналіз, який дає більш точний результат.
    - **Оцінка небезпеки ризиків.** Порівняння отриманих на попередньому етапі рівнів ризиків із критеріями прийняття ризиків, отриманими на етапі визначення контексту.
- **Обробка ризиків**. Діяльність, яка складається з модифікації, збереження, запобігання та передачі ризиків іншій стороні (наприклад страхування ризику).
- **Прийняття ризиків.** Здійснюється визначення та затвердження ризиків, які приймаються керівництвом.
- **Впровадження Плану обробки ризиків**. Закуповуються та налаштовуються засоби захисту, укладаються договори з технічної підтримки та моніторингу, запроваджуються заходи з реагування на інциденти, здійснюється управління вразливостями тощо.
- **Безперервний моніторинг та перегляд ризиків.** Ризики можуть непомітно змінюватися з часом: змінюються активи та їхня цінність, з'являються нові загрози та вразливості, змінюються ймовірність реалізації загроз та рівень їхнього негативного впливу.
- **Підтримка та покращення** процесу управління ризиками інформаційної безпеки. Контекст, оцінка та План обробки ризиків постійно переглядаються та корегуються для того, щоб залишатися релевантними поточній ситуації та обставинам.

4.1. Визначення контексту

4.1.1. Визначення контексту складається з визначення середовища, в якому функціонує заклад охорони здоров’я, визначення пов’язаних з цим середовищем ризик-факторів, їх контекстна оцінка, встановлення критеріїв прийняття ризиків та правил управління ризиками.

4.1.2. **Визначення середовища** в якому функціонує заклад охорони здоров’я складається з аналізу фізичного середовища об’єкта (закладу), інформаційного середовища та середовища користувачів. Для кожного типу середовища визначаються притаманні цьому середовищу ризик-фактори.

4.1.3. Для **фізичного середовища** визначаються фізичні явища та стороні сили, системи підтримки життєдіяльності закладу, як можуть вплинути на виконання заходом своїх функцій. Для фізичного середовища притаманними ризик-факторами можуть вважатися стихійні лиха, землетруси, повені, пожежі, бойові дії, пошкодження комунальних мереж водо- та електропостачання, каналізації тощо.

4.1.4. Аналіз **інформаційного середовища** полягає в визначені наявних інформаційних систем та даних, інформаційної інфраструктури, телекомунікаційного обладнання, медичних цифрових пристроїв, які впливають на функціонування закладу. Для інформаційного середовища поширеними ризик-факторами є поломки та відмова у роботі, технічні збої та пошкодження, що призводять до порушення цілісності, доступності та конфіденційності даних.

4.1.4. Аналіз **середовища користувачів** передбачає визначення кола осіб, які мають доступ та використовують інформаційні активи та телекомунікаційні системи закладу. Для середовища користувачів найбільш поширеними ризик-факторами є компрометація облікових даних, порушення політики інформаційної безпеки, навмисні чи ненавмисні дії, що призводять до порушення цілісності, доступності та конфіденційності даних.

4.1.5. При здійснені контекстної оцінки визначається попереднє **значення рівня ризик-факторів (як низький, середній та високий)**. Для цього для кожного відомого ризик-фактору оціночним методом визначається ймовірність настання події, яка несе певний ризик-фактор та визначаються наслідки такої події. Значення ризик-фактору при контекстній оцінці вираховується, як множення значення ймовірності на оцінку наслідків.

Для визначення ймовірності застосовується шкала:

- Навряд чи (подія навряд чи відбудується протягом року) – 1 бал;
- Малоймовірно (подія має малу ймовірність здійснення протягом року)– 2 бали;
- Ймовірно (існує ймовірність настання події протягом року) – 3 бали;
- Дуже ймовірно (існує велика ймовірність настання події протягом року) – 4 бали;
- Напевно – (подія повинна відбутися протягом року) - 5 балів.

Для оцінки наслідків застосовується наступна шкала:

- Без наслідків (настання події не створить наслідків для закладу) – 1 бал;
- Незначні наслідки (подія спричинить незначні наслідки) – 2 бали;
- Середні наслідки (подія спричинить наслідки середньої важкості) – 3 бали;
- Тяжкі наслідки (подія спричинить тяжкі наслідки) – 4 бали;
- Дуже тяжкі наслідки (подія спричинить дуже тяжкі наслідки для закладу)– 5 балів.

Наслідки **x** Вірогідність	Без наслідків (1)	Незначні наслідки (2)	Середні наслідки (3)	Тяжкі наслідки (4)	Дуже тяжкі наслідки (5)
Напевно (5)	5	10	15	20	25
Дуже ймовірно (4)	4	8	12	16	20
Ймовірно (3)	3	6	9	12	15
Малоймовірно (2)	2	4	6	8	10
Навряд чи (1)	1	2	3	4	5

Таблиця 1. Кількісна контекстна оцінка ризик-факторів

При значені контекстної оцінки ризик-фактору 6 та менш балів ризик, що пов'язаний з цим ризик-фактором, вважається **низьким** (позначено зеленим кольором); при значені від 8 до 15 балів ризик вважається **середнім** (позначено жовтим кольором), від 16 балів та вище ризик вважається **високим** (позначено червоним).

4.1.6. Попередня оцінка ризиків на основі аналізу ризик-факторів фізичного, інформаційного середовищ та середовища користувачів робиться для визначення послідовності та пріоритетності обробки ризиків.

4.1.7. При аналізі, оцінці та обробці пріоритет надається ризикам з високим та середнім рівнями. Ризики з низьким рівнем зазвичай приймаються на етапі визначення контексту та в подальшому не обробляються. Також на етапі визначення контексту приймаються ризики з середнім та високим рівнем, якщо встановлюється, що вартість їх усунення перевищує вартість наслідків, які вони можуть спричинити.

Попередня оцінка ризиків, відповідно до первинного якісного аналізу показана в **Таблиці 2.**

Ризик-фактори фізичного середовища	**Бали**	**Ризик-фактори інформаційного середовища**	**Бали**	**Ризик-фактори середовища користувачів**	**Бали**
Припинення електроживлення та водопостачання закладу.	25	Пошкодження активів, втрата чутливих даних в наслідок порушень правил та умов експлуатації систем та мереж (наприклад в наслідок неконтрольованих перепадів напруги мережі електроживлення).	25	Навмисні дії персоналу або підрядників, що призвели до пошкодження активів закладу.	25
Пошкодження охоронної та пожежної сигналізації. Порушення вимог зберігання небезпечних матеріалів.	25	Зовнішні шкідливі впливи на активи, зокрема атаки шкідливим програмним забезпеченням та вірусами на інформаційні активи.	25	Крадіжка критичних даних та порушення цілісності даних персоналом закладу або підрядниками.	25
Припинення надання комунальних послуг закладу в наслідок форс-мажору.	20	Пошкодження (вихід з ладу) медичного обладнання та IT-інфраструктури закладу.	20	Ненавмисні дії персоналу або підрядників, що призвели до пошкодження активів закладу.	20
Пошкодження телемереж та ліній доступу до інтернет, до яких підключений заклад.	20	Відмови та збої в роботі медичного обладнання та IT-інфраструктури закладу.	20	Велике навантаження на медичний персонал, що призводить до збільшення помилок та порушень політики ІБ.	16
Пошкодження активів закладу в наслідок бойових дій.	15	Припинення підтримки постачальниками IT-та телеком. послуг.	15	Брак спеціалістів з технічної підтримки та інформаційної безпеки.	15

Пошкодження активів в наслідок повінню чи стихійного лиха.	10	Пошкодження серверної кімнати, автоматизованих робочих місць лікарів в наслідок стихійного лиха чи повінню.	12	Не зрозумілий розподіл обов'язків та відповідальності.	15
Припинення діяльності чи пошкодження закладу в наслідок землетрусу, техногенних катастроф, тощо.	5	Відмова в роботі окремих некритичних інформаційних систем (наприклад WiFi мережі або веб-сайту) закладу	9	Низька обізнаність персоналу щодо ризик-факторів та способів запобігання ризиків.	15

Таблиця 2. Контекстна оцінка типових ризик-факторів закладу охорони здоров'я.

4.1.8. Ризики, які в наслідок попередньої оцінки оцінюються як середні та високі підлягають подальшій обробці.

4.1.9. При запровадженні принципів обробки ризиків встановлюються наступні правила:

- запобігання ризиків є пріоритетом;

- увесь персонал ЗОЗ долучається до процесу управління ризиками з метою їх запобігання або мінімізації наслідків;

- встановлюється пріоритет з обробки ризиків, зазвичай спочатку оцінюються та обробляються ризики з найбільш високим рівнем ймовірності та тяжкості наслідків;

- встановлюється прийнятний рівень ризику, який визначає на якому рівні залишковий ризик може бути прийнятий.

4.2. Оцінка ризиків інформаційної безпеки

4.2.1 Оцінка ризиків це процес, який складається з ідентифікації, аналізу та оцінки небезпеки ризиків.

4.2.2. Для **ідентифікації ризиків** інформаційної безпеки проводиться інвентаризація та аналіз наявних інформаційних систем та ресурсів (даних) ЗОЗ, а також встановлення вразливостей цих систем та ресурсів.

4.2.3. Для інвентаризації ІС передбачається наступна послідовність дій:

- 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; час здійснення оновлення або розробки/змін мережевої архітектури.

- Оновлюється або розробляється карта інформаційних та телекомунікаційних систем закладу, 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 карт інформаційних та телекомунікаційних систем закладу 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. Показники чутливості даних прив’язуються до показників критичності інформаційних систем;
    - визначені засоби контролю безпеки для кожного ідентифікованого програмного забезпечення, що застосовується в інформаційних системах, із зазначенням процедури контролю та засобів контролю.

- При аналізі вразливостей **оцінюються загрози** конфіденційності, цілісності та доступності даних, які створені, отримані, зберігаються, передаються чи обробляються закладом. При цьому звертається увага на таке:

    - загрози пошкодження даних та IT-систем навколишнім середовищем, наприклад, землетрусом, повінню, штормом, в наслідок бойових дій, тощо;
    - загрози надзвичайних ситуацій - пошкодження даних та IT-систем пожежею чи повінем, відключення IT та медичних пристроїв в наслідок аварії електромережі або припинення 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, зловмисне використання вразливостей тощо.

4.2.3. Наступним кроком є **виявлення вразливості** інформаційних систем. Для виконання цього завдання проводиться аналіз стосовно використання та застосування вимог Політики 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 (обчислюється з коефіцієнтом 3);
- **«Ймовірно»** - такий, що має значний шанс на виникнення (обчислюється з коефіцієнтом 2);
- **«Мало ймовірно»** - незначний шанс на виникнення (обчислюється з коефіцієнтом 1).

Одночасно визначається рівень критичної вразливості (КВ) інформаційної системи для забезпечення конфіденційності (КВк), цілісності (КВц), доступності (КВд) інформації та даних, що зберігаються, обробляються чи передаються даною ІС.

Рівень критичної вразливості інформаційної систем розраховується як здобуток від множення показника ймовірності інциденту (Й) на показник ризику порушення конфіденційності (К) або цілісності (Ц) чи доступності (Д):

КВк = К х Й; КВц= Ц х Й; КВд=Д х Й

Таким чином знаходяться окремі значення показника рівня критичної вразливостей ІС стосовно порушень конфіденційності (КВк), цілісності (КВц) та доступності (КВд).

- Можливі значення показника ризику порушення **конфіденційності (К):**
  3 бали - є ризик незворотного порушення конфіденційності, зловмисник/порушник при реалізації ризика отримує повний доступ до конфіденційної інформації;
  2 бали – часткове порушення конфіденційності, зловмисник/порушник отримує не повний доступ (частковий) до конфіденційної інформації;
  1 бал – створення передумов порушення конфіденційності, зловмисник/порушник отримує доступ до проміжної інформації, даних, використання яких може сприяти отриманню повного чи часткового доступу до конфіденційної інформації Закладу.

  Можливі значення КВк наведені у Таблиці 3

Ймовірність /Ризик порушення конфіденц. (К)	1	2	3
Мало ймовірно – 1	1	2	3
Ймовірно - 2	2	4	6
Дуже ймовірно - 3	3	6	9

Вразливість ІС стосовно порушення конфіденційності вважається **низькою** при значені КВк 1 чи 2; **середньою** при КВк рівному 3 чи 4; **високою** при значені КВк 6 або 9.

- Можливі значення показника ризика забезпечення **цілісності (Ц):**
  3 бали - повне та незворотне порушення цілісності даних;
  2 бали – часткове незворотне порушення цілісності даних;
  1 бал – зворотне порушення цілісності даних з можливістю відновлення.

  Можливі значення КВц наведені у Таблиці 4

Ймовірність /Ризик порушення цілісності (Ц)	**1**	**2**	**3**
Мало ймовірно – 1	1	2	3
Ймовірно - 2	2	4	6
Дуже ймовірно - 3	3	6	9

  Вразливість ІС стосовно порушення цілісності вважається **низькою** при значені КВц 1 чи 2; **середньою** при КВц рівному 3 чи 4; **високою** при значені КВц 6 або 9.

- Можливі значення показника ризика забезпечення **доступності (Д):**
  3 бали - незворотне знищення даних без можливості відновлення;
  2 бали – часткове знищення даних з неможливістю відновлення;
  1 бал – тимчасова втрата доступу до даних.

  Можливі значення КВд наведені у Таблиці 5

Ймовірність /Ризик порушення цілісності (Ц)	**1**	**2**	**3**
Мало ймовірно – 1	1	2	3
Ймовірно - 2	2	4	6
Дуже ймовірно - 3	3	6	9

  Вразливість ІС стосовно порушення доступності вважається **низькою** при значені КВд 1 чи 2; **середньою** при КВд рівному 3 чи 4; **високою** при значені КВд 6 або 9.

Інтегрована оцінка вразливості ІС складається з поєднання показника рівня критичної вразливостей ІС стосовно порушень конфіденційності (КВк), цілісності (КВц) та доступності (КВд).

- Якщо використання певної вразливості ІС не призводить до негативних наслідків стосовно порушень конфіденційності, цілісності та доступності то відповідна інтегрована оцінка вразливості ІС вважається **низькою**, така вразливість не розглядається, як ризик інформаційної безпеки.
- Якщо всі показники КВк, КВц та КВд дорівнюють 1 чи 2, то така вразливість ІС вважається **середньою.** Вона може призвести до втрати або компрометації деяких медичних записів, нетривалого порушення в роботі ІС, тимчасової втрати доступу до даних.
- Якщо хоча б один або більше одного показника КВк, КВц чи КВд дорівнює 3 або 4, то така вразливість вважається **високою.** Може мати значний вплив на медичну

практику, призвести до втрати або компрометації окремих масивів даних, порушень роботи певних ІС.

- Якщо хоча б один або більше одного показника КВк, КВц чи КВд дорівнює 6 чи 9, то така вразливість вважається **критичною**. Це така вразливість, що може мати катастрофічний вплив на медичну практику, призвести до втрати чи компрометації значної кількості медичних записів, зупинці роботи закладу, тривалих порушень в роботі ІС.

4.2.4 **Оцінка небезпеки ризиків** завершує етап оцінки ризиків інформаційної безпеки. При оцінці небезпеки показник інтегрованої оцінки вразливості ІС порівнюється з встановленим на етапі контексту прийнятним рівнем ризику. Якщо показник інтегрованої оцінки вразливості менший або дорівнює прийнятному рівню ризику, такий ризик приймається. Якщо показник вищий прийнятного рівня - ризик підлягає подальшій обробці.

4.3. Обробка ризиків

4.3.1. При обробці ризиків визначаються відповідні заходи безпеки для усунення, мінімізації або приведення до прийнятного рівня ризиків. Основні зусилля зосереджуються на усунені критичних вразливостей притаманних високим ризикам, що значно перевищують прийнятний рівень.

4.3.2. Обробка ризиків починається з найбільш небезпечних ризиків, які пов’язані з високими значеннями КВк, КВц, КВд та послідовно проводиться для усіх ризиків, які на етапі оцінки були вищими за прийнятний рівень ризику.

4.3.3. При обробці ризиків перевага надається таким заходам інформаційної безпеки, які дозволять запобігти ризиків. Це може бути перегляд переліку забороненої діяльності для персоналу закладу з метою впровадження додаткових заходів запобігання ризиків.

4.3.4. Обробка ризиків передбачає модифікацію, збереження, запобігання та передачу ризиків.

4.3.5. Модифікація ризиків

4.3.5.1. При здійсненні модифікації ризиків встановлюються необхідні заходи захисту застосування яких призведе до оцінки залишкового ризику як прийнятного. При модифікації ризиків вибираються виправдані та релевантні заходи захисту, які відповідають вимогам, ~~визначеним~~ на етапах оцінки та обробки ризиків. При цьому треба враховувати:

- яка вартість володіння засобами захисту (з урахуванням впровадження, адміністрування та впливу на ІТ-інфраструктуру);
- фінансові витрати та потреби в персоналі для обслуговування цих засобів захисту;
- вимоги щодо інтеграції з поточними та новими заходами захисту;
- також потрібно порівнювати вартість зазначених витрат з вартістю інформаційного активу, що захищається.

4.3.5.2. При модифікації ризиків можуть розглядатися такі типи захисту: корекція, усунення, запобігання, мінімізація негативного впливу, попередження потенційних порушників, детектування, відновлення, моніторинг та забезпечення обізнаності працівників.

4.3.5.3. Результатом здійснення модифікації ризиків має стати список можливих заходів захисту з їх вартості, визначеними перевагами та послідовністю впровадження.

4.3.5.4. При модифікації ризиків пов'язаних з забезпеченням **конфіденційності** особливу увагу приділяють заходам передбаченим відповідними розділами Політики інформаційної безпеки, а саме:

- антивірусного захисту;
- криптографічного захисту;
- політики чистого столу, чистого екрану;
- забезпечення фізичної безпеки закладу;
- утилізації носіїв інформації, тощо.

4.3.5.5. При модифікації ризиків пов'язаних з забезпеченням **доступності** особливу увагу приділяють заходам ПІБ стосовно:

- управління доступом;
- управління змінами;
- управління вразливостями;
- підключенням до мереж,
- забезпеченням безперервної діяльності, тощо.

4.3.5.6. При модифікації ризиків пов'язаних із забезпеченням **цілісності** даних особлива увага приділяється заходам встановленим Політикою інформаційної безпеки із забезпечення:

- цілісності даних пацієнтів;
- криптографічного захисту;
- антивірусного захисту;
- резервного копіювання;
- аварійного відновлення, тощо.

4.3.6. Збереження ризиків. Збереження ризику означає, що за результатами оцінки небезпеки ризику прийнято рішення, та подальші дії щодо його обробки не потрібні. Тобто, залишковий рівень очікуваного ризику відповідає критерію прийняття ризику.

4.3.7. **Запобігання ризиків.** При запобіганні ризику приймається рішення не вести певну діяльність чи змінити умови її ведення таким чином щоб уникнути ризику, асоційованого з цією діяльністю. Це рішення може бути прийняте у разі високих ризиків або перевищення вартості впровадження заходів захисту над очікуваними перевагами. Наприклад, заклад може відмовитися від надання пацієнтам медичних послуг онлайн, якщо в результаті аналізу вартість усунення ризиків витоку персональної та медичної інформації пацієнтів перевищить вартість впровадження адекватних заходів захисту. Запобігання ризиків повинно бути пріоритетним напрямком реалізації політики управління ризиками ЗОЗ.

4.3.8. **Передача ризиків.** Ризик можна передати третій стороні, яка зможе керувати ним найефективніше. На підставі оцінки ризиків приймається рішення про передачу певних ризиків іншій стороні, яка забезпечить ефективний захист інформаційних активів закладу. Передача ризиків може передбачати:

- страхування кібер-ризиків (можливість отримання компенсації від страхової компанії для усунення негативних наслідків подій, що трапилась в наслідок реалізації ризику);
- передачі обов'язків захисту та технічної підтримки автоматизованих робочих місць підключених до ІС провайдеру послуги, зокрема провайдеру медичної інформаційної системи;

- передачі обов'язків з моніторингу та реагування на інциденти ІБ комерційному чи відомчому операційному центру кібербезпеки (SOC).

При прийнятті рішення про передачу ризику слід врахувати, що третій стороні передається відповідальність управління ризиком, але не самі негативні наслідки можливого інциденту ІБ. Тому, передача ризику потребує точної оцінки ризику та можливих негативних наслідків.

4.4. Прийняття ризиків

4.4.1. Стосовно всього переліку оброблених ризиків керівником закладу приймається управлінське рішення щодо здійснення необхідних заходів з їх обробки, усунення та мінімізації. Визначені заходи включаються до Плану обробки ризиків.

4.4.2. Ризики які неможливо усунути чи мінімізувати приймаються без проведення додаткових заходів. Це означає, що керівництво йде на усвідомлене прийняття наслідків очікуваного ризику.

4.4.3. Всі визначені та оброблені ризики включаються до Карти ризиків закладу, яку затверджує Керівник закладу. Карта типових ризиків інформаційної безпеки закладу охорони здоров’я наведена у Додатку 1.

5. План обробки ризиків інформаційної безпеки

5.1. Після аналізу та оцінки ризиків, при необхідності, уточняється політика інформаційної безпеки закладу з урахуванням нових загроз та плануються конкретні критично важливі заходи безпеки з усунення ризиків. Для цього розробляється План обробки ризиків.

5.2. До Плану обробки ризиків включають всі ризики, які визначені у Карті ризиків та визначають необхідні заходи з усунення або мінімізації кожного визначеного ризика.

5.2. План обробки ризиків включає в себе:

- перелік визначених ризиків, які складають загрозу для ІБ закладу;
- визначення необхідних заходів з усунення та мінімізації ризиків, причому для кожного конкретного ризику визначається конкретний захід з мінімізації або усунення наслідків;
- термін реалізації такого заходу;
- витрати на такий захід та джерело фінансування;
- відповідальна особа за здійснення заходу;
- порядок здійснення заходу;
- попередня оцінка ефективності заходу, яка після його здійснення уточнюється.

5.3. План обробки ризиків складається відповідальним за інформаційну безпеку закладу та затверджується Керівником.

5.4. План обробки типових ризиків закладу охорони здоров’я наведений у Додатку 2.

6. Забезпечення безперервного моніторингу та перегляду ризиків

6.1. Середовища та інформаційні активи закладу можуть змінюватися, що може призвести до виникнення нових вразливостей та загроз. Тому забезпечення безперервного моніторингу та перегляду ризиків є обов'язковою умовою забезпечення сталості управління ризиками інформаційної безпеки.

6.2. Відповідальний за ІБ здійснює оцінку ефективності заходів, зазначених у Плані обробки ризиків та при необхідності забезпечує здійснення повторної оцінки ризиків, яка включає:

- огляди інформаційних активів;
- інтерв'ю користувачів з метою аналізу ефективності заходів;
- перегляд процедур, планів та політики інформаційної безпеки з метою підвищення ефективності управління ризиками;
- аналіз інцидентів безпеки та уточнення вразливостей інформаційних та телекомунікаційних систем;
- уточнення програми навчань з інформаційної безпеки з метою підвищення обізнаності персоналу закладу та його залученості до управління ризиками.

6.3. Для здійснення повторної оцінки ризиків відповідальний за інформаційну безпеку може залучати відповідних працівників закладу та/або зовнішніх експертів при необхідності.

6.4. Повторна оцінка ризиків здійснюється не рідше одного разу на рік або частіше при зміні фізичного, інформаційного середовища і середовища користувачів закладу та виникненні нових ризик-факторів, пов'язаних з цими змінами.

7. Підтримка та покращення процесу управління ризиками

7.1. Контекст, оцінка та План обробки ризиків повинні бути релевантні поточній ситуації та стану захищеності закладу охорони здоров'я. Для цього необхідно здійснювати постійну підтримку та покращення процесу управління ризиками.

7.2. Для ефективності процес управління ризиками інформаційної безпеки інтегрується в життєвий цикл управління інформаційними системами (ІС) закладу. Таким чином досягається найбільш вагомого ефекту з мінімально можливими витратами.

7.3. Процес управління ризиками на кожному з етапів життєвого циклу ІС реалізується таким чином:

- **На етапі ініціації** - відомі ризики враховуються при формуванні вимог до інформаційної системи взагалі і засобів інформаційної безпеки зокрема;
- **На етапі закупівлі (розробки)** - визначені ризики враховано при виборі архітектури рішення;
- **На етапі встановлення** - виявлені ризики враховано при конфігурації, тестуванні і перевірці;
- **На етапі впровадження** - повний цикл управління ризиками стосовно ІС передує впровадженню цієї ІС в експлуатацію;
- **На етапі експлуатації -** управління ризиками супроводжує всі істотні зміни в ІС;
- **При виведенні системи з експлуатації** - управління ризиками допомагає переконатися в тому, що міграція даних відбулася безпечним чином.

7.4. Постійна підтримка та покращення процесу управління ризиками закладу охорони здоров'я здійснюється відповідно наступним вимогам:

- до процесу покращення управління ризиками залучаються всі власники (авторизовані користувачі) інформаційних систем, які потім також інформуються про поточний статус управління ризиками;
- повторно оцінюється ефективність проведеної обробки ризиків;
- контролюються та регулярно переглядаються ризики та сам процес управління ними;
- на основі нової інформації процес управління ризиками безперервно покращується;
- проводиться навчання персоналу та керівництва закладу щодо ризиків та дій для їх мінімізації чи запобігання.

Додатки:

1. Карта ризиків інформаційної безпеки ЗОЗ.
2. План обробки ризиків інформаційної безпеки ЗОЗ.

Додаток 1.

Карта ризиків інформаційної безпеки Закладу

ІД Ризи-ку	**Опис ризику**	**Контек. оцінка ризику в балах**	**Показник КВк, КВд, КВц**
1.	Пошкодження, блокування роботи ІС, порушення цілісності, конфіденційності, доступності інформації в наслідок зовнішніх кібератак.	25	КВк -9, КВц -9, КВд -9
2.	Пошкодження ІС, втрата чутливих даних в наслідок порушень правил та умов експлуатації систем та мереж.	25	КВд – 9, КВц - 9
3.	Навмисні дії персоналу чи підрядників, що призвели до порушення роботи ІС, втраті даних, компрометації облікових записів.	25	КВд - 9, КВк – 9.
4.	Крадіжка конфіденційних даних, порушення цілісності, конфіденційності інформації персоналом або підрядниками.	25	КВц – 9, КВк - 9
5.	Тривали збої в роботі ІС в наслідок припинення електроживлення.	25	КВд – 9, КВц-9
6.	Пошкодження, блокування роботи ІС внаслідок припинення технічної підтримки, несвоєчасного оновлення ПЗ, закінчення ліцензійного періоду експлуатації.	25	КВд – 9, КВц-9
7.	Ненавмисні дії персоналу чи підрядників, що призвели до порушення роботи ІС, часткової втраті даних, компрометації облікових записів.	20	КВд – 6, КВк – 6, КВц- 6
8.	Порушення політики інформаційної безпеки персоналом, підрядниками, що призвело до інциденту ІБ.	16	КВд – 6, КВк – 6, КВц- 6
9.	Пошкодження ІС та ІТ-інфраструктури закладу (в т.ч. серверного обладнання, автоматизованих робочих місць) в наслідок військових дій.	15	КВд – 6, КВк – 6, КВц- 6

10.	Неправильні дії або бездіяльність персоналу під час інциденту ІБ, що призвели до пошкоджень ІС, порушення цілісності, конфіденційності, доступності даних.	15	КВд – 6, КВк – 6, КВц- 6
11.	Тривалі збої в роботі ІС, порушення доступності та цілісності даних в наслідок припинення технічної підтримки підрядниками та провайдерами послуг.	15	КВд – 6, КВц- 6
12.	Пошкодження серверної кімнати, автоматизованих робочих місць лікарів в наслідок стихійного лиха чи повінню.	12	КВд – 6, КВц- 4
13.	Відмова в роботі окремих некритичних інформаційних систем (WiFi мережі або веб-сайту)	9	КВд - 4
14.	Порушення сталості роботи телекомунікаційних каналів та каналів доступу до Інтернет	9	КВд-4

Додаток 2

План обробки ризиків інформаційної безпеки Закладу

ІД	**Опис ризику**	**Захід**	**Термін, Порядок здійснення**	**Джерело, фін.**	**Виконавець**	**Оцінка ефективності**
1	Пошкодження, блокування роботи ІС, порушення цілісності, конфіденційності, доступності інформації в наслідок зовнішніх кібератак.	Закупівля антивірусного програмного забезпечення	Січень поточного року, тендерна закупівля на майданчику Прозоро	На рівні ринкової вартості. Бюджет закладу	Відповідальний за ІБ (ВІБ), Керівник	Ризик зменшено до прийнятного рівня
2	Пошкодження ІС, втрата чутливих даних в наслідок порушень правил та умов експлуатації систем та мереж.	Проведення заняття з персоналом із запобігання вказаного ризику	Лютий поточного року. Плановий тренінг.	Не потребує	ВІБ	Ризик зменшено до прийнятного рівня
3	Тривали збої в роботі ІС в наслідок припинення	Закупівля електрогенератора для резервного енергоживлення	Березень п.р., Тендерна закупівля на майданчику Прозоро	На рівні ринкової вартості. Бюджет закладу	Керівник	Ризик усунуто

	електроживлення.					
4	Навмисні дії персоналу чи підрядників, що призвели до порушення роботи ІС, втраті даних, компрометації облікових записів.	Проведення ретельного вивчення особових справ персоналу та репутації контрагентів	На постійній основі відділом кадрів	Не потребує	Начальник кадрового відділу Закладу та ВІБ	Ризик зменшено до прийнятного рівня
5	Крадіжка критичних даних, порушення цілісності, конфіденційності інформації персоналом або підрядниками.	Проведення ретельного вивчення особових справ персоналу та репутації контрагентів	На постійній основі відділом кадрів	Не потребує	Начальник кадрового відділу Закладу та ВІБ	Ризик зменшено до прийнятного рівня
6	Пошкодження, блокування роботи ІС внаслідок припинення технічної підтримки, несвоєчасного оновлення ПЗ, закінчення ліцензійного періоду експлуатації.	Запровадження чи продовження договорів на технічну підтримку, продовження підписки на ліцензійне ПЗ	Квітень п.р., Тендерна закупівля на майданчику Прозоро	На рівні ринкової вартості. Бюджет закладу	ВІБ	Ризик зменшено до прийнятного рівня
7	Ненавмисні дії персоналу чи підрядників, що призвели до порушення роботи ІС, втраті даних, компрометації облікових записів.	Проведення тренінгів з інформаційної безпеки. Перегляд графіку роботи лікарів з метою більш збалансованого розподілу навантаження.	На постійній основі відділом кадрів	Не потребує	Керівник, ВІБ	Ризик зменшено до прийнятного рівня
8	Порушення політики інформаційної безпеки персоналом, підрядниками,	Проведення інструктажів з персоналом та підрядниками щодо дотримання політики ІБ	На постійній основі відповідальним з ІБ	Не потребує	ВІБ	Ризик зменшено до прийнятного рівня

	що призвело до інциденту ІБ.					
9	Пошкодження ІС та ІТ-інфраструктури закладу (в т.ч. серверного обладнання, автоматизованих робочих місць) в наслідок військових дій.	Заходи з усунення ризику значно перевищують наслідки ризику. Ризик приймається.	На період ведення військових дій.	Не потребує	Керівник Закладу	Ризик приймається
10	Тривалі збої в роботі ІС, порушення доступності даних в наслідок припинення технічної підтримки підрядниками та провайдерами послуг.	Закладання в договори з підрядниками та провайдерами положень щодо компенсації ризиків	На період дії договору.	Не потребує	юрист Закладу	Ризик зменшено до прийнятного рівня
11	Неправильні дії або бездіяльність персоналу під час інциденту ІБ, що призвели до пошкоджень ІС, порушення цілісності, конфіденційності, доступності даних.	Проведення тренінгів з персоналом з порядку дій під час інциденту ІБ	На періодичній основі відповідальним з ІБ	Не потребує	ВІБ	Ризик зменшено до прийнятного рівня
12	Пошкодження серверної кімнати, автоматизованих робочих місць лікарів в наслідок стихійного лиха чи повінню.	Заходи з усунення ризику значно перевищують наслідки ризику. Ризик приймається.	На періодичній основі.	Не потребує	Керівник	Ризик приймається
13	Відмова в роботі окремих некритичних інформаційних систем (WiFi	Передача ризику третій стороні.	Травень п.р. тендерна закупівля послуг з підтримки веб-сайту	На рівні ринкової вартості. Бюджет закладу	ВІБ	Ризик передано третій стороні

	мережі або веб-сайту)		(WiFi мережі) на майданчику Прозоро			
14	Порушення сталості роботи телеком. каналів та каналів доступу до Інтернет	Заключення договорів на отримання послуг зв'язку з двома різними провайдерами послуг	Червень п.р. тендерна закупівля послуг зв'язку у резервного провайдера на майданчику Прозоро	На рівні ринкової вартості. Бюджет закладу	ВІБ	Ризик зменшено до прийнятного рівня