Повторення питань біозахисту

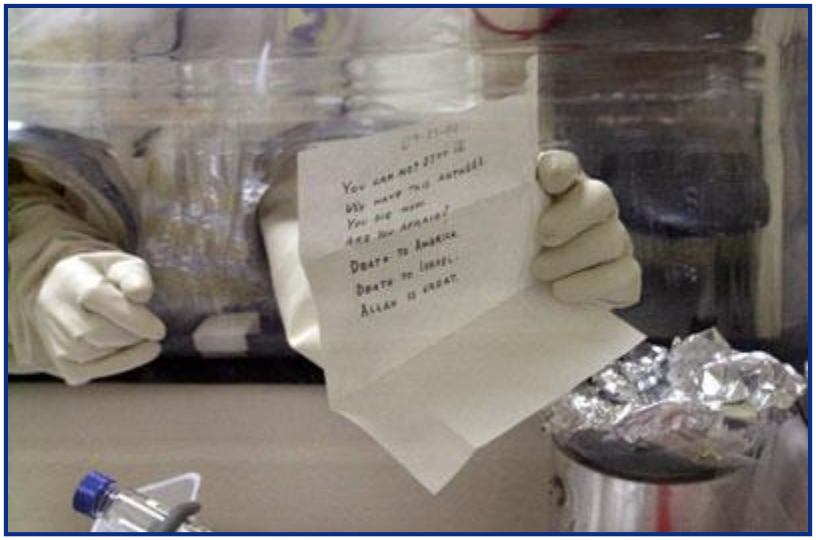
Курс № LM10-T06

Цілі

- Після завершення цього повторного модуля учасники зможуть:
  - Давати визначення поняттю управління біологічними ризиками
  - Обговорювати спільні та відмінні риси біобезпеки та біозахисту
  - Обговорювати програми біозахисту та процес й особливості їх створення
  - Обговорювати оперативний захист (OPSEC)
  - Давати визначення дослідження подвійного призначення
  - Пояснювати поняття обізнаності з питань захисту
  - Надавати приклади заходів, спрямованих на подолання ризиків у сфері біозахисту

Особливо небезпечні патогени

- Унікальна природа особливо небезпечних патогенів вимагає вжиття заходів із захисту
- Листи із сибіркою в Сполучених Штатах у жовтні 2001 р. у повній мірі показали загрозу
- Проблеми, пов'язані із такою загрозою, є спільними для всіх біологічних лабораторій у світі, що працюють з ОНП



Автор фото: Sandia National Laboratories

Приклади інших цінних біологічних матеріалів

- Колекції і референс штами
- Біологічні токсини
- Вакцини та інші фармацевтичні продукти
- Харчові продукти
- Генетично модифіковані організми
- Позаземні зразки
- Клітинні компоненти та генетичні елементи
- Радіоактивні біологічні сполуки

Джерело: WHO Biorisk management: Laboratory biosecurity guidance, September 2006

Управління біологічними ризиками

- Управління біологічними ризиками – це цілісний підхід до забезпечення безпеки та захисту працівників і матеріально-технічної бази лабораторій, а також широкого загалу.
- Охоплює практики із забезпечення біобезпеки та біозахисту
  - Біобезпека спрямована на забезпечення захисту працівників, матеріально-технічної бази та громади від використовуваних біологічних матеріалів.
  - Біозахист спрямований на недопущення потрапляння цінних біологічних матеріалів та інформації, пов'язаної з ними, у розпорядження осіб, що можуть зловживати ними.

Біобезпека та біозахист

Спільні цілі

- Фізичний захист
- Контроль за матеріалами та підзвітність
- Надійність персоналу
- Перевезення матеріалів

Потенційні конфлікти

- Заходи реагування на надзвичайні ситуації
- Інформаційні вказівники
- Контроль за доступом до лабораторій
- План об'єкта

Практики та процедури на об'єкті повинні забезпечувати баланс між біобезпекою та біозахистом у разі виникнення конфліктів між ними.

Лабораторний біозахист сприяє лабораторній біобезпеці

- Безпечні та захищені лабораторії допомагають:
  - Забезпечувати ізоляцію небезпечних інфекційних речовин в лабораторіях
  - Зберігати впевненість громадян у діяльності громади дослідників у царині біологічних наук
  - Покращувати прозорість для інвесторів у галузі біомедицини та біотехнологій
  - Захищати цінні дослідницькі та комерційні активи
  - Знизити ризик злочинів та біотероризму

Біозахист – відповідальність кожного

Цілі програми біозахисту

- Здійснювати безпечні операції з небезпечними матеріалами.
- Набрати надійний персонал.
- Створити захищене середовище.
- Запровадити політики та процедури у сфері біозахисту, що є релевантними та можуть бути реалізовані

Приклад: розробка програми біозахисту на основі результатів оцінки ризику

1. Визначити та пріоритизувати цінні біологічні матеріали
   - Що є в наявності? Які є можливі шляхи використання не за призначенням?
2. Ідентифікувати та пріоритизувати загрозу цінним біологічним матеріалам
   - Внутрішня загроза; зовнішня загроза; засоби, мотиви та можливість
3. Проаналізувати ризик тих чи інших випадків порушення захисту
4. Розробити відповідну програму з біобезпеки
5. Регулярно здійснювати повторну оцінку принципів протидії ризикам та цілей щодо захисту установи

Джерело: CDC. *BMBL 5th edition*

Спільні елементи програм біозахисту

- Чітко визначене управління програмою
- Фізичний захист – контроль доступу та моніторинг
- Управління персоналом
- Матеріально-технічні ресурси та підзвітність
- Інформаційна безпека (операційна безпека)
- Транспортування цінних біологічних матеріалів
- Плани реагування на травматизм та інциденти
- Звітування та комунікація
- Профпідготовка та тренінгові заходи
- Оновлення та повторна оцінка принципів і стратегій захисту
- Керівні принципи щодо роботи з вибраними збудниками/ особливо небезпечними патогенами

Джерело: CDC. *BMBL 5th edition*

Внутрішня загроза

- Штатні працівники становлять принципову загрозу безпеці установи
- Ризик, який створюють ті, хто працює в установі, зазвичай недооцінюють
- Несанкціоновані дії можуть становити загрозу безпеці та захисту усієї установи

Приклади несанкціонованих дій

- Зумисне приховування контейнерів або пробірок із ОНП
- Приховане винесення ОНП з лабораторії
- Надання неуповноваженим особам доступу до зон із обмеженим доступом
- Внесення змін до записів та обладнання
- Проведення несанкціонованих експериментів з використанням ОНП
- Здійснення маніпуляцій з ОНП поза межами відповідних лабораторій
- Несанкціоноване поширення даних про ОНП

Операційний захист

- Біологічні зразки – тільки один із продуктів біологічних досліджень.
- Іншим основним продуктом дослідницької діяльності є інформація.

Операційний захист – це процес визначення, контролю та захисту інформації, якою можуть скористатися конкуренти чи противники на шкоду вам.

- Операційний захист зосереджений на ненаданні конкурентові чи противникові доступу до інформації, яку ви бажаєте захистити від зловживань.

Загрози та противники

- Фізичні особи, організації або країни
- Загроза вимірюється наміром та здатністю використовувати вразливості та отримувати бажану інформацію
- Методи збору інформації можуть охоплювати увесь діапазон від дешевих та нетехнологічних до дорогих та високотехнологічних

П'ятикроковий процес забезпечення операційного захисту

Операційний захист – визначити інформацію

- **Що ви намагаєтеся захистити?**
  - Власний продукт чи процес?
  - Інтелектуальний капітал?
  - Персональну інформацію?
  - Професійну чи державну таємницю?

- У залежності від того, що ви хочете захистити, обираються відповідні методи захисту.

Джерела інформації

- Інформація в загальному доступі
  - Веб-сайти
  - Маркетингова інформація
- Люди
  - Балакучі працівники, які не знають, що їх використовують
  - Загроза від штатних працівників
  - Соціальні мережі

- Сміттєві баки та смітники
  - Транспортні документи та етикетки
  - Викинуті документи та записи лабораторії
- Високотехнологічні
  - Електронне прослуховування
  - Комп'ютерні віруси
  - Зламані акаунти електронної пошти

Політика установи щодо операційного захисту

- Визначає типи службової інформації
  - Збір патогенів
  - Розміщення зразків
  - Особливості та можливості установи
  - Обладнання
  - Персонал
- Визначає рівень захисту, необхідний для кожного типу службової інформації
- Описує політики та процедури захисту службової інформації
- Працівникам необхідно періодично проходити навчання з питань політики та процедур операційного захисту

Біозахист та структура експерименту

- Оцінка ризиків у сфері біозахисту повинна проводитися в комплексі з оцінкою ризиків у сфері біобезпеки.
- До запитань, які слід взяти до уваги, відносяться наступні:
  - Чи потрібно обмежувати доступ до лабораторії?
  - Для кого слід обмежити доступ до лабораторії?
  - Яким чином буде обмежено доступ до лабораторії?
  - Яким чином буде забезпечено захист біологічних зразків?
  - Яким чином будуть захищені дані?
  - Чи може запропонована робота вважатися «роботою подвійного призначення»?

Дослідження подвійного призначення

- Визначення: «дослідження, в результаті якого можуть бути створені знання, продукти або технології, що можуть бути використані з метою завдання шкоди громадському здоров'ю або національній безпеці». (Національна наукова консультаційна рада з питань біозахисту США)
- Рекомендується здійснювати додатковий контроль за виконанням робіт
  - Ризики у сфері біозахисту щодо потенціалу дослідження подвійного призначення повинні брати до уваги комітети або комісії, що здійснюють затвердження експериментів

Обізнаність в питаннях захисту

- Для забезпечення ефективності біозахисту необхідно запровадити культуру обізнаності в питаннях біозахисту

Обізнаність щодо біозахисту = визнання проблемних питань у сфері захисту + вжиття відповідних заходів реагування

- Біозахист – відповідальність кожного
- Кожен має розуміти проблемні питання у сфері захисту, які стосуються установи, та те, яким чином необхідно реагувати на них
- Двостороння комунікація між усіма рівнями персоналу відіграє визначальну роль

Складові обізнаності з питань захисту

Заходи реагування на інциденти

- Швидке, ефективне реагування на тривожні сигнали, проблеми контролю доступу та інші проблеми
- Координація заходів реагування із зовнішніми силами реагування
- Чітко визначені та повідомлені заходи реагування на порушення захисту

Служба безпеки установи

- Високопрофесійна
- Залучена до планування в установі
- Регулярно проводить навчання щодо захисту та реалізує заходи й програми у сфері підвищення обізнаності
- Підтримує зв'язок з відповідними компетентними органами

Відновлення після інцидентів

- Прийняті плани відновлення у відповідь на порушення захисту, стихійні лиха, крадіжки матеріалів, даних тощо.
- Запроваджені механізми розробки планів коригувальних дій за необхідності

Комунікація

- Між працівниками та керівництвом установи
- Із службою безпеки установи
- Зі службами швидкого реагування
- Із Міністерством внутрішніх справ
- Із правоохоронними органами
- Із громадою

Приклади заходів із протидії ризикам у сфері біозахисту

Біозахист в лабораторії

Операційний захист
- Навчання персоналу
- Обмеження кола осіб користування службовою інформацією тими, кому «необхідно знати»
- Захист інформації на електронних та паперових носіях

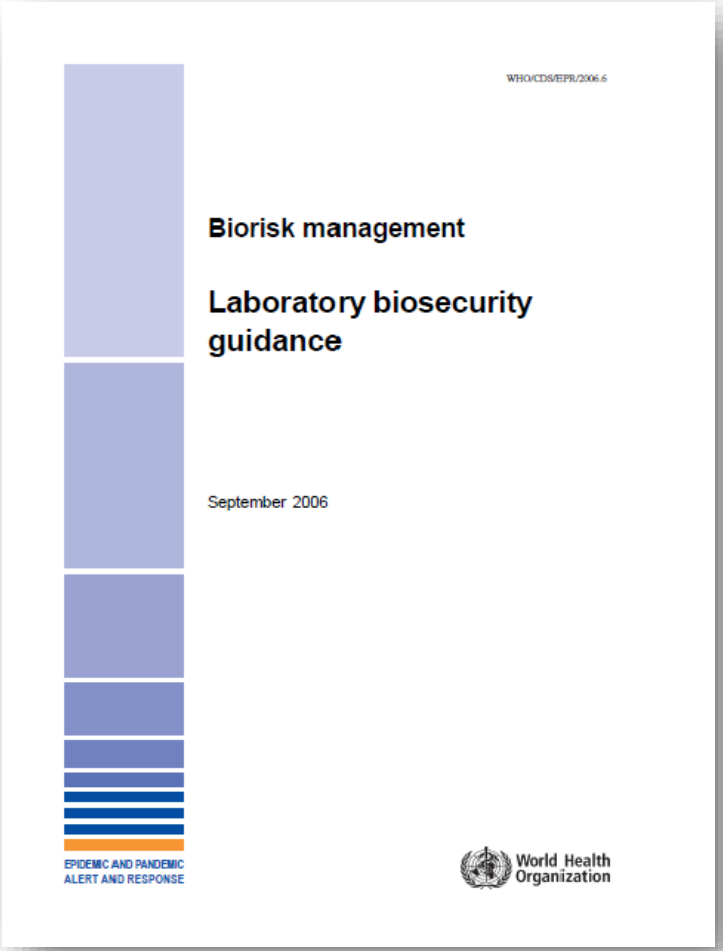
Фізичний захист
- Обмежений доступ
- Внутрішній/зовнішній моніторинг та реагування
- Сповіщення про вторгнення та моніторинг
- Випадкові пошукові операції та перевірки
- Подвійні замки на контейнерах із ОНП

Надійність персоналу
- Комплексна спеціальна перевірка
- Медичний скринінг
- Постійний нагляд за поведінкою
- Випадкові скринінгові перевірки на алкоголь/наркотичні речовини
- Періодичні повторні перевірки

Підзвітність
- Обмежений доступ до ОНП
- Реєстрація ОНП
- Зазначення місцезнаходження ОНП
- Запровадження правила роботи в парі
- Наскрізна підзвітність щодо ОНП
- Записи аудиторських перевірок, які можна прослідкувати

Джерела додаткової інформації

- Публікації ВООЗ з теми управління біоризиками: http://www.who.int/ihr/publications/biosafety/en/index.html
- Національна наукова консультативна рада США з питань біозахисту: http://oba.od.nih.gov/biosecurity/about_nsabb.html
- CDC *Біобезпека в мікробіологічних і біомедичних лабораторіях*, 5-те видання, розділ VI



Резюме

- Біозахист спрямований на захист біологічних агентів та пов'язаної з ними інформації від потрапляння їх у розпорядження осіб, котрі можуть використати їх не за призначенням
- Біозахист реалізується у комплексі з біобезпекою в рамках процесу управління біоризиками
- До основних етапів забезпечення ефективної практики біозахисту в лабораторії відносяться наступні:
  - Розробка та реалізація плану управління захистом/операційного плану
  - Розробка та впровадження політик операційного захисту
  - Сприяння формуванню культури обізнаності у сфері захисту
  - Запровадження належних заходів протидії біоризикам
- Біозахист – відповідальність кожного!

ЗАПИТАННЯ?