Аннотация – в статье "Human Factors in Biocybersecurity Wargames" подчёркивается необходимость понимания уязвимостей при обработке биологических препаратов и их пересечения с кибернетическими и киберфизическими системами. Это понимание необходимо для обеспечения целостности продукта и бренда и обслуживания ИТ-систем.

I. Введение

A. Влияние био-обработки:

- Био-обработка охватывает весь жизненный цикл биосистем и их компонентов, от начальных исследований до разработки, производства и коммерциализации.
- Она вносит значительный вклад в мировую экономику, применяясь в производстве продуктов питания, топлива, косметики, лекарств и экологически чистых технологий.

B. Уязвимость трубопроводов для биопереработки:

- Конвейер био-обработки подвержен атакам на различных этапах, особенно там, где оборудование для био-обработки подключено к Интернету.
- Уязвимости требуют тщательного контроля при проектировании и мониторинге трубопроводов для биопереработки для предотвращения воздействий.

C. Роль информационных технологий (ИТ):

- Прогресс в био-обработке все больше зависит от автоматизации и передовых алгоритмических процессов, требующих значительного участия ИТ.
- Расходы на ИТ значительны и растут параллельно с ростом био-обработки.

D. Методологии:

- Внедрение open-source методологий привело к значительному росту развития коммуникаций и цифровых технологий во всем мире.
- Этот рост ещё более ускоряется благодаря достижениям в области биологических вычислений и технологий хранения данных.

E. Потребность в новых знаниях:

- Интеграция технологий биокомпьютинга, био-обработки и хранения данных потребует новых знаний в области эксплуатации (взлома), защиты.
- Основные меры защиты данных и процессов остаются критически важными, несмотря на технический прогресс.

F. Важность «игр»:

- Для управления инфраструктурой био-обработки и обеспечивать её безопасность, ИТ необходимо использовать игры для моделирования возможных рисков и устранения их последствий.
- Симуляции направлены на подготовку организаций к устранению уязвимостей.

II. Особое значение биокомпонента в биокибербезопасности

A. Эволюция биологических процессов:

- Биологические процессы являются неотъемлемой частью различных функций, таких как блокировки (например, сканеры сетчатки глаза и отпечатков пальцев), принятие решений (например, мониторы состояния здоровья) и даже сами методы обработки данных (например, биокомпьютеры).

B. Биологические явления в кибербиобезопасности:

- Биологические явления могут служить связующими звеньями и вспомогательными шагами в рамках систем кибербезопасности. Такая интеграция открывает множество потенциальных объектов для использования, от простых форм поведения организмов до свойств органических соединений.

C. Мониторинг и таргетирование:

- Возможность контролировать транспортировку биомолекул внутри организмов или между ними и нацеливаться на конкретные гены как на макро-, так и на микроуровне.

D. Прогностический анализ:

- Страховые компании могут использовать геномные данные для установления тарифов на основе прогнозируемых заболеваний.

E. Биокомпьютинг и био-обработка:

- Инфраструктура био-обработки все больше полагается на биокомпьютеры, поэтому необходимо будет изучать биологические системы аналогично тому, как они изучают цифровые системы.
- ДНК может использоваться для кодирования для атаки на оборудование, взаимодействующее с трубопроводами для переработки биоматериалов, или как средство контрабанды.

F. Необходимость тщательного обследования:

- Отсутствие строгого дизайна и протокола имеет последствия для организации, поэтому необходимо

проводить исследования для выявления уязвимостей и смягчения их последствий.

III. Игровой симулятор

A. Предварительные шаги

- **Отбор**: выбор эксперта, разбирающегося в кибербезопасности и навыках межличностного общения, для проведения игрового мероприятия.
- **Обзор**: анализ текущих процедур обеспечения безопасности и оценка участников, таких как незащищённые устройства или ненадлежащее использование паролей.

B. Шаг 1 - Тренировка

- Разделение на команды "защитников" и "хакеров".
- Хакер обнаруживает уязвимость, и защитник её исправляет (например, вредоносные USB-накопители и отключение USB-портов).
- Смена ролей каждые 5–10 минут.

C. Шаг 2 - Групповое формирование идей

- Разработка стратегий защиты от уязвимостей.
- Разработка эксплойтов, нацеленных на уязвимости объекта.
- Выделение времени для обдумывания идей.

D. Шаг 3 – игровой процесс

- Группа хакеров объявляет о плане эксплойта.
- Группа защитников в ответ предлагает стратегию смягчения последствий.
- Этот ответ продолжается до тех пор, пока не зайдёт в тупик или не закончится время.
- Активность регистрируется для анализа слабых мест и потенциальных улучшений безопасности.

IV. Оценка эффективности

A. Выявлены распространенные случаи использования:

- **Неэффективность систем безопасности**: Меры безопасности, которые являются скорее показными, чем реальной защитой, могут быть неэффективными и пригодными для использования.
- **Низкооплачиваемые сотрудники**: Работники, не получающие адекватной компенсации, могут представлять угрозу безопасности.
- **Недопонимание традиционных угроз безопасности**: часто возникают недопонимания относительно традиционных угроз безопасности.
- **Недостаточная осведомлённость о новых угрозах**: Персонал может быть недостаточно осведомлён о новых и зарождающихся угрозах.

B. Пробелы в знаниях:

- В фирмах, занимающихся операциями по био-переработке, существуют значительные пробелы в знаниях персонала, ввиду отсутствия непрерывного образования и профессиональной подготовки.

C. Важность смены ролей и постоянного обновления:

- Участники должны меняться ролями и быть в курсе новых тенденций в области био-кибербезопасности, кибербезопасности и биозащиты

D. Частота и вариации игр:

- Необходима регулярность, чтобы персонал тренировался и был осведомлён о потенциальных опасностях. Стиль и порядок работы wargaming могут варьироваться в соответствии с организационными потребностями.

E. Исследование сложных сценариев:

- Предлагается изучить игры с участием нескольких противостоящих групп, таких как действующие лица государственного уровня, корпоративные действующие лица, внутренние действующие лица и этичные хакеры. Это обеспечит более полное понимание потенциальной динамики безопасности.

F. Общая судьба информационных технологий и био-обработки:

- ИТ и биопроцессы все более взаимосвязанны, как умственные, так и физические операции должны отражать это общее предназначение для обеспечения оптимальной безопасности.

V. Важность и выводы

- **Динамичная разработка**: Стремительный прогресс в биологии и био-обработке требует постоянных совместных усилий по безопасности.
- **Разнообразные требования и инструменты**: Разные лаборатории предъявляют разные требования, инструменты, кибер-физические взаимодействия и обходные пути, которые влияют на их конкретные потребности в безопасности.
- **Уязвимость лабораторий с низким уровнем финансирования**: Лаборатории с меньшим объёмом финансирования более восприимчивы к традиционным методам проникновения из-за ограниченных ресурсов.
- **Атаки на хорошо финансируемые лаборатории**: Лаборатории со значительным финансированием могут быть специально атакованы из-за их ценных активов и исследований.
- **Неполные цепочки поставок**: исследовательские учреждения не имеют полной сквозной цепочки поставок, что делает их уязвимыми для эксплуатации в различных точках взаимодействия.
- **Необходимость обеспечения комплексной безопасности**: Достижение комплексного обеспечения безопасности требует представительства и сотрудничества со стороны всех инвестируемых групп в рамках объекта.