КИБЕР-ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ: НОВАЯ ГИГИЕНА ТРУДА

Доклад для круглого стола «Безопасность труда в эпоху цифровых технологий: интеграция науки, практики и управления»

Эпоха подключенного работника

СМЕНА ПАРАДИГМЫ ОХРАНЫ ТРУДА

Традиционный подход

- **Пассивные** средства индивидуальной защиты (СИЗ)
- **Реактивное** реагирование на инциденты
- **Изолированные** рабочие места

Индустрия 4.0

- **Активные** цифровые экосистемы защиты
- Концепция «подключенного работника» (Connected Worker)
- **Интеграция** IoT в производственные процессы

ТЕХНОЛОГИЧЕСКИЙ СТЕК «ПОДКЛЮЧЕННОГО РАБОТНИКА»

Умные СИЗ

Каски с датчиками, умные жилеты и **браслеты** мониторинга состояния.

Экзоскелеты

Физическая поддержка с программным **управлением** и датчиками нагрузки.

Нейромониторинг

Видеоаналитика и контроль концентрации **внимания** в реальном времени.

ДАННЫЕ КАК ИНСТРУМЕНТ ЗАЩИТЫ И ИСТОЧНИК РИСКА

Возможности защиты

- Мониторинг усталости, пульса и температуры в реальном времени.
- Проактивное предотвращение тепловых ударов и переутомления.
- Автоматическое оповещение при критических показателях здоровья.

Риски конфиденциальности

- Утечка конфиденциальных медицинских и биометрических данных.
- Риск использования данных для дискриминации сотрудников.
- Психологическое давление из-за тотального мониторинга.

КОГДА КОД СТАНОВИТСЯ УГРОЗОЙ: УЯЗВИМОСТИ СИСТЕМ

Взлом систем управления

Несанкционированный доступ к экзоскелетам или роботам может привести к неконтролируемым движениям и травмам.

Искажение данных мониторинга

Манипуляция показаниями датчиков создает ложное чувство безопасности при наличии реальной угрозы.

Отказ критически важного ПО

Программные сбои в момент опасности превращают средства защиты в ловушки или источники дополнительного риска.

Киберугрозы трансформируются в реальные производственные риски, требуя новых подходов к **техносферной** безопасности.

АНАТОМИЯ КИБЕР-ФИЗИЧЕСКОГО ИНЦИДЕНТА

Цифровой слой

Программный сбой, уязвимость **или** кибератака на контроллер **устройства**.

Ошибка логики

Передача некорректной **команды** исполнительному **механизму** (экзоскелету).

Физический акт

Неконтролируемое движение или **отказ** системы блокировки в **опасной** зоне.

Последствие

Реальная производственная **травма**, вызванная ошибкой в **коде**.

Расследование инцидентов теперь требует компетенций на стыке ИТ и охраны труда.

ЧЕЛОВЕЧЕСКИЙ ФАКТОР В ЦИФРОВОЙ СРЕДЕ

Когнитивная перегрузка

Избыток уведомлений, данных и сигналов от умных устройств рассеивает **внимание** работника.

Цифровая усталость

Снижение концентрации из-за постоянного ощущения «подключенности» и **мониторинга**.

Избыточное доверие

Делегирование бдительности алгоритмам («система подскажет»), что ведет к **потере** контроля.

Риск деградации базовых навыков **самосохранения** и снижения личной **ответственности** за безопасность.

ЭТИКА И ПРИВАТНОСТЬ В ЦИФРОВОЙ ОХРАНЕ ТРУДА

Границы мониторинга

Определение пределов сбора биометрических данных: **только** то, что критично для безопасности жизни.

Право на «отключение»

Возможность работника временно выходить из системы **мониторинга** в нерабочее время или во время перерывов.

Прозрачность алгоритмов

Работник должен понимать, как ИИ оценивает его риски и **какие** решения принимаются на основе его данных.

Защита от дискриминации

Запрет на использование данных о здоровье для оценки **эффективности** или принятия кадровых решений.

БЕЗОПАСНОСТЬ НЕ ДОЛЖНА ДОСТИГАТЬСЯ ЦЕНОЙ ТОТАЛЬНОЙ ДЕГУМАНИЗАЦИИ ТРУДА.

КОНЦЕПЦИЯ «КИБЕР-ФИЗИЧЕСКОЙ ГИГИЕНЫ»

Безопасность требует новых протоколов поведения, где цифровая гигиена становится неотъемлемой частью **техносферной** безопасности.

Цифровая чистота

Регламенты обслуживания умных СИЗ, своевременное **обновление** ПО и контроль состояния датчиков.

Zero Trust Architecture

Принцип «нулевого доверия»: проверка каждого действия **системы** и авторизация изменений параметров.

Кибер-грамотность

Обучение персонала пониманию алгоритмов защиты и **распознаванию** цифровых аномалий.

Интеграция в культуру ОТ

Слияние ИТ-безопасности с классическими инструктажами и **практиками** охраны труда.

СТРАТЕГИЧЕСКИЙ АЛГОРИТМ СИНЕРГИИ ИТ И ОТ

01

Совместный аудит

Выявление точек пересечения цифровых **уязвимостей** и физических рисков на **рабочих** местах.

02

Единые протоколы

Разработка регламентов реагирования на **инциденты**, объединяющих ИТ-**безопасность** и охрану труда.

03

Двойной контроль

Внедрение систем верификации **критических** действий: алгоритмический **мониторинг** + человек.

Объединение компетенций — залог защиты жизни в условиях цифровой прозрачности.

БУДУЩЕЕ: ОТ КОНТРОЛЯ К ИНТЕЛЛЕКТУАЛЬНОЙ ПОДДЕРЖКЕ

Предиктивная аналитика

Прогнозирование рисков на основе Big Data и предотвращение инцидентов до их возникновения.

Адаптивные системы

Средства защиты, которые подстраиваются под текущее психофизическое состояние конкретного работника.

Коллективный иммунитет

Единая интеллектуальная сеть предприятия, мгновенно реагирующая на любые кибер-физические аномалии.