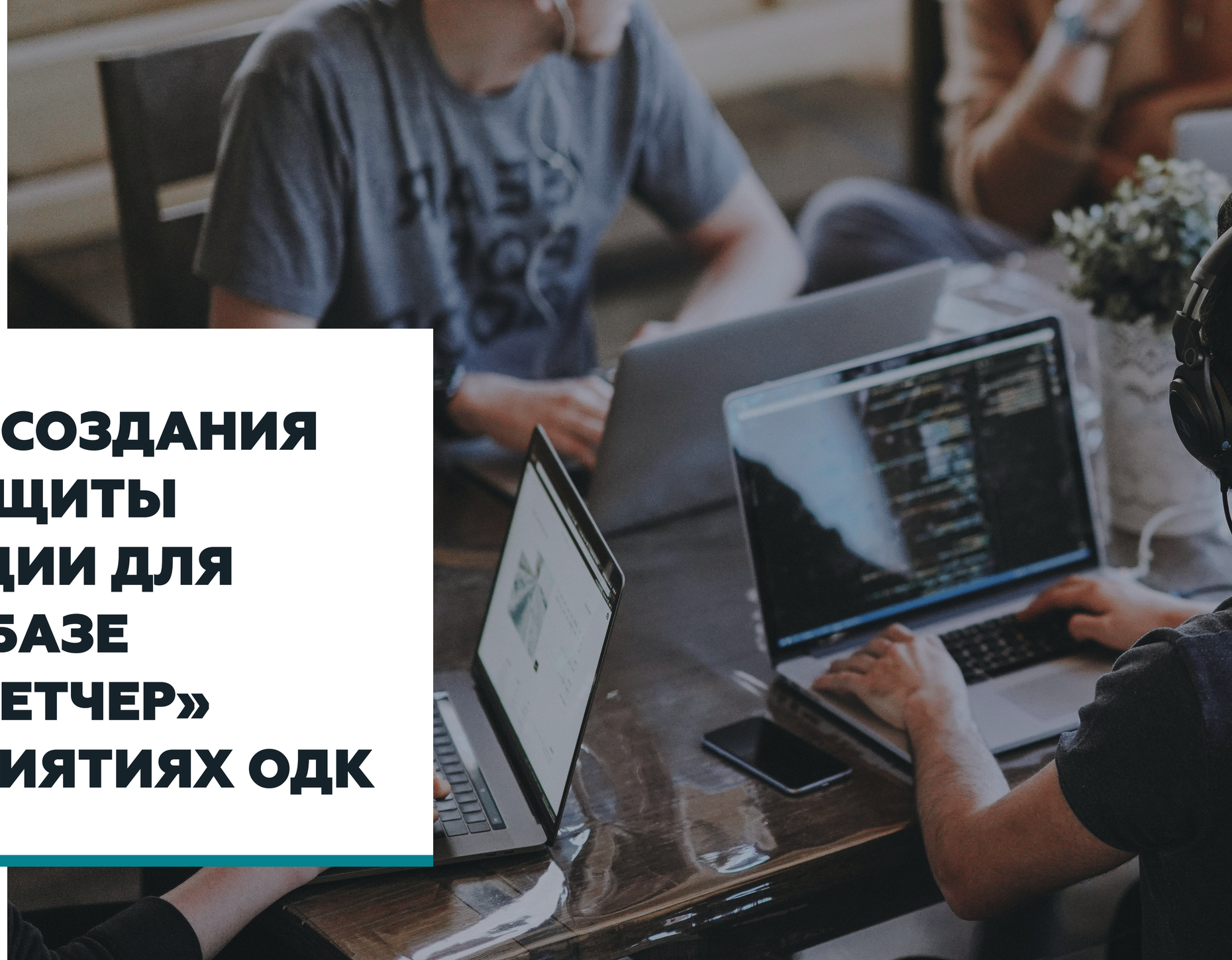
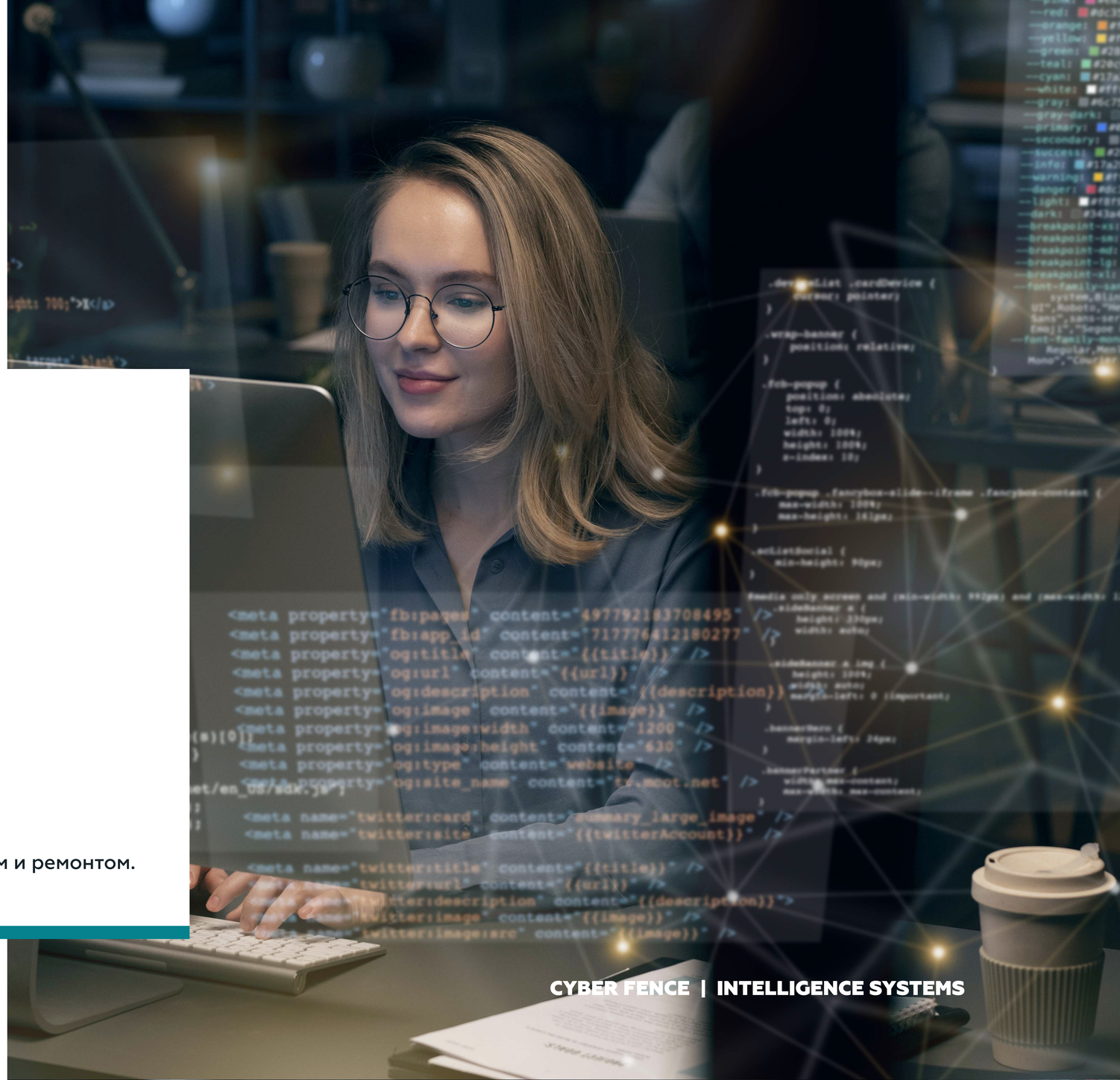
CYBER FENCE
INTELLIGENCE SYSTEMS

ПРАКТИКА СОЗДАНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ АСУ ТП НА БАЗЕ АИС «ДИСПЕТЧЕР» НА ПРЕДПРИЯТИЯХ ОДК



АИС «ДИСПЕТЧЕР» ЯВЛЯЕТСЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМОЙ МОНИТОРИНГА И ДИАГНОСТИКИ ТЕХНИЧЕСКОГО СОСТОЯНИЯ СТАНКОВ С ЧПУ И ОБРАБАТЫВАЕТ СЛЕДУЮЩУЮ ИНФОРМАЦИЮ:

- Техническое состояние оборудования;
- Время работы и простоев оборудования, причины;
- Идентифицирующая информация персонала;
- Коэффициенты загрузки и готовности оборудования;
- Время выполнения технологических операций;
- **Управляющие программы;**
- Данные с многоканальных систем ЧПУ;
- Маршрутные карты, сменно-суточные задания;
- Планы и типы ремонтных работ сервисно-ремонтных служб;
- Данные системы управления технологическим оборудованием и ремонтом.



ЦЕЛЯМИ ВНЕДРЕНИЯ АИС ДИСПЕТЧЕР НА ПРЕДПРИЯТИЯХ ОПК И СОЗДАНИЯ СООТВЕТСТВУЮЩИХ СИСТЕМ ЗАЩИТЫ ЯВЛЯЛИСЬ:

01

Оценка и повышение эффективности работы производственных цехов за счет определения фактического значения и дальнейшего повышения эффективности использования станочного оборудования и производственного персонала;

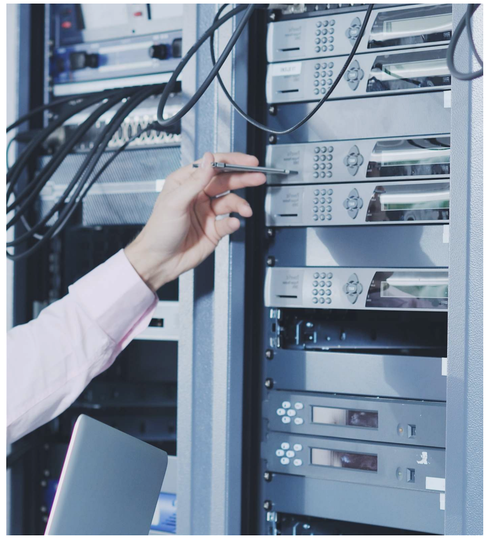
02

Обеспечение целостности, конфиденциальности и доступности защищаемой информации.

АИС ДИСПЕТЧЕР КАК ОБЪЕКТ ЗАЩИТЫ:

- Локальная информационная система с автоматизированными рабочими местами операторов и сервером, расположенными внутри одной контролируемой зоны;
- При выполнении своих функций АИС взаимодействует между своими компонентами и не имеет прямого выхода в Интернет;
- Многопользовательский режим доступа с разграничением прав доступа;
- Как правило соответствует третьему К3 классу защищенности, уровень значимости (критичности) информации – низкий (УЗ 3), степень возможного ущерба – низкая;
- Является объектом КИИ, как правило, 3 (третьей) категории значимости.

АИС ДИСПЕТЧЕР КАК ОБЪЕКТ ЗАЩИТЫ:

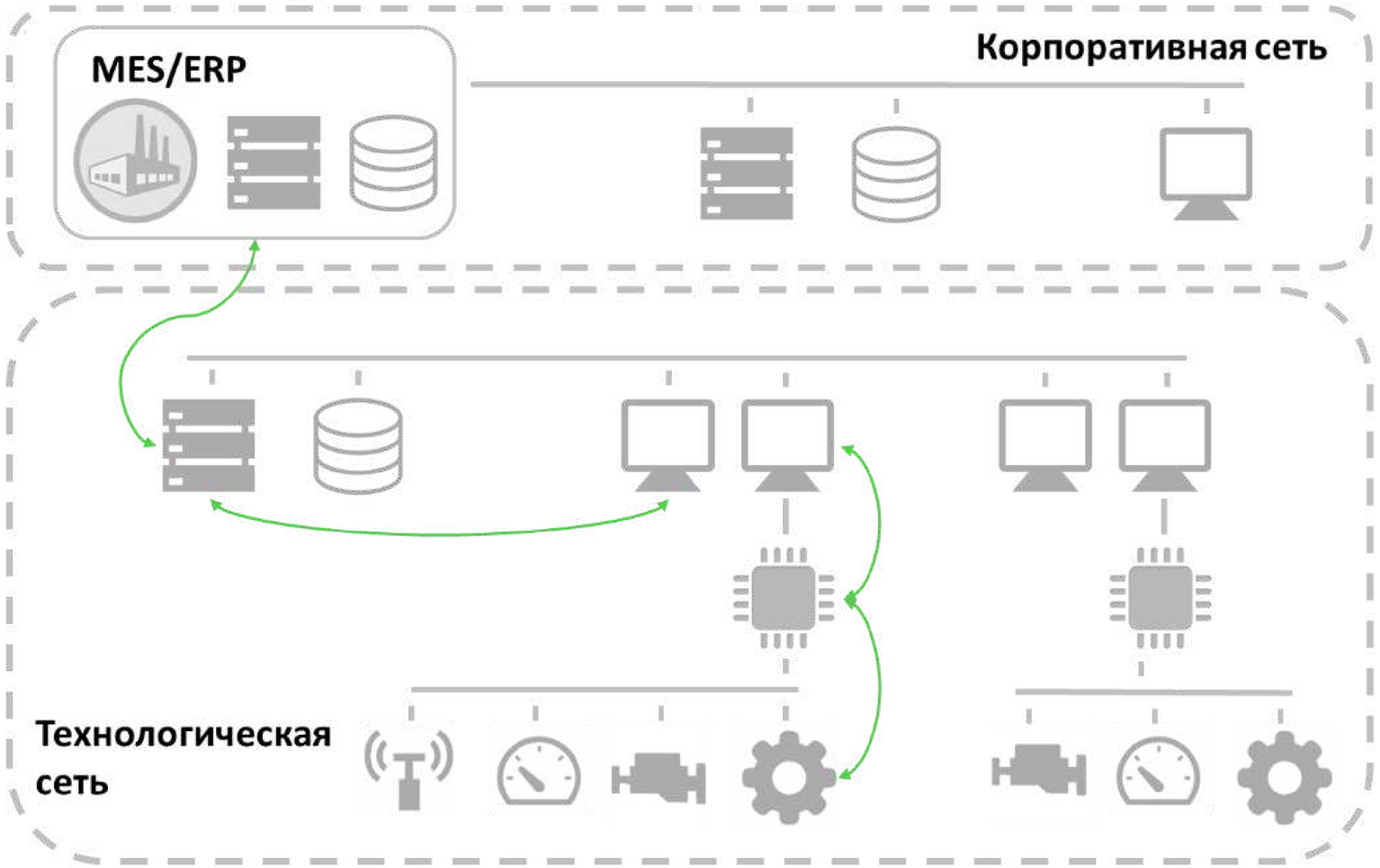


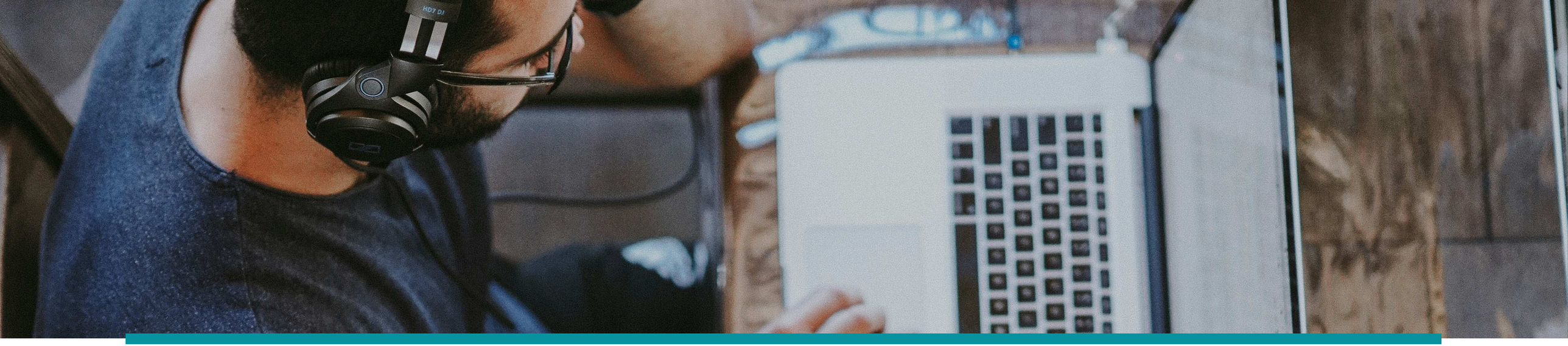
СТРУКТУРНО АИС СОДЕРЖИТ ТРИ УРОВНЯ (СМ. ПРИКАЗ ФСТЭК РОССИИ 14.03.2014 №31):

- нижний уровень, состоящий из устройств детектирования, преобразующих физические значения измеряемых ими величин в точках измерения и передающих данную информацию на средний уровень;
- средний уровень, состоящий из блоков обработки и передачи данных Р-03Д3, БР-03Д, ТР-06Д3, АИ-01Д, ТВВ-10М, передающих информацию на верхний уровень;
- верхний уровень, состоящий из центральных устройств обработки и предоставления информации и сетевого оборудования, обеспечивающих сбор, обработку, хранение, представление и вывод информации операторам (ТВВ-10, ПМ-10) и на средства оповещения. Верхний уровень представляет собой сервер СМДТС и рабочие места пользователей.

Обмен информацией между оборудованием, входящим с состав СМДТС, осуществляется по каналам связи средствами интерфейсов Ethernet стандарта IEEE 802.3 (100Base-TX), а также стандарту RS-485 (ANSI TIA/EIA-485-A:1998).

Архитектура АСУ ТП





В соответствии с «Требованиями к обеспечению защиты информации, содержащейся в информационных системах управления производством, используемых организациями оборонно-промышленного комплекса», утвержденных Приказом ФСТЭК России от 28.02.2017 г. №31 и ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ:

разработка мероприятий по обеспечению безопасности информации в АИС должна осуществляться с учетом «Требований по защите информации, не составляющей государственную тайну, содержащейся в государственных ИС», утвержденным Приказом ФСТЭК России от 11.02.2013 г. №17, к третьему К3 классу защищенности (ГИС) и согласно Приказу ФСТЭК России №239 от 25.12.2017 «Об утверждении требований к обеспечению безопасности значимых объектов критической информационной инфраструктуры» **3 категории** значимости.

СОЗДАНИЕ СИСТЕМ ЗАЩИТЫ ОСУЩЕСТВЛЯЛОСЬ В НЕСКОЛЬКО ПОСЛЕДОВАТЕЛЬНЫХ ЭТАПОВ:

01 формирование требований к защите информации, содержащейся в информационной системе;

02 разработка системы защиты информации информационной системы;

03 внедрение системы защиты информации информационной системы;

04 аттестация информационной системы по требованиям защиты информации (далее - аттестация информационной системы) и ввод ее в действие;

05 обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы.

ВАЖНЫЕ ОСОБЕННОСТИ ПРОЕКТОВ ПО ЗАЩИТЕ АСУ ТП:

Системы АСУ ТП и офисные ИТ-системы имеют различные назначения и условия эксплуатации.
Это обуславливает различие в подходах по обеспечению ИБ, методиках и стратегиях реализации ИБ.

ТРЕБОВАНИЯ	«ОФИСНЫЕ» СИСТЕМЫ	АСУ ТП
Время реакции	Некритично	| Работа в реальном времени | Гарантированная доставка данных
Доступность	Остановки возможны	| Работа в реальном времени | Гарантированная доставка данных
Приоритеты ИБ	| Конфиденциальность | Целостность | Доступность	| Доступность | Целостность
Архитектура ИБ	Возможно использование стандартных средств обеспечения ИБ	Использование стандартных средств обеспечения ИБ возможно частично
Физическое воздействие на критические процессы	Нет	Да

ТРЕБОВАНИЯ	«ОФИСНЫЕ» СИСТЕМЫ	АСУ ТП
Эксплуатационные и функциональные ограничения	Нет	| Нестандартные ОС, протоколы связи и т.д. | Отсутствие встроенных механизмов обеспечения ИБ (шифрование, журналирование, аутентификация и т.п.) | Наличие большого числа компонент с ограниченной функциональностью
Коммуникации	Стандартно	| Низкая пропускная способность | Многообразие средств и систем связи | Нестандартные протоколы | Нетиповые топологии

ТРЕБОВАНИЯ	«ОФИСНЫЕ» СИСТЕМЫ	АСУ ТП
Управление изменениями	Стандартно	| Долгий период/невозможность обновления ОС и ПО | Устаревшее ПО и оборудование | Обновление аппаратного и микропрограммного обеспечения
Время жизни	3-5 лет	15-30 лет
Доступность компонентов	Стандартно	| Территориальная распределенность объектов | Наличие труднодоступных объектов. Сложные условия эксплуатации (агрессивные среды, экстремальные температуры, загазованность и т.д.)

СПАСИБО
ЗА ВНИМАНИЕ!

c-fence.com