ЦЕНТР КИБЕРБЕЗОПАСНОСТИ (ЧУ, ДПО)

УТВЕРЖДАЮ
Директор ЦЕНТР КИБЕРБЕЗОПАСНОСТИ (ЧУ, ДПО)
_____ С.И. Василиади
«10» января 2026 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Защита информации в промышленных системах (АСУ ТП, промышленные вычислительные сети, встроенные системы и т.п.)»

Вид: дополнительная профессиональная программа повышения квалификации.

Показатель	Значение
Объём	256 учебных часов
Форма обучения	Заочная, с применением электронного обучения и дистанционных образовательных технологий
Способ реализации	Дистанционно: электронные материалы, консультации, практические задания и дистанционный контроль
Категория слушателей	Специалисты по ИБ и АСУ ТП, инженеры промышленной автоматизации, специалисты эксплуатации технологических сетей и производственных систем.
Порядок допуска	Лица, имеющие или получающие среднее профессиональное и (или) высшее образование (ч. 3 ст. 76 № 273-ФЗ).
Итоговый документ	Удостоверение о повышении квалификации при успешной итоговой аттестации

1. Общая характеристика и цель

Цель: Совершенствование профессиональных компетенций по выявлению угроз и реализации мер кибербезопасности для промышленных автоматизированных систем.

Продолжительность и учебный график устанавливаются настоящей программой; даты проведения занятий определяются расписанием конкретной группы. Учёт трудоёмкости ведётся в учебных часах. Для занятий применяется академический час 45 минут.

Нормативная основа: Федеральный закон от 29.12.2012 № 273-ФЗ; приказ Минобрнауки России от 24.03.2025 № 266; постановление Правительства РФ от 11.10.2023 № 1678. Приказ Минобрнауки России от 19.10.2020 № 1316 (ред. от 04.09.2024) применяется в части специальных требований к ДПП в области информационной безопасности.

Содержание учитывает характер профессиональной деятельности и необходимые квалификационные требования к заявленной категории слушателей; освоение программы не присваивает новую квалификацию.

2. Планируемые результаты

Формируемые и совершенствуемые компетенции:

- ПК1. Анализировать архитектуру АСУ ТП и промышленных коммуникаций с учетом технологических ограничений.
- ПК2. Проводить оценку угроз, сегментировать промышленные сети и обосновывать защитные меры.
- ПК3. Организовывать безопасную эксплуатацию, мониторинг и реагирование на инциденты в промышленной среде.

По завершении обучения слушатель должен знать: архитектуру АСУ ТП, типовые промышленные протоколы, особенности угроз, требования доступности и безопасности технологического процесса.

По завершении обучения слушатель должен уметь: составлять схему сегментирования, каталог активов и угроз, план защиты и алгоритм безопасного реагирования на инцидент.

3. Учебный план

№	Дисциплина (модуль)	Всего	Теор.	Практ.	Сам.	Контроль
1	Архитектура АСУ ТП и встроенных систем	40	14	16	10	Текущий контроль
2	Моделирование угроз промышленной среде	48	16	19	13	Текущий контроль
3	Сегментация, доступ и сетевые меры	60	20	24	16	Текущий контроль
4	Защита рабочих станций, серверов и контроллеров	60	20	24	16	Текущий контроль
5	Мониторинг, инциденты и устойчивость	44	15	18	11	Текущий контроль
	Итоговая аттестация	4	0	4	0	Тест и кейс
	ВСЕГО	256	85	105	66	

Теор. — теоретическое освоение материала; практ. — практические занятия и задания с обратной связью; самост. — самостоятельная работа. Итоговый контроль включён в общую трудоёмкость.

4. Календарный учебный график

Период	Объём, ч.	Модули/контроль (№ и часы)
Неделя 1	30	1 (30 ч.)
Неделя 2	30	1 (10 ч.); 2 (20 ч.)
Неделя 3	30	2 (28 ч.); 3 (2 ч.)
Неделя 4	30	3 (30 ч.)
Неделя 5	30	3 (28 ч.); 4 (2 ч.)
Неделя 6	30	4 (30 ч.)
Неделя 7	30	4 (28 ч.); 5 (2 ч.)
Неделя 8	30	5 (30 ч.)
Неделя 9	16	5 (12 ч.); 6 (4 ч.)

График рассчитан из условной нагрузки не более 30 учебных часов в неделю. При формировании учебной группы конкретные даты и распределение занятий утверждаются расписанием без изменения общей трудоёмкости и итоговых результатов.

5. Рабочие программы дисциплин (модулей)

Модуль 1. Архитектура АСУ ТП и встроенных систем — 40 ч.

Содержание: Уровни автоматизации и взаимодействие ИТ/ОТ; Контроллеры, станции оператора и инженерные рабочие места; Промышленные сети и коммуникационные протоколы.

Практическая работа: Построить схему учебного технологического сегмента.

Текущий контроль: проверка выполнения задания и ответы на контрольные вопросы по темам модуля.

Модуль 2. Моделирование угроз промышленной среде — 48 ч.

Содержание: Активы и технологические последствия нарушения работы; Каналы проникновения и цепочки атак; Учет отказоустойчивости и требований промышленной безопасности.

Практическая работа: Разработать фрагмент модели угроз и карту последствий.

Текущий контроль: проверка выполнения задания и ответы на контрольные вопросы по темам модуля.

Модуль 3. Сегментация, доступ и сетевые меры — 60 ч.

Содержание: Зоны и каналы обмена, межсетевое разделение; Административный и удалённый доступ; Применение сетевых средств защиты без нарушения технологического процесса.

Практическая работа: Разработать матрицу коммуникаций и концепцию сегментации.

Текущий контроль: проверка выполнения задания и ответы на контрольные вопросы по темам модуля.

Модуль 4. Защита рабочих станций, серверов и контроллеров — 60 ч.

Содержание: Управление конфигурациями и уязвимостями ОТ; Контроль изменений и резервирование конфигураций; Меры против вредоносного кода и несанкционированных изменений.

Практическая работа: Составить план защиты и регламент согласования изменений.

Текущий контроль: проверка выполнения задания и ответы на контрольные вопросы по темам модуля.

Модуль 5. Мониторинг, инциденты и устойчивость — 44 ч.

Содержание: Источники событий в промышленных сетях; Сценарии обнаружения и разбор инцидентов; Непрерывность технологических процессов и восстановление.

Практическая работа: Разработать сценарий реагирования с учётом безопасности производства.

Текущий контроль: проверка выполнения задания и ответы на контрольные вопросы по темам модуля.

6. Организационно-педагогические условия

Обучение организуется в электронной образовательной среде с индивидуальным доступом слушателя к учебным материалам, заданиям и средствам связи с преподавателем. Взаимодействие возможно синхронно и асинхронно. Результаты работ и контроля фиксируются в электронной среде или в учётных ведомостях.

Кадровое обеспечение: преподаватели (специалисты), имеющие образование, профессиональную подготовку и опыт деятельности, соответствующие тематике преподаваемых модулей; при необходимости привлекаются практикующие специалисты.

Материально-техническое и информационное обеспечение: компьютер с доступом к сети Интернет, программные средства чтения учебных материалов, демонстрационные материалы, тестовая среда и учебные кейсы. Для практических заданий используются учебные данные, демонстрационные конфигурации, симуляторы или специально выделенные стенды по тематике курса.

Методическое обеспечение: конспекты и презентации, нормативные и эксплуатационные материалы из раздела 8, задания для самостоятельной работы, инструкции к практическим работам, контрольные вопросы и критерии оценивания.

Особенности ИБ: программа не предполагает использование сведений, составляющих государственную тайну, либо реальных ключей, паролей и конфиденциальных данных обучающихся или заказчиков. Дистанционно изучаются материалы и выполняются учебные задачи с применением стендов/симуляторов. Если конкретная практическая работа требует физического доступа к защищаемому оборудованию или иного режима, она проводится лишь при обеспечении соответствующих условий; возможность полностью дистанционного освоения проверяется до начала реализации.

Порядок актуализации и передачи: изменения содержания вносятся после проверки применимых требований законодательства и утверждаются директором. Передача программы сторонней образовательной организации

допускается по оформленному соглашению с соблюдением прав на материалы и режима доступа; сведения ограниченного доступа в программу не включаются.

7. Контроль результатов и оценочные материалы

Текущий контроль проводится по заданиям модулей с результатом «зачтено/не зачтено». Слушатель получает комментарии к ошибкам и возможность повторного выполнения задания в пределах срока обучения.

Итоговый контроль: дистанционный тест и практико-ориентированный кейс. Тест содержит не менее 10 заданий по содержанию всех модулей. Для положительного результата требуется не менее 70% верных ответов и выполнение ключевых требований практического кейса. Допускается повторная проверка в порядке, предусмотренном локальными актами.

Типовые контрольные вопросы:

1. Чем ОТ-среда отличается от корпоративной ИТ-среды?

2. Почему обновления контроллеров требуют предварительного согласования?

3. Какие взаимодействия между сегментами должны быть документированы?

4. Как определить критичность промышленного актива?

5. Какие действия запрещены при реагировании без согласования с технологами?

Практическое итоговое задание: Для учебного промышленного сегмента разработать схему зон безопасности, ограничения удаленного доступа, план мониторинга и порядок реагирования, исключающий неконтролируемые действия на технологическом оборудовании.

Критерии оценки кейса: (1) корректно выделены исходные условия и риски; (2) действия и документы предложены последовательно; (3) применены уместные технические и организационные меры; (4) не предложены действия, противоречащие требованиям безопасности. Результат «зачтено» — выполнение не менее трёх из четырёх критериев при обязательном соблюдении критерия 4.

Освоение завершается итоговой аттестацией. Успешно прошедшему итоговую аттестацию слушателю выдаётся удостоверение о повышении квалификации в установленном организацией порядке. При неудовлетворительном результате действуют правила выдачи справки об обучении.

8. Основные нормативные и методические источники

- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».
- Приказ Минобрнауки России от 24.03.2025 № 266.
- Постановление Правительства РФ от 11.10.2023 № 1678.
- Приказ Минобрнауки России от 19.10.2020 № 1316 (ред. от 04.09.2024).
- Федеральный закон от 26.07.2017 № 187-ФЗ — если объект относится к соответствующей сфере применения.
- Действующие нормативные требования ФСТЭК России к защите АСУ ТП и значимых объектов КИИ, если они применимы.
- Отраслевые инструкции изготовителей промышленного оборудования.

Учебные и справочные материалы актуализируются перед реализацией очередной группы с учётом действующих редакций нормативных документов.