ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«АКАДЕМИЯ ИНФОВОТЧ»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 02214E9D008AB20DBB4227DE786E91AAFB
Владелец: ХАРИТОНОВ СЕРГЕЙ ВЛАДИМИРОВИЧ
Действителен: с 20.02.2025 до 20.05.2026

Утверждена

Генеральный директор
С.В. Харитонов

МП

Дополнительная профессиональная программа повышения квалификации «Защита ИТ-инфраструктуры от сетевых атак»

Форма обучения: заочная
с применением дистанционных образовательных технологий

Москва 2025

Оглавление

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Настоящая образовательная программа (далее – Программа) представляет собой совокупность требований, обязательных при реализации программы дополнительного профессионального образования повышения квалификации для сертификации преподавателей учебных заведений «Защита ИТ-инфраструктуры от сетевых атак».

Программа разработана в соответствии с требованиями профессионального стандарта «Специалист по безопасности компьютерных систем и сетей», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 533н (далее – Профстандарт), также на основании Приказа Министерства образования и науки Российской Федерации (Минобрнауки России) от 1 июля 2013 г. № 499 г. Москва "Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам" и на основании Федерального закона "Об образовании в Российской Федерации" от 29.12.2012 № 273-ФЗ.

Цели:

- формирование знаний и навыков по вопросам применения законодательства в сфере информационной безопасности компьютерных систем и сетей, выполнения требований регулятора, обнаружения и предотвращения инцидентов потенциальных сетевых атак и определения комплекса мер по защите инфраструктуры сети.
- практическая подготовка преподавателя для обучения студентов выполнению работ по внедрению и администрированию программных решений защиты ИТ-инфраструктуры от сетевых атак, разработке, реализации и оценке эффективности правил системы обнаружения и предотвращения вторжений, а также проведения расследований инцидентов сетевых атак.

Категория слушателей:

- мастер производственного обучения
- преподаватель
- старший преподаватель
- ведущий преподаватель
- доцент

Организационно-педагогические условия

Образовательный процесс осуществляется на основании учебного плана и регламентируется расписанием занятий для каждого слушателя.

Срок обучения: 40/6/2 (ак. час, нед., мес.).

Режим занятий: 39 академических часов самостоятельного обучения, 1 академический час итоговой аттестации (зачета).

Форма обучения: заочная с применением дистанционных образовательных технологий

Характеристика профессиональной деятельности слушателей

Область профессиональной деятельности слушателей:

- преподавание дисциплин, связанных с сетевыми технологиями и защитой информации в компьютерных системах и сетях

Преподаватель готовит студентов к следующим видам деятельности: к участию в обеспечении безопасности сетевой инфраструктуры в компьютерных системах и сетях, к участию в выявлении угроз безопасности сетевой инфраструктуры в промышленном и корпоративном сегментах сетей, к участию в принятии мер защиты сетевой инфраструктуры при выявлении новых угроз безопасности.

Требования к результатам освоения дополнительной профессиональной образовательной программы

Специалист должен обладать общими компетенциями, включающими в себя способность:

- Понимать сущность и социальную значимость своей профессии, проявлять к ней устойчивый интерес.
- Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
- Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
- Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
- Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
- Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
- Развивать культуру межличностного общения, взаимодействия между людьми, устанавливать психологические контакты с учетом межкультурных и этнических различий.

Специалист должен обладать профессиональными компетенциями, соответствующими основным видам профессиональной деятельности:

- Определение состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях.
- Разработка порядка применения программно-аппаратных средств защиты информации в компьютерных сетях.
- Формирование шаблонов конфигурации программно-аппаратных средств защиты информации в компьютерных сетях.
- Управление функционированием программно-аппаратных средств защиты информации в компьютерных сетях.
- Контроль корректности функционирования программно-аппаратных средств защиты информации в компьютерных сетях.
- Управление средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями.

- Оценка соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам.
- Определение угроз безопасности и их возможных источников в компьютерных системах и сетях.
- Определение каналов утечки информации в компьютерных системах и сетях.

Требование к слушателям

Требования к образованию и обучению	Высшее профессиональное образование/Среднее профессиональное образование

Для реализации программы задействован следующий кадровый потенциал:

- **Преподаватели учебных дисциплин** - обеспечивается необходимый уровень компетенции преподавательского состава, включающий высшее образование в области соответствующей дисциплины программы или высшее образование в иной области и стаж преподавания по изучаемой тематике не менее трех лет; использование при изучении дисциплин программы эффективных методик преподавания, предполагающих выполнение слушателями практических заданий.

- **Административный персонал** - обеспечивает условия для эффективной работы педагогического коллектива, осуществляет контроль и текущую организационную работу.

- **Информационно-технологический персонал** - обеспечивает функционирование информационной структуры (включая ремонт техники, оборудования, макетов иного технического обеспечения образовательного процесса).

Содержание программы повышения квалификации определяется учебным планом и календарным учебным графиком программы дисциплин (модулей), требованиями к итоговой аттестации и требованиями к уровню подготовки лиц, успешно освоивших Программу.

Текущий контроль знаний проводится в форме наблюдения за работой обучающихся и контроля их активности на образовательной платформе, проверочного тестирования.

Промежуточный контроль знаний, полученных обучающимися посредством самостоятельного обучения (освоения части образовательной программы), проводится в виде тестирования.

Итоговая аттестация по Программе проводится в форме зачета посредством тестирования и должна выявить теоретическую и практическую подготовку специалиста.

Слушатель допускается к итоговой аттестации после самостоятельного изучения дисциплин Программы в объеме, предусмотренном для обязательных внеаудиторных занятий и подтвердивший самостоятельное изучение сдачей тестов.

Лица, освоившие Программу и успешно прошедшие итоговую аттестацию, получают удостоверение о повышении квалификации.

Оценочными материалами по Программе являются блоки контрольных вопросов по дисциплинам, формируемые образовательной организацией и используемые при текущем контроле знаний (тестировании), теоретические вопросы и практические задания для итоговой аттестации.

Методическими материалами к Программе являются нормативные правовые акты и техническая документация по изучаемым программным продуктам, положения которых изучаются при освоении дисциплин Программы. Перечень методических материалов приводится в рабочей программе образовательной организации.

УЧЕБНЫЙ ПЛАН
ПО ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЕ
повышения квалификации

«ЗАЩИТА ИТ-ИНФРАСТРУКТУРЫ ОТ СЕТЕВЫХ АТАК»

(профстандарт «Специалист по безопасности компьютерных систем и сетей» код B)

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - внеаудиторная (самостоя-тельная работа)	Внеауди-торная (самостоя-тельная работа)	Промежу-точная /итоговая аттестация	
1	Теоретические основы защиты ИТ - инфраструктуры от сетевых атак	7,0	2,1	4,5	0,4	Тестирование
2	Подготовка среды функционирова-ния и первоначальная настройка комплекса InfoWatch ARMA	5,0	1,0	3,6	0,4	Тестирование
3	Обзор и практическая реализация возможностей комплекса InfoWatch ARMA	27,0	5,1	21,5	0,4	Тестирование
4	ИТОГОВАЯ АТТЕСТАЦИЯ	1,0			1,0	Зачет
	Всего:	40,0	8,3	29,5	2,2	

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН
ПО
ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЕ
повышения квалификации

«ЗАЩИТА ИТ-ИНФРАСТРУКТУРЫ ОТ СЕТЕВЫХ АТАК»

(профстандарт «Специалист по безопасности компьютерных систем и сетей» код B)

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - Внеаудиторная (самостоятельная работа)	Внеаудиторная (самостоятельная работа)	Промежуточная /итоговая аттестация	
1	**Теоретические основы защиты ИТ - инфраструктуры от сетевых атак**	**7,0**	**2,1**	**4,5**	**0,4**	**Тестирование**
1.1	Введение в InfoWatch ARMA IF	0,8	0,3	0,5		
1.2	Безопасность АСУ ТП. Автоматизированные системы управления	0,5	0,1	0,4		
1.3	Кибератаки и векторы угроз	0,6	0,2	0,4		
1.4	Атаки на АСУ ТП	0,6	0,2	0,4		
1.5	Проблематика ИБ АСУ ТП	0,6	0,2	0,4		
1.6	Нормативно-правовое регулирование	0,6	0,2	0,4		
1.7	Системы защиты информации. Межсетевые экраны	0,6	0,2	0,4		
1.8	Системы обнаружения и предотвращения вторжений	0,5	0,1	0,4		

1.9	Система защиты информации КИИ на промышленных предприятиях	0,6	0,2	0,4		
1.10	Промышленный межсетевой экран. Функции и возможности	0,7	0,3	0,4		
1.11	Промышленный межсетевой экран. Опыт и практика	0,5	0,1	0,4		
	Тестирование	0,4			0,4	
2	**Подготовка среды функционирования и первоначальная настройка комплекса InfoWatch ARMA**	**5,0**	**1,0**	**3,6**	**0,4**	**Тестирование**
2.1	Информация для выполнения практической части	2,0	0,2	1,8		
2.2	Основы внедрения и использования ПАК Infowatch ARMA. Установка комплекса	1,0	0,4	0,6		
2.3	Настройка и тестирование механизма синхронизации системного времени	1,0	0,2	0,4		
2.4	Создание внутренних пользователей и назначение привилегий (ролей)	1,0	0,2	0,8		
	Тестирование	0,4			0,4	
3	**Обзор и практическая реализация возможностей комплекса InfoWatch ARMA**	**27,0**	**5,1**	**21,5**	**0,4**	**Тестирование**
3.1	Настройка и тестирование	2,4	0,4	2,0		

	правил межсетевого экранирования					
3.2	Настройка и тестирование механизма экспорта событий безопасности по протоколу Syslog	1,8	0,3	1,5		
3.3	Настройка и тестирование правил модуля обнаружения вторжений	2,4	0,4	2,0		
3.4	Настройка и тестирование подсистемы контроля промышленных протоколов	2,4	0,4	2,0		
3.5	Блокировка команды остановки ПЛК	1,9	0,4	1,5		
3.6	Настройка и тестирование модуля DNSmasq	1,8	0,3	1,5		
3.7	Настройка и тестирование механизма SNMP мониторинга	1,2	0,2	1,0		
3.8	Резервное копирование, сброс и восстановление. Расширенный откат изменений	1,2	0,2	1,0		
3.9	Настройка и тестирование прозрачного режима работы	1,9	0,4	1,5		
3.10	Установка продукта InfoWatch ARMA Management Console	2,0	0,5	1,5		
3.11	Установка продукта InfoWatch ARMA Industrial	1,2	0,2	1,0		

	Endpoint. Обзор интерфейса.					
3.12	Карта сети и определение активов	1,3	0,3	1,0		
3.13	Добавление дополнительных источников	1,3	0,3	1,0		
3.14	Просмотр событий информационной безопасности	1,2	0,2	1,0		
3.15	Настройка правил корреляции	1,4	0,4	1,0		
3.16	Анализ инцидентов	1,2	0,2	1,0		
	Тестирование	0,4			0,4	
4	**ИТОГОВАЯ АТТЕСТАЦИЯ**	**1,0**			**1,0**	**Зачет**
	Всего:	**40,0**	**8,3**	**29,5**	**2,2**	**-**

КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Календарный график обучения является примерным, составляется и утверждается для каждого слушателя.

Срок освоения программы – 6 недель. Начало обучения 1 июля 2025 года. Примерный режим занятий: 1,0-2,0 академических часа в день. Промежуточная и итоговые аттестации проводятся согласно графику.

№	Наименование модулей / дни	ВР	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	Теоретические основы защиты ИТ - инфраструктуры от сетевых атак	СР	1,0	1,0	1,0	1,0	1,0	1,0	1,0													
2	Подготовка среды функционирования и первоначальная настройка комплекса InfoWatch ARMA	СР								2,0	1,0	1,0	1,0									
3	Обзор и практическая реализация возможностей комплекса InfoWatch ARMA	СР												1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0

№	Наименование модулей / дни	ВР	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
3	Обзор и практическая реализация возможностей комплекса InfoWatch ARMA	СР	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	
4	Итоговая аттестация																				1,0

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ «ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИТ - ИНФРАСТРУКТУРЫ ОТ СЕТЕВЫХ АТАК» (КОД В)

Цель: обеспечение глубокими знаниями обучающихся в области назначения, возможностей и принципов работы комплекса защиты от сетевых аномалий.

Задачи:

- Владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения.
- Анализировать рабочую ситуацию, осуществлять текущий и итоговый контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы.
- Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.

Место дисциплины в структуре программы

Дисциплина позволяет слушателям изучить возможности, процесс внедрения, особенности межсетевого экрана в инфраструктуре сети.

Требования к результатам освоения дисциплины

В результате обучения дисциплине слушатели должны:

Знать:

- Теоретические основы использования промышленного межсетевого экрана в инфраструктуре сети.
- Порядок внедрения программного комплекса в промышленную среду.
- Принципы работы технологий комплекса.
- Нормативно-правовое регулирование.

Уметь:

- Обосновывать необходимость использования комплекса защиты информации в инфраструктуре сети.

- Определять функции и возможности межсетевого экрана.

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 7 академических часов; из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 4,5 академических часа.

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - внеаудиторная (самостоя-тельная работа)	Внеауди-торная (самостоя-тельная работа)	Промежу-точная /итоговая аттестация	
1	**Теоретические основы защиты ИТ - инфраструктуры от сетевых атак**	**7,0**	**2,1**	**4,5**	**0,4**	**Тестирование**
1.1	Введение в InfoWatch ARMA IF	0,8	0,3	0,5		
1.2	Безопасность АСУ ТП. Автоматизированные системы управления	0,5	0,1	0,4		
1.3	Кибератаки и векторы угроз	0,6	0,2	0,4		
1.4	Атаки на АСУ ТП	0,6	0,2	0,4		
1.5	Проблематика ИБ АСУ ТП	0,6	0,2	0,4		
1.6	Нормативно-правовое регулирование	0,6	0,2	0,4		
1.7	Системы защиты информации. Межсетевые экраны	0,6	0,2	0,4		
1.8	Системы обнаружения и предотвращения вторжений	0,5	0,1	0,4		
1.9	Система защиты информации КИИ на промышленных предприятиях	0,6	0,2	0,4		
1.10	Промышленный межсетевой экран. Функции и возможности	0,7	0,3	0,4		
1.11	Промышленный межсетевой экран. Опыт и практика	0,5	0,1	0,4		
	Тестирование	0,4			0,4	

Тема 1.1. Введение в InfoWatch ARMA IF

- Индустрия 4.0;
- Векторы угрозы сегодня;
- Комплекс InfoWatch ARMA IF;
- Сегментация промышленной сети.

Тема 1.2. Безопасность АСУ ТП. Автоматизированные системы управления

- Определения АСУ,
- АСУ П и АСУ ТП;
- Структура и функции;
- Уровни АСУ и их назначение.

Тема 1.3. Кибератаки и векторы угроз

- Определение кибератаки;
- Типы кибератак;
- Целевая кибератака и ее фазы;
- Векторы угроз;
- Состав комплекса.

Тема 1.4. Атаки на АСУ ТП

- Хронология атак на АСУ ТП и их последствия.

Тема 1.5. Проблематика ИБ АСУ ТП

- Анализ проблематики информационной безопасности в области АСУ ТП.

Тема 1.6. Нормативно-правовое регулирование

- Определение критической информационной инфраструктуры (КИИ);
- Ключевые нормативно-правовые акты в области КИИ;
- Административный и уголовный кодекс (в разрезе ИБ КИИ).

Тема 1.7. Системы защиты информации. Межсетевые экраны

- Общие сведения о межсетевых экранах (МЭ);
- МЭ в соответствии ГОСТ;
- Классификация МЭ.

Тема 1.8. Системы обнаружения и предотвращения вторжений

- Характеристика;
- Назначение;
- Функциональные возможности.

Тема 1.9. Система защиты информации КИИ на промышленных предприятиях

- Состав и назначение элементов комплексной системы защиты InfoWatch ARMA;
- Методология комплексного подхода InfoWatch ARMA к защите промышленной сети;
- Преимущества осуществления комплексной информационной безопасности.

Тема 1.10. Промышленный межсетевой экран. Функции и возможности

- Назначение, соответствие требованиям ФСТЭК;
- Основные функции.

Тема 1.11. Промышленный межсетевой экран. Опыт и практика

- Опыт и практика использования Infowatch ARMA Industrial Firewall.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ «ПОДГОТОВКА СРЕДЫ ФУНКЦИОНИРОВАНИЯ И ПЕРВОНАЧАЛЬНАЯ НАСТРОЙКА КОМПЛЕКСА INFOWATCH ARMA» (КОД В)

Цель: обеспечение глубокими знаниями обучающихся в области корректной установки и первичной настройки комплекса сетевой безопасности.

Задачи:

- Владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения.
- Анализировать рабочую ситуацию, осуществлять текущий контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы.
- Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.

Место дисциплины в структуре программы

Дисциплина позволяет слушателям изучить процесс установки и первоначальную настройку комплекса InfoWatch ARMA Industial Firewall.

Требования к результатам освоения дисциплины

В результате обучения дисциплине слушатели должны:

Знать:

- Средства виртуализации для установки программного комплекса.
- Способы установки InfoWatch ARMA Industrial Firewall.
- Первоначальную настройку системы с указанием необходимых интерфейсов.

Уметь:

- Подготавливать виртуальные стенды для работы с комплексом.
- Устанавливать InfoWatch ARMA Industrial Firewall.
- Проводить первичную настройку системы.

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 5 академических часов; из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 3,6 академических часа.

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - внеаудиторная (самостоя-тельная работа)	Внеауди-торная (самостоя-тельная работа)	Промежу-точная /итоговая аттеста-ция	
2	**Подготовка среды функционирования и первоначальная настройка комплекса InfoWatch ARMA**	**5,0**	**1,0**	**3,6**	**0,4**	**Тестирование**
2.1	Информация для выполнения практической части	2,0	0,2	1,8		
2.2	Основы внедрения и использования ПАК Infowatch ARMA. Установка комплекса	1,0	0,4	0,6		
2.3	Настройка и тестирование механизма синхронизации системного времени	0,6	0,2	0,4		
2.4	Создание внутренних пользователей и назначение привилегий (ролей)	1,0	0,2	0,8		
	Тестирование	0,4			0,4	

Тема 2.1. Информация для выполнения практической части

- Подготовка стенда;
- Сетевые настройки.

Тема 2.2. Основы внедрения и использования ПАК Infowatch ARMA. Установка комплекса.

- Установка;
- Первоначальная настройка комплекса.

Тема 2.3 Настройка и тестирование механизма синхронизации системного времени

- Работа со службами;
- Конфигурация NTP –сервера;
- Проверка статуса.

Тема 2.4 Создание внутренних пользователей и назначение привилегий (ролей)

- Создание пользователей;
- Работа с группами пользователей;
- Настройка системных привилегий.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ «ОБЗОР И ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ ВОЗМОЖНОСТЕЙ КОМПЛЕКСА INFOWATCH ARMA» (КОД В)

Цель: обеспечение глубокими знаниями обучающихся в области использования сетевого комплекса для обеспечения информационной безопасности компьютерных систем и сетей.

Задачи:

- Владеть культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения.
- Анализировать рабочую ситуацию, осуществлять текущий контроль, оценку и коррекцию собственной деятельности, нести ответственность за результаты своей работы.
- Осуществлять поиск информации, необходимой для эффективного выполнения профессиональных задач.

Место дисциплины в структуре программы

Дисциплина позволяет слушателям изучить процесс настройки и использования технологий сетевого комплекса InfoWatch Arma Industrial Firewall, Management Console и Industrial EndPoint.

Требования к результатам освоения дисциплины

В результате обучения дисциплине слушатели должны:

Знать:

- Процессы и этапы настройки технологий в составе сетевого комплекса, а также использования его для выявления аномалий в инфраструктуре сети, предотвращения сетевых атак.
- Инструментарий, технологии, область их применения и ограничения при формировании защиты промышленного сегмента от внешних и внутренних угроз информационной безопасности на основе InfoWatch ARMA Industrial Firewall и комплементарных продуктов.
- Сбор и анализ событий, формирование инцидентов согласно правил корреляций.

Уметь:

- Работать с интерфейсом InfoWatch ARMA Industrial Firewall, Management Console и Industrial EndPoint.
- Устанавливать InfoWatch ARMA Management Console и Industrial EndPoint.
- Производить необходимые настройки системы и технологий.
- Использовать комплекс InfoWatch ARMA Industrial Firewall, Management Console и Industrial EndPoint для выявления инцидентов информационной безопасности.

Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 27 академических часов; из них внеаудиторные занятия (самостоятельное изучение теоретического материала) – 21,5 академических часа.

№ п/п	Наименование разделов и дисциплин	Всего ак. часов	В том числе			Форма контроля
			Видеолекции - внеаудиторная (самостоя-тельная работа)	Внеауди-торная (самостоя-тельная работа)	Промежу-точная /итоговая аттеста-ция	
3	**Обзор и практическая реализация возможностей комплекса InfoWatch ARMA**	**27,0**	**5,1**	**21,5**	**0,4**	**Тестирование**
3.1	Настройка и тестирование правил межсетевого экранирования	2,4	0,4	2,0		
3.2	Настройка и тестирование механизма экспорта событий безопасности по протоколу Syslog	1,8	0,3	1,5		
3.3	Настройка и тестирование правил модуля обнаружения вторжений	2,4	0,4	2,0		
3.4	Настройка и тестирование подсистемы контроля промышленных протоколов	2,4	0,4	2,0		
3.5	Блокировка команды остановки ПЛК	1,9	0,4	1,5		
3.6	Настройка и тестирование модуля DNSmasq	1,8	0,3	1,5		
3.7	Настройка и тестирование механизма SNMP мониторинга	1,2	0,2	1,0		
3.8	Резервное копирование, сброс и восстановление. Расширенный откат изменений	1,2	0,2	1,0		
3.9	Настройка и тестирование	1,9	0,4	1,5		

	прозрачного режима работы					
3.10	Установка продукта InfoWatch ARMA Management Console	2,0	0,5	1,5		
3.11	Установка продукта InfoWatch ARMA Industrial Endpoint. Обзор интерфейса.	1,2	0,2	1,0		
3.12	Карта сети и определение активов	1,3	0,3	1,0		
3.13	Добавление дополнительных источников	1,3	0,3	1,0		
3.14	Просмотр событий информационной безопасности	1,2	0,2	1,0		
3.15	Настройка правил корреляции	1,4	0,4	1,0		
3.16	Анализ инцидентов	1,2	0,2	1,0		
	Тестирование	0,4			0,4	

Тема 3.1. Настройка и тестирование правил межсетевого экранирования

- Модуль межсетевого экрана;
- Настройка комплекса по умолчанию;
- Настройка и тестирование правил фильтрации.

Тема 3.2. Настройка и тестирование механизма экспорта событий безопасности по протоколу Syslog

- Настройка экспорта по syslog;
- Тестирование механизма;

Тема 3.3. Настройка и тестирование правил модуля обнаружения вторжений

- Настройка режима обнаружения вторжений;
- Выбор предустановленных правил;
- Сканирование портов.

Тема 3.4. Настройка и тестирование подсистемы контроля промышленных протоколов

- Редактирование предустановленного правила с указанием необходимого шаблона;
- Сбор и анализ предупреждений.

Тема 3.5. Блокировка команды остановки ПЛК

- Настройка блокировки ПЛК;
- Проверка настройки правила.

Тема 3.6. Настройка и тестирование модуля DNSmasq

- Работа с модулем DNSmasq;
- Переадресация DNS-адресов;
- Указание DNS –серверов.

Тема 3.7. Настройка и тестирование механизма SNMP мониторинга

- Механизм мониторинга ресурсов;
- Общие настройки SNMP;
- Тестирование.

Тема 3.8. Резервное копирование, сброс и восстановление. Расширенный откат изменений

- Сброс и откат к предыдущим настройкам;
- Контроль и история изменений;
- Резервное копии.

Тема 3.9. Настройка и тестирование прозрачного режима работы

- Сброс настройки комплекса;
- Создание моста и назначения портов;
- Настройка параметров.

Тема 3.10. Установка продукта InfoWatch ARMA Management Console

- Установка и настройка сетевых интерфейсов;
- Подключение к веб-интерфейсу;
- Подключение с помощью SSH.

Тема 3.11. Установка продукта InfoWatch ARMA Industrial Endpoint. Обзор интерфейса.

- Контроль запуска программ и запуска съемных носителей;
- Контроль целостности программного обеспечения;
- Синхронизация и управление.

Тема 3.12. Карта сети и определение активов

- Добавление и регистрация активов;
- Карта сети и типы карт;
- Связи и управление активами.

Тема 3.13. Добавление дополнительных источников

- Добавление IFW;
- Добавление IEW.

Тема 3.14. Просмотр событий информационной безопасности

- Информация о событии;
- Помощь по коррелятору.

Тема 3.15. Настройка правил корреляции

- Карточка правила корреляции;

- Добавление правила корреляции;
- Типы действий.

Тема 3.16. Анализ инцидентов

- Управление инциденты

ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ

Формы аттестации

Для проведения промежуточной и итоговой аттестации программы разработан фонд оценочных средств по Программе, являющийся неотъемлемой частью учебно-методического комплекса.

Объектами оценивания выступают:

- степень освоения теоретических знаний;
- уровень овладения практическими умениями и навыками по всем видам учебной работы, активность на занятиях.

Текущий контроль знаний проводится в форме наблюдения за работой обучающихся и контроля их активности на образовательной платформе, проверочного тестирования.

Промежуточная аттестация - оценка качества усвоения обучающимися содержания учебных блоков непосредственно по завершении их освоения, проводимая в форме зачета посредством тестирования.

Итоговая аттестация - процедура, проводимая с целью установления уровня знаний, обучающихся с учетом прогнозируемых результатов обучения и требований к результатам освоения образовательной программы. Итоговая аттестация обучающихся осуществляется в форме зачета посредством тестирования.

Слушатель допускается к итоговой аттестации после изучения тем образовательной программы в объеме, предусмотренном для лекционных и практических занятий.

Лицам, освоившим образовательную программу повышения квалификации «Защита ИТ-инфраструктуры от сетевых атак» и успешно прошедшим итоговую аттестацию, выдается **удостоверение о повышении квалификации** установленного образца с указанием названия программы, календарного периода обучения, длительности обучения в академических часах.

Для аттестации обучающихся на соответствие их персональных достижений требованиям соответствующей ОП созданы фонды оценочных средств, включающие типовые задания, тесты и методы контроля, позволяющие оценить знания, умения и уровень приобретенных компетенций.

Фонды оценочных средств соответствуют целям и задачам программы подготовки специалиста, учебному плану и обеспечивают оценку качества общепрофессиональных и профессиональных компетенций, приобретаемых обучающимся.

Критерии оценки обучающихся

Предмет оценивания (компетенции)	**Объект оценивания (навыки)**	**Показатель оценки (знания, умения)**
Специалист должен обладать общими компетенциями (ОК), включающими в себя способность: • Понимать сущность и социальную значимость своей профессии, проявлять к ней устойчивый интерес. • Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество. • Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность. • Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. • Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями. • Ориентироваться в условиях частой смены технологий в	**Специалист должен обладать профессиональными компетенциями (ПК), соответствующими основным видам профессиональной деятельности:** • Определение состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях. • Разработка порядка применения программно-аппаратных средств защиты информации в компьютерных сетях. • Формирование шаблонов конфигурации программно-аппаратных средств защиты информации в компьютерных сетях. • Управление функционированием программно-аппаратных средств защиты информации в компьютерных сетях.	**Знания:** • Принципы построения компьютерных сетей. • Порядок реализации методов и средств межсетевого экранирования • Источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению. • Состав типовых конфигураций программно-аппаратных средств защиты информации и режимов их функционирования в компьютерных сетях **Умения:** • Оценивать угрозы безопасности информации в компьютерных сетях • Настраивать правила фильтрации пакетов в компьютерных сетях • Обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях • Конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях

профессиональной деятельности. • Развивать культуру межличностного общения, взаимодействия между людьми, устанавливать психологические контакты с учетом межкультурных и этнических различий.	• Контроль корректности функционирования программно-аппаратных средств защиты информации в компьютерных сетях. • Управление средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями; • Оценка соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам; • Определение угроз безопасности и их возможных источников в компьютерных системах и сетях;	• Проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях • Оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях • Анализировать угрозы безопасности информации программного обеспечения • Применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации • Применять действующую законодательную базу в области обеспечения защиты информации в компьютерных системах и сетях

Оценка качества освоения учебных модулей проводится в процессе промежуточной аттестации в форме тестирования.

Оценка	Критерии оценки
Зачтено	Оценка **«Зачтено»** выставляется слушателю, если он твердо знает материал курса, грамотно и по существу использует его, не допуская существенных неточностей в ответе на тестовые вопросы. Не менее 70% правильных ответов при решении тестов.
Не зачтено	Оценка **«Не зачтено»** выставляется слушателю, который не знает значительной части программного материала, допускает существенные ошибки. Менее 70% правильных ответов при решении тестов.

Оценка качества освоения учебной программы проводится в процессе итоговой аттестации в форме зачета посредством тестирования.

Оценка (стандартная)	**Критерии оценки**
Зачтено	Оценка **«Зачтено»** выставляется слушателю, продемонстрировавшему твердое и всесторонние знания материалы, умение применять полученные в рамках занятий практические навыки и умения. Достижения за период обучения и результаты текущей аттестации демонстрировали отличный уровень знаний и умений слушателя. Не менее 70% правильных ответов при решении тестов.
Не зачтено	Оценка **«Не зачтено»** выставляется слушателю, который в недостаточной мере овладел теоретическим материалом по дисциплине, допустил ряд грубых ошибок при выполнении практических заданий, а также не выполнил требований, предъявляемых к промежуточной аттестации. Достижения за период обучения и результаты текущей аттестации демонстрировали неудовлетворительный уровень знаний и умений слушателя. Менее 70% правильных ответов при решении тестов.

Фонд оценочных средств
Оценочные материалы

ТЕСТОВЫЕ ВОПРОСЫ

Дисциплина «Теоретические основы защиты ИТ - инфраструктуры от сетевых атак»

1. Установите соответствия между атакой и годом происшествия.

STUXNET	2020
HAVEX	2019
BLACKENERGY	2017
WannaCry	2017
TRITON	2015

DUGU 2.0	2013
Sodinokibi SolarWind	2010

2. В каком порядке организована структура АСУ ТП (снизу-вверх)?
   - I/O – PLC – SCADA – MES – ERP
   - I/O –SCADA – MES – ERP – PLC
   - I/O – PLC – SCADA – ERP – MES
   - I/O – SCADA – PLC – MES – ERP

3. В каком Федеральном законе (ФЗ) изложены требования по обеспечению безопасности КИИ?
   - ФЗ №187
   - ФЗ №239
   - ФЗ №149
   - ФЗ №152

4. Установите последовательность фаз целевой атаки?
   - Достижение целей
   - Проникновение
   - Подготовка
   - Распространение

5. Какая ответственность предусмотрена согласно статье 274.1 УК РФ за невыполнение требований по безопасности КИИ, нарушение правил эксплуатации?
   - до 6 лет лишения свободы.
   - штраф от 100 до 500 тысяч рублей для организаций, от 10 до 20 тысяч рублей для должностных лиц
   - до 3 лет лишения свободы
   - до 10 лет лишения свободы

6. Классифицируйте межсетевые экраны согласно Модели OSI.

Шлюзы сеансового уровня	Сетевой, Транспортный, Сеансовый, Уровень представления, Прикладной
Посредники прикладного уровня	Прикладной уровень

Пакетные фильтры	Транспортный, Сетевой, Сеансовый
Управляемые коммутаторы	Транспортный, Сетевой
Инспекторы состояния	Физический, Канальный

7. Что позволяет обнаруживать система IPS?
   - изменения тенденций сетевого трафика
   - несанкционированный доступ
   - обращения к небезопасным ресурсам из сети организации
   - блокировать небезопасный трафик

8. Определите какие протоколы из данных вариантов являются промышленными?
   - ModBus
   - SNMP
   - S7Comm
   - OPC UA
   - Profibus
   - HTTP
   - DNS

9. Чем отличается уровень SCADA от уровня I/O?
   - SCADA контролирует выполнение технологического процесса и инициирует управляющие команды, I/O это исполнительные устройства и датчики, непосредственно воздействующие на технологический процесс.
   - SCADA передает информацию о состоянии объекта напрямую в ERP, получая ее напрямую от I/O.
   - I/O относится к АСУ ТП, SCADA относится к АСУ П.
   - SCADA не может работать без I/O, а I/O может работать без SCADA.

10. Какие существуют проблемы информационной безопасности промышленных объектов?
    - Отсутствие средств обнаружения и предотвращения компьютерных атак.
    - Использование операционных систем, программных и программно-аппаратных средств иностранных производителей
    - Использование средств защиты различных производителей
    - Разделений функций по управлению и администрированию автоматизированной системы

Дисциплина «Подготовка среды функционирования и первоначальная настройка комплекса InfoWatch ARMA»

1. Какое программное обеспечение дополнительно рекомендуется установить для выполнения практических заданий?
   - ModbusPal
   - Zenmap
   - Snap7 Server Demo
   - MIB Browser
   - qModMaster
   - WinSCP
   - PowerShell

2. Укажите минимальные ресурсные требования для ВМ Комплекс AIF.
   - Одноядерный процессор(2 ГГц), ОЗУ 4 ГБ, Сетевые интерфейсы Ethernet - 3 шт., HDD-25 ГБ
   - Одноядерный процессор(2 ГГц), ОЗУ 8 ГБ, Сетевые интерфейсы Ethernet - 2 шт., HDD-25 ГБ
   - Одноядерный процессор(1,5 ГГц), ОЗУ 8 ГБ, Сетевые интерфейсы Ethernet - 1 шт., HDD-45 ГБ
   - Одноядерный процессор(2 ГГц), ОЗУ 4 ГБ, Сетевые интерфейсы Ethernet - 4 шт., HDD-25 ГБ

3. Распределите на соответствия виртуальные машины и их сетевые настройки согласно тренировочному стенду.

ВМ "Клиент"	em0 (net 1)- 192.168.1.1/24, em2 (net 2) - 192.168.2.1/24, em1 - dhcp (nat)
ВМ "Сервер"	Net 2, 192.168.2.100/24, 192.168.1.1
ВМ Комплекс	Net 1, 192.168.1.200/24, 192.168.2.1

4. Выберите верный порядок настройки сетевого времени:
   - Службы→Сетевое время→Общие настройки
   - Службы→Общие настройки→Сетевое время
   - Система →Параметры →Сетевое время
   - Службы →Кэширующий DNS-сервер

5. Какая информация отсутствует в статусе службы "Сетевое время"?
   - Часовой слой
   - Тип
   - Ref ID
   - Опрос
   - Порядок
   - Охват
   - Неустойчивость
   - Мировое время

6. Как добавить нового пользователя?
   - Система →Доступ →Группы
   - Система →Доступ →Пользователи
   - Система →Настройки →Пользователи
   - Система →Конфигурация

7. Можно ли указать новому пользователю дату окончания срока действия учетной записи?
   - Да
   - Нет
   - Только администраторам
   - Только users

8. Укажите верный вариант проверки доступности хоста?
   - Интерфейсы → Диагностика → Ping
   - Интерфейсы →Ping
   - Интерфейсы →Другие типы →Сетевой мост
   - Интерфейсы →Диагностика →Просмотр DNS-записей

9. В процессе создания пользователя возможно ли указать доступ к консольному интерфейсу?
   - Да
   - Нет

10. Для чего указываются системные привилегии при создании пользователя?
    - для определения видимых разделов веб-интерфейса данного пользователя
    - для указания статуса пользователя
    - для настройки приоритета доступа пользователя
    - для гибкой настройки возможностей

Дисциплина «Обзор и практическая реализация возможностей комплекса InfoWatch ARMA»

1. Какие из представленных типов можно выбрать в процессе создания псевдонима?
   - Хосты
   - Сети
   - Порты
   - URL
   - HTTPS
   - Сетевая группа
   - Мосты

2. В процессе редактирования межсетевого правила какое действие невозможно использовать?
   - Блокирование
   - Отклонить
   - Разрешить
   - Отбросить

3. Определите порядок действий для добавления расписания срабатывания межсетевого правила?
   - Перейти в «Межсетевой экран» → «Настройки» → «Расписания».
   - Нажать кнопку «Добавить»
   - В открывшейся форме задать параметры расписания
   - Нажать кнопку "Добавить время"
   - Применить расписание к правилам

4. Определите верный порядок экспорта событий по протоколу syslog/cef?
   - Перейти в настройки экспорта событий системы «Система» - «Настройки» - «Экспорт событий»
   - Проверить результаты экспорта
   - В открывшейся форме установить флажок для параметра «Включен».
   - Выбрать Формат, Имя хоста, Порт

5. На базе какого программного обеспечения реализован "Модуль системы обнаружения вторжений" в AIF?
   - SNORT
   - NFTABLES
   - SURICATA
   - IPTABLES

6. За счет чего функционал подсистемы контроля промышленных протоколов обеспечивает интеллектуальное распознавание протоколов прикладного уровня?
   - сигнатурного анализа
   - EtherCat
   - контроля ошибок
   - приоритета устройств

7. Установите верный порядок просмотра отличий между версиями конфигураций?
   - Система
   - Конфигурация
   - Отличия
   - История изменений

8. Установите верную последовательность настройки прозрачного режима работы?
   - Интерфейсы → Другие типы →Сетевой мост
   - Указать интерфейсы – участники
   - Интерфейсы→Назначение портов→Добавить
   - Создание разрешающего правила для интерфейса прозрачного моста
   - Включение и настройка созданного интерфейса прозрачного моста

9. Укажите какие пакеты программного обеспечения необходимо установить перед установкой Arma Management Console?
   - elasticsearch 7.12.0
   - gettext
   - bash
   - openssl
   - acl
   - iptables
   - make
   - gcc
   - nano

10. С помощью какого сервиса выполняется обнаружение устройств в Arma Industrial Firewall?
    - ARPwatch
    - Cron
    - Cef
    - Devwatch

ИТОГОВАЯ АТТЕСТАЦИЯ

1. Установите верную последовательность настройки прозрачного режима работы?
   - Интерфейсы → Другие типы →Сетевой мост
   - Указать интерфейсы – участники
   - Интерфейсы→Назначение портов→Добавить
   - Создание разрешающего правила для интерфейса прозрачного моста
   - Включение и настройка созданного интерфейса прозрачного моста

2. Укажите какие пакеты программного обеспечения необходимо установить перед установкой Arma Management Console?
   - elasticsearch 7.12.0
   - gettext
   - bash
   - openssl
   - acl
   - iptables
   - make
   - gcc
   - nano

3. На базе какого программного обеспечения реализован "Модуль системы обнаружения вторжений" в AIF?
   - SNORT
   - NFTABLES
   - SURICATA
   - IPTABLES

4. За счет чего функционал подсистемы контроля промышленных протоколов обеспечивает интеллектуальное распознавание протоколов прикладного уровня?
   - сигнатурного анализа
   - EtherCat
   - контроля ошибок
   - приоритета устройств

5. Определите верный порядок экспорта событий по протоколу syslog/cef?
   - Перейти в настройки экспорта событий системы «Система» - «Настройки» - «Экспорт событий»
   - Проверить результаты экспорта
   - В открывшейся форме установить флажок для параметра «Включен».
   - Выбрать Формат, Имя хоста, Порт

6. Как добавить нового пользователя?
   - Система →Доступ →Группы
   - Система →Доступ →Пользователи
   - Система →Настройки →Пользователи
   - Система →Конфигурация

7. Можно ли указать новому пользователю дату окончания срока действия учетной записи?
   - Да
   - Нет
   - Только администраторам
   - Только users

8. Выберите верный порядок настройки сетевого времени:
   - Службы→Сетевое время→Общие настройки
   - Службы→Общие настройки→Сетевое время
   - Система →Параметры →Сетевое время
   - Службы →Кэширующий DNS-сервер

9. Какая информация отсутствует в статусе службы "Сетевое время"?
   - Часовой слой
   - Тип
   - Ref ID
   - Опрос
   - Порядок
   - Охват
   - Неустойчивость
   - Мировое время

10. Какое программное обеспечение дополнительно рекомендуется установить для выполнения практических заданий?
    - ModbusPal
    - Zenmap
    - Snap7 Server Demo
    - MIB Browser
    - qModMaster
    - WinSCP
    - PowerShell

11. В каком порядке организована структура АСУ ТП (снизу-вверх)?

- I/O – PLC – SCADA – MES – ERP
- I/O –SCADA – MES – ERP – PLC
- I/O – PLC – SCADA – ERP – MES
- I/O – SCADA – PLC – MES – ERP

12. В каком Федеральном законе (ФЗ) изложены требования по обеспечению безопасности КИИ?
    - ФЗ №187
    - ФЗ №239
    - ФЗ №149
    - ФЗ №152

13. Установите последовательность фаз целевой атаки?
    - Достижение целей
    - Проникновение
    - Подготовка
    - Распространение

14. Какая ответственность предусмотрена согласно статье 274.1 УК РФ за невыполнение требований по безопасности КИИ, нарушение правил эксплуатации?
    - до 6 лет лишения свободы.
    - штраф от 100 до 500 тысяч рублей для организаций, от 10 до 20 тысяч рублей для должностных лиц
    - до 3 лет лишения свободы
    - до 10 лет лишения свободы

15. Классифицируйте межсетевые экраны согласно Модели OSI.

Шлюзы сеансового уровня	Сетевой, Транспортный, Сеансовый, Уровень представления, Прикладной
Посредники прикладного уровня	Прикладной уровень
Пакетные фильтры	Транспортный, Сетевой, Сеансовый
Управляемые коммутаторы	Транспортный, Сетевой

Инспекторы состояния	Физический, Канальный

16. Что позволяет обнаруживать система IPS?
    - изменения тенденций сетевого трафика
    - несанкционированный доступ
    - обращения к небезопасным ресурсам из сети организации
    - блокировать небезопасный трафик

17. Определите какие протоколы из данных вариантов являются промышленными?
    - ModBus
    - SNMP
    - S7Comm
    - OPC UA
    - Profibus
    - HTTP
    - DNS

18. Чем отличается уровень SCADA от уровня I/O?
    - SCADA контролирует выполнение технологического процесса и инициирует управляющие команды, I/O это исполнительные устройства и датчики, непосредственно воздействующие на технологический процесс.
    - SCADA передает информацию о состоянии объекта напрямую в ERP, получая ее напрямую от I/O.
    - I/O относится к АСУ ТП, SCADA относится к АСУ П.
    - SCADA не может работать без I/O, а I/O может работать без SCADA.

19. Какие существуют проблемы информационной безопасности промышленных объектов?
    - Отсутствие средств обнаружения и предотвращения компьютерных атак.
    - Использование операционных систем, программных и программно-аппаратных средств иностранных производителей
    - Использование средств защиты различных производителей
    - Разделений функций по управлению и администрированию автоматизированной системы

20. В процессе редактирования межсетевого правила какое действие невозможно использовать?
    - Блокирование
    - Отклонить
    - Разрешить
    - Отбросить

ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

Требования к квалификации педагогических кадров, представителей предприятий и организаций, обеспечивающих реализацию образовательного процесса

Требования к образованию и обучению лица, занимающего должность преподавателя: высшее образование - специалитет или магистратура, направленность (профиль) которого, как правило, соответствует преподаваемому учебному курсу, дисциплине (модулю).

Дополнительное профессиональное образование на базе высшего образования (специалитета или магистратуры) - профессиональная переподготовка, направленность (профиль) которой соответствует преподаваемому учебному курсу, дисциплине (модулю).

Педагогические работники обязаны проходить в установленном законодательством Российской Федерации порядке обучение и проверку знаний и навыков в области охраны труда.

Рекомендуется обучение по дополнительным профессиональным программам по профилю педагогической деятельности не реже чем один раз в три года.

Требования к опыту практической работы: при несоответствии направленности (профиля) образования преподаваемому учебному курсу, дисциплине (модулю) – наличие у преподавателей опыта работы в области профессиональной деятельности, осваиваемой обучающимися или соответствующей преподаваемому учебному курсу, дисциплине (модулю).

Преподаватель: стаж работы в образовательной организации не менее одного года; при наличии ученой степени (звания) - без предъявления требований к стажу работы.

Особые условия допуска к работе: отсутствие ограничений на занятие педагогической деятельностью, установленных законодательством Российской Федерации.

Прохождение обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований), а также внеочередных медицинских осмотров (обследований) в порядке, установленном законодательством Российской Федерации

Прохождение в установленном законодательством Российской Федерации порядке аттестации на соответствие занимаемой должности.

Требования к материально-техническим условиям

Образовательный процесс осуществляется с применением дистанционных образовательных технологий, с учетом чего созданы условия для функционирования электронной информационно-образовательной среды.

Требования к оборудованию слушателя для проведения занятий

- персональный компьютер под управлением операционной системы Windows 10 и выше;
- видеокамера, микрофон и аудиосистема (колонки или наушники), подключенные к компьютеру;
- пакет Microsoft Office 2016 и выше;
- выход в Интернет;
- Интернет-браузер;

Требования к информационным и учебно-методическим условиям

Список литературы

1. InfoWatch ARMA Industrial Firewall. Руководство по установке https://docs.iwarma.ru/AFW/ra_firewall/Content/afw_ra_02_install.html
2. InfoWatch ARMA Industrial Firewall. Варианты развертывания https://docs.iwarma.ru/AFW/ra_firewall/Content/afw_ra_03_deployment-variants.html
3. InfoWatch ARMA Industrial Firewall. Описание локального интерфейса https://docs.iwarma.ru/AFW/ra_firewall/Content/afw_ra_06_cli.html
4. InfoWatch ARMA Industrial Firewall. Руководство по интерфейсу https://docs.iwarma.ru/AFW/rp_interface/index_afw_ri.html
5. InfoWatch ARMA Industrial Firewall. Межсетевой экран https://docs.iwarma.ru/AFW/rp_firewall/Content/afw_rp_01_firewall.html
6. InfoWatch ARMA Industrial Firewall. Система обнаружение и предотвращения вторжений https://docs.iwarma.ru/AFW/rp_firewall/Content/afw_rp_05_suricata.html
7. InfoWatch ARMA Industrial Firewall. Обнаружение устройств https://docs.iwarma.ru/AFW/rp_firewall/Content/afw_rp_06_device-detection.html
8. InfoWatch ARMA Industrial Firewall. SNMP https://docs.iwarma.ru/AFW/rp_firewall/Content/afw_rp_07_snmp.html
9. InfoWatch ARMA Industrial Firewall. Сервис Syslog https://docs.iwarma.ru/AFW/rp_firewall/Content/afw_rp_08_syslog.html
10. InfoWatch ARMA Industrial Firewall. Служба NTP https://docs.iwarma.ru/AFW/rp_firewall/Content/afw_rp_14_ntp.html
11. InfoWatch ARMA Industrial Firewall. Сетевой мост https://docs.iwarma.ru/AFW/rp_firewall/Content/afw_rp_17_bridge.html
12. InfoWatch ARMA Industrial Firewall. Учетные записи и права доступа https://docs.iwarma.ru/AFW/rp_firewall/Content/afw_rp_23_users-accounts.html
13. InfoWatch ARMA Industrial Firewall. DNSMasq https://docs.iwarma.ru/AFW/rp_firewall/Content/afw_rp_26_dnsmasq.html
14. InfoWatch ARMA Industrial Firewall. Журналирование https://docs.iwarma.ru/AFW/rp_firewall/Content/afw_rp_30_logging.html
15. InfoWatch ARMA Management Console. Установка и первоначальная настройка системы https://docs.iwarma.ru/AMC/ra_console/Content/amc_ra_install.html
16. InfoWatch ARMA Management Console. Управление лицензиями https://docs.iwarma.ru/AMC/ra_console/Content/amc_ra_license.html
17. InfoWatch ARMA Management Console. Веб-интерфейс, описание и работа https://docs.iwarma.ru/AMC/rp_console/Content/amc_rp_02_interface.html
18. InfoWatch ARMA Management Console. Карта сети https://docs.iwarma.ru/AMC/rp_console/Content/amc_rp_15_map.html
19. InfoWatch ARMA Management Console. Источники событий https://docs.iwarma.ru/AMC/rp_console/Content/amc_rp_devices.html
20. InfoWatch ARMA Management Console. Правила корреляции https://docs.iwarma.ru/AMC/rp_console/Content/amc_rp_10_rules.html

21. InfoWatch ARMA Management Console. Активы
https://docs.iwarma.ru/AMC/rp_console/Content/amc_rp_14_assets.html
22. InfoWatch ARMA Management Console. События
https://docs.iwarma.ru/AMC/rp_console/Content/amc_rp_events.html
23. InfoWatch ARMA Industrial Endpoint. Начало работы
https://docs.iwarma.ru/AIE/rp_endpoint/Content/aie_rp_02.html
24. InfoWatch ARMA Industrial Endpoint. Описание локального графического интерфейса
https://docs.iwarma.ru/AIE/rp_endpoint/Content/aie_rp_03.html
25. InfoWatch ARMA Industrial Endpoint. Настройка синхронизации с МС
https://docs.iwarma.ru/AIE/rp_endpoint/Content/aie_rp_04.html

Нормативные правовые акты

1. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ
2. «Конституция Российской Федерации» принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020
3. «Трудовой кодекс Российской Федерации» от 30.12.2001 № 197-ФЗ
4. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ
5. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ
6. Федеральный закон "О коммерческой тайне" от 29.07.2004 № 98-ФЗ
7. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ
8. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ
9. Приказ ФСТЭК России от 14.03.2014 N 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»
10. Указ Президента РФ от 01.05.2022 N 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

Интернет-ресурсы

1. https://docs.iwarma.ru
2. https://www.infowatch.ru/