областное государственное бюджетное
профессиональное образовательное учреждение
«Смоленская академия профессионального образования»

УТВЕРЖДАЮ
Директор ОГБПОУ СмолАПО
_____ М. В. Белокопытов

ПРОГРАММА ПРОФЕССИОНАЛЬНОГО ОБУЧЕНИЯ
ПОВЫШЕНИЕ КВАЛИФИКАЦИИ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

(в объеме 256 часов)

автор-составитель:
Кисельман М.В.,
преподаватель, ОГБПОУ
СмолАПО

Смоленск 2020 год

1. Наименование программы

Программа профессионального обучения повышение квалификации «Информационная безопасность».

2. Общая характеристика образовательной программы

2.1. Цель реализации программы:

Программа профессионального обучения повышения квалификации, направлена на формирование профессиональных компетенций, необходимых для профессиональной деятельности в области обеспечения информационной безопасности

2.2. Перечень нормативных документов, определяющих квалификационные требования к выпускнику программы.

Программа разработана на основе требований:

– Постановления Правительства Российской Федерации: № 313 от 16 апреля 2012 года «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»;

– Постановления Правительства Российской Федерации № 79 от 3 февраля 2012 года «О лицензировании деятельности по технической защите конфиденциальной информации»;

– профессионального стандарта «Специалист по безопасности компьютерных систем и сетей» утвержденного Приказом Минтруда России N 598н от 01.11.2016.

– спецификацией стандартов Ворлдскиллс по компетенции «Кибербезопасность».

2.3. Характеристика новой квалификации и связанных с нею видов профессиональной деятельности (квалификационных уровней) и трудовых функций:

– принимать участие в эксплуатации подсистем управления информационной безопасностью различных объектов информатизации;

– администрировать подсистемы информационной безопасности различных объектов информатизации;

– выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации;

– принимать участие в организации контрольных проверок работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

– формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности;

– организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры автоматизированных систем, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;

– проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области защиты информации;

– использовать нормативные правовые документы в своей профессиональной деятельности;

– разрабатывать проекты нормативных и методических документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности;

– организовать и сопровождать аттестацию объектов информатизации по требованиям безопасности информации.

2.4. Планируемые результаты обучения

По итогам освоения программы слушатель должен:

Знать:

– методы администрирования подсистем информационной безопасности различных объектов информатизации;

– комплекс мер по информационной безопасности;

– методы анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области защиты информации;

– нормативные правовые документы в своей профессиональной деятельности;

– основные нормативные и методические документы, регламентирующие работу по обеспечению информационной безопасности автоматизированных систем.

Уметь:

– формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности;

– организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры автоматизированных систем, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;

– проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области защиты информации;

– использовать нормативные правовые документы в своей профессиональной деятельности;

– разрабатывать проекты нормативных и методических документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем, а также положений, инструкций и других организационно-распорядительных документов в сфере профессиональной деятельности;

– организовать и сопровождать аттестацию объектов информатизации по требованиям безопасности информации.

Владеть:

– навыками организации контрольных проверок работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;

– навыками разработки комплекса мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности;

– средствами и способами анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области защиты информации;

– навыками разработки проектов нормативных и методических документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем.

3. Учебный и учебно-тематический планы

УЧЕБНЫЙ ПЛАН

программы профессионального обучения

«Информационная безопасность»

Требования к уровню образования поступающих на обучение	Обучение осуществляется на базе высшего и среднего профессионального образования.
Категория слушателей	Для сотрудников предприятий и организаций, работающих в сфере ИТ, желающихповысить профессиональный уровень в рамках имеющейся квалификации.
Срок обучения	16 недель
Форма обучения	очнаяс применением ЭО и ДОТ, очно-заочная ЭО и ДОТ
Режим занятий	16 часов в неделю

Учебно-тематический план программы профессионального обучения

№№ п/п	Наименование дисциплины (модуля), темы	Трудоемкость		В том числе				Форма контроля, в часах
				Аудиторные занятия*			Самостоятельная работа*	
				Всего часов	из них			
		В зачетныхединицах	В часах		Лекции	Практические занятия		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
1	**Модуль 1. Основы информационной безопасности**		**16**	**14**	**10**	**4**	**2**	Тестирование, 2 ч.
1.1	Тема 1.1. Теория информационной безопасности и методология защиты информации		4	4	2	-	2	-
1.2	Тема 1.2. Правовое, нормативное и методическое регулирование деятельности в области защиты информации		6	6	2 2*	2*	-	-
1.3	Тема 1.3. Правовые		6	4	2*	2*	-	2

*С применением дистанционных образовательных технологий и электронного обучения

	основы организации защиты государственной тайны, задачи органов защиты государственной тайны							
2	**Модуль 2. Техническая защита информации**		**48**	**40**	**18**	**22**	**6**	Тестирование, решение практической задачи, 2 ч.
2.1	Тема 2.1. Угрозы и уязвимости автоматизированных информационных систем.		8	8	2 2*	2 2*	-	-
2.2	Тема 2.2. Классификация технических каналов утечки информации.		10	8	2 2*	2 2*	2	-
2.3	Тема 2.3. Виды уязвимостей автоматизированных информационных систем.		8	8	2 2*	2 2*	-	-
2.4	Тема 2.4. Оценка уровня защищённости информационных систем.		14	10	4	2 4*	4	-
2.5	Тема 2.5. Методы и средства технической защиты информации		8	6	2	2 2*	-	2
3	**Модуль 3. Защита информации с использованием шифровальных (криптографических) средств**		***96***	***82***	***38***	***48***	***10***	Тестирование, решение практической задачи, 4 ч.
3.1	Тема 3.1. Криптографические методы защиты информации.		*48*	*42*	*6* *12**	*12* *12**	*6*	-
3.2	Тема 3.2. Обеспечение применения электронной подписи и инфраструктуры открытого ключа с использованием сертифицированных средств		*48*	*40*	*6* *10**	*12* *12**	*4*	4

***С применением дистанционных образовательных технологий и электронного обучения**

4	**Модуль 4. Комплексная защита объектов информатизации**		***32***	***28***	***12***	***18***	***2***	Тестирование,решение практической задачи, 2 ч.
4.1	Тема 4.1. Информационная безопасность автоматизированных систем.		*6*	*6*	*2*	*2* *2**	-	-
4.2	Тема 4.2. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах (ИСПДн).		*12*	*6*	*2* *2**	*2* *4**	*2*	-
4.3	Тема 4.3. Особенности защиты информации, составляющей коммерческую тайну компании.		*6*	*6*	*2**	*4*	-	-
4.4	Тема 4.4. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры		*8*	*6*	*2*	*4*	-	2
5	**Модуль 5. Управление информационной безопасностью**		***42***	***36***	***12***	***24***	***4***	Тестирование, решение практической задачи, 2 ч.
5.1	Тема 5.1. Управление информационной безопасностью.		*8*	*8*	*2*	*6**	-	-
5.2	Тема 5.2. Организация конфиденциального делопроизводства.		*12*	*10*	*2* *2**	*6**	*2*	-
5.3	Тема 5.3. Аудит информационной безопасности.		*10*	*10*	*2* *2**	*2* *4**	-	-
5.4	Тема 5.4. Экономика защиты информации.		*12*	*8*	*2*	*2* *4**	*2*	2
6	**Модуль 6. Дополнительные инструменты обеспечения информационной**		***16***	***14***	***6***	***8***	-	Тестирование, 2 ч.

***С применением дистанционных образовательных технологий и электронного обучения**

	безопасности							
6.1	Тема 6.1. Методики обоснования выбора средств технической и криптографической защиты информации.		*2*	*2*	-	*2*		
6.2	Тема 6.2. Особенности эксплуатации технических средств защиты информации.		*4*	*4*	*2*	*2*		
6.3	Тема 6.3. Выбор, установка, настройка и эксплуатация средств антивирусной защиты.		*4*	*4*	*2*	*2*		
6.4	Тема 6.4. Программные средства анализа рисков информационной безопасности		*6*	*4*	*2*	*2*	-	2
	Всего:		250	214	88	124	24	14
	Итоговая аттестация		6	6				Итоговая аттестация
	Общая трудоемкость программы:	256						

4. Календарный учебный график

Программа профессионального обучения «Информационная безопасность»

Объем программы 256 час.
Продолжительность обучения 11 недель
Форма обучения – очнаяс применением ЭО и ДОТ, очно-заочная с применением ЭО и ДОТ

Образовательный процесс по программе может осуществляться в течение всего учебного года. Занятия проводятся по мере комплектования групп.

Период обучения (недели)*	Наименование модуля
1 неделя	Модуль 1. Основы информационной безопасности
2-4 неделя	Модуль 2. Техническая защита информации
5-10 неделя	Модуль 3. Защита информации с использованием шифровальных (криптографических) средств
11-12 неделя	Модуль 4. Комплексная защита объектов информатизации
13-15 неделя	Модуль 5. Управление информационной безопасностью
15-16 неделя	Модуль 6. Дополнительные инструменты обеспечения информационной безопасности
16 неделя	Итоговая аттестация
*-Точный порядок реализации модулей (дисциплин) обучения определяется в расписании занятий.	

5. Содержание программы

Модуль 1. Основы информационной безопасности

Тема 1.1. Теория информационной безопасности и методология защиты информации

Составляющие интересов РФ по ИБ. Методы обеспечения ИБ. Угрозы информационной безопасности.

Тема 1.2. Правовое, нормативное и методическое регулирование деятельности в области защиты информации

Система документов в области ТЗИ, а также ТКЗИ. Нормативные правовые акты ФСТЭК России. Методические документы. Документы в области технического регулирования и стандартизации. Техническая документация

Тема 1.3. Правовые основы организации защиты государственной тайны, задачи органов защиты государственной тайны

Государственная тайна. Принципы засекречивания информации.Перечень сведений, составляющих государственную тайну. Степени секретности.

Модуль 2. Техническая защита информации

Тема 2.1. Угрозы и уязвимости автоматизированных информационных систем

Атаки на автоматизированные системы. Уязвимости автоматизированных систем. Классификация и модели компьютерных атак. Модели атак.

Тема 2.2. Классификация технических каналов утечки информации

Структура, задачи и функции системы технической защиты информации. Утечка. Среда распространения носителя. Понятие информационного сигнала. Опасные сигналы и их источники.

Тема 2.3. Виды уязвимостей автоматизированных информационных систем

Уязвимость информационной системы.Уязвимости отдельных протоколов стека протоколов TCP/IP. Уязвимости прикладного программного обеспечения.

Тема 2.4. Оценка уровня защищённости информационных систем.

Уровни защищенности персональных данных.Защита типовой системы. Оценки защищенности на основе модели комплекса механизмов защиты. Семантические показатели защищенности ИС.

Тема 2.5. Методы и средства технической защиты информации

Основные угрозы целостности. Основные угрозы конфиденциальности. Методы и средства инженерно-технической защиты. Криптографические методы защиты и шифрование. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.

Модуль 3. Защита информации с использованием шифровальных (криптографических) средств

Тема 3.1. Криптографические методы защиты информации.

Криптография. Симметричное шифрование. Асимметричное шифрование.Криптография с открытыми ключами. Сертификаты открытых ключей.

Тема 3.2. Обеспечение применения электронной подписи и инфраструктуры открытого ключа с использованием сертифицированных средств

Электронная цифровая подпись. Назначение и применение ЭП. Виды электронных подписей в Российской Федерации.

Модуль 4. Комплексная защита объектов информатизации

Тема 4.1. Информационная безопасность автоматизированных систем.

Уязвимости. Информационные атаки. Последствия информационных атак. Существующие методы и средства защиты от информационных атак.

Тема 4.2. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах (ИСПДн).

Термины и определения.Понятие информационной системы персональных данных. Классификацияинформационных систем персональных данных. Общий порядок организации обеспечения безопасности персональных данных.

Тема 4.3. Особенности защиты информации, составляющей коммерческую тайну компании.

Определение понятий. Угрозы. Способы получения информации, составляющей коммерческую тайну. Меры защиты.

Тема 4.4. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры

Комплексы организационных и технических мер. Комплексный подход к обеспечению информационной безопасности.

Модуль 5. Управление информационной безопасностью

Тема 5.1. Управление информационной безопасностью.

InformationSecurityManagement.Политика информационной безопасности. Ключевые деятельности.

Тема 5.2. Организация конфиденциального делопроизводства.

Персональные данные.Правила получения персональных данных. Правила передачи персональных данных работника. Роль HR-менеджеров.

Тема 5.3. Аудит информационной безопасности.

Что такое аудит безопасности.Виды аудита безопасности. Состав работ. Сбор исходных данных для проведения аудита. Результаты аудита безопасности.

Тема 5.4. Экономика защиты информации

Рынок информации. Правовые аспекты взаимодействия субъектов на рынке информации. Экономическая эффективность защиты информации. Интеллектуальная собственность предприятия и ее защита. Предпринимательский риск.

Модуль 6. Дополнительные инструменты обеспечения информационной безопасности

Тема 6.1. Методики обоснования выбора средств технической и криптографической защиты информации.

Оценки целесообразности использования СКЗИ. Когда же необходимо использовать СКЗИ.

Тема 6.2. Особенности эксплуатации технических средств защиты информации.

Особенности проведения аттестации объектов информатизации.Специфика аттестации автоматизированных систем.

Тема 6.3. Выбор, установка, настройка и эксплуатация средств антивирусной защиты.

Как обеспечить надежную антивирусную защиту.Какой антивирус выбрать. Установка и настройка.

Тема 6.4. Программные средства анализа рисков информационной безопасности

Проблема оценки рисков ИБ. Методики и программные продукты для оценки рисков. Основные этапы оценки рисков.

6. Организационно-педагогические условия реализации программы

6.1. Материально-технические условия

Для реализации программы профессионального обучения «Информационная безопасность» предусмотрены мастерская «Сетевого и системного администрирования» и мастерская «Кибер-безопасности».

Мастерская «Кибер-безопасности» оснащена следующим оборудованием и программным обеспечением:

- Персональный компьютер в сборе: Processor - AMD Ryzen X8 R7-1700, DDR4 DIMM 32Гб, Видеокарта - ASUS GeForce GTX 1650 PHOENIX OC [PH-GTX1650-04G], SD накопитель A-DATA S11 Pro AGAMMIXS11P-512GT-C 512 Гб;
- Компьютерный монитор AOC 24" G2460VQ6;
- Клавиатура USB CBR KB 107;
- Компьютерная мышь USB CBR CM-302;
- Источник бесперебойного питания Powercom UPS RPT-800A EURO;
- Сервер [2U / 2 x Intel Xeon Silver 4210R (2.4GHz,10C) / 8 x 32Gb DDR4 2933, ECC R(24up) / 4x960Gb SSD SATA / 4 x 10GE / 2 x 800w;
- Управляемый Коммутатор Cisco WS-C2960L-48;
- Коммутатор L3 WS-C3650-24;
- Телевизор 50” LED Haier LE50K5500TF;
- Флипчат электронный SMART kapp 42;
- Интерактивная доска ScreenMedia;
- Проектор CASIO XJ-V110W с потолочным креплением и коммутацией;
- МФУ Canon i-SENSYS MF426dw;
- USB-токен JaCarta-2 PKI/ГОСТ (XL) JC-MediaKit-4 - "ПКJaCarta – MediaKit,
- РутокенЭЦП 2.0 64 кб;
- RDS-01 USB считывательключей Dallas Touch Memory (iButton);
- DS1996 сизогнутымбрелоком - электронныйключDallasTouchMemory (IButton);
- FindkeyHamster III (HFDU06S) - настольный биометрический считыватель;
- Установочный комплект. Средство защиты информации SecretNetStudio 8;
- Установочный комплект. Средство защиты информации vGate R2;
- Дистрибутив СКЗИ КриптоПро CSP версии 5.0 КС1 и КС2 на DVD;
- Формуляры DallasLock 8.0-К. Право на использование** (СЗИ НСД.СКН); Бессрочная лицензия DallasLock 8.0. Сертифицированный комплект для установки;

- Программное обеспечение клиентского доступа к виртуальным машинам AcademicVMwareWorkstation 15 ProforLinuxandWindows;
- СистемавиртуализацииVMWare ESXI 7.0, VMWare Workstation Pro, Oracle VirtualBox;
- ПО операционная система Windows 10 с интегрированной программной платформой .NET Framework, 4.8;
- ПО для просмотра документов в формате PDF AdobeReader DC;
- ПО для архивации 7-Zip;
- ПО офисный пакет MicrosoftOffice 2019;
- СистемавиртуализацииVMWare ESXI 7.0, VMWare Workstation Pro, Oracle VirtualBox;
- Антивирусное программное обеспечение KasperskyEndpointSecurity.

Мастерская «Сетевого и системного администрирования» оснащена следующим оборудованием и программным обеспечением:

- Персональный компьютер в сборе ЦПУ: Intel® Core™ i7-9700, ОЗУ: объем 32 Гб SSDIntelSSD 760P 512GB;
- Компьютерный монитор AOC 24" G2460VQ6
- Клавиатура USB ZERO-X51/X52/X08
- Компьютерная мышь USB CBR CM-302
- Источник бесперебойного питания PowercomUPSRPT-800AEURO
- Сервер Сервер [2U / 2 xIntelXeonSilver 4210R (2.4GHz,10C) / 8 x 32GbDDR4 2933 ECCR(24up) / 4x960GbSSDSATA / 4 x 10GE / 2 x 800w]
- Маршрутизатор Cisco ISR4321
- Управляемый коммутатор КоммутаторCisco WS-C2960R-24-TC-L
- Межсетевой экран ASA5506-SEC-BUN-K9
- IP телефон Cisco IP Phone CP-7841-K9
- Коммутатор L3 WS-C3650-24
- Консольный сервер Aten
- Телевизор 50” LED Haier LE50K5500TF
- Флипчат электронный SMART kapp 42
- Интерактивная доска ScreenMedia
- Проектор CASIO XJ-V110W с потолочным креплением и коммутацией
- МФУ Canoni-SENSYSMF426dw
- ПО операционная система Windows 10 с интегрированной программной платформой .NET Framework, 4.8

- ПО для просмотра документов в формате PDF AdobeReader DC
- ПО для архивации 7-Zip
- ПО офисный пакет MicrosoftOffice 2019
- СистемавиртуализацииVMWare ESXI 7.0, VMWare Workstation Pro, Oracle VirtualBox

Каждое рабочее место, оснащено персональным компьютером с высокоскоростным доступом к сети Интернет

6.2. Учебно-методическое и информационное обеспечение программы

– Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — М.: КноРус, 2016. — 136 с.

– Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2017. — 384 с.

– Запечников, С.В. Информационная безопасность открытых систем. В 2-х т. Т.1 — Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г. Милославская. — М.: ГЛТ, 2017. — 536 с.

– Нурдинов Р.А. ОБОСНОВАНИЕ ЦЕЛЕСООБРАЗНОСТИ ВЫБОРА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ // Современные наукоемкие технологии. – 2014. – № 5-1. – С. 81-82;

– Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. — М.: Форум, 2016. — 432 с.

– Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ, 2017. — 336 с.

– Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. — М.: ДМК, 2017. — 702 с.

– Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. — М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2017. — 416 с.

– официальный сайт оператора международного некоммерческого движения WorldSkillsInternational - Союз «Молодые профессионалы (Ворлдскиллс Россия)» (электронный ресурс) режим доступа: https://worldskills.ru;

– единая система актуальных требований Ворлдскиллс (электронный ресурс) режим доступа: https://esat.worldskills.ru

6.3. Кадровые условия

Физические лица, привлеченные для реализации программы, которые могут являться:

- Преподаватель профессиональных модулей по специальностям10.02.01 Организация и технология защиты информации, 09.02.06 Сетевое и системное администрирование.

- Сертифицированный эксперт Ворлдскиллс по компетенцииКибербезопасность, Сетевое и системное администрирование.

- Сертифицированный эксперт-мастер Ворлдскиллс по компетенции Кибербезопасность, Сетевое и системное администрирование.

- Эксперт с правом проведения чемпионата по стандартам Ворлдскиллс по компетенции Кибербезопасность, Сетевое и системное администрирование.

- Эксперт с правом оценки демонстрационного экзамена по стандартам Ворлдскиллспокомпетенции Кибербезопасность, Сетевое и системное администрирование.

6.4. Условия для функционирования электронной информационно-образовательной среды (при реализации программ с использованием дистанционных образовательных технологий):

- наличие системы дистанционного обучения на основе Moodle - http://do.smolapo.ru/

- системы видеоконференцсвязи(ВКС) – Zoom, Discord.

7. Описание контроля качества освоения программы

7.1. Формы текущего контроля успеваемости, особенности их применения

Проводятся в форме Тестирования (при реализации программ с использованием дистанционных образовательных технологий – онлайн тестирование в системе http://do.smolapo.ru/).

7.2. Формы промежуточной аттестации

- Тестирование.
- Решения практической задачи.

7.3. Форма итоговой аттестации

Экзамен по методике Ворлдскиллс.