МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение
высшего образования

«САНКТ–ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

УТВЕРЖДЕНО

решением Ученого совета ГУАП

«28» 09 2021 г.

(протокол № Ж-07)

Ректор ГУАП

_____ Ю.А. Антохина

«28» 09 2021 г.

ПРОГРАММА

ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Корпоративная защита от внутренних угроз информационной безопасности с использованием современных DLP технологий» (с учетом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»)»

(наименование программы)

Санкт-Петербург, 2021

Лист согласования

Программу составили

Ст. преподаватель каф. №52 должность, уч. степень, звание	подпись, дата	Н.В. Матвеев инициалы, фамилия

Декан ФДПО

Д-р экон. наук, профессор каф. 82 должность, уч. степень, звание	подпись, дата	А.М. Мельниченко инициалы, фамилия

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Цель реализации программы

Целью реализации программы является совершенствование и (или) формирование у слушателей новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации в области информационной безопасности.

Программа разработана с учетом потребностей специалистов в области информационной безопасности и компьютерных систем и сетей.

Программа разработана на основании требований профессионального стандарта 06.032 профессиональным стандартом «Специалист по безопасности компьютерных систем и сетей» (утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 года N 598н) и с учетом спецификации стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности».

1.2. Планируемые результаты обучения

Изучение данной программы направлено на формирование и (или) совершенствование у слушателей следующих компетенций:

профессиональные компетенции:

ПК-1 - Осуществлять и обосновывать выбор решений по использованию систем защиты информации от внутренних угроз DLPIWTM.

Знать:

- спецификацию стандарта компетенции «Корпоративная защита от внутренних угроз информационной безопасности»
- современные профессиональные технологии в предметной (профессиональной) сфере деятельности;
- принципы проектирования системы корпоративной защиты от внутренних угроз;
- основные правовые понятия и нормативно-правовые документы, регламентирующие организацию корпоративной защиты от внутренних угроз в хозяйствующих субъектах;
- инструментарий, технологии, их область применения и ограничения при формировании корпоративной защиты от внутренних угроз.
- типовые организационно-штатные структуры организаций различных сфер деятельности и размера;
- типовой набор объектов защиты, приоритеты доступа к информации, типовые роли пользователей;
- каналы передачи данных: определение и виды;
- подходы и методы обследования объекта информатизации для последующей защиты;
- сетевые устройства, которые могут быть использованы как источники событий для анализа;
- технологии работы с политиками информационной безопасности;
- основные функции системы DLPIWTM;
- категорирование информации в РФ;
- типы угроз информационной безопасности, понимать их актуальность и степень угрозы для конкретной организации;
- алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных;
- технику безопасности и экологию производства.

Уметь:

- разрабатывать нормативно-правовые документы хозяйствующего субъекта по организации корпоративной защиты от внутренних угроз информационной безопасности;

- проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации;
- администрировать автоматизированные технические средства управления и контроля информации и информационных потоков;
- осуществлять установку и конфигурирование систем DLPIWTM;
- разрабатывать политики детектирования и блокировки утечек с использованием DLP-систем;
- показать свой профессионализм и отношение к профессии;
- поддерживать в чистоте и подготовить рабочее место;
- работать в DLP-системе с событиями, запросами, объектами защиты, политиками, сводками, виджетами, персонами.

Лицам, успешно освоившим программу повышения квалификации и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации.

1.3. Требования к уровню подготовки поступающего на обучение, необходимому для освоения программы

К освоению ДПП ПК допускаются:
- лица, имеющие среднее профессиональное и (или) высшее образование;
- лица, получающие среднее профессиональное и (или) высшее образование.

1.4. Объем ДПП и форма обучения

Объем ДПП, который включает все виды аудиторной и самостоятельной работы слушателя, практики и время, отводимое на контроль качества освоения слушателем программы составляет 144 часа.

Форма обучения: очная с использованием дистанционных образовательных технологий.

2. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

2.1. Требования к организации образовательного процесса

Учебные занятия проводятся по 4-6 часов в день.

Для всех видов аудиторных занятий академический час устанавливается продолжительностью 45 минут.

Учебные занятия проводятся парами (два академических часа), продолжительность одной пары 90 минут.

Между парами предусмотрены перерывы не менее 10 минут.

При реализации ДПП ПК используются следующие образовательные технологии: личностно-ориентированная, проблемная, учебно-модульная.

2.2. Кадровое обеспечение

Образовательный процесс по ДПП ПК обеспечивается научно-педагогическими кадрами, имеющими высшее образование, направленность (профиль) которого, как правило, соответствует преподаваемому курсу, дисциплине (модулю), опыт работы в соответствующей профессиональной сфере и (или) систематически занимающимися научной деятельностью.

При отсутствии педагогического образования научно-педагогические кадры, обеспечивающие образовательный процесс по ДПП ПК, имеют дополнительное профессиональное образование в области профессионального образования и (или) обучения.

Также научно-педагогические кадры проходят в установленном законодательством Российской Федерации порядке обучение и проверку знаний и навыков в области охраны труда.

К образовательному процессу по ДПП ПК также привлечены преподаватели из числа действующих руководителей и ведущих работников профильных организаций, предприятий и учреждений.

Количество педагогических работников (физических лиц), привлеченных для реализации программы _4_чел. Из них:

- сертифицированных экспертов Ворлдскиллс по соответствующей компетенции _1_ чел.;
- сертифицированных экспертов-мастеров Ворлдскиллс по соответствующей компетенции _1_ чел.;
- экспертов с правом проведения чемпионата по стандартам Ворлдскиллс по соответствующей компетенции _2_чел.

Ведущий преподаватель программы – эксперт Ворлдскиллс со статусом сертифицированного эксперта Ворлдскиллс, или сертифицированного эксперта-мастера Ворлдскиллс, или эксперта с правом и опытом проведения чемпионата по стандартам Ворлдскиллс. Ведущий преподаватель программы принимает участие в реализации всех модулей и занятий программы, а также является главным экспертом на демонстрационном экзамене.

2.3. Материально-технические условия

Материально-технические условия приведены в п.п. 3.3. «Рабочие программы учебных предметов, курсов, дисциплин (модулей)».

2.4. Учебно-методическое и информационное обеспечение

Учебно-методическое и информационное обеспечение приведено в п.п. 3.3. «Рабочие программы учебных предметов, курсов, дисциплин (модулей)».

3. СОДЕРЖАНИЕ ПРОГРАММЫ

3.1. Календарный учебный график

Календарный учебный график приведен в таблице 1.

Срок обучения: 25 дней.

Объем ДПП ПК: 144 (час.)

Таблица 1 – Календарный учебный график

№ п/п	Наименование дисциплин (модулей)	Всего, час.	Календарный период, (дни)				
			1 день	2 день	3 день	4 день	5 день
1	Стандарты Ворлдскиллс и спецификация стандартов Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности». Разделы спецификации	3	Л/ПА*				
2	Актуальные требования рынка труда, современные технологии в профессиональной сфере	9	Л	Л	Л/ПА		
3	Требования охраны труда и техники безопасности	3			Л/ПА		
4	Практическое занятие на определение стартового уровня владения компетенцией	2				ПР*	
5	Основы цифровой гигиены	9				Л/ПР	ПР/ПА
			6 день	7 день	8 день	9 день	10 день
6	Программно-аппаратная защита	12	Л/ПР	Л/			

	информации			ПР/ПА			
7	Криптографическая защита информации	15			Л/ПР	Л/ПР	ПР/ПА
8	Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	23					Л
			11 день	12 день	13 день	14 день	15 день
			Л/ПР	Л/ПР	Л/ПР	ПР/ПА	
9	Технологии агентского мониторинга	21				Л/ПР	Л/ПР
			16 день	17 день	18 день	19 день	20 день
			Л/ПР	ПР/ПА			
10	Разработка политик безопасности, анализ выявленных инцидентов	21		Л	Л/ПР	Л/ ПР	Л/ПР
			21 день	22 день	23 день	24 день	25 день
			ПР/ПА				
11	Обследование (аудит) организации с целью защиты от угроз информационной безопасности	17	Л/ПР	Л/ПР	Л/ПР	ПА	
12	Итоговая аттестация	9				ИА*	ИА
ИТОГО, час.		144					

Примечания:

** Обозначение видов учебной деятельности:*
Л – лекции;
ПР – практические занятия;
СРС – самостоятельная работа;
ИА – итоговая аттестация.

3.2. Учебный план

Учебный план ДПП ПК, реализуемой в полном объеме с использованием аудиторных занятий (или дистанционных образовательных технологий) приведен в таблице 2.

Таблица 2 – Учебный план ДПП ПК, реализуемой в полном объеме с использованием аудиторных занятий (дистанционных образовательных технологий)

№ п/п	**Наименование дисциплин (модулей)**	**ОТ*, час.**	**Аудиторные/ дистанционные занятия, час.**				**Форма промежу-точной аттестации** (при наличии)	**Компетенции**
			Всего	**из них*** **				
				Лекции	**Лаб. раб.**	**Практ. занят., семинары**		
1	**2**	**3**	**4**	**5**	**6**	**7**	**9**	**10**
1	Стандарты Ворлдскиллс и спецификация стандартов Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности». Разделы спецификации	3	2	2			1 (тест)	ПК-1

2	Актуальные требования рынка труда, современные технологии в профессиональной сфере	9	7	7			2 (тест)	ПК-1
3	Требования охраны труда и техники безопасности	3		2			1 (тест)	ПК-1
4	Практическое занятие на определение стартового уровня владения компетенцией	2	2			2	-	ПК-1
5	Основы цифровой гигиены	9	8	2		6	1 (тест)	ПК-1
6	Программно-аппаратная защита информации	12	11	5		6	1 (тест)	ПК-1
7	Криптографическая защита информации	15	14	6		8	1 (тест)	ПК-1
8	Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	23	22	6		16	1 (тест)	ПК-1
9	Технологии агентского мониторинга	21	20	4		16	1 (тест)	ПК-1
10	Разработка политик безопасности, анализ выявленных инцидентов	21	20	4		16	1 (тест)	ПК-1
11	Обследование (аудит) организации с целью защиты от угроз информационной безопасности	17	16	8		8	1 (тест)	ПК-1
Итоговая аттестация		9					ДЭ**	ПК-1
ИТОГО:		144	124	46		78	11	

Примечания:

** ОТ – общая трудоемкость;*
*** ДЭ – демонстрационный экзамен.*

3.3. Рабочие программы учебных предметов, курсов, дисциплин (модулей)

Формы рабочей программы учебного предмета, курса, дисциплины (модуля), практики/ стажировки по ДПП ПК приведены ниже.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

«Стандарты Ворлдскиллс и спецификация стандартов Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности». Разделы спецификации»
(Название)

По ДПП ПК «Корпоративная защита от внутренних угроз информационной безопасности с использованием современных DLP технологий (с учетом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»)»
(Наименование ДПП)

Форма обучения: очная с использованием дистанционных образовательных технологий

1. Цель

Целью данного курса является изучение основных принципов, методов и средств защиты информации от утечек по техническим каналам передачи информации, с осуществлением выбора по использованию систем защиты информации от внутренних угроз DLP IWTM.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения ДПП

В результате освоения курса слушатель должен обладать следующими компетенциями:
профессиональные компетенции:
ПК-1 - Осуществлять и обосновывать выбор решений по использованию систем защиты информации от внутренних угроз DLPIWTM.
Знать:

- спецификацию стандарта компетенции «Корпоративная защита от внутренних угроз информационной безопасности»
- современные профессиональные технологии в предметной (профессиональной) сфере деятельности;
- принципы проектирования системы корпоративной защиты от внутренних угроз;
- основные правовые понятия и нормативно-правовые документы, регламентирующие организацию корпоративной защиты от внутренних угроз в хозяйствующих субъектах;
- инструментарий, технологии, их область применения и ограничения при формировании корпоративной защиты от внутренних угроз.
- типовые организационно-штатные структуры организаций различных сфер деятельности и размера;
- типовой набор объектов защиты, приоритеты доступа к информации, типовые роли пользователей;
- каналы передачи данных: определение и виды;
- подходы и методы обследования объекта информатизации для последующей защиты;
- сетевые устройства, которые могут быть использованы как источники событий для анализа;
- технологии работы с политиками информационной безопасности;
- основные функции системы DLPIWTM;
- категорирование информации в РФ;
- типы угроз информационной безопасности, понимать их актуальность и степень угрозы для конкретной организации;

- алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных;
- технику безопасности и экологию производства.

Уметь:

- разрабатывать нормативно-правовые документы хозяйствующего субъекта по организации корпоративной защиты от внутренних угроз информационной безопасности;
- проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации;
- администрировать автоматизированные технические средства управления и контроля информации и информационных потоков;
- осуществлять установку и конфигурирование систем DLPIWTM;
- разрабатывать политики детектирования и блокировки утечек с использованием DLP-систем;
- показать свой профессионализм и отношение к профессии;
- поддерживать в чистоте и подготовить рабочее место;
- работать в DLP-системе с событиями, запросами, объектами защиты, политиками, сводками, виджетами, персонами.

3. Объем

Данные об общем объеме курса трудоемкости отдельных видов учебной работы представлены в таблице 1

Таблица 1 – Объем и трудоемкость курса

Вид учебной работы	**Всего**
1	2
Общая трудоемкость дисциплины (модуля), (час)	3
Аудиторные занятия, всего час., ***В том числе****	2
Лекции (Л), (час)	2
Практические/семинарские занятия (ПЗ), (час)	X
Лабораторные работы (ЛР), (час)	X
Самостоятельная работа, всего (час)	X
Вид промежуточной аттестации (при наличии)	зачет

4. Содержание

4.1. Распределение трудоемкости по разделам, темам и видам занятий

Разделы, темы и их трудоемкость приведены в таблице 2.

Таблица 2 – Разделы, темы курса и их трудоемкость

Разделы, темы	Виды учебных занятий*	
	Лекции	Практика
Модуль 1. Стандарты Ворлдскиллс и спецификация стандартов Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности». Разделы спецификации	2	X

Тема 1.1. Актуальное техническое описание по компетенции. Спецификация стандарта Ворлдскиллс по компетенции	2	X
Итого:	2	X

5. Организационно-педагогические условия

5.1. Материально-технические условия

Состав материально-технической базы представлен в таблице 3.

Таблица 3 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы*	Номер аудитории (при необходимости)
1	Лаборатория, компьютерный класс	
2	Мультимедийная лекционная аудитория	

Программа повышения квалификации реализуется с использованием электронного обучения и дистанционных образовательных технологий. К материально-техническому оснащению рабочего места преподавателя программы относятся:

- Компьютер, мультимедийный проектор, экран, доска, флипчарт;
- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог (1 шт.);
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор) (1 шт.);
- Клавиатура USB (2 шт.);
- Мышь Wireless или USB (2 шт.);
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6 (4 шт.);
- Кабель HDMI 3 метра (2 шт.);
- USB-носитель не менее USB2.0, не менее 8ГБ (2 шт.);
- Точка доступа с поддержкой диапазонов 2ГГц и 5ГГц, возможностью подключения не менее 10 клиентов, создания не менее 3 SSID, подержкаVLAN, поддержка PoE (1 шт.);
- Коммутатор не менее 24 портов Gigabit, управляемый, поддержка настройки VLAN (1 шт.);
- Маршрутизатор не менее 4 портов Gigabit, управляемый, поддержка NAT, DHCP, VLAN, VPN, управляемый, L3 (1 шт.);
- Принтер (1 шт.).

К материально-техническому оснащению рабочего места слушателя программы относятся:

- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог;
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор);
- Клавиатура USB;
- Мышь Wireless или USB;
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6;
- Кабель HDMI 3 метра;
- USB-носитель не менее USB2.0, не менее 8ГБ.

5.2. Учебно-методическое и информационное обеспечение

Перечень основной и дополнительной литературы приведен в таблице 4.

Таблица 4 – Перечень основной и дополнительной литературы

Шифр / URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
Основная литература		
https://kb.infowatch.com/ pages/viewpage.action? pageId=32079878	Техническая документация по решению Info Watch Traffic Monitor 4.1 [электронный ресурс]	
https://bit.mephi.ru/index.php/bit/article/view/14/22	А.С. Зайцев, А.А. Малюк, Разработка классификации внутренних угроз информационной безопасности посредством классификации инцидентов, Москва, журнал БИТ № 3 2016 г. [электронный ресурс]	
https://www.twirpx.com/ file/185060/	Партыка Т.Л., Попов И.И. Информационная безопасность, учебное пособие. 5-е изд., перераб. и доп. - М.: ФОРУМ, 2012. - 432 с.	
http://padabum.com/ d.php?id=27762	Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер, 2008. – 320 с.	
Х404.3М 48	Информационная безопасность и защита информации: учебное пособие/ В. П. Мельников, С.А. Клейменов, А.М. Петраков; ред. С.А. Клейменов. -5-е изд., стер.- М.: Академия, 2011.-331с.	25
004 М 87	Мошак Н.Н. Организация безопасного доступа к информационным ресурсам [Текст]: учебное пособие /Н.Н. Мошак, Т. М. Татарникова; М-во образования и науки Российской Федерации, Федеральное гос. авт. образовательное учреждение высш. проф. образования Санкт-Петербургский гос. ун-т аэрокосмического приборостроения. - Санкт-Петербург : ГУАП, 2014. - 121 с. : ил., табл.	40
3-40	Защита от внутренних угроз информационной безопасности с использованием современных DLP-технологий: учеб. пособие / А.В. Сергеев, Е.В. Трапезников, Н.В. Матвеев, А.А. Крылова, А.А. Овчинников; под ред. д-ра техн. наук, проф. А.М. Тюрликова. – СПб.: ГУАП, 2021. – 202с.: ил.	100
004М 87-604316-ED	Мошак Н.Н. Защищенные инфотелекоммуникации. Анализ и синтез [Электронный ресурс]: монография/ Н. Н. Мошак ; М-во образования и науки Российской Федерации, Федеральное	40

	гос. авт. образовательное учреждение высш. проф. образования Санкт-Петербургский гос. ун-т аэрокосмического приборостроения. - Санкт-Петербург : ГУАП, 2014. - 197 с. :ил., табл.	

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения курса, приведен в таблице 5.

Таблица 5 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ

URL адрес	Наименование
www.fstec.ru	Сайт «Федеральной службы технического и экспортного контроля РФ»
https://worldskills.ru	Официальный сайт оператора международного некоммерческого движения WorldSkills International - Союз «Молодые профессионалы (Ворлдскиллс Россия)»
https://esat.worldskills.ru	Единая система актуальных требований Ворлдскиллс

Перечень используемого программного обеспечения представлен в таблице 6.

Таблица 6 – Перечень программного обеспечения

№ п/п	Наименование
1	ПО для виртуализации VMWareWorkstation/VirtualBox или аналог, офисный пакет MSOffice/LibreOffice или аналог, notepad++ или аналог, браузер Firefox и Chrome или аналог
2	ПО для борьбы с внутренними утечками информации InfoWatchTrafficMonitor EducationLab не ниже 6.9 (минимальынй состав InfowatchTrafficMonitor, InfowatchDeviceMonitor, Crawler)
3	OS MS Windows 10
4	OS MS Windows Server 2012
5	OS MS Windows Server 2016
6	Почтовый сервер в составе postfix и dovecot или аналогов, поддержка работы в режиме SMTPRelay, поддержка интеграции с DLP системой для перехвата почтовых сообщений
7	ПО для проведения тестов на безопасность с предустановленными утилитами и наборами тестов на базе ОС Linux (например, KaliLinux, Parrot и другие)

Перечень используемых информационно-справочных систем представлен в таблице 7.

Таблица 7 – Перечень информационно-справочных систем

№ п/п	Наименование
1	Официальный сайт оператора международного некоммерческого движения WorldSkillsInternational - Автономная некоммерческая организация «Агентство развития профессионального мастерства (Ворлдскиллс Россия)» (электронный ресурс) режим доступа: https://worldskills.ru
2	Единая система актуальных требований Ворлдскиллс (электронный ресурс) режим доступа: https://esat.worldskills.ru

6 Оценочные материалы для проведения промежуточной аттестации

6.1 Состав оценочных материалов приведен в таблице 8.

Таблица 8 - Состав оценочных материалов для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных материалов
Тест	Список вопросов

6.2 В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала университета. В таблице 9 представлена 4-балльная шкала для оценки сформированности компетенций.

Таблица 9 –Критерии оценки уровня сформированности компетенций

Оценка компетенции (4-балльная шкала)	Характеристика сформированных компетенций
«отлично» «зачтено»	- слушатель глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой специализированных понятий.
«хорошо» «зачтено»	- слушатель твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью направления; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	- слушатель усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний направления; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой специализированных понятий.
«неудовлетворительно» «не зачтено»	- слушатель не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений.

6.3 Типовые контрольные задания или иные материалы:

Вопросы (задачи) для экзамена (таблица 10)

Таблица 10 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена

	Не предусмотрено

Вопросы (задачи) для зачета / дифференцированного зачета (таблица 11)

Таблица 11 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	Не предусмотрено

Вопросы для проведения промежуточной аттестации при тестировании (таблица 12)

Таблица 12 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
1.	Инфраструктурный лист – это список... (выбрать наиболее полное определение) A) Оборудования для работы площадки B) Оборудования, программного обеспечения для работы площадки C) Программного обеспечения для работы площадки Ответ: B
2.	Сколько модулей в конкурсном задании демоэкзамена? A) от 3 до 9 B) 3 C) 9 Ответ: B
3.	Общее время, которое отводят на выполнение всех модулей демоэкзамена составляет... A) 5 часов B) 6 часов C) больше 6 часов Ответ: C
4.	В каком году появилось движение WorldSkills A) 1947 год B) 1953 год C) 1970 год Ответ: A

Контрольные и практические задачи / задания по дисциплине (модулю) (таблица 13)

Таблица 13 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
	Не предусмотрено

Программу составили:

Ст. преподаватель каф. № 52 — подпись, дата — Н.В. Матвеев
должность, уч. степень, звание — инициалы, фамилия

Декан ФДПО

Д-р экон. наук, профессор каф. 82 — подпись, дата — А.М. Мельниченко
должность, уч. степень, звание — инициалы, фамилия

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

«Актуальные требования рынка труда, современные технологии в профессиональной сфере»
(Название)

По ДПП ПК «Корпоративная защита от внутренних угроз информационной безопасности с использованием современных DLP технологий (с учетом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»)»
(Наименование ДПП)

Форма обучения: очная с использованием дистанционных образовательных технологий

1. Цель

Целью данного курса является изучение основных принципов, методов и средств защиты информации от утечек по техническим каналам передачи информации, с осуществлением выбора по использованию систем защиты информации от внутренних угроз DLP IWTM.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения ДПП

В результате освоения курса слушатель должен обладать следующими компетенциями:
профессиональные компетенции:
ПК-1 - Осуществлять и обосновывать выбор решений по использованию систем защиты информации от внутренних угроз DLPIWTM.
Знать:

- спецификацию стандарта компетенции «Корпоративная защита от внутренних угроз информационной безопасности»
- современные профессиональные технологии в предметной (профессиональной) сфере деятельности;
- принципы проектирования системы корпоративной защиты от внутренних угроз;
- основные правовые понятия и нормативно-правовые документы, регламентирующие организацию корпоративной защиты от внутренних угроз в хозяйствующих субъектах;
- инструментарий, технологии, их область применения и ограничения при формировании корпоративной защиты от внутренних угроз.
- типовые организационно-штатные структуры организаций различных сфер деятельности и размера;
- типовой набор объектов защиты, приоритеты доступа к информации, типовые роли пользователей;
- каналы передачи данных: определение и виды;
- подходы и методы обследования объекта информатизации для последующей защиты;
- сетевые устройства, которые могут быть использованы как источники событий для анализа;
- технологии работы с политиками информационной безопасности;
- основные функции системы DLPIWTM;
- категорирование информации в РФ;
- типы угроз информационной безопасности, понимать их актуальность и степень угрозы для конкретной организации;
- алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных;

- технику безопасности и экологию производства.

Уметь:

- разрабатывать нормативно-правовые документы хозяйствующего субъекта по организации корпоративной защиты от внутренних угроз информационной безопасности;
- проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации;
- администрировать автоматизированные технические средства управления и контроля информации и информационных потоков;
- осуществлять установку и конфигурирование систем DLPIWTM;
- разрабатывать политики детектирования и блокировки утечек с использованием DLP-систем;
- показать свой профессионализм и отношение к профессии;
- поддерживать в чистоте и подготовить рабочее место;
- работать в DLP-системе с событиями, запросами, объектами защиты, политиками, сводками, виджетами, персонами.

3. Объем

Данные об общем объеме курса трудоемкости отдельных видов учебной работы представлены в таблице 1

Таблица 1 – Объем и трудоемкость курса

Вид учебной работы	**Всего**
1	2
Общая трудоемкость дисциплины (модуля), (час)	9
Аудиторные занятия, всего час., ***В том числе****	7
Лекции (Л), (час)	7
Практические/семинарские занятия (ПЗ), (час)	X
Лабораторные работы (ЛР), (час)	X
Самостоятельная работа, всего (час)	X
Вид промежуточной аттестации (при наличии)	зачет

4. Содержание

4.1. Распределение трудоемкости по разделам, темам и видам занятий

Разделы, темы и их трудоемкость приведены в таблице 2.

Таблица 2 – Разделы, темы курса и их трудоемкость

Разделы, темы	Виды учебных занятий*	
	Лекции	Практика
Модуль 2. Актуальные требования рынка труда, современные технологии в профессиональной сфере	7	X
Тема 2.1. Региональные меры содействия занятости в том числе поиска работы, осуществления индивидуальной предпринимательской деятельности, работы в качестве самозанятого	0.5	X
Тема 2.2. Актуальная ситуация на региональном рынке труда	0.5	X

Тема 2.3. Современные технологии в профессиональной сфере, соответствующей компетенции	6	Х
Итого:	7	Х

5. Организационно-педагогические условия

5.1. Материально-технические условия

Состав материально-технической базы представлен в таблице 3.

Таблица 3 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы*	Номер аудитории (при необходимости)
1	Лаборатория, компьютерный класс	
2	Мультимедийная лекционная аудитория	

Программа повышения квалификации реализуется с использованием электронного обучения и дистанционных образовательных технологий. К материально-техническому оснащению рабочего места преподавателя программы относятся:

- Компьютер, мультимедийный проектор, экран, доска, флипчарт;
- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог (1 шт.);
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор) (1 шт.);
- Клавиатура USB (2 шт.);
- Мышь Wireless или USB (2 шт.);
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6 (4 шт.);
- Кабель HDMI 3 метра (2 шт.);
- USB-носитель не менее USB2.0, не менее 8ГБ (2 шт.);
- Точка доступа с поддержкой диапазонов 2ГГц и 5ГГц, возможностью подключения не менее 10 клиентов, создания не менее 3 SSID, подержкаVLAN, поддержка PoE (1 шт.);
- Коммутатор не менее 24 портов Gigabit, управляемый, поддержка настройки VLAN (1 шт.);
- Маршрутизатор не менее 4 портов Gigabit, управляемый, поддержка NAT, DHCP, VLAN, VPN, управляемый, L3 (1 шт.);
- Принтер (1 шт.).

К материально-техническому оснащению рабочего места слушателя программы относятся:

- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог;
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор);
- Клавиатура USB;
- Мышь Wireless или USB;
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6;
- Кабель HDMI 3 метра;
- USB-носитель не менее USB2.0, не менее 8ГБ.

5.2. Учебно-методическое и информационное обеспечение

Перечень основной и дополнительной литературы приведен в таблице 4.

Таблица 4 – Перечень основной и дополнительной литературы

Шифр / URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
Основная литература		
	Зарипова, З. Н. Трудовое право : учебник и практикум для среднего профессионального образования / З. Н. Зарипова, В. А. Шавин. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 320 с.	
Дополнительная литература		
	Епанешникова, Е.А., Малкина, С.А. Статистика рынка труда / Е.А. Епанешникова, С.А. Малкина // Территория инноваций. 2017. № 6 (10). С. 38-42.	
	Овчинникова, А.Ю. Текущее состояние рынка труда в России / А.Ю. Овчинникова // Научные исследования. 2019. № 9 (10). С. 44-46.	
	Шаисламова, М. Р. Рынок труда и его основные понятия в условиях информационного общества / М.Р. Шаисламова // Молодой ученый. — 2017. — №7. — С. 305-307.	
	Шацкая, И.В. Развитие государственной системы управления трудовыми ресурсами на современном этапе / И.В. Шацкая // Экономика труда. 2019. Т. 4. № 3. С. 173-182.	

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения курса, приведен в таблице 5.

Таблица 5 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ

URL адрес	Наименование
www.fstec.ru	Сайт «Федеральной службы технического и экспортного контроля РФ»
https://worldskills.ru	Официальный сайт оператора международного некоммерческого движения WorldSkills International - Союз «Молодые профессионалы (Ворлдскиллс Россия)»
https://esat.worldskills.ru	Единая система актуальных требований Ворлдскиллс

Перечень используемого программного обеспечения представлен в таблице 6.

Таблица 6 – Перечень программного обеспечения

№ п/п	Наименование
1	ПО для виртуализации VMWareWorkstation/VirtualBox или аналог, офисный пакет MSOffice/LibreOffice или аналог, notepad++ или аналог, браузер Firefox и Chrome или аналог
2	ПО для борьбы с внутренними утечками информации InfoWatchTrafficMonitor EducationLab не ниже 6.9 (минимальынй состав InfowatchTrafficMonitor, InfowatchDeviceMonitor, Crawler)

3	OS MS Windows 10
4	OS MS Windows Server 2012
5	OS MS Windows Server 2016
6	Почтовый сервер в составе postfix и dovecot или аналогов, поддержка работы в режиме SMTPRelay, поддержка интеграции с DLP системой для перехвата почтовых сообщений
7	ПО для проведения тестов на безопасность с предустановленными утилитами и наборами тестов на базе ОС Linux (например, KaliLinux, Parrot и другие)

Перечень используемых информационно-справочных систем представлен в таблице 7.

Таблица 7 – Перечень информационно-справочных систем

№ п/п	Наименование
1	Официальный сайт оператора международного некоммерческого движения WorldSkillsInternational - Автономная некоммерческая организация «Агентство развития профессионального мастерства (Ворлдскиллс Россия)» (электронный ресурс) режим доступа: https://worldskills.ru
2	Единая система актуальных требований Ворлдскиллс (электронный ресурс) режим доступа: https://esat.worldskills.ru

6 Оценочные материалы для проведения промежуточной аттестации

6.1 Состав оценочных материалов приведен в таблице 8.

Таблица 8 - Состав оценочных материалов для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных материалов
Тест	Список вопросов

6.2 В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала университета. В таблице 9 представлена 4-балльная шкала для оценки сформированности компетенций.

Таблица 9 –Критерии оценки уровня сформированности компетенций

Оценка компетенции (4-балльная шкала)	Характеристика сформированных компетенций
«отлично» «зачтено»	- слушатель глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой специализированных понятий.
«хорошо» «зачтено»	- слушатель твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью направления; - аргументирует научные положения; - делает выводы и обобщения;

	- владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	- слушатель усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний направления; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой специализированных понятий.
«неудовлетворительно» «не зачтено»	- слушатель не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений.

6.3 Типовые контрольные задания или иные материалы:

Вопросы (задачи) для экзамена (таблица 10)

Таблица 10 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена
	Не предусмотрено

Вопросы (задачи) для зачета / дифференцированного зачета (таблица 11)

Таблица 11 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	Не предусмотрено

Вопросы для проведения промежуточной аттестации при тестировании (таблица 12)

Таблица 12 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
1.	Отметьте понятия, относящиеся к рынку труда: А) Ликвидность Б) Средства производства В) Рабочая сила Г) Труд Ответ: Б, В, Г
2.	Чем является цена реализации труда или цена реализации рабочей силы? А) Оптовой ценой Б) Ценой без НДС В) Ззаработная плата Ответ: В
3.	Отметьте элементы, которые включает в себя современная структура рынка труда: А) Производственная система Б) Система найма В) Система подготовки кадров Г) Система переподготовки и переквалификации Ответ: Б, В, Г

4.	Рынком труда является товарно-денежные отношения, связанные: А) Со временем формирования рабочей силы Б) Со временем использования рабочей силы В) Со спросом на рабочую силу, определяемым спросом на товар в обществе Г) С использованием профессиональных востребованных способностей и их вознаграждением Ответ: Б, В, Г
5.	Чем является подвижное использование рабочего времени и функциональная смена рабочих мест: А) Стандартные режимы использования полного рабочего времени Б) Режимы использования полного рабочего времени В) Нестандартные режимы использования полного рабочего времени Ответ: В

Контрольные и практические задачи / задания по дисциплине (модулю) (таблица 13)

Таблица 13 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
	Не предусмотрено

Программу составили:

Ст. преподаватель каф. № 52 — подпись, дата — Н.В. Матвеев
должность, уч. степень, звание — инициалы, фамилия

Декан ФДПО

Д-р экон. наук, профессор каф. 82. — подпись, дата — А.М. Мельниченко
должность, уч. степень, звание — инициалы, фамилия

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

«Требования охраны труда и техники безопасности»
(Название)

По ДПП ПК «Корпоративная защита от внутренних угроз информационной безопасности с использованием современных DLP технологий (с учетом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»)»
(Наименование ДПП)

Форма обучения: очная с использованием дистанционных образовательных технологий

1. Цель

Целью данного курса является изучение основных принципов, методов и средств защиты информации от утечек по техническим каналам передачи информации, с осуществлением выбора по использованию систем защиты информации от внутренних угроз DLP IWTM.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения ДПП

В результате освоения курса слушатель должен обладать следующими компетенциями:
профессиональные компетенции:
ПК-1 - Осуществлять и обосновывать выбор решений по использованию систем защиты информации от внутренних угроз DLPIWTM.
Знать:

- спецификацию стандарта компетенции «Корпоративная защита от внутренних угроз информационной безопасности»
- современные профессиональные технологии в предметной (профессиональной) сфере деятельности;
- принципы проектирования системы корпоративной защиты от внутренних угроз;
- основные правовые понятия и нормативно-правовые документы, регламентирующие организацию корпоративной защиты от внутренних угроз в хозяйствующих субъектах;
- инструментарий, технологии, их область применения и ограничения при формировании корпоративной защиты от внутренних угроз.
- типовые организационно-штатные структуры организаций различных сфер деятельности и размера;
- типовой набор объектов защиты, приоритеты доступа к информации, типовые роли пользователей;
- каналы передачи данных: определение и виды;
- подходы и методы обследования объекта информатизации для последующей защиты;
- сетевые устройства, которые могут быть использованы как источники событий для анализа;
- технологии работы с политиками информационной безопасности;
- основные функции системы DLPIWTM;
- категорирование информации в РФ;
- типы угроз информационной безопасности, понимать их актуальность и степень угрозы для конкретной организации;
- алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных;

- технику безопасности и экологию производства.

Уметь:

- разрабатывать нормативно-правовые документы хозяйствующего субъекта по организации корпоративной защиты от внутренних угроз информационной безопасности;
- проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации;
- администрировать автоматизированные технические средства управления и контроля информации и информационных потоков;
- осуществлять установку и конфигурирование систем DLPIWTM;
- разрабатывать политики детектирования и блокировки утечек с использованием DLP-систем;
- показать свой профессионализм и отношение к профессии;
- поддерживать в чистоте и подготовить рабочее место;
- работать в DLP-системе с событиями, запросами, объектами защиты, политиками, сводками, виджетами, персонами.

3. Объем

Данные об общем объеме курса трудоемкости отдельных видов учебной работы представлены в таблице 1

Таблица 1 – Объем и трудоемкость курса

Вид учебной работы	**Всего**
1	2
Общая трудоемкость дисциплины (модуля), (час)	3
Аудиторные занятия, всего час., ***В том числе******	2
Лекции (Л), (час)	2
Практические/семинарские занятия (ПЗ), (час)	X
Лабораторные работы (ЛР), (час)	X
Самостоятельная работа, всего (час)	X
Вид промежуточной аттестации (при наличии)	зачет

4. Содержание

4.1. Распределение трудоемкости по разделам, темам и видам занятий

Разделы, темы и их трудоемкость приведены в таблице 2.

Таблица 2 – Разделы, темы курса и их трудоемкость

Разделы, темы	Виды учебных занятий*	
	Лекции	Практика
Модуль 3. Требования охраны труда и техники безопасности	2	X
Тема 3.1. Требования охраны труда и техники безопасности	1	X
Тема 3.2. Специфичные требования охраны труда, техники безопасности и окружающей среды по компетенции	1	X
Итого:	2	X

5. Организационно-педагогические условия

5.1. Материально-технические условия

Состав материально-технической базы представлен в таблице 3.

Таблица 3 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы*	Номер аудитории (при необходимости)
1	Лаборатория, компьютерный класс	
2	Мультимедийная лекционная аудитория	

Программа повышения квалификации реализуется с использованием электронного обучения и дистанционных образовательных технологий. К материально-техническому оснащению рабочего места преподавателя программы относятся:

- Компьютер, мультимедийный проектор, экран, доска, флипчарт;
- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог (1 шт.);
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор) (1 шт.);
- Клавиатура USB (2 шт.);
- Мышь Wireless или USB (2 шт.);
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6 (4 шт.);
- Кабель HDMI 3 метра (2 шт.);
- USB-носитель не менее USB2.0, не менее 8ГБ (2 шт.);
- Точка доступа с поддержкой диапазонов 2ГГц и 5ГГц, возможностью подключения не менее 10 клиентов, создания не менее 3 SSID, подержкаVLAN, поддержка PoE (1 шт.);
- Коммутатор не менее 24 портов Gigabit, управляемый, поддержка настройки VLAN (1 шт.);
- Маршрутизатор не менее 4 портов Gigabit, управляемый, поддержка NAT, DHCP, VLAN, VPN, управляемый, L3 (1 шт.);
- Принтер (1 шт.).

К материально-техническому оснащению рабочего места слушателя программы относятся:

- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог;
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор);
- Клавиатура USB;
- Мышь Wireless или USB;
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6;
- Кабель HDMI 3 метра;
- USB-носитель не менее USB2.0, не менее 8ГБ.

5.2. Учебно-методическое и информационное обеспечение

Перечень основной и дополнительной литературы приведен в таблице 4.

Таблица 4 – Перечень основной и дополнительной литературы

Шифр / URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке

		(кроме электронных экземпляров)
Основная литература		
	Г.И. Беляков. Охрана труда и техника безопасности. Учебник. – М.: Юрайт, 2017. – 406 с.	
	Н.Н. Карнаух. Охрана труда. Учебник. – М.: Юрайт, 2017. – 382 с.	

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения курса, приведен в таблице 5.

Таблица 5 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ

URL адрес	Наименование
www.fstec.ru	Сайт «Федеральной службы технического и экспортного контроля РФ»
https://worldskills.ru	Официальный сайт оператора международного некоммерческого движения WorldSkills International - Союз «Молодые профессионалы (Ворлдскиллс Россия)»
https://esat.worldskills.ru	Единая система актуальных требований Ворлдскиллс

Перечень используемого программного обеспечения представлен в таблице 6.

Таблица 6 – Перечень программного обеспечения

№ п/п	Наименование
1	ПО для виртуализации VMWareWorkstation/VirtualBox или аналог, офисный пакет MSOffice/LibreOffice или аналог, notepad++ или аналог, браузер Firefox и Chrome или аналог
2	ПО для борьбы с внутренними утечками информации InfoWatchTrafficMonitor EducationLab не ниже 6.9 (минимальынй состав InfowatchTrafficMonitor, InfowatchDeviceMonitor, Crawler)
3	OS MS Windows 10
4	OS MS Windows Server 2012
5	OS MS Windows Server 2016
6	Почтовый сервер в составе postfix и dovecot или аналогов, поддержка работы в режиме SMTPRelay, поддержка интеграции с DLP системой для перехвата почтовых сообщений
7	ПОдля проведения тестов на безопасность с предустановленными утилитами и наборами тестов на базе ОС Linux (например, KaliLinux, Parrot и другие)

Перечень используемых информационно-справочных систем представлен в таблице 7.

Таблица 7 – Перечень информационно-справочных систем

№ п/п	Наименование
1	официальный сайт оператора международного некоммерческого движения WorldSkillsInternational - Автономная некоммерческая организация «Агентство развития профессионального мастерства (Ворлдскиллс Россия)» (электронный ресурс) режим доступа: https://worldskills.ru
2	единая система актуальных требований Ворлдскиллс (электронный ресурс)

	режим доступа: https://esat.worldskills.ru

6 Оценочные материалы для проведения промежуточной аттестации

6.1 Состав оценочных материалов приведен в таблице 8.

Таблица 8 - Состав оценочных материалов для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных материалов
Тест	Список вопросов

6.2 В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала университета. В таблице 9 представлена 4-балльная шкала для оценки сформированности компетенций.

Таблица 9 –Критерии оценки уровня сформированности компетенций

Оценка компетенции (4-балльная шкала)	Характеристика сформированных компетенций
«отлично» «зачтено»	- слушатель глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой специализированных понятий.
«хорошо» «зачтено»	- слушатель твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью направления; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	- слушатель усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний направления; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой специализированных понятий.
«неудовлетворительно» «не зачтено»	- слушатель не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений.

6.3 Типовые контрольные задания или иные материалы:

Вопросы (задачи) для экзамена (таблица 10)

Таблица 10 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена
	Не предусмотрено

Вопросы (задачи) для зачета / дифференцированного зачета (таблица 11)

Таблица 11 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	Не предусмотрено

Вопросы для проведения промежуточной аттестации при тестировании (таблица 12)

Таблица 12 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
1.	Каково оптимальное расстояние от экрана монитора до глаз пользователя? A) 30-40 см B) 40-50 см C) 50-70 см Ответ: C
2.	В случае пожара необходимо A) Немедленно прекратить работу и под руководством преподавателя покинуть аудиторию B) Выключить компьютер и покинуть здание C) Собрать свои вещи и покинуть здание Ответ: A
3.	Можно ли работать за компьютером с продуктами питания и напитками? A) Нет B) Да, только в том случае, если сильно хочется, есть или пить C) Да Ответ: A

Контрольные и практические задачи / задания по дисциплине (модулю) (таблица 13)

Таблица 13 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
	Не предусмотрено

Программу составили:

Ст. преподаватель каф. № 52 — Н.В. Матвеев
должность, уч. степень, звание — подпись, дата — инициалы, фамилия

Декан ФДПО

Д-р экон. наук, профессор каф. 82 — А.М. Мельниченко
должность, уч. степень, звание — подпись, дата — инициалы, фамилия

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

«Практическое занятие на определение стартового уровня владения компетенцией»
(Название)

По ДПП ПК «Корпоративная защита от внутренних угроз информационной безопасности с использованием современных DLP технологий (с учетом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»)»
(Наименование ДПП)

Форма обучения: очная с использованием дистанционных образовательных технологий

1. Цель

Целью данного курса является изучение основных принципов, методов и средств защиты информации от утечек по техническим каналам передачи информации, с осуществлением выбора по использованию систем защиты информации от внутренних угроз DLP IWTM.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения ДПП

В результате освоения курса слушатель должен обладать следующими компетенциями:
профессиональные компетенции:
ПК-1 - Осуществлять и обосновывать выбор решений по использованию систем защиты информации от внутренних угроз DLPIWTM.
Знать:

- спецификацию стандарта компетенции «Корпоративная защита от внутренних угроз информационной безопасности»
- современные профессиональные технологии в предметной (профессиональной) сфере деятельности;
- принципы проектирования системы корпоративной защиты от внутренних угроз;
- основные правовые понятия и нормативно-правовые документы, регламентирующие организацию корпоративной защиты от внутренних угроз в хозяйствующих субъектах;
- инструментарий, технологии, их область применения и ограничения при формировании корпоративной защиты от внутренних угроз.
- типовые организационно-штатные структуры организаций различных сфер деятельности и размера;
- типовой набор объектов защиты, приоритеты доступа к информации, типовые роли пользователей;
- каналы передачи данных: определение и виды;
- подходы и методы обследования объекта информатизации для последующей защиты;
- сетевые устройства, которые могут быть использованы как источники событий для анализа;
- технологии работы с политиками информационной безопасности;
- основные функции системы DLPIWTM;
- категорирование информации в РФ;
- типы угроз информационной безопасности, понимать их актуальность и степень угрозы для конкретной организации;

- алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных;
- технику безопасности и экологию производства.

Уметь:

- разрабатывать нормативно-правовые документы хозяйствующего субъекта по организации корпоративной защиты от внутренних угроз информационной безопасности;
- проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации;
- администрировать автоматизированные технические средства управления и контроля информации и информационных потоков;
- осуществлять установку и конфигурирование систем DLPIWTM;
- разрабатывать политики детектирования и блокировки утечек с использованием DLP-систем;
- показать свой профессионализм и отношение к профессии;
- поддерживать в чистоте и подготовить рабочее место;
- работать в DLP-системе с событиями, запросами, объектами защиты, политиками, сводками, виджетами, персонами.

3. Объем

Данные об общем объеме курса трудоемкости отдельных видов учебной работы представлены в таблице 1

Таблица 1 – Объем и трудоемкость курса

Вид учебной работы	**Всего**
1	2
Общая трудоемкость дисциплины (модуля), (час)	2
Аудиторные занятия, всего час., ***В том числе****	2
Лекции (Л), (час)	X
Практические/семинарские занятия (ПЗ), (час)	2
Лабораторные работы (ЛР), (час)	X
Самостоятельная работа, всего (час)	X
Вид промежуточной аттестации (при наличии)	Не предусмотрено

4. Содержание

4.1. Распределение трудоемкости по разделам, темам и видам занятий

Разделы, темы и их трудоемкость приведены в таблице 2.

Таблица 2 – Разделы, темы курса и их трудоемкость

Разделы, темы	Виды учебных занятий*	
	Лекции	Практика
Модуль 4. Практическое занятие на определение стартового уровня владения компетенцией	X	2
Тема 4.1. Практическое занятие на определение стартового уровня владения компетенцией	X	2
Итого:	X	2

5. Организационно-педагогические условия

5.1. Материально-технические условия

Состав материально-технической базы представлен в таблице 3.

Таблица 3 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы*	Номер аудитории (при необходимости)
1	Лаборатория, компьютерный класс	
2	Мультимедийная лекционная аудитория	

Программа повышения квалификации реализуется с использованием электронного обучения и дистанционных образовательных технологий. К материально-техническому оснащению рабочего места преподавателя программы относятся:
- Компьютер, мультимедийный проектор, экран, доска, флипчарт;
- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог (1 шт.);
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор) (1 шт.);
- Клавиатура USB (2 шт.);
- Мышь Wireless или USB (2 шт.);
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6 (4 шт.);
- Кабель HDMI 3 метра (2 шт.);
- USB-носитель не менее USB2.0, не менее 8ГБ (2 шт.);
- Точка доступа с поддержкой диапазонов 2ГГц и 5ГГц, возможностью подключения не менее 10 клиентов, создания не менее 3 SSID, подержкаVLAN, поддержка PoE (1 шт.);
- Коммутатор не менее 24 портов Gigabit, управляемый, поддержка настройки VLAN (1 шт.);
- Маршрутизатор не менее 4 портов Gigabit, управляемый, поддержка NAT, DHCP, VLAN, VPN, управляемый, L3 (1 шт.);
- Принтер (1 шт.).

К материально-техническому оснащению рабочего места слушателя программы относятся:
- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог;
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор);
- Клавиатура USB;
- Мышь Wireless или USB;
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6;
- Кабель HDMI 3 метра;
- USB-носитель не менее USB2.0, не менее 8ГБ.

5.2. Учебно-методическое и информационное обеспечение

Перечень основной и дополнительной литературы приведен в таблице 4.

Таблица 4 – Перечень основной и дополнительной литературы

Шифр / URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке

		(кроме электронных экземпляров)
Основная литература		
	Не предусмотрено	
Дополнительная литература		
	Не предусмотрено	

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения курса, приведен в таблице 5.

Таблица 5 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ

URL адрес	Наименование
www.fstec.ru	Сайт «Федеральной службы технического и экспортного контроля РФ»
https://worldskills.ru	Официальный сайт оператора международного некоммерческого движения WorldSkills International - Союз «Молодые профессионалы (Ворлдскиллс Россия)»
https://esat.worldskills.ru	Единая система актуальных требований Ворлдскиллс

Перечень используемого программного обеспечения представлен в таблице 6.

Таблица 6 – Перечень программного обеспечения

№ п/п	Наименование
1	ПО для виртуализации VMWareWorkstation/VirtualBox или аналог, офисный пакет MSOffice/LibreOffice или аналог, notepad++ или аналог, браузер Firefox и Chrome или аналог
2	ПО для борьбы с внутренними утечками информации InfoWatchTrafficMonitor EducationLab не ниже 6.9 (минимальынй состав InfowatchTrafficMonitor, InfowatchDeviceMonitor, Crawler)
3	OS MS Windows 10
4	OS MS Windows Server 2012
5	OS MS Windows Server 2016
6	Почтовый сервер в составе postfix и dovecot или аналогов, поддержка работы в режиме SMTPRelay, поддержка интеграции с DLP системой для перехвата почтовых сообщений
7	ПОдля проведения тестов на безопасность с предустановленными утилитами и наборами тестов на базе ОС Linux (например, KaliLinux, Parrot и другие)

Перечень используемых информационно-справочных систем представлен в таблице 7.

Таблица 7 – Перечень информационно-справочных систем

№ п/п	Наименование
1	Официальный сайт оператора международного некоммерческого движения WorldSkillsInternational - Автономная некоммерческая организация «Агентство развития профессионального мастерства (Ворлдскиллс Россия)» (электронный ресурс) режим доступа: https://worldskills.ru
2	Единая система актуальных требований Ворлдскиллс (электронный ресурс) режим доступа: https://esat.worldskills.ru

6 Оценочные материалы для проведения промежуточной аттестации

6.1 Состав оценочных материалов приведен в таблице 8.

Таблица 8 - Состав оценочных материалов для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных материалов
Не предусмотрено	Список вопросов

6.2 В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала университета. В таблице 9 представлена 4-балльная шкала для оценки сформированности компетенций.

Таблица 9 –Критерии оценки уровня сформированности компетенций

Оценка компетенции (4-балльная шкала)	Характеристика сформированных компетенций
«отлично» «зачтено»	- слушатель глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой специализированных понятий.
«хорошо» «зачтено»	- слушатель твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью направления; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	- слушатель усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний направления; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой специализированных понятий.
«неудовлетворительно» «не зачтено»	- слушатель не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений.

6.3 Типовые контрольные задания или иные материалы:

Вопросы (задачи) для экзамена (таблица 10)

Таблица 10 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена

	Не предусмотрено

Вопросы (задачи) для зачета / дифференцированного зачета (таблица 11)

Таблица 11 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	Не предусмотрено

Вопросы для проведения промежуточной аттестации при тестировании (таблица 12)

Таблица 12 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
	Не предусмотрено

Контрольные и практические задачи / задания по дисциплине (модулю) (таблица 13)

Таблица 13 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
	Не предусмотрено

Программу составили:

Ст. преподаватель каф. № 52 — подпись, дата — Н.В. Матвеев
должность, уч. степень, звание — инициалы, фамилия

Декан ФДПО

Д-р экон. наук, профессор каф. 82 — подпись, дата — А.М. Мельниченко
должность, уч. степень, звание — инициалы, фамилия

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

«Основы цифровой гигиены»
(Название)

По ДПП ПК «Корпоративная защита от внутренних угроз информационной безопасности с использованием современных DLP технологий (с учетом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»)»
(Наименование ДПП)

Форма обучения: очная с использованием дистанционных образовательных технологий

1. Цель

Целью данного курса является изучение основных принципов, методов и средств защиты информации от утечек по техническим каналам передачи информации, с осуществлением выбора по использованию систем защиты информации от внутренних угроз DLP IWTM.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения ДПП

В результате освоения курса слушатель должен обладать следующими компетенциями:
профессиональные компетенции:
ПК-1 - Осуществлять и обосновывать выбор решений по использованию систем защиты информации от внутренних угроз DLPIWTM.
Знать:

- спецификацию стандарта компетенции «Корпоративная защита от внутренних угроз информационной безопасности»
- современные профессиональные технологии в предметной (профессиональной) сфере деятельности;
- принципы проектирования системы корпоративной защиты от внутренних угроз;
- основные правовые понятия и нормативно-правовые документы, регламентирующие организацию корпоративной защиты от внутренних угроз в хозяйствующих субъектах;
- инструментарий, технологии, их область применения и ограничения при формировании корпоративной защиты от внутренних угроз.
- типовые организационно-штатные структуры организаций различных сфер деятельности и размера;
- типовой набор объектов защиты, приоритеты доступа к информации, типовые роли пользователей;
- каналы передачи данных: определение и виды;
- подходы и методы обследования объекта информатизации для последующей защиты;
- сетевые устройства, которые могут быть использованы как источники событий для анализа;
- технологии работы с политиками информационной безопасности;
- основные функции системы DLPIWTM;
- категорирование информации в РФ;
- типы угроз информационной безопасности, понимать их актуальность и степень угрозы для конкретной организации;
- алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных;

- технику безопасности и экологию производства.

Уметь:

- разрабатывать нормативно-правовые документы хозяйствующего субъекта по организации корпоративной защиты от внутренних угроз информационной безопасности;
- проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации;
- администрировать автоматизированные технические средства управления и контроля информации и информационных потоков;
- осуществлять установку и конфигурирование систем DLPIWTM;
- разрабатывать политики детектирования и блокировки утечек с использованием DLP-систем;
- показать свой профессионализм и отношение к профессии;
- поддерживать в чистоте и подготовить рабочее место;
- работать в DLP-системе с событиями, запросами, объектами защиты, политиками, сводками, виджетами, персонами.

3. Объем

Данные об общем объеме курса трудоемкости отдельных видов учебной работы представлены в таблице 1

Таблица 1 – Объем и трудоемкость курса

Вид учебной работы	**Всего**
1	2
Общая трудоемкость дисциплины (модуля), (час)	9
Аудиторные занятия, всего час., ***В том числе****	8
Лекции (Л), (час)	2
Практические/семинарские занятия (ПЗ), (час)	6
Лабораторные работы (ЛР), (час)	X
Самостоятельная работа, всего (час)	X
Вид промежуточной аттестации (при наличии)	зачет

4. Содержание

4.1. Распределение трудоемкости по разделам, темам и видам занятий

Разделы, темы и их трудоемкость приведены в таблице 2.

Таблица 2 – Разделы, темы курса и их трудоемкость

Разделы, темы	Виды учебных занятий*	
	Лекции	Практика
Модуль 5. Основы цифровой гигиены	2	6
Тема 5.1. Цифровая гигиена. Киберугрозы. Виды киберугроз. Интернет угрозы. Внешние (вредоносный программный код, спам, фишинг, сетевые атаки, взлом устройства, взлом аккаунтов и т.д.) и внутренние (интернет зависимость, интернет прокрастинация) интернет угрозы.	2	X

Коммуникационные и технологические интернет угрозы.		
Тема 5.2. Правила безопасного поведения в сети Интернет. Размещение и использование персональных и личных данных. Безопасные пароли. Настройки приватности в социальных сетях. Резервное копирование.	Х	3
Тема 5.3. Программы защиты от вредоносного программного кода. Программы родительского контроля. Средства шифрования данных. Средства блокирования нежелательного контента.	Х	3
Итого:	2	6

5. Организационно-педагогические условия

5.1. Материально-технические условия

Состав материально-технической базы представлен в таблице 3.

Таблица 3 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы*	Номер аудитории (при необходимости)
1	Лаборатория, компьютерный класс	
2	Мультимедийная лекционная аудитория	

Программа повышения квалификации реализуется с использованием электронного обучения и дистанционных образовательных технологий. К материально-техническому оснащению рабочего места преподавателя программы относятся:

- Компьютер, мультимедийный проектор, экран, доска, флипчарт;
- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог (1 шт.);
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор) (1 шт.);
- Клавиатура USB (2 шт.);
- Мышь Wireless или USB (2 шт.);
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6 (4 шт.);
- Кабель HDMI 3 метра (2 шт.);
- USB-носитель не менее USB2.0, не менее 8ГБ (2 шт.);
- Точка доступа с поддержкой диапазонов 2ГГц и 5ГГц, возможностью подключения не менее 10 клиентов, создания не менее 3 SSID, подержкаVLAN, поддержка PoE (1 шт.);
- Коммутатор не менее 24 портов Gigabit, управляемый, поддержка настройки VLAN (1 шт.);
- Маршрутизатор не менее 4 портов Gigabit, управляемый, поддержка NAT, DHCP, VLAN, VPN, управляемый, L3 (1 шт.);
- Принтер (1 шт.).

К материально-техническому оснащению рабочего места слушателя программы относятся:

- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог;
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор);
- Клавиатура USB;

- Мышь Wireless или USB;
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6;
- Кабель HDMI 3 метра;
- USB-носитель не менее USB2.0, не менее 8ГБ.

5.2. Учебно-методическое и информационное обеспечение

Перечень основной и дополнительной литературы приведен в таблице 4.

Таблица 4 – Перечень основной и дополнительной литературы

Шифр / URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
Основная литература		
https://kb.infowatch.com/ pages/viewpage.action? pageId=32079878	Техническая документация по решению Info Watch Traffic Monitor 4.1 [электронный ресурс]	
https://bit.mephi.ru/index.php/bit/article/view/14/22	А.С. Зайцев, А.А. Малюк, Разработка классификации внутренних угроз информационной безопасности посредством классификации инцидентов, Москва, журнал БИТ № 3 2016 г. [электронный ресурс]	
https://www.twirpx.com/ file/185060/	Партыка Т.Л., Попов И.И. Информационная безопасность, учебное пособие. 5-е изд., перераб. и доп. - М.: ФОРУМ, 2012. - 432 с.	
http://padabum.com/ d.php?id=27762	Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер, 2008. – 320 с.	
Х404.3М 48	Информационная безопасность и защита информации: учебное пособие/ В. П. Мельников, С.А. Клейменов, А.М. Петраков; ред. С.А. Клейменов. -5-е изд., стер.- М.: Академия, 2011.-331с.	25
004 М 87	Мошак Н.Н. Организация безопасного доступа к информационным ресурсам [Текст]: учебное пособие /Н.Н. Мошак, Т. М. Татарникова; М-во образования и науки Российской Федерации, Федеральное гос. авт. образовательное учреждение высш. проф. образования Санкт-Петербургский гос. ун-т аэрокосмического приборостроения. - Санкт-Петербург : ГУАП, 2014. - 121 с. : ил., табл.	40
3-40	Защита от внутренних угроз информационной безопасности с использованием современных DLP-технологий: учеб. пособие / А.В. Сергеев, Е.В. Трапезников, Н.В. Матвеев, А.А. Крылова, А.А. Овчинников; под ред. д-ра техн.	100

	наук, проф. А.М. Тюрликова. – СПб.: ГУАП, 2021. – 202с.: ил.	
004М 87-604316-ED	Мошак Н.Н. Защищенные инфотелекоммуникации. Анализ и синтез [Электронный ресурс]: монография/ Н. Н. Мошак ; М-во образования и науки Российской Федерации, Федеральное гос. авт. образовательное учреждение высш. проф. образования Санкт-Петербургский гос. ун-т аэрокосмического приборостроения. - Санкт-Петербург : ГУАП, 2014. - 197 с. :ил., табл.	40

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения курса, приведен в таблице 5.

Таблица 5 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ

URL адрес	Наименование
www.fstec.ru	Сайт «Федеральной службы технического и экспортного контроля РФ»
https://worldskills.ru	Официальный сайт оператора международного некоммерческого движения WorldSkills International - Союз «Молодые профессионалы (Ворлдскиллс Россия)»
https://esat.worldskills.ru	Единая система актуальных требований Ворлдскиллс

Перечень используемого программного обеспечения представлен в таблице 6.

Таблица 6 – Перечень программного обеспечения

№ п/п	Наименование
1	ПО для виртуализации VMWareWorkstation/VirtualBox или аналог, офисный пакет MSOffice/LibreOffice или аналог, notepad++ или аналог, браузер Firefox и Chrome или аналог
2	ПО для борьбы с внутренними утечками информации InfoWatchTrafficMonitor EducationLab не ниже 6.9 (минимальынй состав InfowatchTrafficMonitor, InfowatchDeviceMonitor, Crawler)
3	OS MS Windows 10
4	OS MS Windows Server 2012
5	OS MS Windows Server 2016
6	Почтовый сервер в составе postfix и dovecot или аналогов, поддержка работы в режиме SMTPRelay, поддержка интеграции с DLP системой для перехвата почтовых сообщений
7	ПОдля проведения тестов на безопасность с предустановленными утилитами и наборами тестов на базе ОС Linux (например, KaliLinux, Parrot и другие)

Перечень используемых информационно-справочных систем представлен в таблице 7.

Таблица 7 – Перечень информационно-справочных систем

№ п/п	Наименование
1	Официальный сайт оператора международного некоммерческого движения WorldSkillsInternational - Автономная некоммерческая организация «Агентство развития профессионального мастерства (Ворлдскиллс Россия)» (электронный ресурс) режим доступа: https://worldskills.ru

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

6. Оценочные материалы для проведения промежуточной аттестации

6.1 Состав оценочных материалов приведен в таблице 8.

Таблица 8 - Состав оценочных материалов для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных материалов
Тест	Список вопросов

6.2 В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала университета. В таблице 9 представлена 4-балльная шкала для оценки сформированности компетенций.

Таблица 9 –Критерии оценки уровня сформированности компетенций

Оценка компетенции (4-балльная шкала)	Характеристика сформированных компетенций
«отлично» «зачтено»	- слушатель глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой специализированных понятий.
«хорошо» «зачтено»	- слушатель твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью направления; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	- слушатель усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний направления; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой специализированных понятий.
«неудовлетворительно» «не зачтено»	- слушатель не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений.

6.3 Типовые контрольные задания или иные материалы:

Вопросы (задачи) для экзамена (таблица 10)

Таблица 10 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена
	Не предусмотрено

Вопросы (задачи) для зачета / дифференцированного зачета (таблица 11)

Таблица 11 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	Не предусмотрено

Вопросы для проведения промежуточной аттестации при тестировании (таблица 12)

Таблица 12 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
1.	Что необходимо предпринять, чтобы оставить минимум личной информации при работе в сети Интернет за чужим компьютером? A) Удалять историю своих посещений сайтов после каждого сеанса работы B) Не сохранять пароли во время работы в сети Интернет C) Использовать режим инкогнито во время работы в браузере D) Заходить под своей учетной записью Ответ: B
2.	Особенности безопасного пароля: A) Длинный, небанальный в пароле есть и большие, и маленькие буквы, а также цифры и спецсимволы B) Содержит не более 8 символов, имеет в своем составе только буквы C) Содержит не более 10 символов, имеет в своем составе только цифры D) Пароль от разных сервисов должны быть один и тот же Ответ: A
3.	Программами–антивирусами являются: A) McAfee, Panda, Антивирус "Лаборатории Касперского" B) Panda, Avera C) Norton, McCofee D) Norton, McAfee, Avera Ответ: A
4.	Преследование пользователя сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью различных интернет-сервисов … A) Секстинг B) Груминг C) Кибербуллинг D) Кибертроллинг Ответ: C
5.	Вредоносное программное обеспечение, проникающее в компьютер под видом легального программного обеспечения, называется… A) Фишинг B) Спам C) «Троянский конь» D) «Логическая бомба» Ответ: C
6.	Как необходимо поступить с вложенным документом, поступившим в письме на вашу рабочую почту от неизвестного адресата? A) Удалить письмо и не отвечать на него B) Ответить отправителю, чтобы выяснить, кто он и что содержится в полученном

	документе C) Открыть вложенный документ и изучить его D) Не открывая вложенный документ сразу переслать сообщение сотрудникам ИТ отдела или службы безопасности Ответ: A
7.	Запугивание, подражание, хулиганство пользователя в сети Интернет называется… A) Секстинг B) Груминг C) Кибербуллинг D) Кибертроллинг Ответ: D
8.	KasperskySafeKids является: A) Программой родительского контроля и работает с помощью My Kaspersky B) Программой удаления вредоносных кодов C) Программой помощи детям в поисках сайтов D) Программой помощи детям в поисках детских развлекательных программ в Интернет Ответ: A

Контрольные и практические задачи / задания по дисциплине (модулю) (таблица 13)

Таблица 13 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
	Не предусмотрено

Программу составили:

Ст. преподаватель каф. № 52 — подпись, дата — Н.В. Матвеев
должность, уч. степень, звание — инициалы, фамилия

Декан ФДПО

Д-р экон. наук, профессор каф. 82 — подпись, дата — А.М. Мельниченко
должность, уч. степень, звание — инициалы, фамилия

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

«Программно-аппаратная защита информации»
(Название)

По ДПП ПК «Корпоративная защита от внутренних угроз информационной безопасности с использованием современных DLP технологий (с учетом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»)»
(Наименование ДПП)

Форма обучения: очная с использованием дистанционных образовательных технологий

1. Цель

Целью данного курса является изучение основных принципов, методов и средств защиты информации от утечек по техническим каналам передачи информации, с осуществлением выбора по использованию систем защиты информации от внутренних угроз DLP IWTM.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения ДПП

В результате освоения курса слушатель должен обладать следующими компетенциями:
профессиональные компетенции:
ПК-1 - Осуществлять и обосновывать выбор решений по использованию систем защиты информации от внутренних угроз DLPIWTM.
Знать:

- спецификацию стандарта компетенции «Корпоративная защита от внутренних угроз информационной безопасности»
- современные профессиональные технологии в предметной (профессиональной) сфере деятельности;
- принципы проектирования системы корпоративной защиты от внутренних угроз;
- основные правовые понятия и нормативно-правовые документы, регламентирующие организацию корпоративной защиты от внутренних угроз в хозяйствующих субъектах;
- инструментарий, технологии, их область применения и ограничения при формировании корпоративной защиты от внутренних угроз.
- типовые организационно-штатные структуры организаций различных сфер деятельности и размера;
- типовой набор объектов защиты, приоритеты доступа к информации, типовые роли пользователей;
- каналы передачи данных: определение и виды;
- подходы и методы обследования объекта информатизации для последующей защиты;
- сетевые устройства, которые могут быть использованы как источники событий для анализа;
- технологии работы с политиками информационной безопасности;
- основные функции системы DLPIWTM;
- категорирование информации в РФ;
- типы угроз информационной безопасности, понимать их актуальность и степень угрозы для конкретной организации;
- алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных;
- технику безопасности и экологию производства.

Уметь:

- разрабатывать нормативно-правовые документы хозяйствующего субъекта по организации корпоративной защиты от внутренних угроз информационной безопасности;
- проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации;
- администрировать автоматизированные технические средства управления и контроля информации и информационных потоков;
- осуществлять установку и конфигурирование систем DLPIWTM;
- разрабатывать политики детектирования и блокировки утечек с использованием DLP-систем;
- показать свой профессионализм и отношение к профессии;
- поддерживать в чистоте и подготовить рабочее место;
- работать в DLP-системе с событиями, запросами, объектами защиты, политиками, сводками, виджетами, персонами.

3. Объем

Данные об общем объеме курса трудоемкости отдельных видов учебной работы представлены в таблице 1

Таблица 1 – Объем и трудоемкость курса

Вид учебной работы	**Всего**
1	2
Общая трудоемкость дисциплины (модуля), (час)	12
Аудиторные занятия, всего час., ***В том числе****	11
Лекции (Л), (час)	5
Практические/семинарские занятия (ПЗ), (час)	6
Лабораторные работы (ЛР), (час)	X
Самостоятельная работа, всего (час)	X
Вид промежуточной аттестации (при наличии)	зачет

4. Содержание

4.1. Распределение трудоемкости по разделам, темам и видам занятий

Разделы, темы и их трудоемкость приведены в таблице 2.

Таблица 2 – Разделы, темы курса и их трудоемкость

Разделы, темы	Виды учебных занятий*	
	Лекции	Практика
Модуль 6. Программно-аппаратная защита информации	5	6
Тема 6.1. Ключевые методы и способы программно-аппаратной защиты информации.	2	X
Тема 6.2. Антивирусная защита информации. Понятие вируса. Средства защиты от несанкционированного доступа.	1	3
Тема 6.3. Защита локальной вычислительной сети. Межсетевое экранирование. Частные виртуальные сети.	2	3
Итого:	5	6

5. Организационно-педагогические условия

5.1. Материально-технические условия

Состав материально-технической базы представлен в таблице 3.

Таблица 3 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы*	Номер аудитории (при необходимости)
1	Лаборатория, компьютерный класс	
2	Мультимедийная лекционная аудитория	

Программа повышения квалификации реализуется с использованием электронного обучения и дистанционных образовательных технологий. К материально-техническому оснащению рабочего места преподавателя программы относятся:
- Компьютер, мультимедийный проектор, экран, доска, флипчарт;
- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог (1 шт.);
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор) (1 шт.);
- Клавиатура USB (2 шт.);
- Мышь Wireless или USB (2 шт.);
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6 (4 шт.);
- Кабель HDMI 3 метра (2 шт.);
- USB-носитель не менее USB2.0, не менее 8ГБ (2 шт.);
- Точка доступа с поддержкой диапазонов 2ГГц и 5ГГц, возможностью подключения не менее 10 клиентов, создания не менее 3 SSID, подержкаVLAN, поддержка PoE (1 шт.);
- Коммутатор не менее 24 портов Gigabit, управляемый, поддержка настройки VLAN (1 шт.);
- Маршрутизатор не менее 4 портов Gigabit, управляемый, поддержка NAT, DHCP, VLAN, VPN, управляемый, L3 (1 шт.);
- Принтер (1 шт.).

К материально-техническому оснащению рабочего места слушателя программы относятся:
- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог;
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор);
- Клавиатура USB;
- Мышь Wireless или USB;
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6;
- Кабель HDMI 3 метра;
- USB-носитель не менее USB2.0, не менее 8ГБ.

5.2. Учебно-методическое и информационное обеспечение

Перечень основной и дополнительной литературы приведен в таблице 4.

Таблица 4 – Перечень основной и дополнительной литературы

Шифр / URL адрес	Библиографическая ссылка	Количество

		экземпляров в библиотеке (кроме электронных экземпляров)
Основная литература		
https://kb.infowatch.com/ pages/viewpage.action? pageId=32079878	Техническая документация по решению Info Watch Traffic Monitor 4.1 [электронный ресурс]	
https://bit.mephi.ru/index.php/bit/article/view/14/22	А.С. Зайцев, А.А. Малюк, Разработка классификации внутренних угроз информационной безопасности посредством классификации инцидентов, Москва, журнал БИТ № 3 2016 г. [электронный ресурс]	
https://www.twirpx.com/ file/185060/	Партыка Т.Л., Попов И.И. Информационная безопасность, учебное пособие. 5-е изд., перераб. и доп. - М.: ФОРУМ, 2012. - 432 с.	
http://padabum.com/ d.php?id=27762	Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер, 2008. – 320 с.	
Х404.3М 48	Информационная безопасность и защита информации: учебное пособие/ В. П. Мельников, С.А. Клейменов, А.М. Петраков; ред. С.А. Клейменов. -5-е изд., стер.- М.: Академия, 2011.-331с.	25
004 М 87	Мошак Н.Н. Организация безопасного доступа к информационным ресурсам [Текст]: учебное пособие /Н.Н. Мошак, Т. М. Татарникова; М-во образования и науки Российской Федерации, Федеральное гос. авт. образовательное учреждение высш. проф. образования Санкт-Петербургский гос. ун-т аэрокосмического приборостроения. - Санкт-Петербург : ГУАП, 2014. - 121 с. : ил., табл.	40
3-40	Защита от внутренних угроз информационной безопасности с использованием современных DLP-технологий: учеб. пособие / А.В. Сергеев, Е.В. Трапезников, Н.В. Матвеев, А.А. Крылова, А.А. Овчинников; под ред. д-ра техн. наук, проф. А.М. Тюрликова. – СПб.: ГУАП, 2021. – 202с.: ил.	100
004М 87-604316-ED	Мошак Н.Н. Защищенные инфотелекоммуникации. Анализ и синтез [Электронный ресурс]: монография/ Н. Н. Мошак ; М-во образования и науки Российской Федерации, Федеральное гос. авт. образовательное учреждение высш. проф. образования Санкт-Петербургский гос. ун-т аэрокосмического приборостроения. - Санкт-Петербург : ГУАП, 2014. - 197 с. :ил., табл.	40

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения курса, приведен в таблице 5.

Таблица 5 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ

URL адрес	Наименование
www.fstec.ru	Сайт «Федеральной службы технического и экспортного контроля РФ»
https://worldskills.ru	Официальный сайт оператора международного некоммерческого движения WorldSkills International - Союз «Молодые профессионалы (Ворлдскиллс Россия)»
https://esat.worldskills.ru	Единая система актуальных требований Ворлдскиллс

Перечень используемого программного обеспечения представлен в таблице 6.

Таблица 6 – Перечень программного обеспечения

№ п/п	Наименование
1	ПО для виртуализации VMWareWorkstation/VirtualBox или аналог, офисный пакет MSOffice/LibreOffice или аналог, notepad++ или аналог, браузер Firefox и Chrome или аналог
2	ПО для борьбы с внутренними утечками информации InfoWatchTrafficMonitor EducationLab не ниже 6.9 (минимальынй состав InfowatchTrafficMonitor, InfowatchDeviceMonitor, Crawler)
3	OS MS Windows 10
4	OS MS Windows Server 2012
5	OS MS Windows Server 2016
6	Почтовый сервер в составе postfix и dovecot или аналогов, поддержка работы в режиме SMTPRelay, поддержка интеграции с DLP системой для перехвата почтовых сообщений
7	ПОдля проведения тестов на безопасность с предустановленными утилитами и наборами тестов на базе ОС Linux (например, KaliLinux, Parrot и другие)

Перечень используемых информационно-справочных систем представлен в таблице 7.

Таблица 7 – Перечень информационно-справочных систем

№ п/п	Наименование
1	Официальный сайт оператора международного некоммерческого движения WorldSkillsInternational - Автономная некоммерческая организация «Агентство развития профессионального мастерства (Ворлдскиллс Россия)» (электронный ресурс) режим доступа: https://worldskills.ru
2	Единая система актуальных требований Ворлдскиллс (электронный ресурс) режим доступа: https://esat.worldskills.ru

6 Оценочные материалы для проведения промежуточной аттестации

6.1 Состав оценочных материалов приведен в таблице 8.

Таблица 8 - Состав оценочных материалов для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных материалов

Тест	Список вопросов

6.2 В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала университета. В таблице 9 представлена 4-балльная шкала для оценки сформированности компетенций.

Таблица 9 –Критерии оценки уровня сформированности компетенций

Оценка компетенции (4-балльная шкала)	Характеристика сформированных компетенций
«отлично» «зачтено»	- слушатель глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой специализированных понятий.
«хорошо» «зачтено»	- слушатель твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью направления; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	- слушатель усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний направления; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой специализированных понятий.
«неудовлетворительно» «не зачтено»	- слушатель не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений.

6.3 Типовые контрольные задания или иные материалы:

Вопросы (задачи) для экзамена (таблица 10)

Таблица 10 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена
	Не предусмотрено

Вопросы (задачи) для зачета / дифференцированного зачета (таблица 11)

Таблица 11 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	Не предусмотрено

Вопросы для проведения промежуточной аттестации при тестировании (таблица 12)

Таблица 12 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
1.	Какой модуль антивирусного средства отвечает за хранение "подозрительных" файлов и изолирования их от операционной системы? A) Карантин B) Изолятор C) Доктор D) Такой модуль не входит в состав антивирусного средства ЗИ E) Журнал Ответ: A
2.	Что не может относится к вредоносному программному обеспечению? A) Программы вирусы B) Рекламные баннеры C) Средства контроля за действиями пользователя D) Системы обнаружения вторжений E) Средства доверенного уничтожения информации Ответ: D
3.	Сколько уровней доступа должно быть реализовано в автоматизированной системе? A) Три: открытый, конфиденциальный, государственная тайна B) Не менее одного C) Пять: открытый, конфиденциальный, секретный, совершенно секретный, особой важности D) Два: открытый, закрытый E) Четыре: открытый, конфиденциальный, секретный, персональные данные. Ответ: B
4.	С помощью какого модуля Dallas Lock 8.0C можно ограничить права пользователя на удаление файла? A) Доступ B) Аудит C) Доверенная загрузка D) Очистка остаточной информации E) Такого модуля нет. Удалять информацию могут все пользователи системы Ответ: A

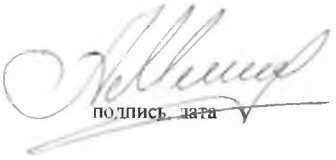
Контрольные и практические задачи / задания по дисциплине (модулю) (таблица 13)

Таблица 13 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
	Не предусмотрено

Программу составили:

Ст. преподаватель каф. № 52 должность, уч. степень, звание	 подпись, дата	Н.В. Матвеев инициалы, фамилия

Декан ФДПО Д-р экон. наук, профессор каф. 82 должность, уч. степень, звание	 подпись, дата	А.М. Мельниченко инициалы, фамилия

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

«Криптографическая защита информации»
(Название)

По ДПП ПК «Корпоративная защита от внутренних угроз информационной безопасности с использованием современных DLP технологий (с учетом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»)»
(Наименование ДПП)

Форма обучения: очная с использованием дистанционных образовательных технологий

1. Цель

Целью данного курса является изучение основных принципов, методов и средств защиты информации от утечек по техническим каналам передачи информации, с осуществлением выбора по использованию систем защиты информации от внутренних угроз DLP IWTM.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения ДПП

В результате освоения курса слушатель должен обладать следующими компетенциями:
профессиональные компетенции:
ПК-1 - Осуществлять и обосновывать выбор решений по использованию систем защиты информации от внутренних угроз DLPIWTM.
Знать:

- спецификацию стандарта компетенции «Корпоративная защита от внутренних угроз информационной безопасности»
- современные профессиональные технологии в предметной (профессиональной) сфере деятельности;
- принципы проектирования системы корпоративной защиты от внутренних угроз;
- основные правовые понятия и нормативно-правовые документы, регламентирующие организацию корпоративной защиты от внутренних угроз в хозяйствующих субъектах;
- инструментарий, технологии, их область применения и ограничения при формировании корпоративной защиты от внутренних угроз.
- типовые организационно-штатные структуры организаций различных сфер деятельности и размера;
- типовой набор объектов защиты, приоритеты доступа к информации, типовые роли пользователей;
- каналы передачи данных: определение и виды;
- подходы и методы обследования объекта информатизации для последующей защиты;
- сетевые устройства, которые могут быть использованы как источники событий для анализа;
- технологии работы с политиками информационной безопасности;
- основные функции системы DLPIWTM;
- категорирование информации в РФ;
- типы угроз информационной безопасности, понимать их актуальность и степень угрозы для конкретной организации;
- алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных;
- технику безопасности и экологию производства.

Уметь:

- разрабатывать нормативно-правовые документы хозяйствующего субъекта по организации корпоративной защиты от внутренних угроз информационной безопасности;
- проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации;
- администрировать автоматизированные технические средства управления и контроля информации и информационных потоков;
- осуществлять установку и конфигурирование систем DLPIWTM;
- разрабатывать политики детектирования и блокировки утечек с использованием DLP-систем;
- показать свой профессионализм и отношение к профессии;
- поддерживать в чистоте и подготовить рабочее место;
- работать в DLP-системе с событиями, запросами, объектами защиты, политиками, сводками, виджетами, персонами.

3. Объем

Данные об общем объеме курса, трудоемкости отдельных видов учебной работы представлены в таблице 1

Таблица 1 – Объем и трудоемкость курса

Вид учебной работы	**Всего**
1	2
Общая трудоемкость дисциплины (модуля), (час)	15
Аудиторные занятия, всего час., ***В том числе****	14
Лекции (Л), (час)	6
Практические/семинарские занятия (ПЗ), (час)	8
Лабораторные работы (ЛР), (час)	X
Самостоятельная работа, всего (час)	X
Вид промежуточной аттестации (при наличии)	зачет

4. Содержание

4.1. Распределение трудоемкости по разделам, темам и видам занятий

Разделы, темы и их трудоемкость приведены в таблице 2.

Таблица 2 – Разделы, темы курса и их трудоемкость

Разделы, темы	Виды учебных занятий*	
	Лекции	Практика
Модуль 7. Криптографическая защита информации	6	8
Тема 7.1. Понятие криптографии. Методы криптографии.	2	X
Тема 7.2. Симметричное и ассиметричное шифрование.	2	4
Тема 7.3. Электронно-цифровая подпись. Методы хэширования информации.	2	4
Итого:	6	8

5. Организационно-педагогические условия

5.1. Материально-технические условия

Состав материально-технической базы представлен в таблице 3.

Таблица 3 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы*	Номер аудитории (при необходимости)
1	Лаборатория, компьютерный класс	
2	Мультимедийная лекционная аудитория	

Программа повышения квалификации реализуется с использованием электронного обучения и дистанционных образовательных технологий. К материально-техническому оснащению рабочего места преподавателя программы относятся:
- Компьютер, мультимедийный проектор, экран, доска, флипчарт;
- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог (1 шт.);
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор) (1 шт.);
- Клавиатура USB (2 шт.);
- Мышь Wireless или USB (2 шт.);
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6 (4 шт.);
- Кабель HDMI 3 метра (2 шт.);
- USB-носитель не менее USB2.0, не менее 8ГБ (2 шт.);
- Точка доступа с поддержкой диапазонов 2ГГц и 5ГГц, возможностью подключения не менее 10 клиентов, создания не менее 3 SSID, подержкаVLAN, поддержка PoE (1 шт.);
- Коммутатор не менее 24 портов Gigabit, управляемый, поддержка настройки VLAN (1 шт.);
- Маршрутизатор не менее 4 портов Gigabit, управляемый, поддержка NAT, DHCP, VLAN, VPN, управляемый, L3 (1 шт.);
- Принтер (1 шт.).

К материально-техническому оснащению рабочего места слушателя программы относятся:
- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог;
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор);
- Клавиатура USB;
- Мышь Wireless или USB;
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6;
- Кабель HDMI 3 метра;
- USB-носитель не менее USB2.0, не менее 8ГБ.

5.2. Учебно-методическое и информационное обеспечение

Перечень основной и дополнительной литературы приведен в таблице 4.

Таблица 4 – Перечень основной и дополнительной литературы

Шифр / URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных

		экземпляров)
Основная литература		
https://kb.infowatch.com/ pages/viewpage.action ? pageId=32079878	Техническая документация по решению Info Watch Traffic Monitor 4.1 [электронный ресурс]	
https://bit.mephi.ru/index.php/bit/article/ view/14/22	А.С. Зайцев, А.А. Малюк, Разработка классификации внутренних угроз информационной безопасности посредством классификации инцидентов, Москва, журнал БИТ № 3 2016 г. [электронный ресурс]	
https://www.twirpx.com/ file/185060/	Партыка Т.Л., Попов И.И. Информационная безопасность, учебное пособие. 5-е изд., перераб. и доп. - М.: ФОРУМ, 2012. - 432 с.	
http://padabum.com/ d.php?id=27762	Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер, 2008. – 320 с.	
Х404.3М 48	Информационная безопасность и защита информации: учебное пособие/ В. П. Мельников, С.А. Клейменов, А.М. Петраков; ред. С.А. Клейменов. -5-е изд., стер.- М.: Академия, 2011.-331с.	25
004 М 87	Мошак Н.Н. Организация безопасного доступа к информационным ресурсам [Текст]: учебное пособие /Н.Н. Мошак, Т. М. Татарникова; М-во образования и науки Российской Федерации, Федеральное гос. авт. образовательное учреждение высш. проф. образования Санкт-Петербургский гос. ун-т аэрокосмического приборостроения. - Санкт-Петербург : ГУАП, 2014. - 121 с. : ил., табл.	40
3-40	Защита от внутренних угроз информационной безопасности с использованием современных DLP-технологий: учеб. пособие / А.В. Сергеев, Е.В. Трапезников, Н.В. Матвеев, А.А. Крылова, А.А. Овчинников; под ред. д-ра техн. наук, проф. А.М. Тюрликова. – СПб.: ГУАП, 2021. – 202с.: ил.	100
004М 87-604316-ED	Мошак Н.Н. Защищенные инфотелекоммуникации. Анализ и синтез [Электронный ресурс]: монография/ Н. Н. Мошак ; М-во образования и науки Российской Федерации, Федеральное гос. авт. образовательное учреждение высш. проф. образования Санкт-Петербургский гос. ун-т аэрокосмического приборостроения. - Санкт-Петербург : ГУАП, 2014. - 197 с. :ил., табл.	40

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения курса, приведен в таблице 5.

Таблица 5 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ

URL адрес	Наименование
www.fstec.ru	Сайт «Федеральной службы технического и экспортного контроля РФ»
https://worldskills.ru	Официальный сайт оператора международного некоммерческого движения WorldSkills International - Союз «Молодые профессионалы (Ворлдскиллс Россия)»
https://esat.worldskills.ru	Единая система актуальных требований Ворлдскиллс

Перечень используемого программного обеспечения представлен в таблице 6.

Таблица 6 – Перечень программного обеспечения

№ п/п	Наименование
1	ПО для виртуализации VMWareWorkstation/VirtualBox или аналог, офисный пакет MSOffice/LibreOffice или аналог, notepad++ или аналог, браузер Firefox и Chrome или аналог
2	ПО для борьбы с внутренними утечками информации InfoWatchTrafficMonitor EducationLab не ниже 6.9 (минимальынй состав InfowatchTrafficMonitor, InfowatchDeviceMonitor, Crawler)
3	OS MS Windows 10
4	OS MS Windows Server 2012
5	OS MS Windows Server 2016
6	Почтовый сервер в составе postfix и dovecot или аналогов, поддержка работы в режиме SMTPRelay, поддержка интеграции с DLP системой для перехвата почтовых сообщений
7	ПОдля проведения тестов на безопасность с предустановленными утилитами и наборами тестов на базе ОС Linux (например, KaliLinux, Parrot и другие)

Перечень используемых информационно-справочных систем представлен в таблице 7.

Таблица 7 – Перечень информационно-справочных систем

№ п/п	Наименование
1	Официальный сайт оператора международного некоммерческого движения WorldSkillsInternational - Автономная некоммерческая организация «Агентство развития профессионального мастерства (Ворлдскиллс Россия)» (электронный ресурс) режим доступа: https://worldskills.ru
2	Единая система актуальных требований Ворлдскиллс (электронный ресурс) режим доступа: https://esat.worldskills.ru

6 Оценочные материалы для проведения промежуточной аттестации

6.1 Состав оценочных материалов приведен в таблице 8.

Таблица 8 - Состав оценочных материалов для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных материалов
Тест	Список вопросов

6.2 В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала университета. В таблице 9 представлена 4-балльная шкала для оценки сформированности компетенций.

Таблица 9 –Критерии оценки уровня сформированности компетенций

Оценка компетенции (4-балльная шкала)	Характеристика сформированных компетенций
«отлично» «зачтено»	- слушатель глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой специализированных понятий.
«хорошо» «зачтено»	- слушатель твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью направления; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	- слушатель усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний направления; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой специализированных понятий.
«неудовлетворительно» «не зачтено»	- слушатель не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений.

6.3 Типовые контрольные задания или иные материалы:

Вопросы (задачи) для экзамена (таблица 10)

Таблица 10 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена
	Не предусмотрено

Вопросы (задачи) для зачета / дифференцированного зачета (таблица 11)

Таблица 11 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	Не предусмотрено

Вопросы для проведения промежуточной аттестации при тестировании (таблица 12)

Таблица 12 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
1.	Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования: A) Зашифрованное сообщение должно поддаваться чтению только при наличии ключа B) Длина шифрованного текста должна быть равной длине исходного текста C) Нет правильного ответа Ответ: A
2.	Что такое криптология? A) Защищенная информация B) Область доступной информации C) Тайная область связи Ответ: C
3.	Показатели криптостойкости: A) Количество всех возможных ключей и среднее время, необходимое для криптоанализа B) Время, необходимое для шифрования текста C) Количество символов в ключе Ответ: A
4.	Наука скрывающая содержимое секретного сообщения - это A) Криптография B) Стеганография C) Криптология Ответ: A
5.	Что такое криптография? A) Область тайной связи, имеющая цель защиту от ознакомления и модификации данных посторонним лицом B) Метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом C) Область доступной информации Ответ: A
6.	Дешифрование – это… A) Пароли для доступа к сетевым ресурсам B) На основе ключа шифрованный текст преобразуется в исходный C) Сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом компьютере Ответ: B
7.	Криптосистемы разделяются на: A) Симметричные и с открытым ключом B) Ассоциативные и простые C) С открытым ключом и запертым ключом Ответ: A
8.	Сколько используется ключей в симметричных криптосистемах для шифрования и дешифрования? A) 1 B) 2 C) 3 Ответ: A
9.	Криптостойкость – это… A) Свойство ключа

	B) Характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа C) Все ответы верны Ответ: B
10.	Символы оригинального текста меняются местами по определенному принципу, являющемуся секретным ключом – это… A) Алгоритм перестановки B) Алгоритм гаммирования C) Алгоритм подстановки Ответ: A
11.	Шифр, при котором каждая буква шифруемого текста заменяется на букву, отстоящую от нее в алфавите на определенное число позиций –это: A) Шифр древней Спарты B) Одиночная перестановка по ключевому слову C) Шифр Цезаря Ответ: C
12.	Электронной подписью называется… A) Присоединяемое к тексту его криптографическое преобразование B) Текст C) Зашифрованный текст Ответ: A

Контрольные и практические задачи / задания по дисциплине (модулю) (таблица 13)

Таблица 13 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
	Не предусмотрено

Программу составили:

Ст. преподаватель каф. № 52 — подпись, дата — Н.В. Матвеев
должность, уч. степень, звание — инициалы, фамилия

Декан ФДПО

Д-р экон. наук, профессор каф. 82 — подпись, дата — А.М. Мельниченко
должность, уч. степень, звание — инициалы, фамилия

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

«Установка, конфигурирование и устранение неисправностей
в системе корпоративной защиты от внутренних угроз»
(Название)

По ДПП ПК «Корпоративная защита от внутренних угроз информационной безопасности с использованием современных DLP технологий (с учетом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»)»
(Наименование ДПП)

Форма обучения: очная с использованием дистанционных образовательных технологий

1. Цель

Целью данного курса является изучение основных принципов, методов и средств защиты информации от утечек по техническим каналам передачи информации, с осуществлением выбора по использованию систем защиты информации от внутренних угроз DLP IWTM.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения ДПП

В результате освоения курса слушатель должен обладать следующими компетенциями:
профессиональные компетенции:
ПК-1 - Осуществлять и обосновывать выбор решений по использованию систем защиты информации от внутренних угроз DLPIWTM.
Знать:

- спецификацию стандарта компетенции «Корпоративная защита от внутренних угроз информационной безопасности»
- современные профессиональные технологии в предметной (профессиональной) сфере деятельности;
- принципы проектирования системы корпоративной защиты от внутренних угроз;
- основные правовые понятия и нормативно-правовые документы, регламентирующие организацию корпоративной защиты от внутренних угроз в хозяйствующих субъектах;
- инструментарий, технологии, их область применения и ограничения при формировании корпоративной защиты от внутренних угроз.
- типовые организационно-штатные структуры организаций различных сфер деятельности и размера;
- типовой набор объектов защиты, приоритеты доступа к информации, типовые роли пользователей;
- каналы передачи данных: определение и виды;
- подходы и методы обследования объекта информатизации для последующей защиты;
- сетевые устройства, которые могут быть использованы как источники событий для анализа;
- технологии работы с политиками информационной безопасности;
- основные функции системы DLPIWTM;
- категорирование информации в РФ;
- типы угроз информационной безопасности, понимать их актуальность и степень угрозы для конкретной организации;

- алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных;
- технику безопасности и экологию производства.

Уметь:

- разрабатывать нормативно-правовые документы хозяйствующего субъекта по организации корпоративной защиты от внутренних угроз информационной безопасности;
- проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации;
- администрировать автоматизированные технические средства управления и контроля информации и информационных потоков;
- осуществлять установку и конфигурирование систем DLPIWTM;
- разрабатывать политики детектирования и блокировки утечек с использованием DLP-систем;
- показать свой профессионализм и отношение к профессии;
- поддерживать в чистоте и подготовить рабочее место;
- работать в DLP-системе с событиями, запросами, объектами защиты, политиками, сводками, виджетами, персонами.

3. Объем

Данные об общем объеме курса трудоемкости отдельных видов учебной работы представлены в таблице 1

Таблица 1 – Объем и трудоемкость курса

Вид учебной работы	**Всего**
1	2
Общая трудоемкость дисциплины (модуля), (час)	23
Аудиторные занятия, всего час., ***В том числе****	22
Лекции (Л), (час)	6
Практические/семинарские занятия (ПЗ), (час)	16
Лабораторные работы (ЛР), (час)	X
Самостоятельная работа, всего (час)	X
Вид промежуточной аттестации (при наличии)	зачет

4. Содержание

4.1. Распределение трудоемкости по разделам, темам и видам занятий

Разделы, темы и их трудоемкость приведены в таблице 2.

Таблица 2 – Разделы, темы курса и их трудоемкость

Разделы, темы	Виды учебных занятий*	
	Лекции	Практика
Модуль 8. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз.	6	16
Тема 8.1. Установка DLPIWTM в виртуальном окружении. Режимы port mirroring и proxy	4	6

Тема 8.2. Конфигурирование DLP IWTM	2	6
Тема 8.3. Исправление типовых неисправностей	X	4
Итого:	6	16

5. Организационно-педагогические условия

5.1. Материально-технические условия

Состав материально-технической базы представлен в таблице 3.

Таблица 3 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы*	Номер аудитории (при необходимости)
1	Лаборатория, компьютерный класс	
2	Мультимедийная лекционная аудитория	

Программа повышения квалификации реализуется с использованием электронного обучения и дистанционных образовательных технологий. К материально-техническому оснащению рабочего места преподавателя программы относятся:

- Компьютер, мультимедийный проектор, экран, доска, флипчарт;
- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог (1 шт.);
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор) (1 шт.);
- Клавиатура USB (2 шт.);
- Мышь Wireless или USB (2 шт.);
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6 (4 шт.);
- Кабель HDMI 3 метра (2 шт.);
- USB-носитель не менее USB2.0, не менее 8ГБ (2 шт.);
- Точка доступа с поддержкой диапазонов 2ГГц и 5ГГц, возможностью подключения не менее 10 клиентов, создания не менее 3 SSID, подержкаVLAN, поддержка PoE (1 шт.);
- Коммутатор не менее 24 портов Gigabit, управляемый, поддержка настройки VLAN (1 шт.);
- Маршрутизатор не менее 4 портов Gigabit, управляемый, поддержка NAT, DHCP, VLAN, VPN, управляемый, L3 (1 шт.);
- Принтер (1 шт.).

К материально-техническому оснащению рабочего места слушателя программы относятся:

- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог;
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор);
- Клавиатура USB;
- Мышь Wireless или USB;
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6;
- Кабель HDMI 3 метра;
- USB-носитель не менее USB2.0, не менее 8ГБ.

5.2. Учебно-методическое и информационное обеспечение

Перечень основной и дополнительной литературы приведен в таблице 4.

Таблица 4 – Перечень основной и дополнительной литературы

Шифр / URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
Основная литература		
https://kb.infowatch.com/ pages/viewpage.action? pageId=32079878	Техническая документация по решению Info Watch Traffic Monitor 4.1 [электронный ресурс]	
https://bit.mephi.ru/index.php/bit/article/view/14/22	А.С. Зайцев, А.А. Малюк, Разработка классификации внутренних угроз информационной безопасности посредством классификации инцидентов, Москва, журнал БИТ № 3 2016 г. [электронный ресурс]	
https://www.twirpx.com/ file/185060/	Партыка Т.Л., Попов И.И. Информационная безопасность, учебное пособие. 5-е изд., перераб. и доп. - М.: ФОРУМ, 2012. - 432 с.	
http://padabum.com/ d.php?id=27762	Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер, 2008. – 320 с.	
Х404.3М 48	Информационная безопасность и защита информации: учебное пособие/ В. П. Мельников, С.А. Клейменов, А.М. Петраков; ред. С.А. Клейменов. -5-е изд., стер.- М.: Академия, 2011.-331с.	25
004 М 87	Мошак Н.Н. Организация безопасного доступа к информационным ресурсам [Текст]: учебное пособие /Н.Н. Мошак, Т. М. Татарникова; М-во образования и науки Российской Федерации, Федеральное гос. авт. образовательное учреждение высш. проф. образования Санкт-Петербургский гос. ун-т аэрокосмического приборостроения. - Санкт-Петербург : ГУАП, 2014. - 121 с. : ил., табл.	40
3-40	Защита от внутренних угроз информационной безопасности с использованием современных DLP-технологий: учеб. пособие / А.В. Сергеев, Е.В. Трапезников, Н.В. Матвеев, А.А. Крылова, А.А. Овчинников; под ред. д-ра техн. наук, проф. А.М. Тюрликова. – СПб.: ГУАП, 2021. – 202с.: ил.	100
004М 87-604316-ED	Мошак Н.Н. Защищенные инфотелекоммуникации. Анализ и синтез [Электронный ресурс]: монография/ Н. Н. Мошак ; М-во образования	40

	и науки Российской Федерации, Федеральное гос. авт. образовательное учреждение высш. проф. образования Санкт-Петербургский гос. ун-т аэрокосмического приборостроения. - Санкт-Петербург : ГУАП, 2014. - 197 с. :ил., табл.	

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения курса, приведен в таблице 5.

Таблица 5 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ

URL адрес	Наименование
www.fstec.ru	Сайт «Федеральной службы технического и экспортного контроля РФ»
https://worldskills.ru	Официальный сайт оператора международного некоммерческого движения WorldSkills International - Союз «Молодые профессионалы (Ворлдскиллс Россия)»
https://esat.worldskills.ru	Единая система актуальных требований Ворлдскиллс

Перечень используемого программного обеспечения представлен в таблице 6.

Таблица 6 – Перечень программного обеспечения

№ п/п	Наименование
1	ПО для виртуализации VMWareWorkstation/VirtualBox или аналог, офисный пакет MSOffice/LibreOffice или аналог, notepad++ или аналог, браузер Firefox и Chrome или аналог
2	ПО для борьбы с внутренними утечками информации InfoWatchTrafficMonitor EducationLab не ниже 6.9 (минимальынй состав InfowatchTrafficMonitor, InfowatchDeviceMonitor, Crawler)
3	OS MS Windows 10
4	OS MS Windows Server 2012
5	OS MS Windows Server 2016
6	Почтовый сервер в составе postfix и dovecot или аналогов, поддержка работы в режиме SMTPRelay, поддержка интеграции с DLP системой для перехвата почтовых сообщений
7	ПОдля проведения тестов на безопасность с предустановленными утилитами и наборами тестов на базе ОС Linux (например, KaliLinux, Parrot и другие)

Перечень используемых информационно-справочных систем представлен в таблице 7.

Таблица 7 – Перечень информационно-справочных систем

№ п/п	Наименование
1	Официальный сайт оператора международного некоммерческого движения WorldSkillsInternational - Автономная некоммерческая организация «Агентство развития профессионального мастерства (Ворлдскиллс Россия)» (электронный ресурс) режим доступа: https://worldskills.ru
2	Единая система актуальных требований Ворлдскиллс (электронный ресурс) режим доступа: https://esat.worldskills.ru

6 Оценочные материалы для проведения промежуточной аттестации

6.1 Состав оценочных материалов приведен в таблице 8.

Таблица 8 - Состав оценочных материалов для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных материалов
Тест	Список вопросов

6.2 В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала университета. В таблице 9 представлена 4-балльная шкала для оценки сформированности компетенций.

Таблица 9 –Критерии оценки уровня сформированности компетенций

Оценка компетенции (4-балльная шкала)	Характеристика сформированных компетенций
«отлично» «зачтено»	- слушатель глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой специализированных понятий.
«хорошо» «зачтено»	- слушатель твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью направления; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	- слушатель усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний направления; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой специализированных понятий.
«неудовлетворительно» «не зачтено»	- слушатель не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений.

6.3 Типовые контрольные задания или иные материалы:

Вопросы (задачи) для экзамена (таблица 10)

Таблица 10 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена

	Не предусмотрено

Вопросы (задачи) для зачета / дифференцированного зачета (таблица 11)

Таблица 11 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	Не предусмотрено

Вопросы для проведения промежуточной аттестации при тестировании (таблица 12)

Таблица 12 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
1.	После установки подсистемы Crawler необходимо внести изменения в конфигурационные файлы IWTM, а именно A) Внести изменения в файл crawler.config, который располагается по пути /etc/iwtm/bin B) Внести изменения в файл tm.config, который располагается по пути /opt/iw/tm5/etc C) Никаких изменений производить не нужно D) Внести изменения в файл web.config, который располагается по пути /opt/iw/tm5/etc Ответ: D
2.	Для синхронизации пользователей домена test.lab, как будет выглядеть LDAP запрос? A) dc=demo, dc=lab B) dc=test, dc=lab C) cn=demo, dc=lab Ответ: B
3.	Логин суперпользователя (администратора) базы данных PostgreSQL? A) Postgres B) Officer C) Admin Ответ: A
4.	В корпоративной сети присутствует сервер Домена, какой запрос позволит получить список пользователей? A) LDAP B) AD C) HTTP Ответ: A
5.	Если сервер IWTM устанавливается в виртуальном окружении, а устройство нарушителя отдельный ПК, какой тип сетевого подключения выбрать? A) Bridge B) NAT C) Host only Ответ: A
6.	Для установка клиента InfoWatch Device Monitor Agent необходимо выполнить: A) Создать и скопировать пакет установки на устройство хранения, установить на виртуальную машину Client1 B) Внести виртуальную машину Client1 в домен, создать и скопировать пакет установки на устройство хранения, установить C) Внести виртуальную машину IWDM в домен, создать задачу первичного распространения агента в IWDM, установить на виртуальную машину IWDM D) Внести виртуальную машину Client1 в домен, создать задачу первичного

	распространения агента в IWDM, установить на виртуальную машину Client1 E) Не вносить виртуальную машину Client1 в домен, создать задачу первичного распространения агента в IWDM, установить на виртуальную машину IWDM Ответ: D
7.	Какой раздел нужно удалить при установке IW Traffic Monitor 6? A) /home B) / C) /media Ответ: A
8.	Какие типовые варианты установки решения InfowathTraffic Monitor существуют? A) Enterprise и Standard B) Basic C) Standart Ответ: A

Контрольные и практические задачи / задания по дисциплине (модулю) (таблица 13)

Таблица 13 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
	Не предусмотрено

Программу составили:

Ст. преподаватель каф. № 52 — должность, уч. степень, звание; подпись, дата; Н.В. Матвеев — инициалы, фамилия

Декан ФДПО

Д-р экон. наук, профессор каф 82 — должность, уч. степень, звание; подпись, дата; А.М. Мельниченко — инициалы, фамилия

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

«Технологии агентского мониторинга»
(Название)

По ДПП ПК «Корпоративная защита от внутренних угроз информационной безопасности с использованием современных DLP технологий (с учетом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»)»
(Наименование ДПП)

Форма обучения: очная с использованием дистанционных образовательных технологий

1. Цель

Целью данного курса является изучение основных принципов, методов и средств защиты информации от утечек по техническим каналам передачи информации, с осуществлением выбора по использованию систем защиты информации от внутренних угроз DLP IWTM.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения ДПП

В результате освоения курса слушатель должен обладать следующими компетенциями:
профессиональные компетенции:
ПК-1 - Осуществлять и обосновывать выбор решений по использованию систем защиты информации от внутренних угроз DLPIWTM.
Знать:

- спецификацию стандарта компетенции «Корпоративная защита от внутренних угроз информационной безопасности»
- современные профессиональные технологии в предметной (профессиональной) сфере деятельности;
- принципы проектирования системы корпоративной защиты от внутренних угроз;
- основные правовые понятия и нормативно-правовые документы, регламентирующие организацию корпоративной защиты от внутренних угроз в хозяйствующих субъектах;
- инструментарий, технологии, их область применения и ограничения при формировании корпоративной защиты от внутренних угроз.
- типовые организационно-штатные структуры организаций различных сфер деятельности и размера;
- типовой набор объектов защиты, приоритеты доступа к информации, типовые роли пользователей;
- каналы передачи данных: определение и виды;
- подходы и методы обследования объекта информатизации для последующей защиты;
- сетевые устройства, которые могут быть использованы как источники событий для анализа;
- технологии работы с политиками информационной безопасности;
- основные функции системы DLPIWTM;
- категорирование информации в РФ;
- типы угроз информационной безопасности, понимать их актуальность и степень угрозы для конкретной организации;
- алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных;

- технику безопасности и экологию производства.

Уметь:

- разрабатывать нормативно-правовые документы хозяйствующего субъекта по организации корпоративной защиты от внутренних угроз информационной безопасности;
- проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации;
- администрировать автоматизированные технические средства управления и контроля информации и информационных потоков;
- осуществлять установку и конфигурирование систем DLPIWTM;
- разрабатывать политики детектирования и блокировки утечек с использованием DLP-систем;
- показать свой профессионализм и отношение к профессии;
- поддерживать в чистоте и подготовить рабочее место;
- работать в DLP-системе с событиями, запросами, объектами защиты, политиками, сводками, виджетами, персонами.

3. Объем

Данные об общем объеме курса трудоемкости отдельных видов учебной работы представлены в таблице 1

Таблица 1 – Объем и трудоемкость курса

Вид учебной работы	**Всего**
1	2
Общая трудоемкость дисциплины (модуля), (час)	21
Аудиторные занятия, всего час., ***В том числе****	20
Лекции (Л), (час)	4
Практические/семинарские занятия (ПЗ), (час)	16
Лабораторные работы (ЛР), (час)	X
Самостоятельная работа, всего (час)	X
Вид промежуточной аттестации (при наличии)	зачет

4. Содержание

4.1. Распределение трудоемкости по разделам, темам и видам занятий

Разделы, темы и их трудоемкость приведены в таблице 2.

Таблица 2 – Разделы, темы курса и их трудоемкость

Разделы, темы	Виды учебных занятий*	
	Лекции	Практика
Модуль 9. Технологии агентского мониторинга	4	16
Тема 9.1. Назначение агентского мониторинга. Установка и настройка агентского мониторинга	2	8
Тема 9.2. Политики агентского мониторинга, особенности их настройки. Создание и проверка политик	2	8
Итого:	4	16

5. Организационно-педагогические условия

5.1. Материально-технические условия

Состав материально-технической базы представлен в таблице 3.

Таблица 3 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы*	Номер аудитории (при необходимости)
1	Лаборатория, компьютерный класс	
2	Мультимедийная лекционная аудитория	

Программа повышения квалификации реализуется с использованием электронного обучения и дистанционных образовательных технологий. К материально-техническому оснащению рабочего места преподавателя программы относятся:
- Компьютер, мультимедийный проектор, экран, доска, флипчарт;
- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог (1 шт.);
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор) (1 шт.);
- Клавиатура USB (2 шт.);
- Мышь Wireless или USB (2 шт.);
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6 (4 шт.);
- Кабель HDMI 3 метра (2 шт.);
- USB-носитель не менее USB2.0, не менее 8ГБ (2 шт.);
- Точка доступа с поддержкой диапазонов 2ГГц и 5ГГц, возможностью подключения не менее 10 клиентов, создания не менее 3 SSID, подержкаVLAN, поддержка PoE (1 шт.);
- Коммутатор не менее 24 портов Gigabit, управляемый, поддержка настройки VLAN (1 шт.);
- Маршрутизатор не менее 4 портов Gigabit, управляемый, поддержка NAT, DHCP, VLAN, VPN, управляемый, L3 (1 шт.);
- Принтер (1 шт.).

К материально-техническому оснащению рабочего места слушателя программы относятся:
- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог;
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор);
- Клавиатура USB;
- Мышь Wireless или USB;
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6;
- Кабель HDMI 3 метра;
- USB-носитель не менее USB2.0, не менее 8ГБ.

5.2. Учебно-методическое и информационное обеспечение

Перечень основной и дополнительной литературы приведен в таблице 4.

Таблица 4 – Перечень основной и дополнительной литературы

Шифр / URL адрес	Библиографическая ссылка	Количество экземпляров в

		библиотеке (кроме электронных экземпляров)
Основная литература		
https://kb.infowatch.com/ pages/viewpage.action? pageId=32079878	Техническая документация по решению Info Watch Traffic Monitor 4.1 [электронный ресурс]	
https://bit.mephi.ru/index.php/bit/article/view/14/22	А.С. Зайцев, А.А. Малюк, Разработка классификации внутренних угроз информационной безопасности посредством классификации инцидентов, Москва, журнал БИТ № 3 2016 г. [электронный ресурс]	
https://www.twirpx.com/ file/185060/	Партыка Т.Л., Попов И.И. Информационная безопасность, учебное пособие. 5-е изд., перераб. и доп. - М.: ФОРУМ, 2012. - 432 с.	
http://padabum.com/ d.php?id=27762	Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер, 2008. – 320 с.	
Х404.3М 48	Информационная безопасность и защита информации: учебное пособие/ В. П. Мельников, С.А. Клейменов, А.М. Петраков; ред. С.А. Клейменов. -5-е изд., стер.- М.: Академия, 2011.-331с.	25
004 М 87	Мошак Н.Н. Организация безопасного доступа к информационным ресурсам [Текст]: учебное пособие /Н.Н. Мошак, Т. М. Татарникова; М-во образования и науки Российской Федерации, Федеральное гос. авт. образовательное учреждение высш. проф. образования Санкт-Петербургский гос. ун-т аэрокосмического приборостроения. - Санкт-Петербург : ГУАП, 2014. - 121 с. : ил., табл.	40
3-40	Защита от внутренних угроз информационной безопасности с использованием современных DLP-технологий: учеб. пособие / А.В. Сергеев, Е.В. Трапезников, Н.В. Матвеев, А.А. Крылова, А.А. Овчинников; под ред. д-ра техн. наук, проф. А.М. Тюрликова. – СПб.: ГУАП, 2021. – 202с.: ил.	100
004М 87-604316-ED	Мошак Н.Н. Защищенные инфотелекоммуникации. Анализ и синтез [Электронный ресурс]: монография/ Н. Н. Мошак ; М-во образования и науки Российской Федерации, Федеральное гос. авт. образовательное учреждение высш. проф. образования Санкт-Петербургский гос. ун-т аэрокосмического приборостроения. - Санкт-Петербург : ГУАП, 2014. - 197 с. :ил., табл.	40

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения курса, приведен в таблице 5.

Таблица 5 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ

URL адрес	Наименование
www.fstec.ru	Сайт «Федеральной службы технического и экспортного контроля РФ»
https://worldskills.ru	Официальный сайт оператора международного некоммерческого движения WorldSkills International - Союз «Молодые профессионалы (Ворлдскиллс Россия)»
https://esat.worldskills.ru	Единая система актуальных требований Ворлдскиллс

Перечень используемого программного обеспечения представлен в таблице 6.

Таблица 6 – Перечень программного обеспечения

№ п/п	Наименование
1	ПО для виртуализации VMWareWorkstation/VirtualBox или аналог, офисный пакет MSOffice/LibreOffice или аналог, notepad++ или аналог, браузер Firefox и Chrome или аналог
2	ПО для борьбы с внутренними утечками информации InfoWatchTrafficMonitor EducationLab не ниже 6.9 (минимальынй состав InfowatchTrafficMonitor, InfowatchDeviceMonitor, Crawler)
3	OS MS Windows 10
4	OS MS Windows Server 2012
5	OS MS Windows Server 2016
6	Почтовый сервер в составе postfix и dovecot или аналогов, поддержка работы в режиме SMTPRelay, поддержка интеграции с DLP системой для перехвата почтовых сообщений
7	ПОдля проведения тестов на безопасность с предустановленными утилитами и наборами тестов на базе ОС Linux (например, KaliLinux, Parrot и другие)

Перечень используемых информационно-справочных систем представлен в таблице 7.

Таблица 7 – Перечень информационно-справочных систем

№ п/п	Наименование
1	Официальный сайт оператора международного некоммерческого движения WorldSkillsInternational - Автономная некоммерческая организация «Агентство развития профессионального мастерства (Ворлдскиллс Россия)» (электронный ресурс) режим доступа: https://worldskills.ru
2	Единая система актуальных требований Ворлдскиллс (электронный ресурс) режим доступа: https://esat.worldskills.ru

6 Оценочные материалы для проведения промежуточной аттестации

6.1 Состав оценочных материалов приведен в таблице 8.

Таблица 8 - Состав оценочных материалов для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных материалов
Тест	Список вопросов

6.2 В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала университета. В таблице 9 представлена 4-балльная шкала для оценки сформированности компетенций.

Таблица 9 –Критерии оценки уровня сформированности компетенций

Оценка компетенции (4-балльная шкала)	Характеристика сформированных компетенций
«отлично» «зачтено»	- слушатель глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой специализированных понятий.
«хорошо» «зачтено»	- слушатель твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью направления; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	- слушатель усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний направления; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой специализированных понятий.
«неудовлетворительно» «не зачтено»	- слушатель не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений.

6.3 Типовые контрольные задания или иные материалы:

Вопросы (задачи) для экзамена (таблица 10)

Таблица 10 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена
	Не предусмотрено

Вопросы (задачи) для зачета / дифференцированного зачета (таблица 11)

Таблица 11 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	Не предусмотрено

Вопросы для проведения промежуточной аттестации при тестировании (таблица 12)

Таблица 12 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
1.	Каким образом обеспечить временный доступ на клиентском компьютере до заблокированного CD привода A) Выдать временный доступ используя консоль управления Device Monitor B) Выдача временного доступа не осуществляется C) Выдача доступа осуществляется администратором на прямую на клиентском компьютере Ответ: A
2.	Сколько политик одновременно может быть назначено группе сотрудников или группе компьютеров A) Множество B) Одна C) Две D) Политики назначаются только конкретным компьютерам Ответ: B
3.	В компании запрещена запись данных на внешние носители информации. Каким образом пользователь может получить временный доступ на запись данных? A) Отправить документ на личную почту и записать данные с другого устройства. B) Запросить доступ, получить код разблокировки, записать данные. C) Попросить директора компании записать данные на флешку. D) Загрузиться с Live-CD и записать данные. Ответ: B
4.	Правило Clipboard Monitor в консоли управления IWDM позволяет … A) контролировать доступ сотрудников к приложениям при помощи черных и белых списков. B) Контролировать вставку данных из буфера обмена. C) Контролировать веб-клиенты облачных хранилищ. D) Контролировать доступ сотрудников к выбранному типу периферийных устройств. Ответ: B
5.	Перехватчик ScreenShot Control Monitor позволяет... A) Контролировать снимков экрана. B) Автоматически создавать снимки экрана на компьютерах. C) Осуществлять мониторинг операций, связанных с печатью документов. Ответ: A
6.	Перехватчик ScreenShot Monitor позволяет... A) Контролировать снимков экрана. B) Автоматически создавать снимки экрана на компьютерах. C) Осуществлять мониторинг операций, связанных с печатью документов. Ответ: B

Контрольные и практические задачи / задания по дисциплине (модулю) (таблица 13)

Таблица 13 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
	Не предусмотрено

Программу составили:

Ст. преподаватель каф. № 52 должность, уч. степень, звание	 подпись, дата	Н.В. Матвеев инициалы, фамилия

Декан ФДПО Д-р экон. наук, профессор каф. 82 должность, уч. степень, звание	 подпись, дата	А.М. Мельниченко инициалы, фамилия

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

«Разработка политик безопасности, анализ выявленных инцидентов»
(Название)

По ДПП ПК «Корпоративная защита от внутренних угроз информационной безопасности с использованием современных DLP технологий (с учетом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»)»
(Наименование ДПП)

Форма обучения: очная с использованием дистанционных образовательных технологий

1. Цель

Целью данного курса является изучение основных принципов, методов и средств защиты информации от утечек по техническим каналам передачи информации, с осуществлением выбора по использованию систем защиты информации от внутренних угроз DLP IWTM.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения ДПП

В результате освоения курса слушатель должен обладать следующими компетенциями:
профессиональные компетенции:
ПК-1 - Осуществлять и обосновывать выбор решений по использованию систем защиты информации от внутренних угроз DLPIWTM.
Знать:

- спецификацию стандарта компетенции «Корпоративная защита от внутренних угроз информационной безопасности»
- современные профессиональные технологии в предметной (профессиональной) сфере деятельности;
- принципы проектирования системы корпоративной защиты от внутренних угроз;
- основные правовые понятия и нормативно-правовые документы, регламентирующие организацию корпоративной защиты от внутренних угроз в хозяйствующих субъектах;
- инструментарий, технологии, их область применения и ограничения при формировании корпоративной защиты от внутренних угроз.
- типовые организационно-штатные структуры организаций различных сфер деятельности и размера;
- типовой набор объектов защиты, приоритеты доступа к информации, типовые роли пользователей;
- каналы передачи данных: определение и виды;
- подходы и методы обследования объекта информатизации для последующей защиты;
- сетевые устройства, которые могут быть использованы как источники событий для анализа;
- технологии работы с политиками информационной безопасности;
- основные функции системы DLPIWTM;
- категорирование информации в РФ;
- типы угроз информационной безопасности, понимать их актуальность и степень угрозы для конкретной организации;
- алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных;

- технику безопасности и экологию производства.

Уметь:

- разрабатывать нормативно-правовые документы хозяйствующего субъекта по организации корпоративной защиты от внутренних угроз информационной безопасности;
- проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации;
- администрировать автоматизированные технические средства управления и контроля информации и информационных потоков;
- осуществлять установку и конфигурирование систем DLPIWTM;
- разрабатывать политики детектирования и блокировки утечек с использованием DLP-систем;
- показать свой профессионализм и отношение к профессии;
- поддерживать в чистоте и подготовить рабочее место;
- работать в DLP-системе с событиями, запросами, объектами защиты, политиками, сводками, виджетами, персонами.

3. Объем

Данные об общем объеме курса трудоемкости отдельных видов учебной работы представлены в таблице 1

Таблица 1 – Объем и трудоемкость курса

Вид учебной работы	**Всего**
1	2
Общая трудоемкость дисциплины (модуля), (час)	21
Аудиторные занятия, всего час., ***В том числе****	20
Лекции (Л), (час)	4
Практические/семинарские занятия (ПЗ), (час)	16
Лабораторные работы (ЛР), (час)	X
Самостоятельная работа, всего (час)	X
Вид промежуточной аттестации (при наличии)	зачет

4. Содержание

4.1. Распределение трудоемкости по разделам, темам и видам занятий

Разделы, темы и их трудоемкость приведены в таблице 2.

Таблица 2 – Разделы, темы курса и их трудоемкость

Разделы, темы	Виды учебных занятий*	
	Лекции	Практика
Модуль 10. Разработка политик безопасности, анализ выявленных инцидентов	4	16
Тема 10.1. Разработка и тестирование политик в системе DLPIWTM	2	8
Тема 10.2. Мониторинг трафика. Проверка применения	2	8
Итого:	4	16

5. Организационно-педагогические условия

5.1. Материально-технические условия

Состав материально-технической базы представлен в таблице 3.

Таблица 3 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы*	Номер аудитории (при необходимости)
1	Лаборатория, компьютерный класс	
2	Мультимедийная лекционная аудитория	

Программа повышения квалификации реализуется с использованием электронного обучения и дистанционных образовательных технологий. К материально-техническому оснащению рабочего места преподавателя программы относятся:
- Компьютер, мультимедийный проектор, экран, доска, флипчарт;
- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог (1 шт.);
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор) (1 шт.);
- Клавиатура USB (2 шт.);
- Мышь Wireless или USB (2 шт.);
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6 (4 шт.);
- Кабель HDMI 3 метра (2 шт.);
- USB-носитель не менее USB2.0, не менее 8ГБ (2 шт.);
- Точка доступа с поддержкой диапазонов 2ГГц и 5ГГц, возможностью подключения не менее 10 клиентов, создания не менее 3 SSID, подержкаVLAN, поддержка PoE (1 шт.);
- Коммутатор не менее 24 портов Gigabit, управляемый, поддержка настройки VLAN (1 шт.);
- Маршрутизатор не менее 4 портов Gigabit, управляемый, поддержка NAT, DHCP, VLAN, VPN, управляемый, L3 (1 шт.);
- Принтер (1 шт.).

К материально-техническому оснащению рабочего места слушателя программы относятся:
- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог;
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор);
- Клавиатура USB;
- Мышь Wireless или USB;
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6;
- Кабель HDMI 3 метра;
- USB-носитель не менее USB2.0, не менее 8ГБ.

5.2. Учебно-методическое и информационное обеспечение

Перечень основной и дополнительной литературы приведен в таблице 4.

Таблица 4 – Перечень основной и дополнительной литературы

Шифр / URL адрес	Библиографическая ссылка	Количество экземпляров в

		библиотеке (кроме электронных экземпляров)
Основная литература		
https://kb.infowatch.com/ pages/viewpage.action? pageId=32079878	Техническая документация по решению Info Watch Traffic Monitor 4.1 [электронный ресурс]	
https://bit.mephi.ru/index.php/bit/article/view/14/22	А.С. Зайцев, А.А. Малюк, Разработка классификации внутренних угроз информационной безопасности посредством классификации инцидентов, Москва, журнал БИТ № 3 2016 г. [электронный ресурс]	
https://www.twirpx.com/ file/185060/	Партыка Т.Л., Попов И.И. Информационная безопасность, учебное пособие. 5-е изд., перераб. и доп. - М.: ФОРУМ, 2012. - 432 с.	
http://padabum.com/ d.php?id=27762	Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер, 2008. – 320 с.	
Х404.3М 48	Информационная безопасность и защита информации: учебное пособие/ В. П. Мельников, С.А. Клейменов, А.М. Петраков; ред. С.А. Клейменов. -5-е изд., стер.- М.: Академия, 2011.-331с.	25
004 М 87	Мошак Н.Н. Организация безопасного доступа к информационным ресурсам [Текст]: учебное пособие /Н.Н. Мошак, Т. М. Татарникова; М-во образования и науки Российской Федерации, Федеральное гос. авт. образовательное учреждение высш. проф. образования Санкт-Петербургский гос. ун-т аэрокосмического приборостроения. - Санкт-Петербург : ГУАП, 2014. - 121 с. : ил., табл.	40
3-40	Защита от внутренних угроз информационной безопасности с использованием современных DLP-технологий: учеб. пособие / А.В. Сергеев, Е.В. Трапезников, Н.В. Матвеев, А.А. Крылова, А.А. Овчинников; под ред. д-ра техн. наук, проф. А.М. Тюрликова. – СПб.: ГУАП, 2021. – 202с.: ил.	100
004М 87-604316-ED	Мошак Н.Н. Защищенные инфотелекоммуникации. Анализ и синтез [Электронный ресурс]: монография/ Н. Н. Мошак ; М-во образования и науки Российской Федерации, Федеральное гос. авт. образовательное учреждение высш. проф. образования Санкт-Петербургский гос. ун-т аэрокосмического приборостроения. - Санкт-Петербург : ГУАП, 2014. - 197 с. :ил., табл.	40

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения курса, приведен в таблице 5.

Таблица 5 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ

URL адрес	Наименование
www.fstec.ru	Сайт «Федеральной службы технического и экспортного контроля РФ»
https://worldskills.ru	Официальный сайт оператора международного некоммерческого движения WorldSkills International - Союз «Молодые профессионалы (Ворлдскиллс Россия)»
https://esat.worldskills.ru	Единая система актуальных требований Ворлдскиллс

Перечень используемого программного обеспечения представлен в таблице 6.

Таблица 6 – Перечень программного обеспечения

№ п/п	Наименование
1	ПО для виртуализации VMWareWorkstation/VirtualBox или аналог, офисный пакет MSOffice/LibreOffice или аналог, notepad++ или аналог, браузер Firefox и Chrome или аналог
2	ПО для борьбы с внутренними утечками информации InfoWatchTrafficMonitor EducationLab не ниже 6.9 (минимальынй состав InfowatchTrafficMonitor, InfowatchDeviceMonitor, Crawler)
3	OS MS Windows 10
4	OS MS Windows Server 2012
5	OS MS Windows Server 2016
6	Почтовый сервер в составе postfix и dovecot или аналогов, поддержка работы в режиме SMTPRelay, поддержка интеграции с DLP системой для перехвата почтовых сообщений
7	ПОдля проведения тестов на безопасность с предустановленными утилитами и наборами тестов на базе ОС Linux (например, KaliLinux, Parrot и другие)

Перечень используемых информационно-справочных систем представлен в таблице 7.

Таблица 7 – Перечень информационно-справочных систем

№ п/п	Наименование
1	Официальный сайт оператора международного некоммерческого движения WorldSkillsInternational - Автономная некоммерческая организация «Агентство развития профессионального мастерства (Ворлдскиллс Россия)» (электронный ресурс) режим доступа: https://worldskills.ru
2	Единая система актуальных требований Ворлдскиллс (электронный ресурс) режим доступа: https://esat.worldskills.ru

6 Оценочные материалы для проведения промежуточной аттестации

6.1 Состав оценочных материалов приведен в таблице 8.

Таблица 8 - Состав оценочных материалов для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных материалов
Тест	Список вопросов

6.2 В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала университета. В таблице 9 представлена 4-балльная шкала для оценки сформированности компетенций.

Таблица 9 –Критерии оценки уровня сформированности компетенций

Оценка компетенции (4-балльная шкала)	Характеристика сформированных компетенций
«отлично» «зачтено»	- слушатель глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой специализированных понятий.
«хорошо» «зачтено»	- слушатель твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью направления; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	- слушатель усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний направления; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой специализированных понятий.
«неудовлетворительно» «не зачтено»	- слушатель не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений.

6.3 Типовые контрольные задания или иные материалы:

Вопросы (задачи) для экзамена (таблица 10)

Таблица 10 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена
	Не предусмотрено

Вопросы (задачи) для зачета / дифференцированного зачета (таблица 11)

Таблица 11 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	Не предусмотрено

Вопросы для проведения промежуточной аттестации при тестировании (таблица 12)

Таблица 12 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
1.	Что такое "объект защиты"? A) Совокупность элементов технологий и используется для классификации событий B) Настраиваемая политика защиты C) Пользователь или компьютер, подлежащий защите Ответ: A
2.	Что такое токен? A) Идентификатор системы Traffic Monitor B) Авторизация внешней системы C) Это токен Device Monitor Ответ: B
3.	Необходимо, чтобы при попытке передачи сканов документов с печатью организации Traffic Monitor оповещал о подобных событиях. Какую технологию необходимо задействовать чтобы обеспечить такую возможность? A) Сканы B) Печать Ответ: B
4.	Какой компонент IWTM позволяет выполнять проверку файлов, хрянящихся в корпоративной сети, на предмет нарушения корпоративных политик безопасности? A) Crawler B) Deploy Agent C) Consul Ответ: A
5.	Необходимо, чтобы при попытке передачи сканов паспорта Traffic Monitor оповещал о подобных событиях. Какую технологию необходимо задействовать чтобы обеспечить такую возможность? A) Сканы B) Печать C) Графические объекты Ответ: C
6.	В корпоративной сети присутствует сервер Домена, какой запрос позволит получить список пользователей в раздел Персоны IWTM? A) LDAP B) AD C) HTTP Ответ: A
7.	Необходимо, чтобы при попытке передачи фрагментов текста, принадлежащих к заранее заданным документам Traffic Monitor оповещал о подобных событиях. Какую технологию необходимо задействовать чтобы обеспечить такую возможность? A) Эталонные документы B) Сканы C) Печать Ответ: A

Контрольные и практические задачи / задания по дисциплине (модулю) (таблица 13)

Таблица 13 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий

	Не предусмотрено

Программу составили:

Ст. преподаватель каф. № 52  Н.В. Матвеев
должность, уч. степень, звание подпись, дата инициалы, фамилия

Декан ФДПО

Д-р экон. наук, профессор каф. 82  А.М. Мельниченко
должность, уч. степень, звание подпись, дата инициалы, фамилия

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

«Обследование (аудит) организации с целью защиты от угроз информационной безопасности»
(Название)

По ДПП ПК «Корпоративная защита от внутренних угроз информационной безопасности с использованием современных DLP технологий (с учетом стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»)»
(Наименование ДПП)

Форма обучения: очная с использованием дистанционных образовательных технологий

1. Цель

Целью данного курса является изучение основных принципов, методов и средств защиты информации от утечек по техническим каналам передачи информации, с осуществлением выбора по использованию систем защиты информации от внутренних угроз DLP IWTM.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения ДПП

В результате освоения курса слушатель должен обладать следующими компетенциями:
профессиональные компетенции:
ПК-1 - Осуществлять и обосновывать выбор решений по использованию систем защиты информации от внутренних угроз DLPIWTM.
Знать:

- спецификацию стандарта компетенции «Корпоративная защита от внутренних угроз информационной безопасности»
- современные профессиональные технологии в предметной (профессиональной) сфере деятельности;
- принципы проектирования системы корпоративной защиты от внутренних угроз;
- основные правовые понятия и нормативно-правовые документы, регламентирующие организацию корпоративной защиты от внутренних угроз в хозяйствующих субъектах;
- инструментарий, технологии, их область применения и ограничения при формировании корпоративной защиты от внутренних угроз.
- типовые организационно-штатные структуры организаций различных сфер деятельности и размера;
- типовой набор объектов защиты, приоритеты доступа к информации, типовые роли пользователей;
- каналы передачи данных: определение и виды;
- подходы и методы обследования объекта информатизации для последующей защиты;
- сетевые устройства, которые могут быть использованы как источники событий для анализа;
- технологии работы с политиками информационной безопасности;
- основные функции системы DLPIWTM;
- категорирование информации в РФ;
- типы угроз информационной безопасности, понимать их актуальность и степень угрозы для конкретной организации;
- алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных;

- технику безопасности и экологию производства.

Уметь:

- разрабатывать нормативно-правовые документы хозяйствующего субъекта по организации корпоративной защиты от внутренних угроз информационной безопасности;
- проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации;
- администрировать автоматизированные технические средства управления и контроля информации и информационных потоков;
- осуществлять установку и конфигурирование систем DLPIWTM;
- разрабатывать политики детектирования и блокировки утечек с использованием DLP-систем;
- показать свой профессионализм и отношение к профессии;
- поддерживать в чистоте и подготовить рабочее место;
- работать в DLP-системе с событиями, запросами, объектами защиты, политиками, сводками, виджетами, персонами.

3. Объем

Данные об общем объеме курса трудоемкости отдельных видов учебной работы представлены в таблице 1

Таблица 1 – Объем и трудоемкость курса

Вид учебной работы	**Всего**
1	2
Общая трудоемкость дисциплины (модуля), (час)	17
Аудиторные занятия, всего час., ***В том числе****	16
Лекции (Л), (час)	8
Практические/семинарские занятия (ПЗ), (час)	8
Лабораторные работы (ЛР), (час)	X
Самостоятельная работа, всего (час)	X
Вид промежуточной аттестации (при наличии)	зачет

4. Содержание

4.1. Распределение трудоемкости по разделам, темам и видам занятий

Разделы, темы и их трудоемкость приведены в таблице 2.

Таблица 2 – Разделы, темы курса и их трудоемкость

Разделы, темы	Виды учебных занятий*	
	Лекции	Практика
Модуль 11. Обследование (аудит) организации с целью защиты от угроз информационной безопасности	8	8
Тема 11.1. Понятие аудита информационной безопасности. Теория и практика обследования организации с целью защиты от угроз информационной безопасности	4	X
Тема 11.2. Законодательство в области защиты конфиденциальной информации. Виды информации ограниченного доступа. Персональные данные.	2	4

Коммерческая тайна		
Тема 11.3. Тестирование защищенности информационных ресурсов	2	4
Итого:	8	8

5. Организационно-педагогические условия

5.1. Материально-технические условия

Состав материально-технической базы представлен в таблице 3.

Таблица 3 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы*	Номер аудитории (при необходимости)
1	Лаборатория, компьютерный класс	
2	Мультимедийная лекционная аудитория	

Программа повышения квалификации реализуется с использованием электронного обучения и дистанционных образовательных технологий. К материально-техническому оснащению рабочего места преподавателя программы относятся:

- Компьютер, мультимедийный проектор, экран, доска, флипчарт;
- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог (1 шт.);
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор) (1 шт.);
- Клавиатура USB (2 шт.);
- Мышь Wireless или USB (2 шт.);
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6 (4 шт.);
- Кабель HDMI 3 метра (2 шт.);
- USB-носитель не менее USB2.0, не менее 8ГБ (2 шт.);
- Точка доступа с поддержкой диапазонов 2ГГц и 5ГГц, возможностью подключения не менее 10 клиентов, создания не менее 3 SSID, подержкаVLAN, поддержка PoE (1 шт.);
- Коммутатор не менее 24 портов Gigabit, управляемый, поддержка настройки VLAN (1 шт.);
- Маршрутизатор не менее 4 портов Gigabit, управляемый, поддержка NAT, DHCP, VLAN, VPN, управляемый, L3 (1 шт.);
- Принтер (1 шт.).

К материально-техническому оснащению рабочего места слушателя программы относятся:

- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог;
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор);
- Клавиатура USB;
- Мышь Wireless или USB;
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6;
- Кабель HDMI 3 метра;
- USB-носитель не менее USB2.0, не менее 8ГБ.

5.2. Учебно-методическое и информационное обеспечение

Перечень основной и дополнительной литературы приведен в таблице 4.

Таблица 4 – Перечень основной и дополнительной литературы

Шифр / URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
Основная литература		
https://kb.infowatch.com/ pages/viewpage.action ? pageId=32079878	Техническая документация по решению Info Watch Traffic Monitor 4.1 [электронный ресурс]	
https://bit.mephi.ru/index.php/bit/article/ view/14/22	А.С. Зайцев, А.А. Малюк, Разработка классификации внутренних угроз информационной безопасности посредством классификации инцидентов, Москва, журнал БИТ № 3 2016 г. [электронный ресурс]	
https://www.twirpx.com/ file/185060/	Партыка Т.Л., Попов И.И. Информационная безопасность, учебное пособие. 5-е изд., перераб. и доп. - М.: ФОРУМ, 2012. - 432 с.	
http://padabum.com/ d.php?id=27762	Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер, 2008. – 320 с.	
Х404.3М 48	Информационная безопасность и защита информации: учебное пособие/ В. П. Мельников, С.А. Клейменов, А.М. Петраков; ред. С.А. Клейменов. -5-е изд., стер.- М.: Академия, 2011.-331с.	25
004 М 87	Мошак Н.Н. Организация безопасного доступа к информационным ресурсам [Текст]: учебное пособие /Н.Н. Мошак, Т. М. Татарникова; М-во образования и науки Российской Федерации, Федеральное гос. авт. образовательное учреждение высш. проф. образования Санкт-Петербургский гос. ун-т аэрокосмического приборостроения. - Санкт-Петербург : ГУАП, 2014. - 121 с. : ил., табл.	40
3-40	Защита от внутренних угроз информационной безопасности с использованием современных DLP-технологий: учеб. пособие / А.В. Сергеев, Е.В. Трапезников, Н.В. Матвеев, А.А. Крылова, А.А. Овчинников; под ред. д-ра техн. наук, проф. А.М. Тюрликова. – СПб.: ГУАП, 2021. – 202с.: ил.	100
004М 87-604316-ED	Мошак Н.Н. Защищенные инфотелекоммуникации. Анализ и синтез [Электронный ресурс]: монография/ Н. Н. Мошак ; М-во образования и науки Российской Федерации, Федеральное	40

	гос. авт. образовательное учреждение высш. проф. образования Санкт-Петербургский гос. ун-т аэрокосмического приборостроения. - Санкт-Петербург : ГУАП, 2014. - 197 с. :ил., табл.	

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения курса, приведен в таблице 5.

Таблица 5 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ

URL адрес	Наименование
www.fstec.ru	Сайт «Федеральной службы технического и экспортного контроля РФ»
https://worldskills.ru	Официальный сайт оператора международного некоммерческого движения WorldSkills International - Союз «Молодые профессионалы (Ворлдскиллс Россия)»
https://esat.worldskills.ru	Единая система актуальных требований Ворлдскиллс

Перечень используемого программного обеспечения представлен в таблице 6.

Таблица 6 – Перечень программного обеспечения

№ п/п	Наименование
1	ПО для виртуализации VMWareWorkstation/VirtualBox или аналог, офисный пакет MSOffice/LibreOffice или аналог, notepad++ или аналог, браузер Firefox и Chrome или аналог
2	ПО для борьбы с внутренними утечками информации InfoWatchTrafficMonitor EducationLab не ниже 6.9 (минимальыний состав InfowatchTrafficMonitor, InfowatchDeviceMonitor, Crawler)
3	OS MS Windows 10
4	OS MS Windows Server 2012
5	OS MS Windows Server 2016
6	Почтовый сервер в составе postfix и dovecot или аналогов, поддержка работы в режиме SMTPRelay, поддержка интеграции с DLP системой для перехвата почтовых сообщений
7	ПОдля проведения тестов на безопасность с предустановленными утилитами и наборами тестов на базе ОС Linux (например, KaliLinux, Parrot и другие)

Перечень используемых информационно-справочных систем представлен в таблице 7.

Таблица 7 – Перечень информационно-справочных систем

№ п/п	Наименование
1	Официальный сайт оператора международного некоммерческого движения WorldSkillsInternational - Автономная некоммерческая организация «Агентство развития профессионального мастерства (Ворлдскиллс Россия)» (электронный ресурс) режим доступа: https://worldskills.ru
2	Единая система актуальных требований Ворлдскиллс (электронный ресурс) режим доступа: https://esat.worldskills.ru

6 Оценочные материалы для проведения промежуточной аттестации

6.1 Состав оценочных материалов приведен в таблице 8.

Таблица 8 - Состав оценочных материалов для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных материалов
Тест	Список вопросов

6.2 В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала университета. В таблице 9 представлена 4-балльная шкала для оценки сформированности компетенций.

Таблица 9 –Критерии оценки уровня сформированности компетенций

Оценка компетенции (4-балльная шкала)	Характеристика сформированных компетенций
«отлично» «зачтено»	- слушатель глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой специализированных понятий.
«хорошо» «зачтено»	- слушатель твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью направления; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	- слушатель усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний направления; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой специализированных понятий.
«неудовлетворительно» «не зачтено»	- слушатель не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений.

6.3 Типовые контрольные задания или иные материалы:

Вопросы (задачи) для экзамена (таблица 10)

Таблица 10 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена

	Не предусмотрено

Вопросы (задачи) для зачета / дифференцированного зачета (таблица 11)

Таблица 11 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	Не предусмотрено

Вопросы для проведения промежуточной аттестации при тестировании (таблица 12)

Таблица 12 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
1.	Защищаемая информация – это A) Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации; B) Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями, устанавливаемыми собственником информации; C) Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов; D) Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями Федерального закона «О защищаемой информации в Российской Федерации» Ответ: A
2.	Требования по защите информации, не содержащей государственную тайну, содержащейся в государственных информационных системах устанавливает A) Приказ ФСТЭК №21; B) Приказ ФСТЭК №17; C) Приказ ФСТЭК №58; Ответ: B
3.	Кто является основным ответственным за определение уровня классификации информации? A) Руководитель среднего звена B) Высшее руководство C) Владелец D) Пользователь Ответ: C
4.	Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены? A) Владельцы данных B) Пользователи C) Администраторы D) Руководство Ответ: D
5.	Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании? A) Чтобы убедиться, что проводится справедливая оценка B) Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ

	C) Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа D) Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку Ответ: C
6.	Идентификация – это A) Присвоение субъектам и объектам доступа идентификатора и сравнение предъявляемого идентификатора с вводимым идентификатором; B) Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов; C) Присвоение субъектам и объектам доступа идентификатора; D) Присвоение субъектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с вводимым идентификатором. Ответ: B
7.	Что понимается под понятием «Конфиденциальность персональных данных»? A) Обязательное для соблюдения оператором или иным лицом требование не допускать их распространения без согласия субъекта персональных данных; B) Обязанность не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотренное федеральным законом; C) Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания Ответ: C
8.	Нарушитель безопасности персональных данных – это A) Физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных; B) Физическое лицо, преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных; C) Физическое или юридическое лицо, преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных. Ответ: A
9.	Какую информацию запрещено относить к конфиденциальной в соответствии с законом РФ? A) Паспортные данные гражданина B) Информация, накапливаемая в открытых фондах библиотек, музеев, архивов C) Себестоимость продукта и объем сбыта D) Контактные данные клиентов Ответ: B
10.	В каком нормативном правовом акте закреплены все виды конфиденциальной информации? A) В ФЗ -152 "О персональных данных" B) В Указе Президента № 188 C) В Трудовом кодексе РФ Ответ: B
11.	В каком случае фотографию можно отнести к биометрическим персональным данным?

	A) В случае если эта фотография находится в личном деле B) В случае если фотография зарегистрирована в СКУД (система контроля управления доступом) C) В случае если эта фотография сделана в публичном месте Ответ: B
12.	Специальные категории персональных данных – это A) Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни; B) Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных убеждений, интимной и личной жизни жизни; C) Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, состояния здоровья, интимной жизни; D) Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни и судимости. Ответ: A
13.	Законодательство Российской Федерации в области персональных данных состоит из A) ФЗ «О Государственной тайне»; B) ФЗ «Об электронной цифровой подписи»; C) ФЗ «О персональных данных»; D) ФЗ, ПП и НПА уполномоченных органов государственной власти РФ в сфере информации и персональных данных Ответ: C

Контрольные и практические задачи / задания по дисциплине (модулю) (таблица 13)

Таблица 13 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
	Не предусмотрено

Программу составили:

Ст. преподаватель каф. № 52 — подпись, дата — Н.В. Матвеев
должность, уч. степень, звание — инициалы, фамилия

Декан ФДПО

Д-р экон. наук, профессор каф 82 — подпись, дата — А.М. Мельниченко
должность, уч. степень, звание — инициалы, фамилия

4. ПРОГРАММА ИТОГОВОЙ АТТЕСТАЦИИ

4.1. Форма итоговой аттестации и оценочные материалы

Итоговая аттестация проводится в форме экзамена.

Форма проведения итогового экзамена – демонстрационный формат. Демонстрационная итоговый экзамена проводится очно с применением специального оборудования.

Перечень рекомендуемой литературы, необходимой при подготовке к итоговому экзамену приводится в подразделе 4.3.

4.2. Требования к итоговой аттестационной работе и порядку ее выполнения

Не предусмотрено.

4.3. Перечень рекомендуемой литературы для итоговой аттестации

Перечень основной и дополнительной литературы, необходимой при подготовке к ИА, приведен в Таблице 1.

Таблица 1 – Перечень основной и дополнительной литературы

Шифр / URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
Основная литература		
https://worldskills.ru/nashi-proektyi/demonstraczionnyij-ekzamen/documents/	Положение об организации и проведении демонстрационного экзамена по стандартам WorldSkills Союза «Молодые профессионалы», электронная публикация	
https://kb.infowatch.com/ pages/viewpage.action? pageId=32079878	Техническая документация по решению Info Watch Traffic Monitor 4.1 [электронный ресурс]	
https://bit.mephi.ru/index.php/bit/article/view/14/22	А.С. Зайцев, А.А. Малюк, Разработка классификации внутренних угроз информационной безопасности посредством классификации инцидентов, Москва, журнал БИТ № 3 2016 г. [электронный ресурс]	
https://www.twirpx.com/ file/185060/	Партыка Т.Л., Попов И.И. Информационная безопасность, учебное пособие. 5-е изд., перераб. и доп. - М.: ФОРУМ, 2012. - 432 с.	
http://padabum.com/ d.php?id=27762	Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер, 2008. – 320 с.	
Х404.3М 48	Информационная безопасность и защита информации: учебное пособие/ В. П. Мельников, С.А. Клейменов, А.М. Петраков;	25

	ред. С.А. Клейменов. -5-е изд., стер.- М.: Академия, 2011.-331с.	
004 М 87	Мошак Н.Н. Организация безопасного доступа к информационным ресурсам [Текст]: учебное пособие /Н.Н. Мошак, Т. М. Татарникова; М-во образования и науки Российской Федерации, Федеральное гос. авт. образовательное учреждение высш. проф. образования Санкт-Петербургский гос. ун-т аэрокосмического приборостроения. - Санкт-Петербург : ГУАП, 2014. - 121 с. : ил., табл.	40
3-40	Защита от внутренних угроз информационной безопасности с использованием современных DLP-технологий: учеб. пособие / А.В. Сергеев, Е.В. Трапезников, Н.В. Матвеев, А.А. Крылова, А.А. Овчинников; под ред. д-ра техн. наук, проф. А.М. Тюрликова. – СПб.: ГУАП, 2021. – 202с.: ил.	100
004М 87-604316-ED	Мошак Н.Н. Защищенные инфотелекоммуникации. Анализ и синтез [Электронный ресурс]: монография/ Н. Н. Мошак ; М-во образования и науки Российской Федерации, Федеральное гос. авт. образовательное учреждение высш. проф. образования Санкт-Петербургский гос. ун-т аэрокосмического приборостроения. - Санкт-Петербург : ГУАП, 2014. - 197 с. :ил., табл.	40

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых при подготовке к ИА, представлен в Таблице 2.

Таблица 2 – Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых при подготовке к ИА

URL-адрес	Наименование
https://worldskills.ru	Официальный сайт оператора международного некоммерческого движения WorldSkills International - Союз «Молодые профессионалы (Ворлдскиллс Россия)»
https://esat.worldskills.ru	Единая система актуальных требований Ворлдскиллс

4.4. Материально-технические условия

Перечень материально-технической базы, необходимой для проведения ИА, представлен в Таблице 3.

Таблица 3– Материально-техническая база

№ п/п	Наименование материально-технической базы	Номер аудитории (при необходимости)
1	Лаборатория, компьютерный класс	
2	Мультимедийная лекционная аудитория	

Итоговая аттестация по программе повышения квалификации реализуется с использованием электронного обучения и дистанционных образовательных технологий. К материально-техническому оснащению рабочего места преподавателя программы относятся:
- Компьютер, мультимедийный проектор, экран, доска, флипчарт;
- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог (1 шт.);
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор) (1 шт.);
- Клавиатура USB (2 шт.);
- Мышь Wireless или USB (2 шт.);
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6 (4 шт.);
- Кабель HDMI 3 метра (2 шт.);
- USB-носитель не менее USB2.0, не менее 8ГБ (2 шт.);
- Точка доступа с поддержкой диапазонов 2ГГц и 5ГГц, возможностью подключения не менее 10 клиентов, создания не менее 3 SSID, подержкаVLAN, поддержка PoE (1 шт.);
- Коммутатор не менее 24 портов Gigabit, управляемый, поддержка настройки VLAN (1 шт.);
- Маршрутизатор не менее 4 портов Gigabit, управляемый, поддержка NAT, DHCP, VLAN, VPN, управляемый, L3 (1 шт.);
- Принтер (1 шт.).

К материально-техническому оснащению рабочего места слушателя программы относятся:
- Компьютер с процессором не менее i5 3,2 ГГц с поддержкой виртуализации или аналог и выше, не менее 4 физических ядер, не менее 16 ГБ ОЗУ, не менее 250 ГБ SSD со свободным местом не менее 100 ГБ, не менее 50 ГБ на дополнительных носителях (HDD/SSD/USB3.0 Flash), ОС Windows/Linux/MacOS с графическим интерфейсом или аналог;
- Монитор не менее 20" и разрешением не менее 1920×1080 пкс (в случае ноутбука до 17" — дополнительный монитор);
- Клавиатура USB;
- Мышь Wireless или USB;
- Сетевой соединительный кабель RJ45, U/UTP, 3 м или длиннее, Cat.6;
- Кабель HDMI 3 метра;
- USB-носитель не менее USB2.0, не менее 8ГБ.

4.5. Оценочные материалы для проведения итоговой аттестации

4.5.1 Фонд оценочных материалов для проведения итогового экзамена

Состав фонда оценочных материалов для проведения итогового экзамена приведен в Таблице 4.

Таблица 4 – Состав фонда оценочных материалов для проведения итогового экзамена

Форма проведения итоговой аттестации	Перечень оценочных материалов
Экзамен	Демонстрационный экзамен (реализация проекта DLP-системы) на основе заданий из Комплекта оценочной документации (КОД) № 1.1 по компетенции WorldSkills «Корпоративная защита от внутренних угроз информационной безопасности».

Описание показателей и критериев для оценки компетенций, а также шкал оценивания для итогового зачета/экзамена.

Описание показателей для оценки компетенций для итогового экзамена:

– способность последовательно, четко и логично излагать материал;

– умение справляться с задачами;

– умение формулировать ответы на вопросы в рамках программы итогового зачета/экзамена с использованием материала научно-методической и научной литературы;

– уровень правильности обоснования принятых решений при выполнении практических задач.

Оценка уровня сформированности (освоения) компетенций осуществляется на основе таких составляющих как: знание, умение, владение навыками и/или опытом деятельности в соответствии с планируемыми результатами обучения по ДПП.

В качестве критериев оценки уровня сформированности (освоения) у слушателей компетенций при проведении итогового зачета/экзамена в формах «устная», «письменная» и с применением средств электронного обучения, применяется 4-балльная шкала (Таблица 5).

Таблица 5 – Критерии оценки уровня сформированности компетенций

Оценка компетенции (4-балльная шкала)	Характеристика сформированных компетенций
«отлично» зачтено	– слушатель глубоко и всесторонне усвоил учебный материал ДПП; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения к практической деятельности; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий.
«хорошо» зачтено	– слушатель твердо усвоил учебный материал ДПП, грамотно и, по существу, излагает его, опираясь на знания основной литературы; – не допускает существенных неточностей; – увязывает усвоенные знания с практической деятельностью; – аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий.
«удовлетворительно» зачтено	– слушатель усвоил только основной учебный материал ДПП, по существу, излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний; – слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий.
«неудовлетворительно» не зачтено	– слушатель не усвоил значительной части учебного материала ДПП; – допускает существенные ошибки и неточности при рассмотрении проблем; – испытывает трудности в практическом применении знаний; – не может аргументировать научные положения; – не формулирует выводов и обобщений.

Типовые контрольные задания или иные материалы представлены в Таблицах 6-7.

Таблица 6 – Список вопросов для итогового зачета/экзамена, проводимого в письменной/ устной форме

№ п/п	Список вопросов для итогового экзамена, проводимого в письменной форме	Компетенции
	Не предусмотрено	

Таблица 7 – Задания для итогового экзамена, проводимого в демонстрационной форме

№ п/п	Задания для итогового экзамена, проводимого в демонстрационной форме	Компетенции
1	Установка и конфигурирование компонентов DLP системы: 1) Настройка контроллера домена 2) Настройка DLP сервера 3) Установка и настройка сервера агентского мониторинга 4) Установка агента мониторинга на машине нарушителя 5) Установка и настройка подсистемы сканирования сетевых ресурсов (Crawler) 6) Проверка работоспособности системы 7) Защита системы с помощью сертификатов	ПК-1
2	Технологии агентского мониторинга: 1) Создать новую политику, применить ее к группе компьютеров по умолчанию 2) Установить дополнительную консоль управления сервером агентского мониторинга на машину нарушителя для удаленного доступа к серверу агентского мониторинга 3) Создать дополнительного локального офицера безопасности для удаленного управления доступом к серверу агентского мониторинга с полными правами на управление и просмотр разделов 4) Запретить пользоваться Microsoft Paint 5) Запретить создание снимков экрана в табличных процессорах 6) Поставить на контроль буфер обмена в текстовых процессорах 7) Запретить печать на сетевых принтерах 8) Запретить запись файлов на все съемные носители информации (флешки), оставив возможность чтения и копирования с них 9) Разрешить запись файлов на доверенный носитель. Запрет на запись на остальные носители оставить в силе 10) Создать политику по блокировке копирования файлов формата zip на USB-накопители 11) Поставить на контроль печать документов на принтерах 12) Установить контроль за компьютером потенциального нарушителя в случае использования браузера путем создания снимков экрана каждые 15 секунд или при переходе на другую страницу	ПК-1

	13) Заблокировать доступ к CD/DVD на клиентском компьютере (виртуальной машине) 14) Осуществить выдачу временного доступа (30 минут) клиенту до заблокированного CD привода 15) Запретить на машине нарушителя использование буфера обмена при подключении к удаленным машинам по протоколу RDP 16) Установить (сменить) пароль для удаления агента мониторинга на машине нарушителя с помощью средств сервера агентского мониторинга (удаленно)	
3	Разработка и применение политик, анализ выявленных инцидентов: 1) Создать локальную группу пользователей «Сотрудники под наблюдением». Добавить в нее трех любых пользователей 2) Настроить периметр компании, создать список веб ресурсов и дать им название, исключить из перехвата почту генерального директора 3) Создать пользователя системы с правами доступа только на чтение и выполнение отчетов, сводок и событий, а также на просмотр каталога локальных и доменных пользователей без возможности редактирования 4) Создать политику на правило передачи текстовых данных за пределы компании (на адреса вне домена), содержащих заданные слова 5) Ведение наблюдения за передачей как пустых, так и заполненных шаблонов документа за пределы компании с учетом того, что содержимое документа может изменяться в пределах 50% 6) Создать запрет на любую внешнюю передачу документов, содержащих заполненные бланки, при этом пустые бланки контролировать не нужно 7) Мониторинг движения официальных документов компании с официальной печатью 8) Создать запрет на передачу кодов за пределы компании. Контроль кодов внутри компании 9) Блокировка любых попыток передачи данных о заданных объектах на внешние адреса 10) Настройка мониторинга выгрузок из БД для контроля движения данных из базы данных компании только при отправке из отдела информатизации 11) Настроить отслеживание в почтовых сообщениях сотрудников упоминания заданных опций 12) Создать запрет на передачу документов с заданной информационной меткой (грифом) 13) Мониторинг использования заданных терминов 14) Создать запрет на передачу персональных данных сотрудников компании, кроме отдела кадров 15) Контроль передачи документов формата электронных таблиц (исключая csv файлы!), а также CAD-документации с учетом того, что файлы могут	ПК-1

	передаваться в том числе и на съемных носителях информации 16) Анализ инцидентов, обычные сводки	

4.5.2. Фонд оценочных материалов для оценки защиты итоговой аттестационной работы
Не предусмотрено.