МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра № 33

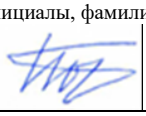
УТВЕРЖДАЮ
Руководитель направления

д.т.н.,проф.

(должность, уч. степень, звание)

А.М. Тюрликов

(инициалы, фамилия)



(подпись)

«26» мая 2022 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Корпоративная защита от внутренних угроз информационной безопасности»
(Наименование дисциплины)

Код направления подготовки/ специальности	11.03.02
Наименование направления подготовки/ специальности	Инфокоммуникационные технологии и системы связи
Наименование направленности	Программно-защищенные инфокоммуникации
Форма обучения	очная

Санкт-Петербург– 2022

Лист согласования рабочей программы дисциплины

Программу составил (а)

д.т.н.,доц.	 26.05.22	С.В. Беззатеев
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Программа одобрена на заседании кафедры № 33

«26» мая 2022 г, протокол № 10

Заведующий кафедрой № 33

д.т.н.,доц.	 26.05.22	С.В. Беззатеев
(уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Ответственный за ОП ВО 11.03.02(03)

доц.,к.т.н.,доц.	 26.05.22	Н.В. Марковская
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Заместитель директора института №2 по методической работе

доц.,к.т.н.,доц.	 26.05.22	О.Л. Балышева
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Аннотация

Дисциплина «Корпоративная защита от внутренних угроз информационной безопасности» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 11.03.02 «Инфокоммуникационные технологии и системы связи» направленности «Программно-защищенные инфокоммуникации». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-9 «Корпоративная защита от внутренних угроз информационной безопасности»

Содержание дисциплины охватывает круг вопросов, связанных с выбором решенийпо использованию систем защиты информации от внутренних угроз DLP IWTM.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа обучающегося.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов.

Язык обучения по дисциплине «русский »

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Целью реализации программы является совершенствование и (или) получениеновой компетенции, необходимой для профессиональной деятельности, с учетом спецификации стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности».

1.2. Дисциплина входит в состав части, формируемой участниками образовательных отношений, образовательной программы высшего образования (далее – ОП ВО).

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП ВО.

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Профессиональные компетенции	ПК-9 Корпоративная защита от внутренних угроз информационной безопасности	ПК-9.З.1 знает принципы проектирования системы корпоративной защиты от внутренних угроз ПК-9.З.2 знает основные функции системы DLP IWTM ПК-9.З.3 знает технологии анализа трафика при работе политиками информационной безопасности в системе корпоративной защиты информации ПК-9.У.1 умеет разрабатывать политики детектирования и блокировки утечек с использованием DLP-систем ПК-9.У.2 умеет работать в DLP-системе с событиями, запросами, объектами защиты, политиками, сводками, виджетами, персонами ПК-9.В.1 владеет навыками установки и конфигурирования систем DLP IWTM ПК-9.В.2 владеет навыками создания фильтров для анализа перехваченного трафика и выявленных инцидентов

2. Место дисциплины в структуре ОП

Дисциплина может базироваться на знаниях, ранее приобретенных обучающимисяпри изучении следующих дисциплин:

– Основы информационной безопасности.

Знания, полученные при изучении материала данной дисциплины, имеют самостоятельное значение.

3. Объем и трудоемкость дисциплины

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 2.

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№4
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	3/ 108	3/ 108
Из них часов практической подготовки	34	34
Аудиторные занятия, всего час.	51	51
в том числе:		
лекции (Л), (час)	17	17
практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	34	34
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)	27	27
Самостоятельная работа, всего (час)	30	30
***Вид промежуточной аттестации*:** зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Экз.	Экз.

Примечание: **кандидатский экзамен

Экзамен может проводиться в форме демонстрационного экзамена.

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий. Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

Таблица 3 – Разделы, темы дисциплины, их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 3					
Раздел 1. Стандарты Ворлдскиллс и спецификация стандартов Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасонсти». Разделы спецификации	1				2
Раздел 2. Требования охраны труда и техники безопасности	1				2
Раздел 3. Современные технологии в профессиональной сфере. Основы защиты информации от внутренних угроз информационной безопасности	2		2		4
Раздел 4. Основы цифровой гигиены	2		4		5
Раздел 5. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз.	2		6		3
Раздел 6. Технологии агентского мониторинга	3		6		4
Раздел 7. Разработка политик безопасности, анализ выявленных инцидентов	3		8		5
Раздел 8. Обследование (аудит) организации с целью защиты от угроз информационной безопасности	3		8		5
Итого в семестре:	17		34		30

Итого	17	0	34	0	30

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

4.2. Содержание разделов и тем лекционных занятий.

Содержание разделов и тем лекционных занятий приведено в таблице 4.

Таблица 4 – Содержание разделов и тем лекционного цикла

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	**Раздел 1. Стандарты Ворлдскиллс и спецификация стандартов Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности». Разделы спецификации** Тема 1.1 Спецификация стандарта компетенции «Корпоративная защита от внутренних угроз информационной безопасности» (конкурсное задание, техническое описание, инфраструктурный лист, схема и оборудование рабочих мест, требования к технике безопасности, критерии оценивания, кодекс этики, основные термины)
2	**Раздел 2. Требования охраны труда и техники безопасности** Тема 2.1 Культура безопасного труда. Тема 2.2 Основы безопасного труда и эффективная организация рабочего места в соответствии со стандартами Ворлдскиллс и спецификацией стандартов Ворлдскиллс по компетенции.
3	**Раздел 3. Современные технологии в профессиональной сфере. Основы защиты информации от внутренних угроз информационной безопасности.** Тема 3.1 Основы защиты корпоративной информации Тема 3.2 Цели, задачи, системы, методы и средства защиты Тема 3.3 Правовые основы. Ключевые алгоритмы и системы. Основные понятия. Безопасность информационных систем. Угрозы информационной безопасности. Источники угроз. Уязвимости. Риски. Атаки. Тема 3.4 Защита информации от внутренних угроз информационной безопасности. Выявление утечек с использованием технологии Data Leakage Prevention (DLP). Теория и практика применения DLP-систем.
4	**Раздел 4. Основы цифровой гигиены** Тема 4.1 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. Коммуникационные и технологические интернет угрозы. Тема 4.2 Правила безопасного поведения в сети Интернет. Размещение и использование персональных и личных данных. Безопасные пароли. Настройки приватности в социальных сетях. Резервное копирование. Тема 4.3 Программы защиты от вредоносного программного

	кода. Программы родительского контроля. Средства шифрования данных. Средства блокирования нежелательного контента
5	**Раздел 5. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз.** Тема 5.1 Установка DLP IWTM в виртуальном окружении. Режимы port mirroring и proxy. Тема 5.2 Конфигурирование DLP IWTM Тема 5.3 Исправление типовых неисправностей.
6	**Раздел 6. Технологии агентского мониторинга** Тема 6.1 Назначение агентского мониторинга. Установка и настройка агентского мониторинга. Интерфейс консоли DLP IWDM. Работа в консоли управления агентом Тема 6.2 Политики агентского мониторинга, особенности их настройки. Создание и проверка политик. Создание политик защиты на агентах;; Фильтрация событий; Настройка совместных событий агентского и сетевого мониторинга; Работа с носителями и устройствами; Работа с файлами; Контроль приложений; Исключение из событий перехвата.
7	**Раздел 7. Разработка политик безопасности, анализ выявленных инцидентов** Тема 7.1 Разработка и тестирование политик в системе DLP IWTM. Работа с разделом технологии системы корпоративной защиты: категории и термины, текстовые объекты; Работа с событиями, запросы, объекты перехвата, идентификация контактов в событии; Работа со сводками, виджетами, сводками; Работа с персонами; Работа с объектами защиты; Провести имитацию процесса утечки конфиденциальной информации в системе; Создать непротиворечивые политики, соответствующие нормативной базе и законодательству; Задокументировать созданные политики используя в соответствии с требованиями современных стандартов в области защиты информации. Работа с категориями и терминами; Использование регулярных выражений; Использование морфологического поиска; • Работа с графическими объектами; Работа с выгрузками и баз данных; Работа с печатями и бланками; Работа с файловыми типами; Тема 7.2 Мониторинг трафика. Проверка применения политик 4-х видов: трафик, персоны, буфер обмена, движение файлов. Работа с краулером.
8	**Раздел 8. Обследование (аудит) организации с целью защиты от угроз информационной безопасности** Тема 8.1 Понятие аудита информационной безопасности. Теория и практика обследования организации с целью защиты от угроз информационной безопасности Тема 8.2 Законодательство в области защиты конфиденциальной информации. Виды информации ограниченного доступа. Персональные данные. Коммерческая тайна.

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Учебным планом не предусмотрено					
Всего					

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 3				
1	Настройка контроллера домена	2	2	3
2	Настройки приватности в социальных сетях	4	4	4
3	Установка компонентов DLP системы	3	3	5
4	Конфигурирование компонентов DLP системы	3	3	5
5	Настройка сервера агентского мониторинга	3	3	6
6	Установка агента мониторинга на машине нарушителя	3	3	6
7	Разработка и применение политик	4	4	7
8	Анализ выявленных инцидентов	4	4	7
9	Создание сертификатов	4	4	8
10	Защита системы с помощью сертификатов	4	4	8
	Всего	34	34	

4.5. Курсовое проектирование/ выполнение курсовой работы

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 3, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	10	10
Подготовка к текущему контролю успеваемости (ТКУ)	10	10
Подготовка к промежуточной аттестации (ПА)	10	10

Всего:	30	30

5. Перечень учебно-методического обеспечения
для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны вп.п. 7-11.

6. Перечень печатных и электронных учебных изданий

Перечень печатных и электронных учебных изданий приведен в таблице 8.

Таблица 8– Перечень печатных и электронных учебных изданий

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
http://lib.aanet.ru/jirbis2/components/ com_irbis/pdf_view/?462678	Защита от внутренних угроз информационной безопасности с использованием современных DLP-технологий : [Электронный ресурс] : учебное пособие / А. В. Сергеев [и др.] ; ред. А. М. Тюрликов ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Электрон. текстовые дан. - Санкт-Петербург : Изд-во ГУАП, 2021. - 202 с.	
http://lib.aanet.ru/jirbis2/components /com_irbis/pdf_view/?448792	Организация безопасного доступа к информационным ресурсам : [Электронный ресурс] : учебное пособие / Н. Н. Мошак, Т. М. Татарникова ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Электрон. текстовые дан. - СПб. : Изд-во ГУАП, 2014. - 121 с.	
http://lib.aanet.ru/jirbis2/components/ com_irbis/pdf_view/?548371	Основы защиты информации. Защита персонального компьютера от умышленных угроз : [Электронный ресурс] :	

	учебное пособие / А. В. Воронов, Ю. В. Трифонова ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Электрон. текстовые дан. - СПб. : Изд-во ГУАП, 2015. - 99 с.	
http://lib.aanet.ru/jirbis2/components/ com_irbis/pdf_view/?455079	Безопасность информационных систем : [Электронный ресурс] : учебное пособие / Н. Н. Мошак ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Электрон. текстовые дан. - Санкт-Петербург : Изд-во ГУАП, 2019. - 169 с.	
https://e.lanbook.com/book/182491	Леонтьев А. С. Защита информации: учебное пособие / МИРЭА - Российский технологический университет, 2021. – 79 с.	
https://znanium.com/catalog/document?id=388766	Сычев Ю.Н. Защита информации и информационная безопасность / М.: НИЦ ИНФРА-М, 2021. – 201 с.	
http://lib.aanet.ru/jirbis2/components/ com_irbis/pdf_view/?980256	Безопасность информационных систем : [Электронный ресурс] : учебно-методическое пособие / Н. Н. Мошак ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Электрон. текстовые дан. - Санкт-Петербург : Изд-во ГУАП, 2020. - 73 с.	
http://lib.aanet.ru/jirbis2/components/ com_irbis/pdf_view/?958924	Безопасность операционных систем : [Электронный ресурс] : методические указания к выполнению лабораторных работ / С.-Петерб. гос. ун-т аэрокосм. приборостроения ; сост. В. А. Мыльников. - Электрон. текстовые	

	дан. - Санкт-Петербург : Изд-во ГУАП, 2020. - 53 с.	
http://lib.aanet.ru/jirbis2/components/ com_irbis/pdf_view/?763764	Защита информации в автоматизированных системах : [Электронный ресурс] : учебно-методическое пособие / В. С. Коломойцев ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Электрон. текстовые дан. - Санкт-Петербург : Изд-во ГУАП, 2021. - 27 с.	
https://kb.infowatch.com/ pages/viewpage.action? pageId=32079878	Техническая документация по решению InfoWatch Traffic Monitor 4.1 [электронный ресурс]	
https://worldskills.ru/nashi-proektyi/demonstraczionnyij-ekzamen/documents/	Положение об организации и проведении демонстрационного экзамена по стандартам WorldSkills Союза «Молодые профессионалы», электронная публикация	
https://worldskills.ru/nashi-proektyi/demonstraczionnyij-ekzamen/documents/	Положение об организации и проведении демонстрационного экзамена по стандартам WorldSkills Союза «Молодые профессионалы», электронная публикация	

7. Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

URL адрес	Наименование
https://worldskills.ru	Основной портал Союза «Молодые профессионалы (Ворлдскиллс Россия)
https://kb.infowatch.com	База знаний по продуктам и решениям InfoWatch

8. Перечень информационных технологий

8.1. Перечень программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине.

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
1	Adobe Reader
2	Браузер Google Chrome или Yandex
3	Гипервизор Oracle VirtualBox версии не ниже 5.1.14 или VMWare Workstation не ниже 12
4	InfoWatch Traffic Monitor
5	InfoWatch Device Monitor
6	Виртуальная машина с ОС RedHat
7	Виртуальная машина с ОС Windows

8.2. Перечень информационно-справочных систем,используемых при осуществлении образовательного процесса по дисциплине

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Мультимедийная лекционная аудитория	
2	Компьютерный класс (не менее 10 компьютеров)	
3	Программное DLP для борьбы с внутренними утечками информации и обеспечения корпоративной безопасности	
4	Виртуальная машина (сервер DLP)	
5	Виртуальная машина (контроллер домена)	
6	Виртуальная машина (сервер)	
7	Виртуальная машина (клиент)	

10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средствдля проведения промежуточной аттестации обучающихся по дисциплине приведен в таблице 13.

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Экзамен	Задачи Комплекты оценочной документации (К.О.Д.)

10.2. В качестве критериев оценки уровня сформированности (освоения) компетенций обучающимися применяется 5-балльная шкала оценки сформированности компетенций, которая приведена в таблице 14. В течение семестра может использоваться 100-балльная шкала модульно-рейтинговой системы Университета, правила использования которой, установлены соответствующим локальным нормативным актом ГУАП.

Таблица 14 –Критерии оценки уровня сформированности компетенций

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«отлично» «зачтено»	– обучающийся 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»	– обучающийся 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»	– обучающийся 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»	– обучающийся 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.

В качестве критериев оценки уровня сформированности (освоения) компетенций (части компетенции) обучающимися, сдающими экзамен в форме демонстрационного экзамена, применяются критерии установленные в комплекте оценочной документации (К.О.Д.).

Рекомендованная методика перевода полученных баллов по результатам выполнения задания демонстрационного экзамена в аттестационную оценку по итогам прохождения экзамена, представлена в РДО ГУАП. СМК 3.78.

10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
1	Провести конфигурацию сетевой инфраструктуры: настроить хост машину, сетевое окружение, виртуальные машины, и т. п. Студенту необходимо: • Установить и настроить систему корпоративной защиты от внутренних угроз; • Запустить систему, проверить функциональность и соответствие настроек целевой сетевой инфраструктуре • Провести имитацию процесса утечки конфиденциальной информации в системе; • Устранить проблемы при появлении; • Продемонстрировать работоспособность системы • Подготовить отчёт по оценке работоспособности системы;	ПК-9.З.1 ПК-9.У.2 ПК-9.В.1 ПК-9.В.2
2	Применить политики информационной безопасности в системе, автоматически выполнить поиск инцидентов информационной безопасности. Студенту необходимо: • Продемонстрировать знание механизмов работы агентского мониторинга; • Разработать и применить политики агентского мониторинга для работы с носителями и устройствами; • Разработать и применить политики агентского мониторинга для работы с файлами; • Работа с исключениями из перехвата;	ПК-9.З.3 ПК-9.У.2 ПК-9.В.2
3	Разработать политики информационной безопасности, используя инструментарий автоматизированной системы IWTM 6 и успешно их применить для выявления и/или блокирования инцидентов безопасности. Студенту необходимо: • Разработать новые и/или модифицировать существующие политики безопасности, перекрывающие каналы передачи данных и возможные инциденты согласно экзаменационному заданию; • Занести политики информационной безопасности в DLP-систему; • Разработать или/и модифицировать объекты защиты, категории, технологии защиты в DLP-системе и т. п.; • Применить политики для контроля трафика, выявления и/или блокирования инцидентов безопасности. Максимизировать число выявленных инцидентов безопасности; • Продемонстрировать владение технологиями и умение работать с интерфейсом управления системы	ПК-9.З.2 ПК-9.З.3 ПК-9.У.1 ПК-9.В.2

	корпоративной защиты информации IWTM. Участнику необходимо применить политики информационной безопасности в системе IWTM, автоматически выполнить поиск инцидентов информационной безопасности. Политики можно модифицировать, с целью выявления максимального числа инцидентов и утечек. Необходимо использовать весь набор технологий поиска и выявления уязвимостей, доступный в системе корпоративной защиты. Итоговый вариант политик должен быть зафиксирован в отчете. В число инцидентов могут входить, например: • передача персональных данных сотрудников и контрагентов по электронной почте; • передача базы клиентов организации в архиве с использованием файловых протоколов; • нецензурная лексика сотрудников в переписке с контрагентами; • передача информации, составляющей коммерческую тайну и др. • Применить механизмы создания фильтров для анализа перехваченного трафика и выявленных инцидентов; • Подготовить детализированные отчёты о нарушениях; • Провести классификацию уровня угрозы инцидента;	

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 16.

Таблица 16 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код индикатора
	Учебным планом не предусмотрено	

Перечень тем для курсового проектирования/выполнения курсовой работы представлены в таблице 17.

Таблица 17 – Перечень тем для курсового проектирования/выполнения курсовой работы

№ п/п	Примерный перечень тем для курсового проектирования/выполнения курсовой работы
	Учебным планом не предусмотрено

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	Не предусмотрено	

Перечень тем контрольных работ по дисциплине обучающихся заочной формы обучения, представлены в таблице 19.

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

Примерный перечень заданий для обучающихся, сдающих экзамен в форме демонстрационного экзамена, указаны в комплекте оценочной документации (К.О.Д.):
https://esat.worldskills.ru/competencies/dac59f20-134b-4aa4-94e5-518c488ccc9e/categories/4ba5e47c-fc5a-4ffa-9c2a-f29d8c6efb7c
https://cdn.dp.worldskills.ru/esatk-prod/public_files/8b6009f0-a646-4810-aaaa-3eb5558bfc36-3ae682d91e17f450dbb59db4304d455d.pdf

10.4. Методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру проведения текущего контроля успеваемости и промежуточной аттестации обучающихся ГУАП.

11. Методические указания для обучающихся по освоению дисциплины

11.1. Методические указания для обучающихся по освоению лекционного материала

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимися лекционного материала:

– получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;

– получение опыта творческой работы совместно с преподавателем;

– развитие профессионально-деловых качеств, любви к предмету и самостоятельного творческого мышления.

– появление необходимого интереса, необходимого для самостоятельной работы;

– получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;

– научиться методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);

– получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

Раздел 1. Стандарты Ворлдскиллс и спецификация стандартов Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности». Разделы спецификации

Тема 1.1 Спецификация стандарта компетенции «Корпоративная защита от внутренних угроз информационной безопасности» (конкурсное задание, техническое описание, инфраструктурный лист, схема и оборудование рабочих мест, требования к технике безопасности, критерии оценивания, кодекс этики, основные термины)

Раздел 2. Требования охраны труда и техники безопасности

Тема 2.1 Культура безопасного труда.

Тема 2.2 Основы безопасного труда и эффективная организация рабочего места в соответствии со стандартами Ворлдскиллс и спецификацией стандартов Ворлдскиллс по компетенции.

Раздел 3. Современные технологии в профессиональной сфере. Основы защиты информации от внутренних угроз информационной безопасности.

Тема 3.1 Основы защиты корпоративной информации

Тема 3.2 Цели, задачи, системы, методы и средства защиты

Тема 3.3 Правовые основы.

Ключевые алгоритмы и системы. Основные понятия. Безопасность информационных систем. Угрозы информационной безопасности. Источники угроз. Уязвимости. Риски. Атаки.

Тема 3.4 Защита информации от внутренних угроз информационной безопасности. Выявление утечек с использованием технологии Data Leakage Prevention (DLP). Теория и практика применения DLP-систем.

Раздел 4. Основы цифровой гигиены

Тема 4.1 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. Коммуникационные и технологические интернет угрозы.

Тема 4.2 Правила безопасного поведения в сети Интернет. Размещение и использование персональных и личных данных. Безопасные пароли. Настройки приватности в социальных сетях. Резервное копирование.

Тема 4.3 Программы защиты от вредоносного программного кода. Программы родительского контроля. Средства шифрования данных. Средства блокирования нежелательного контента

Раздел 5. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз.

Тема 5.1 Установка DLP IWTM в виртуальном окружении. Режимы port mirroring и proxy.

Тема 5.2 Конфигурирование DLP IWTM

Тема 5.3 Исправление типовых неисправностей.

Раздел 6. Технологии агентского мониторинга

Тема 6.1 Назначение агентского мониторинга. Установка и настройка агентского мониторинга. Интерфейс консоли DLP IWDM. Работа в консоли управления агентом

Тема 6.2 Политики агентского мониторинга, особенности их настройки. Создание и проверка политик. Создание политик защиты на агентах; Фильтрация событий; Настройка совместных событий агентского и сетевого мониторинга; Работа с носителями и устройствами; Работа с файлами; Контроль приложений; Исключение из событий перехвата.

Раздел 7. Разработка политик безопасности, анализ выявленных инцидентов

Тема 7.1 Разработка и тестирование политик в системе DLP IWTM. Работа с разделом технологии системы корпоративной защиты: категории и термины, текстовые объекты; Работа с событиями, запросы, объекты перехвата, идентификация контактов в событии; Работа со сводками, виджетами, сводками; Работа с персонами; Работа с объектами защиты; Провести имитацию процесса утечки конфиденциальной информации в системе; Создать непротиворечивые политики, соответствующие нормативной базе и законодательству; Задокументировать созданные политики используя в соответствии с требованиями современных стандартов в области защиты информации. Работа с категориями и терминами; Использование регулярных выражений; Использование

морфологического поиска; • Работа с графическими объектами; Работа с выгрузками и баз данных; Работа с печатями и бланками; Работа с файловыми типами;

Тема 7.2 Мониторинг трафика. Проверка применения политик 4-х видов: трафик, персоны, буфер обмена, движение файлов. Работа с краулером.

Раздел 8. Обследование (аудит) организации с целью защиты от угроз информационной безопасности

Тема 8.1 Понятие аудита информационной безопасности. Теория и практика обследования организации с целью защиты от угроз информационной безопасности

Тема 8.2 Законодательство в области защиты конфиденциальной информации. Виды информации ограниченного доступа. Персональные данные. Коммерческая тайна.

11.2. Методические указания для обучающихся по выполнению лабораторных работ

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач обучающегося:

– приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;

– закрепление, развитие и детализация теоретических знаний, полученных на лекциях;

– получение новой информации по изучаемой дисциплине;

– приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ

Вариант задания по каждой лабораторной работе обучающийся получает в соответствии с номером в списке группы. Перед проведением лабораторной работы обучающемуся следует внимательно ознакомиться с методическими указаниями по ее выполнению. В соответствии с заданием обучающийся должен подготовить необходимые данные, получить от преподавателя допуск к выполнению лабораторной работы, выполнить указанную последовательность действий, получить требуемые результаты, защитить лабораторную работу у преподавателя.

Структура и форма отчета о лабораторной работе

Отчет не требуется

11.3. Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

В процессе выполнения самостоятельной работы, у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет им развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихсяявляются:

– учебно-методический материал по дисциплине.

11.4. Методические указания для обучающихся по прохождению текущего контроля успеваемости.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины. Форма проведения текущего контроля – защита лабораторных работ. Результаты текущего контроля учитываются при проведении промежуточной аттестации в соответствии с требованиями СТО ГУАП. СМК 3.76 «Положение о текущем контроле успеваемости и промежуточной аттестации студентов и аспирантов ГУАП, обучающихся по образовательным программам высшего образования».

11.5. Методические указания для обучающихся по прохождению промежуточной аттестации.

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя: экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Экзамен в форме демонстрационного экзамена проводится в соответствии с комплектом оценочной документации, содержащем примерные оценочные материалы, размещенным/ представленным по адресу:

https://esat.worldskills.ru/competencies/dac59f20-134b-4aa4-94e5-518c488ccc9e/categories/4ba5e47c-fc5a-4ffa-9c2a-f29d8c6efb7c

https://cdn.dp.worldskills.ru/esatk-prod/public_files/8b6009f0-a646-4810-aaaa-3eb5558bfc36-3ae682d91e17f450dbb59db4304d455d.pdf

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой