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

Кафедра № 33

УТВЕРЖДАЮ
Руководитель образовательной программы

доц.,к.т.н.,доц.
(должность, уч. степень, звание)

Н.В. Марковская
(инициалы, фамилия)

(подпись)
«27» июня 2024 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
Год приема	2024

Санкт-Петербург– 2024

Лист согласования рабочей программы дисциплины

Программу составил (а)

доц.,к.т.н..	27.06.2024	В.С. Коломойцев
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Программа одобрена на заседании кафедры № 33

«27» июня 2024 г, протокол № 11

Заведующий кафедрой № 33

д.т.н.,доц.	27.06.2024	С.В. Беззатеев
(уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Заместитель директора института №2 по методической работе

доц.,к.т.н.,доц.	27.06.2024	Н.В. Марковская
(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-7 «Корпоративная защита от внутренних угроз информационной безопасности»

Содержание дисциплины охватывает круг вопросов, связанных с выбором решений по 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) получение новой 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-7 Корпоративная защита от внутренних угроз информационной безопасности	ПК-7.З.1 знает принципы проектирования системы корпоративной защиты от внутренних угроз ПК-7.З.2 знает основные функции системы DLP IWTM ПК-7.З.3 знает технологии анализа трафика при работе политиками информационной безопасности в системе корпоративной защиты информации ПК-7.У.1 умеет разрабатывать политики детектирования и блокировки утечек с использованием DLP-систем ПК-7.У.2 умеет работать в DLP-системе с событиями, запросами, объектами защиты, политиками, сводками, виджетами, персонами ПК-7.В.1 владеет навыками установки и конфигурирования систем DLP IWTM ПК-7.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 обучающимися при изучении следующих дисциплин:

- Информационное право;
- Информатика;

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и могут использоваться при изучении других дисциплин:

- Комплексная защита объектов информатизации;
- Основы управления информационной безопасностью;

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.

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий.

Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

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

5. Содержание дисциплины

5.1. 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 4					
Модуль 1. Стандарты Ворлдскиллс и спецификация стандартов Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасонсти». Разделы спецификации	1				1
Модуль 2. Требования охраны труда и техники безопасности	1				1
Модуль 3. Современные технологии в профессиональной сфере. Основы защиты информации от внутренних угроз информационной безопасности	2		2		4
Модуль 4. Основы цифровой гигиены	2		4		4
Модуль 5. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз.	2		6		5
Модуль 6. Технологии агентского мониторинга	3		6		5
Модуль 7. Разработка политик безопасности, анализ выявленных инцидентов	3		8		5
Модуль 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.

5.2. 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	**Модуль 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	**Модуль 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	**Модуль 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	**Модуль 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	**Модуль 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	**Модуль 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	**Модуль 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	**Модуль 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.

5.3. 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					

5.4. 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 4				
1	Настройки приватности в социальных сетях	6		3,4
2	Установка и конфигурирование компонентов DLP системы	9		5,6,7,8
3	Технологии агентского мониторинга	9		5,6,7,8

4	Разработка и применение политик, анализ выявленных инцидентов	10		5,6,7,8
	Всего	34		

5.5. Курсовое проектирование/ выполнение курсовой работы
Учебным планом не предусмотрено

5.6. 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 4, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	20	20
Подготовка к текущему контролю успеваемости (ТКУ)	10	10
Всего:	30	30

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

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

7. 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)
https://kb.infowatch.com/pages/viewpage.action?pageId=32079878	Техническая документация по решению InfoWatch 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.	
https://worldskills.ru/nashi-proektyi/demonstraczionnyij-	Положение об организации и проведении демонстрационного	

ekzamen/documents/	экзамена по стандартам WorldSkills Союза «Молодые профессионалы», электронная публикация	
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.	

8. 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

9. Перечень информационных технологий

9.1. 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	ПО Microsoft Office 2018

9.2. 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

10. 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	14-28
2	Компьютерный класс (не менее 14 компьютеров)	52-48

11. Оценочные средства для проведения промежуточной аттестации

11.1. 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	Список вопросов к экзамену; Экзаменационные билеты; Задачи; Тесты.

11.2. 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

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
	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.

11.3. 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	Установка и конфигурирование компонентов DLP-системы. 1. Провести конфигурацию сетевой инфраструктуры: настроить хост машину, сетевое окружение, виртуальные машины, доменных пользователей и т. п.; 2. Настройка DLP-сервера: • Необходимо вычислить IP-адрес сервера через локальную консоль виртуальной машины. • Необходимо синхронизировать каталог пользователей и компьютеров LDAP с домена с помощью ранее созданного пользователя. • Записать IP-адреса, токен, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные) настроенной системы в отчет с заголовком IWTM. 3. Проверка работоспособности сервера и клиента агентского мониторинга: • Запустить и войти в консоль управления сервером агентского мониторинга. • Синхронизировать каталог пользователей и компьютеров с Active Directory. • Проверить соединение агента мониторинга с сервером агентского мониторинга. • Записать IP-адреса, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные) системы в отчет с заголовком IWDM. 4. Установка и настройка подсистемы сканирования сетевых ресурсов (Crawler): • Необходимо установить и настроить подсистему сканирования сетевых ресурсов на сервер с установленным сервером агентского мониторинга. • Необходимо создать общий каталог в корне диска и установить права доступа на запись и чтение для	ПК-7.З.1 ПК-7.У.1 ПК-7.У.2

	всех пользователей. • Необходимо настроить подсистему сканирования сетевых ресурсов на автоматическое ежедневное сканирование только ранее созданного каталога. • Зафиксировать выполнение задания скриншотом настройки в web-консоли. 5. Проверка работоспособности системы: • Необходимо создать проверочную политику на правило передачи, копирования, хранения и буфера обмена (все 4 варианта срабатывания событий) для данных, содержащих слово «Экзамен», установить низкий уровень угрозы для всех событий, добавить тег «Экзамен». • Проверить срабатывание всеми четырьмя возможными способами (передачи, копирования, хранения и буфера обмена, хотя бы 1 событие на каждый тип) с помощью виртуальной машины нарушителя с установленным агентом. • Сделать одну выборку, в которой будет отображено только по одному событию каждого типа (суммарно 4 события: передачи, копирования, хранения и буфера обмена). • Зафиксировать выполнение скриншотом выполненной выборки или конструктора выборки.	
2	Технологии агентского мониторинга. Задания выполняются только с помощью компонентов DLP-системы. Результат выполнения каждого задания должен быть зафиксирован в виде скриншота, с указанием уникального имени, соответствующего номеру выполненного задания (подпункта задания). 1. Необходимо создать новую политику, применить ее к группе компьютеров по умолчанию. Последующие правила по заданиям должны быть добавлены в эту политику. 2. Необходимо установить дополнительную консоль управления сервером агентского мониторинга на машину нарушителя для удаленного доступа к серверу агентского мониторинга. Проверить работоспособность, зафиксировать выполнение скриншотом запущенной консоли с указанием адреса. 3. Для удаленного управления необходимо создать дополнительного локального офицера безопасности для доступа к серверу агентского мониторинга с полными правами на управление и просмотр разделов. Проверить работоспособность с удаленной консоли, установленной ранее. 4. Необходимо запретить пользоваться графическим редактором ОС Windows (MS Paint). Проверить работоспособность. 5. Необходимо запретить создание снимков экрана в табличных процессорах для предотвращения	ПК-7.З.2 ПК-7.В.1

	утечки секретных расчетов и баз данных. Проверить работоспособность. 6. Необходимо поставить на контроль буфер обмена в текстовых процессорах. Проверить работоспособность и зафиксировать выполнение занесением пары событий в веб-консоль DLP-сервера на любые политики. 7. Необходимо запретить печать на сетевых принтерах. Зафиксировать создание политики скриншотом. 8. Необходимо поставить на контроль печать документов на принтерах. Проверить работоспособность. 9. Необходимо установить контроль за компьютером потенциального нарушителя в случае использования браузера путем создания снимков экрана каждые 15 секунд или при переходе на другую страницу. Проверить работоспособность и зафиксировать выполнение, что снимки экрана из задания появляются в веб-консоли DLP-сервера. Подтвердить выполнение задания скриншотами. 10. Заблокируйте доступ к CD/DVD на клиентском компьютере (виртуальной машине). Проверить работоспособность. 11. На машине нарушителя необходимо запретить использование буфера обмена при подключении к удаленным машинам по протоколу RDP. Проверить работоспособность.	
3	Разработка и применение политик, анализ выявленных инцидентов. Создание в DLP-системе политики безопасности согласно приведенным заданиям. Политики должны автоматически блокировать трафик и/или предупреждать о нарушении в соответствии с заданием. Результат выполнения каждого задания должен быть зафиксирован в виде скриншота, с указанием уникального имени, соответствующего номеру выполненного задания (подпункта задания). 1. Необходимо создать локальную группу пользователей «Сотрудники под наблюдением». Добавить в нее трех любых пользователей. 2. Для работы системы необходимо настроить периметр компании: почтовый домен; список веб ресурсов «Доверенные домены»; группу персон являющихся пользователями домена. Исключить из перехвата почту генерального директора. 3. Необходимо 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. Области видимости: все. 4. Создание политик безопасности:	ПК-7.З.3 ПК-7.В.2

	4.1. Необходимо создать политику на правило передачи текстовых данных за пределы компании (на адреса вне домена), содержащие специальные слова. Необходимо учесть, что в словах могут содержаться комбинации латиницы и кириллицы, а также стоять пробел между словами. Ложных срабатываний быть не должно (например, на часть слова. Вердикт: разрешить; уровень нарушения: средний; тег: мобильники. Проверить работоспособность. 4.2. Необходимо вести наблюдение за передачей как пустых, так и заполненных шаблонов документа за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах 50%. Для пустого документа: вердикт: разрешить; уровень нарушения: нет; тег: договор. Для заполненного документа: вердикт: разрешить. уровень нарушения: низкий; тег: договор. Проверить работоспособность. 4.3. Необходимо вести наблюдение за анкетами компании, запрещая любую внешнюю передачу документов, содержащих заполненные бланках, при этом пустые бланки контролировать не нужно. Вердикт: запретить; уровень нарушения: средний; тег: бланк. Проверить работоспособность. 4.4. Необходимо вести наблюдение за документами компании с официальной печатью. При этом совет директоров и генеральный директор могут отправлять эти документы без ограничений. Вердикт: разрешить; уровень нарушения: низкий; тег: печать. Проверить работоспособность. 4.5. Необходимо контролировать специальные коды доступа (10 штук) внутри компании, но запрещать передачу за пределы. Передача кодов внутри компании: вердикт: разрешить; уровень нарушения: низкий; тег: коды. Передача кодов за пределы компании: вердикт: запретить; уровень нарушения: средний; тег: бланк. Проверить работоспособность. 4.6. Необходимо настроить мониторинг выгрузок из базы данных (БД) для контроля движения данных из базы данных только при отправке из отдела информатизации. Вердикт: разрешить; уровень нарушения: средний; тег: база. Проверить работоспособность. 4.7. Необходимо отслеживать специальные термины, указывающие на требующую	

	внимания информацию внутри компании. Вердикт: разрешить; уровень нарушения: низкий; тег: важно. Проверить работоспособность. 4.8. Необходимо запрещать всем, кроме отдела кадров передавать информацию, содержащую данные паспортов (в том числе и сканы/фото), а также СНИЛС и ИНН. Вердикт: запретить; уровень нарушения: высокий; тег: пдн. Проверить работоспособность. 5. Анализ инцидентов, обычные сводки. Создайте новую вкладку сводки в разделе «Сводка» и создайте в ней 4 виджета: Динамика активности по событиям за последнюю неделю; Статистика по политикам за последние 7 дней. По типу событий: необработанные нарушения за три дня; По топ-нарушителям за текущий месяц. 6. Анализ инцидентов, специальные выборки. Необходимо создать новую вкладку в разделе «Сводка» и добавить в нее виджет, отображающий события с уровнем угрозы от низкого до высокого на правила копирования (внешние носители, печать) за последние 7 дней.	

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

11.4. 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.

12. Методические указания для обучающихся по освоению дисциплины
13. Методические указания для обучающихся по освоению дисциплины

13.1. 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:

Модуль 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)

Модуль 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.

Модуль 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.

Модуль 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

Модуль 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.

Модуль 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.

Модуль 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.

Модуль 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.

13.2. 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, оформить и защитить отчет по лабораторной работе.

Структура и форма отчета о лабораторной работе

Отчет не требуется

13.3. 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 обучающихся являются: учебно-методический материал по дисциплине.

13.4. 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 отчетов по лабораторным работам. 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».

13.5. 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».

Итоговая аттестация проводится в форме демонстрационного экзамена. Оценка уровня освоения компетенций осуществляется на основе таких составляющих как: знание, умение, владение навыками, которые слушатель демонстрирует на демонстрационном экзамене. Для итоговой аттестации используется Комплект оценочной документации (КОД) по компетенции «Корпоративная защита от внутренних угроз информационной безопасности».

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