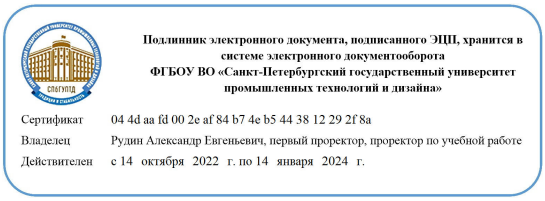
Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный университет промышленных технологий и дизайна»
(СПбГУПТД)



УТВЕРЖДАЮ
Первый проректор, проректор по УР
_____А.Е. Рудин
«31»____10____ 2023 года

Рабочая программа дисциплины

Б1.О.11 Управление информационной безопасностью

Учебный план: 2024-2025 10.04.01 ИИТА ПСЗИнП ОО №2-1-159.plx

Кафедра: 20 Интеллектуальных систем и защиты информации

Направление подготовки: (специальность) 10.04.01 Информационная безопасность

Профиль подготовки: (специализация) Проектирование систем защиты информации на предприятии

Уровень образования: магистратура

Форма обучения: очная

План учебного процесса

Семестр (курс для ЗАО)		Контактная работа обучающихся			Сам. работа	Контроль, час.	Трудоёмкость, ЗЕТ	Форма промежуточной аттестации
		Лекции	Практ. занятия	Лаб. занятия				
3	УП	17	34	34	20,75	2,25	3	Курсовая работа, Зачет
	РПД	17	34	34	20,75	2,25	3	
Итого	УП	17	34	34	20,75	2,25	3	
	РПД	17	34	34	20,75	2,25	3	

Санкт-Петербург
2023

Рабочая программа дисциплины составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 10.04.01 Информационная безопасность, утверждённым приказом Минобрнауки России от 26.11.2020 г. № 1455

Составитель (и):

кандидат технических наук, Доцент	_____	Штеренберг С.И.
От кафедры составителя: Заведующий кафедрой интеллектуальных систем и защиты информации	_____	Макаров Авинир Геннадьевич
От выпускающей кафедры: Заведующий кафедрой	_____	Макаров Авинир Геннадьевич

Методический отдел:

_____

1 ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1 Цель дисциплины: формирование компетенций обучающегося в области разработки, реализации, эксплуатации, анализа, сопровождения и совершенствования систем управления информационной безопасностью.

1.2 Задачи дисциплины:

- сформировать у обучающихся понимания системного подхода к управлению информационной безопасностью;
- сформировать навыки формализации процессов управления информационной безопасностью;
- раскрыть процесс управления информационными рисками, как базового процесса управления информационной безопасностью.

1.3 Требования к предварительной подготовке обучающегося:

Предварительная подготовка предполагает создание основы для формирования компетенций, указанных в п. 2, при изучении дисциплин:

Защищенные информационные системы

Математическое моделирование технических объектов и систем управления

Технологии обеспечения информационной безопасности

2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОПК-3: Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности
Знать: основы отечественных и зарубежных стандартов в области сертификации и аттестации объектов информатизации, в области управления информационной безопасностью
Уметь: проводить технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности; разрабатывать проекты нормативных документов, регламентирующих работу по защите информации
Владеть: навыками разработки политик безопасности различных уровней и работы с нормативными правовыми актами в области информационной безопасности, учитывая типологию и специализацию предприятия-заказчика

3 РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Наименование и содержание разделов, тем и учебных занятий	Семестр (курс для ЗАО)	Контактная работа			СР (часы)	Инновац. формы занятий	Форма текущего контроля
		Лек. (часы)	Пр. (часы)	Лаб. (часы)			
Раздел 1. Основы управления информационной безопасностью	3						Л
Тема 1. Системный подход к управлению информационной безопасностью Практическое занятие:Стандартизация в сфере управления информационной безопасностью. Лабораторная работа:Формирование перечня конфиденциальных документов в организации		1	2	3	1,75		
Тема 2. Элементы разработки систем управления информационной безопасностью в информационных системах Практическое занятие:Средства управления информационной безопасностью Лабораторная работа:Контроль целостности программной среды, проверка разрешительной системы доступа		1	3	3	2	ИЛ	

Тема 3. Элементы разработки систем управления информационной безопасностью на значимых объектах критической информационной инфраструктуры Практическое занятие:Построение функциональной модели процессов обеспечения информационной безопасности Лабораторная работа:Программные средства поддержки процессов управления		2	3	2	2		
Тема 4. Практическое занятие:Классификация государственных информационных систем по требованиям защиты информации Лабораторная работа:Изучение DLP-систем			2	2	2		
Тема 5. Организационные меры обеспечения безопасности компьютерных информационных систем. Практическое занятие:Разработка модели угроз безопасности информации в государственной информационной системе Лабораторная работа:Моделирование с помощью различных нотаций. Модель угроз		2	2	4	2		
Тема 6. Определение мер защиты информации в государственной информационной системе Практическое занятие:Управление инцидентами ИБ Лабораторная работа: Основные программно-технические меры. Парольная аутентификация. Сервер аутентификации Kerberos		1	2	4	2		
Раздел 2. Стандартизация в области управления информационной безопасностью							Л
Тема 7. Разработка плана и концепции СУИБ Практическое занятие:Логистика процессов управления информационной безопасностью на основе стандартов. Лабораторная работа:Стандарты информационной безопасности серии ГОСТ Р ИСО/МЭК 27000		2	4	2	1	ГД	
Тема 8. Политика информационной безопасности и технология её разработки Практическое занятие: Процедуры, регламенты и инструкции по информационной безопасности; Лабораторная работа:Стандарты информационной безопасности ГОСТ Р ИСО/МЭК 15408		2	4	2	1		

Тема 9. Правовые меры обеспечения информационной безопасности. Практическое занятие:Законодательно-правовая база обеспечения информационной безопасности на предприятии. Формы правовой защиты информации на предприятии. Лабораторная работа:Нормативные акты предприятия по информационной безопасности		2	2	2	1		
Раздел 3. Анализ и управление рисками при организации систим информационной безопасности							
Тема 10. Методики анализа информационных рисков Практическое занятие:Изучение информационных сервисов для получения данных об организациях или гражданах для снижения репутационных и экономических рисков при ведении бизнес- процессов Лабораторная работа: Методика оценки рисков информационной безопасности компании Digital Security		2	4	4	2		Л
Тема 11. Практическое занятие:Математические модели и методы управления информационными рисками Лабораторная работа:Инвентаризация активов, анализ защищенности и управление инцидентами в компьютерной системе с использованием «Сканер- ВС», ITSM- инфра-менеджер, R-Vision			4	4	2	ИЛ	
Тема 12. Управление рисками информационной безопасности Практическое занятие:Современные методы и средства анализа и управление рисками информационных систем организаций Лабораторная работа: Протоколирование и аудит, шифрование, контроль целостности		2	2	2	2		
Итого в семестре (на курсе для ЗАО)		17	34	34	20,75		
Консультации и промежуточная аттестация (Курсовая работа, Зачет)		2,25					
Всего контактная работа и СР по дисциплине		87,25			20,75		

4 КУРСОВОЕ ПРОЕКТИРОВАНИЕ

4.1 Цели и задачи курсовой работы (проекта): Цель написания курсовой работы - глубоко и подробно изучить современные процессы управления информационной безопасности на предприятии.

Задачи :

- выбор объекта исследования,
- определение методики исследования
- проведение литературного обзора по теме,
- формулировка проблематики,
- предложение решения проблемы либо всесторонний анализ уже существующих с указанием их сильных и слабых мест

4.2 Тематика курсовой работы (проекта): 1. Организация защиты персональных данных в медицинском учреждении.

2. Организация выполнения требований Роскомнадзора для образовательных учреждений.

3. Организация защиты персональных данных в образовательном учреждении.

4. Построение типовой модели угроз безопасности информации кредитной организации.

5. Обеспечение информационной безопасности банков при обработке биометрических данных.

6. Разработка системы управления кадровой безопасностью образовательной организации.

7. Методы управления резервированием данных на базе облачных хранилищ.

8. Автоматизация процессом управления инцидентами информационной безопасности на основе данных системных журналов.

9. Комплексное обеспечение информационной безопасности при реализации угрозы попытки доступа в удалённую систему.

10. Система обеспечения защиты информации в переговорной комнате.

11. Расследование компьютерных инцидентов на базе поведенческого анализа действий пользователей

12. Сравнительный анализ практических правил стандарта ГОСТ Р ИСО/МЭК 27002 и требова-ний нормативных документов по защите ГИС.

13.Методы и технологии защиты ГИС, содержащих биометрические данные больших объемов (свыше 100 000 чел).

14. Сравнительный анализ практических правил стандарта ГОСТ Р ИСО/МЭК 27002 и требований нормативных документов по защите КИИ.

15. Управление технической уязвимостью в информационной системе: суть, особенности примеры.

16. Управление приложениями (производительностью информационных приложений и т.д.). суть,особенности примеры.

17. Управление резервным копированием и хранение данных. Суть, особенности примеры.

18. Управление интернет-технологиями. Суть, особенности примеры.

19. Управление рисками информационной безопасности в банковской организации

20. Управление нарушением риса информационной безопасности при аутсорсинге

21. Управление информационной безопасностью в телекоммуникационных организациях

22. Управление процессами утечки информации

23. Управление непрерывностью бизнеса

24. Управление безопасностью сетей

25. Управление контролем обеспечения информационной безопасностью.

26. Управление документооборотом на основе web- технологий. Примеры

27. Протоколирование действий пользователей в СЭД. Их роль в управлении информационной безопасностью.

28. Характеристика системы управления электронными документами различных классов, их архитектуры, методов поиска и технологий использования.

29. Риск-ориентированный подход при управлении информационной безопасности. Достоинства и недостатки применения.

4.3 Требования к выполнению и представлению результатов курсовой работы (проекта):

Курсовая работа включает в себя оформленную пояснительную записку объемом 15-25 стр, в которой подробно изложены цели и задачи работы, объект исследования, а также ход выполнения работы и подробное описание полученного результата. Курсовая распечатывается односторонней печатью, сшивается в папку-скоросшиватель, имеет титульный лист установленного образца. Пояснительная записка оформляется согласно ГОСТ 7.32. Шрифт Times New Roman, высота строчных символов не меньше 12 кегля, межстрочный интервал 1.

 КР должна представлять собой логически целостный научно-технический документ, аргументированно раскрывающий вопрос исследования на

основании современного уровня развития объекта и предмета исследования.

 КР должна содержать исследовательский компонент и соотноситься с темой ВКР магистранта.

 Желательно, чтобы в КР использовались источники не старше чем пятилетней давности.

 Желательно наличие аннотации на английском языке.

Защита КР состоит в публичной презентации материала (целесообразно использование средств презентации) и ответе на вопросы аудитории.

Материалы работы и защиты носят открытый характер, доступный неопределённому кругу лиц.

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5.1 Описание показателей, критериев и системы оценивания результатов обучения

5.1.1 Показатели оценивания

Код компетенции	Показатели оценивания результатов обучения	Наименование оценочного средства
ОПК-3	Перечисляет области применения, функции и особенности использования стандартов и технической документации в области управления информационной безопасности. Реализует алгоритм разработки проекта нормативной документации при проектировании систем обеспечения информационной безопасности. Перечисляет и применяет принципы построения политик безопасности в зависимости от специфики деятельности предприятия. Выполняет основные расчеты для подготовки технико-экономического обоснования	вопросы для устного собеседования и практико - ориентированные задания

5.1.2 Система и критерии оценивания

Шкала оценивания	Критерии оценивания сформированности компетенций	
	Устное собеседование	Письменная работа
5 (отлично)	Студент может ответить на любые вопросы, связанные с работой, ее созданием, логикой построения повествования, технической частью	Тема КР полностью раскрыта на основе достаточной аналитической базы, достоверной и полной информационной базы, адекватности и обоснованности примененных методов исследования. Материал изложен грамотно и логично, разделы работы обоснованы и взаимосвязаны. Пояснительная записка оформлена в соответствии с требованиями ГОСТ 7.32-2017.
4 (хорошо)	студент отвечает на вопросы даны не в полном объеме, слабо использует категориальный аппарат, наблюдаются небольшие неточности в докладе	Тема КР полностью раскрыта на основе достаточной аналитической базы, достоверной и полной информационной базы. Результаты исследования в КР изложены грамотно, но выявлены нарушения системности изложения, повторы, неточности. Недостаточно обоснованы выводы и рекомендации, неочевиден выбор методов исследования. КР является завершенной работой, оригинальность текста составляет более 80%. Пояснительная записка целом оформлена в соответствии с требованиями ГОСТ 7.32-2017. Доклад логичный, полностью отражает результаты проведенного исследования.
3 (удовлетворительно)	Студент с трудом отвечает на вопросы по работе, путается в ее структуре и порядке изложения	Задание выполнено не полностью, имеется дисбаланс составных элементов КР. Информация преобразуется не корректно (нарушена размерность, сопоставимость, применение формул; расчеты выполнены частично, выводы отсутствуют). Отсутствует системность описания методики проведения исследования. КР является завершенной работой, авторский вклад составляет более 55%. Пояснительная записка оформлена с нарушениями требований ГОСТ 7.32-2017. В докладе не обоснованы положения, нарушена логическая последовательность и аргументация.

2 (неудовлетворительно)	Студент не может ответить на вопросы по содержанию КР, доклад низкого качества, нет владения материала	Содержание КР не соответствует заявленной тематике, имеются существенные ошибки в расчетах, примененных методах преобразования информации и баз данных. Заявленные цели работы не достигнуты, недостаточно обоснованы все структурные элементы работы и отсутствует связь между ними. КР является не завершенной работой, авторский вклад составляет менее 55%. Нарушен регламент, имеются ошибки в использовании профессиональных терминов,) обучающийся не ориентируется в тексте доклада.
Зачтено	студент дал полные, развернутые ответы на все основные теоретические вопросы, продемонстрировал знание терминологии, основных элементов, умение применять теоретические знания. Студент без затруднений ответил на все дополнительные вопросы.	не предусмотрена
Не зачтено	обучающийся не может изложить значительной части программного материала, допускает существенные ошибки, допускает неточности в формулировках и доказательствах, нарушения в последовательности изложения программного материала.	нет предусмотрена

5.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

5.2.1 Перечень контрольных вопросов

№ п/п	Формулировки вопросов
Семестр 3	
1	Цели и задачи управления информационной безопасностью
2	Структура и функции системы управления информационной безопасностью
3	Политика безопасности и ее роль в управлении информационной безопасностью
4	Этапы создания системы управления ИБ.
5	Категорирование активов компании.
6	Оценка защищенности информационной системы компании.
7	Оценка информационных рисков.
8	Методика оценки рисков информационной безопасности компании.
9	Управление рисками. Основные понятия.
10	Метод оценки рисков на основе модели угроз и уязвимостей.
11	Метод оценки рисков на основе модели информационных потоков.
12	Качественные методики управления рисками.
13	Количественные методики управления рисками.
14	Управление средствами защиты информации.
15	Правовые основы аудита информационной безопасности
16	Место и роль аудита в управлении информационной безопасности
17	Методология проведения аудита информационной безопасности
18	Менеджмент аудита информационной безопасности
19	Методы оценки эффективности информационной безопасности
20	Способы анализ результатов аудита информационной безопасности
21	Нормативно-технические документы аудита информационной безопасности
22	Виды контроля состояния информационной безопасности объектов
23	Методы анализа состояния информационной безопасности
24	Архитектура системы обеспечения информационной безопасности
25	Роль политики безопасности в задачах управления информационной безопасностью.

26	Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799, основные положения.
27	Международный стандарт ISO/IEC 27001:2005 «Системы управления информационной безопасности. Требования».
28	Сертификация систем управления информационной безопасностью на соответствие ISO 27001.

5.2.2 Типовые тестовые задания

не предусмотрены

5.2.3 Типовые практико-ориентированные задания (задачи, кейсы)

«Разработка модели угроз безопасности информации»

Цель: Построение различных моделей, отображающих архитектуру автоматизированной системы и ограничений доступа к информации. Проведение анализа мест и видов утечки информации. Оценка угроз, уязвимостей и степени защищенности информации.

Задание:

1) Выполнить оценку актуальности разрабатываемой информационной системы

2) Провести структурный системный анализ бизнес-процессов предметной области с точки зрения инженера безопасности информации. Построить диаграммы IDEF0 (AS-IS), DFD (ASIS), (при необходимости – IDEF3 (AS-IS).

3) Описать разработанные диаграммы

4) Выделить активы, подлежащие информационной защите

5) Построить модель угроз разрабатываемой информационной системы

6) Построить модель нарушителя

7) Сформировать реестр актуализированных угроз для каждого актива

8) Сформировать векторы уязвимостей. Оценить возможные риски

9) Оценить степень защищенности информации

"Формирование заданий по безопасности и SIEMэкосистемы"

Цель: На основании формулированных целей безопасности сформировать профили защиты и задания по безопасности информационной системы и СЗИ, реализующих требуемый уровень защищенности системы. Развернуть SIEM-экосистему

Задание:

1) На основании сформулированных целей безопасности сформировать профили защиты информационной (автоматизированной) системы и/или СЗИ.

2) В профилях защиты построить таблицы, которые взаимосвязывают Цели безопасности с угрозами и ПолИБ. Взаимосвязи обосновать и описать.

3) Сформулировать функциональные требования, требования доверия и требования к среде

4) Разработать задание по безопасности. Выделить правила безопасности, реализованные в технических политиках безопасности, которые предстоит реализовать в подсистеме анализа (корреляций) SIEM-системы.

5) Развернуть SIEM-экосистему, используя проект AirSIEM https://github.com/fisher85/AirSIEM

6) Исходный код ядра корреляции - https://github.com/fisher85/AirSIEM/tree/master/AirSIEM

5.3 Методические материалы, определяющие процедуры оценивания знаний, умений, владений (навыков и (или) практического опыта деятельности)

5.3.1 Условия допуска обучающегося к промежуточной аттестации и порядок ликвидации академической задолженности

Проведение промежуточной аттестации регламентировано локальным нормативным актом СПбГУПТД «Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся»

5.3.2 Форма проведения промежуточной аттестации по дисциплине

Устная	+	Письменная	+	Компьютерное тестирование		Иная	

5.3.3 Особенности проведения промежуточной аттестации по дисциплине

студент допускается к зачету при предъявлении принятых отчетов по всем лабораторным работам

зачет проводится в устной форме, студентам рандомно раздаются билет в которых есть теоретические вопросы и практико-ориентированное задание, время подготовки 30 мин, время ответа 5 мин

на защиту курсовой работы отводится не более 20 минут

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
6.1.1 Основная учебная литература				
Ревнивых, А. В.	Информационная безопасность в организациях	Москва: Ай Пи Ар Медиа	2021	https://www.iprbookshop.ru/108227.html

Зенков, А. В.	Основы информационной безопасности	Москва, Вологда: Инфра-Инженерия	2022	https://www.iprbookshop.ru/124242.html
6.1.2 Дополнительная учебная литература				
Милославская, Н. Г., Толстой, А. И.	Управление информационной безопасностью. Конспект лекций	Москва: Национальный исследовательский ядерный университет «МИФИ»	2020	https://www.iprbookshop.ru/125513.html
Газизов, А. Р., Петренкова, С. Б., Фатхи, Д. В.	Управление информационной безопасностью	Ростов-на-Дону: Донской государственный технический университет	2019	https://www.iprbookshop.ru/117771.html
Галатенко, В. А.	Основы информационной безопасности	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа	2020	http://www.iprbookshop.ru/97562.html

6.2 Перечень профессиональных баз данных и информационно-справочных систем

Официальный сайт ФСТЭК России (http://www.fstec.ru)
Справочно-правовая система КонсультантПлюс
Банк данных угроз безопасности информации ФСТЭК России: https://bdu.fstec.ru/
Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00
ГОСТ Эксперт - единая база ГОСТов Российской Федерации
Справочно-правовая система Гарант
ЭБС IPR SMART
Электронная библиотека диссертаций Российской государственной библиотеки

6.3 Перечень лицензионного и свободно распространяемого программного обеспечения

MicrosoftOfficeProfessional

Microsoft Windows

1С-Битрикс: Внутренний портал учебного заведения

Notepad++

6.4 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Аудитория	Оснащение
Компьютерный класс	Специализированная мебель; компьютерная техника; наборы демонстрационного оборудования, служащие для представления учебной информации (стационарное мультимедийное оборудование) - мультимедийная проекционная система (мультимедиа проектор и экран). Рабочие станции, программно-аппаратные комплексы ЗИ; локальная вычислительная сеть с выходом в Интернет, система «Шепот». Многофункциональный поисковый прибор ST 031M "Пиранья". СЗИ НСД «Аккорд-АМДЗ». Универсальный досмотровый набор.