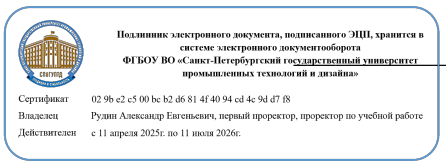
Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный университет промышленных технологий и дизайна»
(СПбГУПТД)

УТВЕРЖДАЮ

Первый проректор, проректор по УР



_____А.Е. Рудин

Рабочая программа дисциплины

Б1.В.09 Информационная безопасность бизнеса

Учебный план: 2025-2026 38.03.01 ИЭСТ Фин тех и цифр ин в биз ОО №1-1-185.plx

Кафедра: 55 Экономики и финансов

Направление подготовки: (специальность) 38.03.01 Экономика

Профиль подготовки: (специализация) Финансовые технологии и цифровые инновации в бизнесе

Уровень образования: бакалавриат

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				
5	УП	32	32	79,75	0,25	4	Зачет
	РПД	32	32	79,75	0,25	4	
Итого	УП	32	32	79,75	0,25	4	
	РПД	32	32	79,75	0,25	4	

Санкт-Петербург
2025

Рабочая программа дисциплины составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 38.03.01 Экономика, утверждённым приказом Минобрнауки России от 12.08.2020 г. № 954

Составитель (и):

-, ст. преп.	_____	Неуструева Анастасия Сергеевна
к.э.н., доцент	_____	Лейзин Иля Борисович
От кафедры составителя: Заведующий кафедрой экономики и финансов	_____	Климова Наталья Сергеевна
От выпускающей кафедры: Заведующий кафедрой	_____	Климова Наталья Сергеевна

Методический отдел:

_____

1 ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1 Цель дисциплины: формирование у обучающихся системы теоретических знаний и практических навыков в области обеспечения информационной безопасности предпринимательской деятельности, защиты конфиденциальной информации, коммерческой тайны и персональных данных, а также развития способности применять современные методы и средства защиты информации при реализации проектов в сфере финансовых технологий и цифровых инноваций.

1.2 Задачи дисциплины:

1. Изучить основные понятия, принципы и нормативно-правовую базу информационной безопасности бизнеса.
2. Освоить классификацию угроз и методов защиты информации в современных цифровых системах.
3. Изучить организационные и технические меры обеспечения информационной безопасности на предприятии.
4. Сформировать навыки анализа рисков информационной безопасности и выбора адекватных мер защиты.
5. Ознакомиться с современными стандартами и лучшими практиками в области информационной безопасности.
6. Развить способность применять полученные знания для защиты информационных активов при реализации проектов в сфере финансовых технологий.

1.3 Требования к предварительной подготовке обучающегося:

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

Учебная практика (ознакомительная практика)

Учебная практика (аналитическая практика)

Правовое обеспечение цифрового бизнеса

Информационные технологии

Документооборот и делопроизводство

Экономика предприятия

Бухгалтерский учет

Бизнес-процессы на предприятии

2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-1: Способен выполнять подготовительные работы по реализации комплексных проектов в области инновационных финансовых технологий
Знать: принципы и методы выполнения подготовительных работ по реализации комплексных проектов в области инновационных финансовых технологий, включая нормативно-правовую базу, актуальные тенденции и современные подходы в сфере информационной безопасности бизнеса.
Уметь: применять теоретические знания для планирования и организации подготовительных этапов реализации проектов, а также выполнять аналитическую работу, необходимую для оценки рисков, формирования требований и разработки предварительных технических заданий в контексте информационной безопасности бизнес-процессов.
Владеть: навыками использования специализированных информационных систем и инструментов для выполнения подготовительных работ, а также навыками коммуникации и координации с командой проекта и заинтересованными сторонами в целях обеспечения соблюдения стандартов информационной безопасности при реализации инновационных финансовых технологий.

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)			
Раздел 1. Теоретические основы информационной безопасности бизнеса	5					О,Пр
Тема 1. Введение в информационную безопасность бизнеса. Понятие и сущность информационной безопасности. Место информационной безопасности в системе экономической безопасности предприятия. Основные составляющие информационной безопасности: конфиденциальность, целостность, доступность. Информация как актив и объект защиты. Практическое занятие: Анализ структуры информационных активов коммерческой организации		2	2	6		
Тема 2. Нормативно-правовое регулирование информационной безопасности. Законодательная база РФ в области информационной безопасности. Ответственность за нарушения в сфере информационной безопасности. Практическое занятие: Анализ нормативно-правовых актов в сфере информационной безопасности		2	2	6		
Тема 3. Угрозы и уязвимости информационной безопасности. Понятие угрозы информационной безопасности. Классификация угроз. Основные виды угроз. Понятие уязвимости. Классификация уязвимостей. Методы выявления уязвимостей. Практическое занятие: Идентификация и классификация угроз информационной безопасности для конкретного бизнеса.		2	2	4		
Тема 4. Риски информационной безопасности и управление ими. Понятие риска информационной безопасности. Составляющие риска. Методологии оценки рисков. Процесс управления рисками. Практическое занятие: Оценка рисков информационной безопасности для предприятия.		2	2	4		
Тема 5. Концепция и политика информационной безопасности. Политика информационной безопасности. Структура и содержание политики информационной безопасности. Регламенты и процедуры обеспечения информационной безопасности. Практическое занятие: Разработка фрагмента политики информационной безопасности организации.		2	2	4		
Раздел 2. Организационно-правовые и технические аспекты защиты информации						Пр,О

Тема 6. Защита коммерческой тайны и конфиденциальной информации. Понятие коммерческой тайны. Перечень сведений, составляющих коммерческую тайну. Режим коммерческой тайны: порядок введения, меры охраны. Работа с персоналом в условиях режима коммерческой тайны. Ответственность за разглашение конфиденциальной информации. Практическое занятие: Разработка перечня сведений, составляющих коммерческую тайну для конкретного предприятия.		2	2	5		
Тема 7. Защита персональных данных. Понятие персональных данных. Классификация персональных данных. Требования законодательства к обработке и защите персональных данных. Меры защиты персональных данных в информационных системах. Ответственность за нарушения в сфере обработки персональных данных. Практическое занятие: Анализ соответствия обработки персональных данных требованиям законодательства.		2	2	5		
Тема 8. Технические средства защиты информации. Классификация средств защиты информации. Средства идентификации и аутентификации. Средства разграничения доступа. Средства регистрации и учета. Средства криптографической защиты информации. Межсетевые экраны. Средства антивирусной защиты. Системы обнаружения вторжений. Практическое занятие: Обзор и сравнительный анализ программных средств защиты информации.		2	2	5		
Тема 9. Криптографические методы защиты информации. Основные понятия криптографии: шифрование, дешифрование, ключ. Симметричные и асимметричные криптосистемы. Электронная подпись: понятие, применение, нормативное регулирование. Хеширование. Инфраструктура открытых ключей. Практическое занятие: Применение средств криптографической защиты и электронной подписи.		2	2	5		
Тема 10. Безопасность сетей и облачных технологий. Особенности обеспечения безопасности в корпоративных сетях. Защита от несанкционированного доступа. VPN: назначение и виды. Безопасность беспроводных сетей. Облачные технологии и риски информационной безопасности. Модели обеспечения безопасности в облаке. Практическое занятие: Анализ рисков информационной безопасности при использовании облачных сервисов.		2	2	4		

Тема 11. Организационное обеспечение информационной безопасности. Организационная структура системы информационной безопасности. Разграничение доступа и управление правами пользователей. Кадровая безопасность. Документационное обеспечение информационной безопасности. Практическое занятие: Разработка регламентов и процедур обеспечения информационной безопасности.		2	2	4		
Раздел 3. Управление информационной безопасностью и инцидентами						О,Пр
Тема 12. Стандарты и лучшие практики в области информационной безопасности. Международные стандарты. Стандарты Банка России для финансовых организаций. Практическое занятие: Сравнительный анализ стандартов информационной безопасности.		2	2	5		
Тема 13. Управление инцидентами информационной безопасности. Понятие инцидента информационной безопасности. Классификация инцидентов. Процесс управления инцидентами: обнаружение, регистрация, анализ, локализация, устранение, восстановление, анализ причин. Расследование инцидентов. Взаимодействие с правоохранительными органами. Практическое занятие: Реагирование на инцидент информационной безопасности.		3	3	8		
Тема 14. Аудит и построение комплексной системы информационной безопасности. Понятие и цели аудита информационной безопасности. Виды аудита: внутренний и внешний. Методы проведения аудита. Оценка соответствия требованиям стандартов и законодательства. Этапы построения системы информационной безопасности. Определение политик и процедур. Выбор и внедрение средств защиты. Обучение персонала. Мониторинг и совершенствование системы. Оценка эффективности. Практическое занятие: Проведение фрагмента аудита информационной безопасности. Разработка концепции системы информационной безопасности для предприятия.		5	5	14,75		
Итого в семестре (на курсе для ЗАО)		32	32	79,75		
Консультации и промежуточная аттестация (Зачет)		0,25				
Всего контактная работа и СР по дисциплине		64,25		79,75		

4 КУРСОВОЕ ПРОЕКТИРОВАНИЕ

Курсовое проектирование учебным планом не предусмотрено

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
ПК-1	Называет основные составляющие информационной безопасности и место информационной безопасности в системе экономической безопасности предприятия; указывает виды ответственности за нарушения в сфере информационной безопасности, коммерческой тайны и персональных данных; раскрывает классификацию угроз, уязвимостей, инцидентов и средств защиты информации. Составляет перечень информационных активов и анализирует их значимость для бизнес-процессов; определяет и классифицирует угрозы, уязвимости и инциденты информационной безопасности; оценивает риски информационной безопасности, включая риски использования облачных сервисов; проводит анализ нормативно-правовых актов и сравнительный анализ средств защиты информации, криптосистем и стандартов. Применяет методики оценки рисков для обоснования приоритетов защиты на подготовительном этапе; разрабатывает фрагменты политики информационной безопасности, регламенты, процедуры и перечень сведений, составляющих коммерческую тайну; использует средства криптографической защиты информации и электронной подписи; обосновывает выбор технических и организационных средств защиты информации с учётом специфики бизнес-процессов и требований стандартов; проводит фрагмент аудита и разрабатывает концепцию комплексной системы информационной безопасности.	

5.1.2 Система и критерии оценивания

Шкала оценивания	Критерии оценивания сформированности компетенций	
	Устное собеседование	Письменная работа
Зачтено	Обучающийся демонстрирует понимание принципов и методов выполнения подготовительных работ в области информационной безопасности. Раскрывает содержание нормативно-правовой базы, называет актуальные тенденции и современные подходы. Приводит примеры применения теоретических знаний для планирования проектов. Обосновывает выбор методов оценки рисков и формирования требований. Ответы логичны, аргументированы, основаны на материале дисциплины.	
Не зачтено	Обучающийся не понимает принципов выполнения подготовительных работ, не может назвать нормативно-правовую базу и современные подходы в сфере информационной безопасности. Не способен применить теоретические знания для планирования проектов и оценки рисков. Ответы отсутствуют либо содержат грубые ошибки, демонстрирующие отсутствие сформированных компетенций.	

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 5	
1	Раскройте понятие и сущность информационной безопасности бизнеса. Назовите основные составляющие информационной безопасности.

2	Перечислите основные законодательные акты РФ, регулирующие сферу информационной безопасности. Какова ответственность за нарушения в этой сфере?
3	Дайте классификацию угроз информационной безопасности по различным признакам.
4	Что понимается под уязвимостью информационной системы? Назовите основные виды уязвимостей и методы их выявления.
5	Раскройте понятие риска информационной безопасности. Назовите составляющие риска и этапы процесса управления рисками.
6	Что такое политика информационной безопасности? Какова ее структура и содержание?
7	Раскройте понятие коммерческой тайны. Каков порядок введения режима коммерческой тайны на предприятии?
8	Какие требования предъявляются к обработке и защите персональных данных в соответствии с законодательством РФ?
9	Перечислите основные технические средства защиты информации. Дайте их краткую характеристику.
10	В чем сущность криптографических методов защиты информации?
11	Что такое электронная подпись? Каково ее назначение и нормативное регулирование?
12	Какие особенности обеспечения безопасности в корпоративных сетях?
13	Назовите основные международные стандарты в области информационной безопасности. Каковы их цели и структура?
14	Что понимается под инцидентом информационной безопасности? Опишите процесс управления инцидентами.
15	Каковы этапы построения комплексной системы информационной безопасности на предприятии?

5.2.2 Типовые тестовые задания

1. Что относится к основным составляющим информационной безопасности?
А) Конфиденциальность, целостность, доступность
Б) Скорость, надежность, производительность
В) Стоимость, эффективность, масштабируемость
Г) Актуальность, полнота, достоверность

2. Какой нормативный акт регулирует отношения в области персональных данных?
А) ФЗ «О коммерческой тайне»
Б) ФЗ «О персональных данных»
В) ФЗ «Об информации, информационных технологиях и о защите информации»
Г) Гражданский кодекс РФ

3. К какому виду угроз относится перехват данных в сети?
А) Естественная угроза
Б) Случайная угроза
В) Умышленная угроза
Г) Внутренняя угроза

4. Что такое уязвимость информационной системы?
А) Недостаток или слабое место в системе, которое может быть использовано для реализации угрозы
Б) Вероятность наступления неблагоприятного события
В) Потенциальная возможность нарушения безопасности
Г) Мера защиты информации

5. Что относится к организационным мерам защиты информации?
А) Межсетевые экраны
Б) Политика информационной безопасности
В) Антивирусные программы
Г) Криптографические средства

5.2.3 Типовые практико-ориентированные задания (задачи, кейсы)

Задача 1. Расчет уровня риска

Условие: В компании произошла утечка данных. Известно, что частота подобных инцидентов в отрасли составляет 2 случая в год. Стоимость актива (база данных клиентов) оценивается в 5 млн рублей. При реализации угрозы компания теряет 70% стоимости актива. Эффективность существующих средств защиты составляет 60%.

Задание: Рассчитайте уровень риска (ожидаемые годовые потери) по формуле: SLE = AV × EF, ALE = SLE × ARO, где ALE с учетом эффективности защиты = ALE × (1 - эффективность защиты).

Задача 2. Расчет показателей эффективности средств защиты

Условие: Компания рассматривает внедрение системы защиты информации стоимостью 500 000 рублей.

Годовые затраты на обслуживание составят 50 000 рублей. По прогнозам, внедрение системы позволит снизить ожидаемые годовые потери от инцидентов с 800 000 рублей до 200 000 рублей. Срок эксплуатации системы – 3 года.

Задание: Рассчитайте:

Годовую экономию от внедрения системы

Простой срок окупаемости

Коэффициент возврата инвестиций (ROI) за 3 года

Кейс 1. Разработка политики информационной безопасности для малого предприятия

Ситуация: Малое предприятие (20 сотрудников) занимается разработкой мобильных приложений. В компании отсутствует системный подход к информационной безопасности. Используются ноутбуки сотрудников, файловое хранилище в локальной сети, облачные сервисы для хранения кода и корпоративная почта на бесплатном домене. Недавно произошла утечка фрагментов кода одного из проектов.

Задание:

Определите основные активы, требующие защиты.

Идентифицируйте основные угрозы и уязвимости.

Предложите перечень первоочередных организационных и технических мер защиты.

Составьте структуру политики информационной безопасности для данного предприятия и раскройте содержание основных разделов.

Кейс 2. Реагирование на инцидент информационной безопасности

Ситуация: В компании, занимающейся онлайн-торговлей, произошла утечка базы данных клиентов, содержащей ФИО, адреса, номера телефонов и данные банковских карт (в зашифрованном виде). Информация появилась в открытом доступе в сети Интернет. Руководство узнало об этом из публикации в СМИ.

Задание:

Опишите порядок действий службы информационной безопасности на каждом этапе управления инцидентом.

Какие неотложные меры необходимо предпринять?

С какими государственными органами необходимо взаимодействовать?

Какие меры следует принять для недопущения подобных инцидентов в будущем?

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»

Допуск к промежуточной аттестации осуществляется при условии выполнения обучающимся всех видов учебной работы, предусмотренных рабочей программой дисциплины, включая посещение занятий, выполнение и защиту практических заданий, а также успешное прохождение текущего контроля успеваемости. Обучающиеся, не выполнившие программу дисциплины без уважительной причины или получившие оценку «не зачтено», имеют академическую задолженность, для ликвидации которой устанавливаются индивидуальные сроки повторной сдачи зачета или повторного изучения дисциплины после устранения выявленных недостатков.

5.3.2 Форма проведения промежуточной аттестации по дисциплине

Устная	+	Письменная		Компьютерное тестирование		Иная	

5.3.3 Особенности проведения промежуточной аттестации по дисциплине

Промежуточная аттестация по дисциплине проводится в форме устного зачета по билетам, каждый из которых включает два теоретических вопроса и одно практико-ориентированное задание. На подготовку отводится 30 минут. Ответ оценивается по системе «зачтено» или «не зачтено»: зачтено выставляется при понимании материала, аргументированных ответах и правильном решении практического задания, не зачтено — при грубых ошибках или отсутствии ответа.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
6.1.1 Основная учебная литература				
Бондаренко, И. С.	Информационная безопасность	Москва: Издательский Дом МИСиС	2023	https://www.iprbookshop.ru/137525.html
Суворова, Г. М.	Информационная безопасность	Саратов: Вузовское образование	2024	https://www.iprbookshop.ru/142805.html
6.1.2 Дополнительная учебная литература				

Дронов, В. Ю., Дронова, Г. А.	Информационная безопасность банковской деятельности	Новосибирск: Новосибирский государственный технический университет	2024	https://www.iprbookshop.ru/155872.html
Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование	2024	https://www.iprbookshop.ru/145912.html

6.2 Перечень профессиональных баз данных и информационно-справочных систем

1. http://publish.sutd.ru/ Электронная библиотека учебных изданий СПбГУПТД содержит полнотекстовые версии монографий, учебников, учебных пособий, методических указаний, сборниках трудов преподавателей и сотрудников университета. В среде реализован многокритериальный поиск данных. В базу данных включены издания, начиная с 2007 года.

2. http://www.iprbookshop.ru/ Электронная библиотека по всем отраслям знаний, в полном объеме соответствующая требованиям законодательства РФ в сфере образования (лицензионные документы, справка соответствия ЭБС ФГОС). В базе ЭБС IPRbooks содержится более 15 000 изданий – это учебники, монографии, журналы по различным направлениям подготовки специалистов высшей школы, другая учебная литература.

3. https://urait.ru/ - Urait это современная обучающая платформа, предлагающая университетам и колледжам доступ к цифровому учебному контенту и различным сервисам, способствующим эффективному образовательному процессу. Платформа предоставляет широкий спектр учебных материалов, включая электронные книги, онлайн-курсы и дополнительные ресурсы, что делает процесс обучения более доступным и разнообразным.

4. http://government.ru/department/456/events/ - на этом портале размещаются актуальные данные и информация о деятельности Федеральной службы государственной статистики. Росстат предоставляет статистические данные по различным отраслям экономики, демографии, социальной структуре и культурной жизни страны. Информация представлена в виде отчетов, статистических таблиц и публикаций, что позволяет обеспечить прозрачность и доступность данных для государственных органов, бизнеса и граждан.

5. https://www.nalog.gov.ru/rn78/ - официальный сайт ФНС России представляет собой платформу, где размещена полная информация об услугах, предлагаемых налоговыми органами, включая возможность получения электронных услуг, сдачи отчетности, а также актуальные данные о налогах и налоговом законодательстве.

6.3 Перечень лицензионного и свободно распространяемого программного обеспечения

Microsoft Windows

MicrosoftOfficeProfessional

1С:Предприятие 8. Комплект для обучения в высших и средних учебных заведениях. Продажа по договору с учебными заведениями об использовании в учебном процессе по заявкам

1С-Битрикс: Внутренний портал учебного заведения

Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ» версии 3.3

СПС КонсультантПлюс

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

Аудитория	Оснащение
Компьютерный класс	Мультимедийное оборудование, компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду
Лекционная аудитория	Мультимедийное оборудование, специализированная мебель, доска
Учебная аудитория	Специализированная мебель, доска