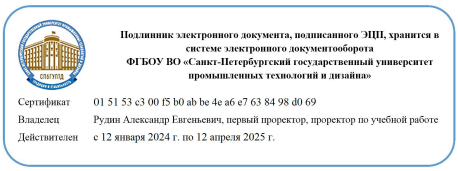
Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный университет промышленных технологий и дизайна»
(СПбГУПТД)

УТВЕРЖДАЮ
Первый проректор, проректор по УР

_____ А.Е. Рудин



Рабочая программа дисциплины

Б1.О.34 Основы информационной безопасности

Учебный план: 38.05.01 Экономическая безопасность бизнеса от 21.01.2025.plx

Кафедра: 20 Интеллектуальных систем и защиты информации

Направление подготовки: (специальность) 38.05.01 Экономическая безопасность

Профиль подготовки: (специализация) Экономическая безопасность бизнеса

Уровень образования: специалитет

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				
8	УП	34	34	75,75	0,25	4	Зачет
	РПД	34	34	75,75	0,25	4	
Итого	УП	34	34	75,75	0,25	4	
	РПД	34	34	75,75	0,25	4	

Санкт-Петербург
2025

Рабочая программа дисциплины составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 38.05.01 Экономическая безопасность, утверждённым приказом Минобрнауки России от 14.04.2021 г. № 293

Составитель (и):

кандидат технических наук, Доцент	Чалова Екатерина Игорьевна
От кафедры составителя: Заведующий кафедрой интеллектуальных систем и защиты информации	Макаров Авинир Геннадьевич
От выпускающей кафедры: Заведующий кафедрой	Фрадина Татьяна Ильинична

Методический отдел:

1 ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1 Цель дисциплины: Сформировать компетенции обучающегося в области обеспечения информационной безопасности государства, подходов к анализу угроз его информационной инфраструктуры; решения задач защиты информации в информационных системах.

1.2 Задачи дисциплины:

- познакомить с основными положениями государственной политики в области обеспечения информационной безопасности Российской Федерации, основными понятиями в области защиты информации и методологическими принципами создания систем защиты информации;
- познакомить с видами защищаемой информации, угрозами информационной безопасности, сущностями и разновидностями информационного оружия, методами и средствами ведения информационных войн;
- научить использовать методы и средства обеспечения информационной безопасности.

1.3 Требования к предварительной подготовке обучающегося:

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

Информационные технологии

Экономика организации (предприятия)

Информационные технологии в профессиональной деятельности

2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОПК-6: Способен использовать современные информационные технологии и программные средства при решении профессиональных задач
Знать: методы и средства обеспечения информационной безопасности, методы нарушения конфиденциальности, целостности и доступности информации; содержание основных понятий по правовому обеспечению информационной безопасности; основы безопасности операционных систем; основы безопасности вычислительных сетей; основные технические средства и методы защиты информации; основные программно-аппаратные средства обеспечения информационной безопасности.
Уметь: правильно проводить анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, применять на практике основные общеметодологические принципы теории информационной безопасности; находить необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации; применять действующую законодательную базу в области информационной безопасности; разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно- распорядительных документов.
Владеть: навыками выполнения работ, связанных с комплексным обеспечением информационной безопасности конкретных автоматизированных систем на основе разработанных программ и методик, в том числе с обеспечением требований нормативных документов для обеспечения экономической безопасности хозяйствующего субъекта.
ОПК-7: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности
Знать: сущность и природу явлений и процессов цифровой трансформации; основы экономической безопасности в цифровой экономике; цифровые инструменты, используемые с целью повышения экономической безопасности.
Уметь: работать в автоматизированных системах информационного обеспечения профессиональной деятельности, получать, интерпретировать и документировать результаты исследований
Владеть: навыками выявления внутренних и внешних угроз информационной безопасности при работе с современными информационными технологиями, используемыми для обеспечение экономической безопасности бизнеса.

3 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование и содержание разделов, тем и учебных занятий	Семестр (курс для ЗАО)	Контактная работа		СР (часы)	Форма текущего контроля
		Лек. (часы)	Пр. (часы)		
Раздел 1. Теоретические основы информационной безопасности	8				О
Тема 1. Введение. Цели и задачи информационной безопасности. Основные понятия и термины. Классификация мер обеспечения информационной безопасности. Основы государственной политики РФ в области информационной безопасности		4		4	

Тема 2. Угрозы информационной безопасности.Уязвимость, риск, инцидент, ущерб информационной безопасности. Риск угрозы и механизм реализации угрозы. Понятия злоумышленника, постороннего и случайного лица. Практическое занятие " Работа с банками данных угроз и уязвимостей"		4	2	8	
Тема 3. Правовое обеспечение информационной безопасности. Доктрина информационной безопасности. Принципы работы регулирующих органов власти. Практическое задание" Обзор законодательных основ обеспечения информационной безопасности в РФ"		4	2	7,75	
Раздел 2. Методология защиты информации					
Тема 4. Методы защиты информации по видам защищаемой информации. Модель угроз информационной безопасности Практическое занятие 1: "Формирование перечня конфиденциальных документов в организации" Практическое занятие 2: «Основные виды несанкционированного доступа.Управление учетными записями пользователей и настройка политик пользователя в СЗИ от НСД Dallas Lock» Практическое занятие 3: «Настройка средств антивиусной и сетевой защиты Kaspersky Endpoint Security"		4	6	9	О
Тема 5. Средства защиты и мониторинга корпоративных компьютерных сетей Практическое занятие 1: "Технологии проактивной защиты, Threat Intelligence и Threat Hunting" Практическое занятие 2: "Настройка межсетевого экрана и СОВ в СЗИ от НСД Secret Net Studio"		2	6	9	
Раздел 3. Защита информации в информационных системах					
Тема 6. Программные и программно-аппаратные средства защиты информации Практическое занятие 1: Настройка политик безопасности и механизмов управления доступом в ОС СН Astra Linux Практическое занятие 2: Сокрытие сообщения методом младших битов (LSB-метод) Практическое занятие 3: Криптоанализ шифров перестановки и простой замены		4	6	12	О
Тема 7. Организационно-распорядительная защита информации.Разработка модели комплексной системы защиты информации Практическое занятие 1: "Контроль целостности программной среды, проверка разрешительной системы доступа" Практическое занятие 2: "Установка, настройка и изучение функций DLP-системы"		4	6	10	
Раздел 4. Менеджмент и аудит информационной безопасности					
Тема 8. Организационные формы обеспечения безопасности. Политика информационной безопасности и технология её разработки Практическое занятие: Процедуры, регламенты и инструкции по информационной безопасности;		4	2	8	О

Тема 9. Управление рисками информационной безопасности. Методы и принципы. Информационные ресурсы в качестве существенных (неотъемлемых) активов организации. Практическое занятие "Изучение информационных сервисов для получения данных об организациях или гражданах для снижения репутационных и экономических рисков при ведении бизнес- процессов"		4	4	8	
Итого в семестре (на курсе для ЗАО)		34	34	75,75	
Консультации и промежуточная аттестация (Зачет)		0,25			
Всего контактная работа и СР по дисциплине		68,25		75,75	

4 КУРСОВОЕ ПРОЕКТИРОВАНИЕ

Курсовое проектирование учебным планом не предусмотрено

5 БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА

Использование балльно-рейтинговой системы не предусмотрено.

6. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ, КРИТЕРИЕВ, СИСТЕМЫ И СРЕДСТВ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

6.1 Показатели оценивания

Код компетенции	Показатели оценивания результатов обучения
ОПК-6	Излагает цели и задачи информационной безопасности; основные понятия и термины. Дает классификацию мер обеспечения информационной безопасности, основные технические средства и методы защиты информации. Перечисляет и знает особенности использования современных методов и средств обеспечения информационной безопасности. Умеет устанавливать и применять основные современные СЗИ для операционных систем и вычислительных сетей; Анализирует предпосылки и причины утраты информационных ресурсов ограниченного доступа. Выполняет основные этапы решения задач информационной безопасности. Применяет на практике законодательные основы обеспечения информационной безопасности в РФ, , в том числе с помощью систем правовой информации; применяет действующую законодательную базу в области информационной безопасности.
ОПК-7	Характеризует методы защиты информации по видам защищаемой информации, основные виды несанкционированного доступа. Раскрывает сущность и природу процессов цифровой трансформации; принципы и основы экономической безопасности в цифровой экономике. Проводит мониторинг экономической безопасности, рабоет в автоматизированных системах информационного обеспечения профессиональной деятельности Проводит разработку практических процедур оценки рисков, связывающих безопасность и требования бизнеса

6.2 Система и критерии оценивания

Шкала оценивания	Критерии оценивания сформированности компетенций	
	Устное собеседование	Письменная работа
Зачтено	Ответ стандартный, в целом качественный, основан на всех обязательных источниках информации. Присутствуют небольшие пробелы в знаниях или несущественные ошибки.	не предусмотрена
Не зачтено	Неспособность ответить на вопрос без помощи экзаменатора. Незнание значительной части принципиально важных элементов дисциплины. Многочисленные грубые ошибки. Попытка списывания, использования неразрешенных технических устройств или пользования подсказкой другого человека (вне зависимости от успешности такой попытки).	не предусмотрена

6.3 Типовые контрольные задания и/или иные материалы, используемые для оценки результатов обучения

6.3.1 Типовые контрольные вопросы

№ п/п	Формулировки вопросов
Семестр 8	
1	Понятие национальной безопасности Российской Федерации.
2	Национальные интересы РФ и стратегические национальные приоритеты.
3	Роль информационной безопасности в обеспечении национальной безопасности государства.
4	Основные составляющие национальных интересов Российской Федерации в информационной сфере.
5	Интересы личности общества и государства в информационной сфере.
6	Доктрина информационной безопасности.
7	ФЗ № 149 «Об информации, информационных технология и о защите информации».
8	Источники понятий в области информационной безопасности.
9	Основные понятия информационной безопасности.
10	Основные свойства информации.
11	Угрозы безопасности информации.
12	Внутренние и внешние источники угроз информационной безопасности.
13	Угрозы утечки информации и угрозы несанкционированного доступа.
14	Методы обеспечения информационной безопасности Российской Федерации.
15	Классификация угроз безопасности информации.
16	Модель угроз безопасности информации.
17	Банк данных угроз безопасности информации (ФСТЭК).
18	Модернизированный раздел угроз (ФСТЭК).
19	Виды защищаемой информации.
20	Перечень сведений конфиденциального характера.
21	Понятие интеллектуальной собственности и особенности ее защиты.
22	Понятие интеллектуальной собственности и особенности ее защиты.
23	Основы правового регулирования ИБ.
24	ФЗ № 98 «О коммерческой тайне».
25	Закон № 5485-1 «О государственной тайне».
26	Указ Президента РФ от 06.03.1997 N 188.
27	Основы организационной защиты информации.
28	Законодательные акты в области защиты информации.
29	Российские и международные стандарты, определяющие требования к защите информации.
30	Система сертификации РФ в области защиты информации.
31	Виды мер и основные принципы защиты информации.
32	Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.
33	Основные механизмы защиты информации.
34	Меры защиты информации, реализуемые в автоматизированных (информационных) системах.
35	Управление доступом и его виды.
36	Авторизация как сервис безопасности.
37	Понятие ролевого управления доступом.
38	Дискреционная модель безопасности.
39	Мандатная модель безопасности.
40	Программные и программно-аппаратные средства защиты информации.
41	Инженерная защита и техническая охрана объектов информатизации.
42	Организационно-распорядительная защита информации.
43	Работа с кадрами.
44	Внутриобъектовый режим.
45	Основные принципы организационной защиты информации.
46	Основные принципы работы с конфиденциальными документами.
47	Основы конфиденциального документооборота.

6.3.2 Типовые тестовые задания

не предусмотрено

6.3.3 Типовые практико-ориентированные задания (задачи, кейсы)

1. Защита документов в Ms Word.

Создать одностраничный документ в Ms Word. Предусмотреть для созданного файла:

-Пароль на открытие, пароль разрешения записи (устанавливаются на файл, то есть относятся к документу/книге в целом).

- Защиту отдельных элементов документов MS Office:

• Парольная защита от изменения частей (разделов) документа Word;

• Электронная подпись.

2. Защита документов в Ms Excel.

Создать книгу в Ms Excel, состоящую из 3-х листов, на каждом из которых располагается одна таблица. Предусмотреть для созданного файла:

-Пароль на открытие, пароль разрешения записи (устанавливаются на файл, то есть относятся к документу/книге в целом).

- Защиту отдельных элементов документов MS Office:

• Парольная защита от просмотра элементов книги Excel (строк, столбцов, листов).

• Парольная защита от изменения содержимого отдельных ячеек и их диапазонов в Excel, структуры листа (вставка, удаление и форматирование строк и столбцов), структуры книги (добавление и удаление листов, отображение, скрытые листов), изменение размеров, положения или видимости окна, настроенного для отображения книги Excel.

3. Информация ограниченного доступа.

Заполнить первый столбец таблицы «Сведения, отнесенные к категории ограниченного доступа» выдержками из нормативно-правовых актов, ссылки на которые указаны во втором столбце (http://www.consultant.ru/document/cons_doc_LAW_93980/) – дать определение.

4. Сокрытие сообщения методом знаков одинакового начертания (стеганография).

Выбрать стеганограмму, контейнер и занести стеганограмму в контейнер. Извлечь стеганограмму из заполненного контейнера.

5. Сокрытие сообщения методом младших битов (LSB-метод).

Изучить метод младших битов (LSB) на примере цветовых кодов заливки ячеек книги MS Excel. Создать модель стегоконтейнера и занести в него сообщение. Провести анализ стегоконтейнера и извлечь из него сообщение.

6. Криптоанализ шифров перестановки.

Дешифровать криптограммы, полученные методами столбцовой и двойной перестановок. Известно, что текст записывался в шифрующую таблицу построчно, знаки пробела в тексте сохранены.

7. Криптоанализ шифров простой замены.

Дешифровать криптограмму, полученную шифром простой замены. В тексте криптограммы сохранены пробелы и знаки пунктуации.

8. Изучение криптографии с открытым ключом на примере программы PGP.

Изучение принципов работы с асимметричной криптосистемой, применения личных и открытых ключей. Изучение работы с цифровыми подписями.

6.4 Методические материалы, определяющие процедуры оценивания результатов обучения

6.4.1 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»

6.4.2 Форма проведения промежуточной аттестации по дисциплине

Устная	+	Письменная		Компьютерное тестирование		Иная	

6.4.3 Особенности проведения промежуточной аттестации по дисциплине

Промежуточная аттестация проводится в виде устного опроса, время на подготовку - 0,5 часа.

Защита курсовой работы проводится посредством предоставления доклада (пояснительная записка объемом 15-25 страниц), презентации и ответов на вопросы.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
7.1.1 Основная учебная литература				
Зенков, А. В.	Основы информационной безопасности	Москва, Вологда: Инфра-Инженерия	2022	https://www.iprbookshop.ru/124242.html
Шаньгин В. Ф.	Информационная безопасность компьютерных систем и сетей	Москва: Форум	2021	https://ibooks.ru/reading.php?short=1&productid=361273

7.1.2 Дополнительная учебная литература				
Галатенко, В. А.	Основы информационной безопасности	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа	2020	https://www.iprbookshop.ru/97562.html
Шаньгин В. Ф.	Комплексная защита информации в корпоративных системах	Москва: Форум	2020	https://ibooks.ru/reading.php?short=1&productid=361312

7.2 Перечень профессиональных баз данных и информационно-справочных систем

Официальный интернет-портал правовой информации (федеральная государственная информационная система) [Электронный ресурс]. URL: http://pravo.gov.ru.

Портал для официального опубликования стандартов Федерального агентства по техническому регулированию и метрологии [Электронный ресурс]. URL: http://standard.gost.ru/wps/portal/.

7.3 Перечень лицензионного и свободно распространяемого программного обеспечения

MicrosoftOfficeProfessional

Microsoft Windows

СПС КонсультантПлюс

7.4 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).