ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования «Петербургский государственный университет путей сообщения
Императора Александра I»
(ФГБОУ ВО ПГУПС)

Кафедра «Бухгалтерский учет и аудит»

РАБОЧАЯ ПРОГРАММА
дисциплины
Б1.В.8 «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»
для направления подготовки
38.03.05 «Бизнес-информатика»
по профилю
«*Цифровые технологии в экономике и бизнесе*»

Форма обучения – очная

Санкт-Петербург
2025

ЛИСТ СОГЛАСОВАНИЙ

Оценочные материалы рассмотрены и утверждены на заседании кафедры «*Бухгалтерский учет и аудит*»
Протокол № 5 от 16 января 2025

Заведующий кафедрой
«Бухгалтерский учет и аудит» _____ *Т.П. Сацук*
16 января 2025

СОГЛАСОВАНО

Руководитель ОПОП ВО _____ *Ж.В. Михайлова*
16 января 2025

1. Цели и задачи дисциплины

Рабочая программа дисциплины «*Управление информационной безопасностью» (Б1.В.8)* (далее – дисциплина) составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки *38.03.05 «Бизнес-информатика*» (далее – ФГОС ВО), утвержденного 29 июля 2020 г., приказ Минобрнауки России № 838 (зарегистрирован Министерством юстиции Российской Федерации 19 августа 2020 г. регистрационный № 59325), с учетом профессионального стандарта 06.015 «Специалист по информационным системам», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 18 ноября 2014 г. № 896н (зарегистрирован Министерством юстиции Российской Федерации 24 декабря 2014 г., регистрационный № 35361), с изменением, внесенным приказом Министерства труда и социальной защиты Российской Федерации от 12 декабря 2016 г. № 727н (зарегистрирован Министерством юстиции Российской Федерации 13 января 2017 г., регистрационный № 45230).

Целью изучения дисциплины является формирование у обучающихся профессиональных компетенций в соответствии с учебным планом.

Для достижения цели дисциплины решаются следующие задачи:

- формирование у обучающегося знаний о методах разработки продуктов в сфере информационно-коммуникационных технологий с учетом требований информационной безопасности;
- формирование у обучающихся умений анализировать актуальные угрозы информационной безопасности и учитывать их в процессе создания и использования продуктов и услуг в сфере информационно-коммуникационных технологий.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

Планируемыми результатами обучения по дисциплине является формирование у обучающихся компетенций и/или части компетенций. Сформированность компетенций и/или части компетенций оценивается с помощью индикаторов достижения компетенций.

Индикаторы достижения компетенций	**Результаты обучения по дисциплине (модулю)**
ПК-2 Анализ, обоснование и выбор решения	
ПК-2.1.5 Знает способы оценки и основы обеспечения информационной безопасности в объеме, необходимом для целей бизнес-анализа	Обучающийся знает: – способы категорирования объектов критической информационной инфраструктуры; – способы оценки текущего состояния информационной безопасности; – алгоритм разработки комплекса мер по обеспечения информационной безопасности на предприятии
ПК-3 Выявление требований к ИС в рамках выполнения работ и управления работами по созданию (модификации) и сопровождению ИС	
ПК-3.1.7 Знает основы ИБ организации	Обучающийся знает: – способы управления разграничением доступа к информации – алгоритмы криптографии, в том числе создания ЭЦП – правила создания защищенных БД и ИС – правовые основы информационной безопасности

3. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина относится вариативной части блока 1 «Дисциплины (модули)».

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Семестр
		7
Контактная работа (по видам учебных занятий) В том числе: – лекции (Л) – практические занятия (ПЗ) – лабораторные работы (ЛР)	64 32 32 -	64 32 32 -
Самостоятельная работа (СРС) (всего)	40	40
Контроль	4	4
Форма контроля (промежуточной аттестации)	З	З
Общая трудоемкость: час / з.е.	108/3	108/3

Примечание: «Форма контроля» – зачет (З).

5. Структура и содержание дисциплины

5.1. Разделы дисциплины и содержание рассматриваемых вопросов

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
1	Общие сведения об информационной безопасности и кибербезопасности.	**Лекция 1.** Общие сведения об информационной безопасности и кибербезопасности (2 часа)	ПК-3.1.7
2	Законодательство Российской Федерации в области информационной безопасности	**Лекция 2.** Законодательство Российской Федерации в области информационной безопасности (2 часа).	ПК-3.1.7
		Практическая работа 1. Нормативно-правовая база, используемая на предприятии для обеспечения информационной безопасности (4 часа)	
		Самостоятельная работа. Изучить нормативно-правовые акты, составить конспект документа по выбору преподавателя	
3	Уязвимости информационных систем и угрозы информационной безопасности	**Лекция 3.** Угрозы и уязвимости безопасности информации (2 часа) **Лекция 4.** Защита информации в телкоммуникационных системах от случайных угроз (2 часа) **Лекция 5.** Методы и средства защиты информации в информационных системах от традиционного шпионажа и диверсий (2 часа)	ПК-2.1.5 ПК-3.1.7
		Практическая работа 2. Изучение защиты информации в информационных системах от случайных угроз (2 часа) **Практическая работа 3.** Изучение защиты информации в информационных системах	ПК-2.1.5 ПК-3.1.7

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		от традиционного шпионажа и диверсий (2 часа) **Практическая работа 4.** Изучение защиты информации в информационных системах от несанкционированного доступа, ПЭМИН, несанкционированной модификации и вредоносных программ (2 часа)	
		Самостоятельная работа. Выполнить практические работы 2-4, оформить отчет по практическим работам 2-4	ПК-2.1.5 ПК-3.1.7
4	Обзор криптографических методов защиты информации	**Лекция 6.** Введение в криптографию (2 часа) **Лекция 7.** Криптографические методы защиты информации. Модели криптосистем. Алгоритм RSA (2 часа) **Лекция 8.** Алгоритмы и протоколы создания ЭЦП (2 часа) **Лекция 9.** Введение в теорию криптовалют. Алгоритм блокчейн (2 часа)	ПК-2.1.5 ПК-3.1.7
		Практическая работа 5. Ручное шифрование-расшифрование с применением разнообразных шифров (2 часа) **Практическая работа 6.** Программирование алгоритма шифрования-расшифрования по выбору преподавателя на выбранном студентом языке программирования (4 часа)	ПК-2.1.5 ПК-3.1.7
		Самостоятельная работа. Выполнить практическую работу 6, оформить отчет по практическим работам 5 и 6, продемонстрировать функционирование алгоритма шифрования-расшифрования	ПК-2.1.5 ПК-3.1.7
5	Обеспечение информационной безопасности информационных систем	**Лекция 10.** Обследование информационной инфраструктуры предприятия. Категорирование объектов информационной инфраструктуры (2 часа) **Лекция 11.** Средства идентификации и аутентификации. Модели доступа и механизмы управления доступом (2 часа) **Лекция 12.** Проектирование защищенных информационных систем: парадигмы, модели ЖЦ, особенности программирования (2 часа) **Лекция 13.** Проектирование защищенных хранилищ информации: базы и банки данных, параметры СУБД, обеспечивающие защищенность (2 часа)	ПК-2.1.5 ПК-3.1.7
		Практическая работа 7. Категорирование объектов критической информационной инфраструктуры (6 часов) **Практическая работа 8.** Разработка архитектуры защищенной ИС: бизнес-логика, структура БД (6 часов) **Практическая работа 9.** Составление совокупности инструментов обеспечения ИБ во время проектирования и эксплуатации ИС (4 часа)	ПК-2.1.5 ПК-3.1.7

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		Самостоятельная работа. Выполнить работы 7-9. Оформить отчеты по практическим работам 7-9, обосновать свои решения	ПК-2.1.5 ПК-3.1.7
6	Организация систем защиты электронного документооборота	**Лекция 14.** Электронный документооборот, виды и способы реализации (2 часа)	ПК-3.1.7
		Самостоятельная работа. Изучить системы защищенного электронного документооборота	ПК-3.1.7
7	Техническая защита информации	**Лекция 15.** Техническая защита информации. Методы и средства защиты информации от утечки по техническим каналам (2 часа)	ПК-3.1.7
		Самостоятельная работа. Изучить описание технических средств защиты информации	ПК-3.1.7
8	Обеспечение экономической безопасности информации	**Лекция 16.** Электронная коммерция и электронный бизнес. Правовое обеспечение ведения электронного бизнеса. Безопасность электронных и мобильных платежей (2 часа)	ПК-3.1.7
		Самостоятельная работа. Подготовка к зачету	ПК-2.1.5 ПК-3.1.7

5.2. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
1	Общие сведения об информационной безопасности и кибербезопасности	2	0	0	2	4
2	Законодательство Российской Федерации в области информационной безопасности	2	4	0	4	10
3	Уязвимости информационных систем и угрозы информационной безопасности	6	6	0	6	18
4	Обзор криптографических методов защиты информации	8	6	0	6	20
5	Обеспечение информационной безопасности информационных систем	8	16	0	16	40
6	Организация систем защиты электронного документооборота	2	0	0	2	4
7	Техническая защита информации	2	0	0	2	4
8	Обеспечение экономической безопасности информации	2	0	0	2	4
	Итого	32	32	-	40	104
					Контроль	4
					Всего (общая трудоемкость, час.)	108

6. Оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Оценочные материалы по дисциплине является неотъемлемой частью рабочей программы и представлены отдельным документом, рассмотренным на заседании кафедры и утвержденным заведующим кафедрой.

7. Методические указания для обучающихся по освоению дисциплины

Порядок изучения дисциплины следующий:

1. Освоение разделов дисциплины производится в порядке, приведенном в разделе 5 «Содержание и структура дисциплины». Обучающийся должен освоить все разделы дисциплины, используя методические материалы дисциплины, а также учебно-методическое обеспечение, приведенное в разделе 8 рабочей программы.
2. Для формирования компетенций обучающийся должен представить выполненные задания, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, предусмотренные текущим контролем успеваемости (см. оценочные материалы по дисциплине).
3. По итогам текущего контроля успеваемости по дисциплине, обучающийся должен пройти промежуточную аттестацию (см. оценочные материалы по дисциплине).

8. Описание материально-технического и учебно-методического обеспечения, необходимого для реализации образовательной программы по дисциплине

8.1. Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой бакалавриата, укомплектованные специализированной учебной мебелью и оснащенные оборудованием и техническими средствами обучения, служащими для представления учебной информации большой аудитории: настенным экраном (стационарным или переносным), маркерной доской и (или) меловой доской, мультимедийным проектором (стационарным или переносным).

Все помещения, используемые для проведения учебных занятий и самостоятельной работы, соответствуют действующим санитарным и противопожарным нормам и правилам.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

8.2. Университет обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

- MS Office;
- Операционная система Windows;
- Антивирус Касперский;
- Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ».
- IDE NetBeans 6.8

8.3. Обучающимся обеспечен доступ (удаленный доступ) к современным профессиональным базам данных:

- Электронно-библиотечная система издательства «Лань». [Электронный ресурс]. – URL: https://e.lanbook.com/ — Режим доступа: для авториз. пользователей;
- Электронно-библиотечная система ibooks.ru («Айбукс»). – URL: https:// ibooks.ru / — Режим доступа: для авториз. пользователей;
- Электронная библиотека ЮРАЙТ. – URL: https://biblio-online.ru/ — Режим доступа: для авториз. пользователей;
- Единое окно доступа к образовательным ресурсам - каталог образовательных интернет-ресурсов и полнотекстовой электронной учебно-методической библиотеке для общего и профессионального образования». – URL: http://window.edu.ru/ — Режим доступа: свободный.

– Словари и энциклопедии. – URL: http://academic.ru/ — Режим доступа: свободный.

– Научная электронная библиотека "КиберЛенинка" – URL: http://cyberleninka.ru/ — Режим доступа: свободный.

8.4. Обучающимся обеспечен доступ (удаленный доступ) к информационным справочным системам:

– Национальный Открытый Университет "ИНТУИТ". Бесплатное образование. [Электронный ресурс]. – URL: https://intuit.ru/ — Режим доступа: свободный.

8.5. Перечень печатных и электронных изданий, используемых в образовательном процессе:

– Информационная безопасность и защита информации на железнодорожном транспорте: в 2 ч.: учебник / под ред. А. А. Корниенко. – Ч. 1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте. - М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2014. – 439 с.

– Бондаренко, И. С. Информационная безопасность : учебник / И. С. Бондаренко. — Москва : МИСИС, 2023. — 254 с. — ISBN 978-5-907560-71-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/360344

– Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2025. — 400 с. — ISBN 978-5-507-52839-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/460715

– Ярочкин, В. И. Информационная безопасность : учебник / В. И. Ярочкин. — 5-е изд. — Москва : Академический Проект, 2020. — 544 с. — ISBN 978-5-8291-3031-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/132242

– А.А. Корниенко, М.Л. Глухарев «Криптографические методы защиты информации», учебное пособие, часть 1, ФГБОУ ВО ПГУПС, 2017 - 64 с.

– Доктрина информационной безопасности Российской Федерации [Электронный ресурс] – Режим доступа: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html.

– Федеральный закон от 27 июля 2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации [Электронный ресурс] – Режим доступа: https://rg.ru/2006/07/29/informacia-dok.html.

8.6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», используемых в образовательном процессе:

– Личный кабинет обучающегося и электронная информационно-образовательная среда. [Электронный ресурс]. – URL: https://my.pgups.ru — Режим доступа: для авториз. пользователей;

– Электронная информационно-образовательная среда. [Электронный ресурс]. – URL: https://sdo.pgups.ru — Режим доступа: для авториз. пользователей;

– Правовая система КонсультантПлюс. – URL:http://www.consultant.ru/ — Режим доступа: свободный.

– Электронный фонд правовой и нормативно-технической документации – URL: http://docs.cntd.ru/ — Режим доступа: свободный.

Разработчик рабочей программы, доцент,
к.э.н. Ж.В.Михайлова
16 января 2025 г.