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

Кафедра «*Учёт и бизнес-анализ*»

РАБОЧАЯ ПРОГРАММА
дисциплины
Б1.О.8 «*ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ*»
для направление подготовки
27.03.04 «*Системный анализ и управление*»

по магистерской программе
«*Системный анализ и управление информационными системами на транспорте*»

Форма обучения – очная

Санкт-Петербург
2026

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа рассмотрена и утверждена на заседании кафедры *«Учёт и бизнес-анализ»*
Протокол № 5 от 27 января 20 26 г.

Заведующий кафедрой
«Учёт и бизнес-анализ» _____ *Т.П. Сацук*
27 января 2026 г.

СОГЛАСОВАНО

Руководитель ОПОП ВО _____ *С.А. Жутяева*
27 января 2026 г.

1. Цели и задачи дисциплины

Рабочая программа дисциплины «*Информационная безопасность и защита информации» (Б1.О.8*) (далее – дисциплина) составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки *27.03.04 «Системный анализ и управление»* (далее – ФГОС ВО), утвержденного 30 октября 2014 г., приказ Министерства образования и науки Российской Федерации № 1413.

Целью изучения дисциплины является формирование у студентов системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации.

Для достижения цели дисциплины решаются следующие задачи:

– Изучение современной методологии системного анализа и управления применительно к задачам защиты информации и обеспечения информационной безопасности;

– Формирование понимания правовых основ и нормативно-правового регулирования в сфере информационной безопасности и интеллектуальной собственности;

– Освоение методов анализа угроз, оценки рисков и выбора оптимальных организационных и технических мер защиты на основе системного подхода;

– Приобретение навыков применения программно-аппаратных и криптографических средств защиты с учетом требований законодательства и защиты прав интеллектуальной собственности.

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

Планируемыми результатами обучения по дисциплине (модулю) является формирование у обучающихся компетенций (части компетенций). Сформированность компетенций (части компетенции) оценивается с помощью индикаторов достижения компетенций.

В рамках изучения дисциплины (модуля) осуществляется практическая подготовка обучающихся к будущей профессиональной деятельности. Результатом обучения по дисциплине является формирования у обучающихся практических навыков.

Индикаторы достижения компетенций	**Результаты обучения по дисциплине (модулю)**
ОПК-5. Способен решать задачи в области развития науки, техники и технологии, применяя современные методы системного анализа и управления с учетом нормативно-правового регулирования в сфере интеллектуальной собственности	
ОПК-5.1. Знать современные методы системного анализа и управления и нормы правового регулирования в сфере интеллектуальной собственности	*Обучающийся знает:* *– современные методы системного анализа (структурный, объектно-ориентированный, функциональный анализ) и их применимость для решения задач обеспечения информационной безопасности;* *– основные положения нормативно-правовых актов в сфере интеллектуальной собственности (ГК РФ, часть 4) и информационной безопасности (ФЗ «Об информации…», «О персональных данных», «О коммерческой тайне», Доктрина информационной безопасности РФ);*

Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
	– классификацию угроз безопасности информации, методы оценки уязвимостей и подходы к управлению рисками; *– принципы построения систем защиты информации на основе системного подхода.*
ОПК-5.2. Уметь решать задачи в области развития науки, техники и технологии на основе применения современных методов системного анализа и управления с учетом нормативно-правового регулирования в сфере интеллектуальной собственности	*Обучающийся умеет:* *– разрабатывать фрагменты политик информационной безопасности, включая разделы, касающиеся регулирования прав на создаваемые объекты интеллектуальной собственности;* *– проводить анализ нормативных правовых актов и судебной практики для квалификации правонарушений в информационной сфере;* *– решать практические задачи по выбору организационных и технических мер защиты информации с учетом требований законодательства.*
ОПК-5.3. Владеть навыками использования современных методов системного анализа и управления с учетом нормативно-правового регулирования в сфере интеллектуальной собственности для решения задач в области развития науки, техники и технологии	*Обучающийся владеет:* *– навыками работы с программными средствами защиты информации (СКЗИ, межсетевые экраны, средства антивирусной защиты);* *– методами криптографической защиты данных (шифрование, хеширование, электронная подпись);* *– навыками анализа логов и событий информационной безопасности.*

3. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина относится к обязательной части/части, формируемой участниками образовательных отношений блока 1 «Дисциплины (модули)».

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Контактная работа (по видам учебных занятий) В том числе: – лекции (Л) – практические занятия (ПЗ) – лабораторные работы (ЛР)	 16 32
Самостоятельная работа (СРС) (всего)	56
Контроль	4
Форма контроля (промежуточной аттестации)	З
Общая трудоемкость: час / з.е.	108 / 3

5. Структура и содержание дисциплины

5.1. Разделы дисциплины и содержание рассматриваемых вопросов

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
1	**Введение в нформационную безопасность**	**Лекция 1. (2 ч.)** Системный анализ как основа построения систем защиты информации. Основные понятия и критерии ИБ. Современные угрозы и уязвимости.	**ОПК-5.1**
		Практическое занятие 1. (2 ч.) Идентификация и систематизация угроз безопасности информации для различных объектов информатизации (анализ кейсов).	**ОПК-5.2**
		Самостоятельная работа (6 ч.) Изучение классификации угроз по методическим документам ФСТЭК России. Подготовка реферата по современным векторам атак.	**ОПК-5.1, ОПК-5.2**
2	**Правовое обеспечение информационной безопасности**	**Лекция 2. (2 ч.)** Система законодательства РФ в области ИБ и интеллектуальной собственности. Доктрина информационной безопасности. Законодательные акты (ГК РФ ч.4, ФЗ «Об информации...», «О персональных данных», «О коммерческой тайне»).	**ОПК-5.1**
		Практическое занятие 2–3. (4 ч.) Анализ нормативных правовых актов в сфере защиты информации и интеллектуальной собственности. Поиск и применение актуальных редакций документов. Решение задач по квалификации правонарушений в информационной сфере.	**ОПК-5.2**
		Самостоятельная работа (10 ч.) Анализ судебной практики по спорам, связанным с нарушением авторских прав в цифровой среде и нарушением законодательства о защите информации.	**ОПК-5.2**
3	**Организационное обеспечение информационной безопасности**	**Лекция 3. (2 ч.)** Управление информационной безопасностью организации. Политики, стандарты и процедуры. Системный подход к управлению рисками (анализ, оценка, обработка).	**ОПК-5.1**
		Практическое занятие 4–6. (6 ч.) Разработка фрагмента политики информационной безопасности для гипотетической организации (в части регулирования прав на создаваемое ПО и базы данных). Оценка рисков информационной безопасности с использованием зарубежных и отечественных методик.	**ОПК-5.2, ОПК-5.3**
		Самостоятельная работа (12 ч.)	**ОПК-5.1,**

		Сравнительный анализ международных и национальных стандартов в области ИБ (ISO/IEC 27000, ГОСТ Р ИСО/МЭК 27001). Изучение структуры пакета организационно-распорядительной документации.	**ОПК-5.2**
4	**Технические средства и методы защиты информации**	**Лекция 4. (2 ч.)** Инженерно-техническая защита информации. Технические каналы утечки информации. Методы и средства защиты объектов информатизации.	**ОПК-5.1**
		Практическое занятие 7–8. (4 ч.) Изучение состава и принципов работы технических средств охраны и систем контроля доступа (на примере конкретных решений). Моделирование угроз для объекта информатизации с целью определения необходимого класса защищенности.	**ОПК-5.2, ОПК-5.3**
		Самостоятельная работа (8 ч.) Подготовка к практическим занятиям. Анализ рынка современных технических средств защиты.	**ОПК-5.1, ОПК-5.2**
5	**Программно-аппаратные средства и методы обеспечения информационной безопасности**	**Лекция 5–6. (4 ч.)** Программно-аппаратные методы защиты. Идентификация и аутентификация, управление доступом. Межсетевые экраны, средства обнаружения вторжений (СОВ). Защита виртуальной инфраструктуры. Защита программного обеспечения как объекта интеллектуальной собственности.	**ОПК-5.1**
		Практическое занятие 9–12. (8 ч.) Настройка и анализ политик безопасности операционных систем. Работа с системами разграничения доступа. Изучение принципов функционирования и настройки межсетевых экранов. Анализ защищенности веб-приложений с использованием сканеров уязвимостей.	**ОПК-5.2, ОПК-5.3**
		Самостоятельная работа (12 ч.) Установка и настройка средств обнаружения вторжений (например, Snort или Suricata) в виртуальной среде. Анализ логов.	**ОПК-5.3**
6	**Криптографические методы защиты информации**	**Лекция 7–8. (4 ч.)** Основы криптографии. Симметричные и асимметричные криптосистемы. Электронная подпись и ее правовое регулирование (ФЗ «Об электронной подписи»). Инфраструктура открытых ключей (PKI). Правовая охрана средств криптографии.	**ОПК-5.1**

		Практическое занятие 13–16. (8 ч.) Изучение работы хеш-функций и алгоритмов шифрования (кейсы использования для защиты авторского контента). Работа со средствами электронной подписи для защиты документов, являющихся объектами интеллектуальной собственности. Знакомство с программными СКЗИ (криптопровайдеры).	**ОПК-5.2, ОПК-5.3**
		Самостоятельная работа (8 ч.) Изучение порядка получения лицензии на деятельность по разработке и распространению СКЗИ. Подготовка к зачету.	**ОПК-5.1**

5.2. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
1	Введение в нформационную безопасность	2	2	-	6	10
2	Правовое обеспечение информационной безопасности	2	4	-	10	16
3	Организационное обеспечение информационной безопасности	2	6	-	12	20
4	Технические средства и методы защиты информации	2	4	-	8	14
5	Программно-аппаратные средства и методы обеспечения информационной безопасности	4	8	-	12	24
6	Криптографические методы защиты информации	4	8	-	8	20
	Итого	16	32	-	56	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/специалитета/ магистратуры, 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. Перечень лицензионных программ представлен на внутреннем портале ФГБОУ ВО ПГУПС по адресу http://eaisu.pgups.edu.mps/info/prog/.

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

– Банк данных безопасности информации [Электронный ресурс]. – URL: bdu.fstec.ru/threat — Режим доступа: свободный.

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

– Справочно-правовая система Консультант Плюс [Электронный ресурс]. – URL: https://www.consultant.ru/ – Режим доступа: свободный;

– Справочно-правовая система ГАРАНТ [Электронный ресурс]. – URL: https://www.garant.ru/ – Режим доступа: свободный.

8.5. Перечень печатных изданий, используемых в образовательном процессе:

– Прохорова О. В. Информационная безопасность и защита информации : учебник для СПО / О. В. Прохорова. – 6-е изд., стер. – Санкт-Петербург : Лань, 2025. – 124 с. : ил. – Текст : непосредственный.

– Зенков, А. В. Информационная безопасность и защита информации : учебник для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588741;

– Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция). Консультант плюс. Правовой сервер [Электронный ресурс]. – URL: http://www.consultant.ru — Режим доступа: свободный;

– Указ Президента РФ от 03.04.1995 N 334 (ред. от 25.07.2000) "О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации

шифровальных средств, а также предоставления услуг в области шифрования информации" – Консультант плюс. Правовой сервер [Электронный ресурс]. – URL: http://www.consultant.ru — Режим доступа: свободный;

– Указ Президента РФ от 17.03.2008 N 351 (ред. от 22.05.2015) "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена" – Консультант плюс. Правовой сервер [Электронный ресурс]. – URL: http://www.consultant.ru — Режим доступа: свободный;

– Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) "О сертификации средств защиты информации" – Консультант плюс. Правовой сервер [Электронный ресурс]. – URL: http://www.consultant.ru — Режим доступа: свободный;

– Постановление Правительства РФ от 03.02.2012 N 79 (ред. от 27.12.2024) "О лицензировании деятельности по технической защите конфиденциальной информации" (вместе с "Положением о лицензировании деятельности по технической защите конфиденциальной информации") – Консультант плюс. Правовой сервер [Электронный ресурс]. – URL: http://www.consultant.ru — Режим доступа: свободный;

– Постановление Правительства РФ от 03.03.2012 N 171 (ред. от 27.12.2024) "О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации" (вместе с "Положением о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации") – Консультант плюс. Правовой сервер [Электронный ресурс]. – URL: http://www.consultant.ru — Режим доступа: свободный;

– Приказ ФСБ РФ от 09.02.2005 N 66 (ред. от 12.04.2010) "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)" (Зарегистрировано в Минюсте РФ 03.03.2005 N 6382) – Консультант плюс. Правовой сервер [Электронный ресурс]. – URL: http://www.consultant.ru — Режим доступа: свободный;

– Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" – Консультант плюс. Правовой сервер [Электронный ресурс]. – URL: http://www.consultant.ru — Режим доступа: свободный.

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

– Личный кабинет ЭИОС [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;

– Федеральная служба по техническому и экспортному контролю [Электронный ресурс]. – URL: https://fstec.ru/ – Режим доступа: свободный;

– Комитет государственной думы по безопасности [Электронный ресурс]. – URL: http://komitet-bezopasnost.duma.gov.ru/ – Режим доступа: свободный;

– Совет безопасности Российской Федерации [Электронный ресурс]. – URL: http://www.scrf.gov.ru// – Режим доступа: свободный;

– Министерство внутренних дел [Электронный ресурс]. – URL: https://www.mvd.ru/ – Режим доступа: свободный.

Разработчик рабочей программы, асситент _____ *А.В. Стрехин*
27 января 20 26 г.