



**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ**

федеральное государственное бюджетное образовательное учреждение
высшего образования
«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФГБОУ ВО «ИГУ»

Кафедра радиофизики и радиоэлектроники



Рабочая программа дисциплины (модуля)

Наименование дисциплины (модуля) **Б1.В.ДВ.05.02 Защита персональных данных**

Направление подготовки 10.03.01 Информационная безопасность

Тип образовательной программы бакалавриат

Направленность (профиль) подготовки №7 Техническая защита информации

Квалификация выпускника бакалавр

Форма обучения очная

Согласовано с УМК физического факультета

Протокол № 25 от «21» апреля 2020 г.

Председатель _____ Буднев Н.М.

**Рекомендовано кафедрой радиофизики и
радиоэлектроники:**

Протокол № 8

От «20» марта 2020 г.

И.О.Зав. кафедрой _____ Колесник С.Н.

Иркутск 2020 г.

Содержание

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ.....	3
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО.....	3
3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....	3
4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ.....	5
4.1. Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и отведенного на них количества академических часов.....	5
4.2. План внеаудиторной самостоятельной работы обучающихся по дисциплине.....	6
4.3. Содержание учебного материала	7
4.3.1. Перечень семинарских, практических занятий и лабораторных работ.....	8
4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы (СРС).....	8
4.4. Методические указания по организации самостоятельной работы студентов.....	9
4.5. Примерная тематика курсовых работ.....	10
5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ.....	10
а) основная литература.....	10
в) базы данных, информационно-справочные и поисковые системы.....	10
6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ.....	10
6.1. Учебно-лабораторное оборудование.....	10
6.2. Программное обеспечение.....	10
6.3. Технические и электронные средства.....	10
7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ.....	11
8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ.....	11

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Формирование знаний и навыков, необходимых для организации и обеспечения безопасности персональных данных, обрабатываемых в информационных системах государственных, муниципальных органов, органов местного самоуправления и организаций различных форм собственности, физических лиц, организующих и (или) осуществляющих обработку персональных данных.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Защита персональных данных» базируется на дисциплинах «Информатика», «Теория информации», «Основы информационной безопасности», «Аппаратные средства вычислительной техники».

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенций в соответствии с ФГОС ВО и ОП ВО по направлению подготовки **10.03.01 Информационная безопасность**.

Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция	Результаты обучения
ОК-7 способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности	знать: основные виды угроз безопасности персональных данных в информационных системах, содержание и порядок организации работ по выявлению угроз персональным данным уметь: обосновывать и задавать требования по обеспечению безопасности персональных данных в ИС; проводить оценки актуальных угроз безопасности персональным данным
ПК-8 способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	владеть навыками: работы с правовыми базами данных; выявления угроз безопасности персональным данным в ИС
ПК-10. способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	

4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетные единицы, 108 часа,
 Форма промежуточной аттестации: зачет

4.1. Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и отведенного на них количества академических часов

№ п/н	Раздел дисциплины/тема	Семестр	Всего часов	Из них практическая подготовка обучающихся	Виды учебной работы, включая самостоятельную работу обучающихся, практическую подготовку и трудоемкость (в часах)				Форма текущего контроля успеваемости
					Контактная работа преподавателя с обучающимися			Самостоятельная работа	
					Лекция	Семинар/ Практическое, лабораторное занятие/	Консультация		
1	2	3	4	5	6	7	8	9	10
1	Тема 1. Основы законодательства в области защиты персональных данных. Права субъекта ПДн и обязанности оператора.	5	20	0	4	2	0	5	решение задач на практических занятиях
2	Тема 2. Основные этапы обработки и защиты персональных данных.	5	20	0	8	4	0	5	решение задач на практических занятиях

3	Тема 3. Анализ объекта информатизации. Составление модели угроз.	5	16	0	8	4	0	5	решение задач на практических занятиях
4	Тема 4. Техническое задание на систему защиты ПДн.	5	20	0	8	4	0	5	решение задач на практических занятиях
5	Тема 5. Стадия проектирования. Требования методических документов.	5	20	0	8	4	0	5	решение задач на практических занятиях
6	Тема 6.. Особенности защиты персональных данных при их обработке в государственных информационных системах.	5	20	0	8	4	0	5	решение задач на практических занятиях

4.2. План внеаудиторной самостоятельной работы обучающихся по дисциплине

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
5	Тема 1. Основы законодательства в области защиты персональных данных. Права субъекта ПДн и обязанности оператора.	Подготовка к контрольной работе №1	1-5 неделя	5	Контрольная работа №1	Учебный сайт
5	Тема 2. Основные этапы обработки и защиты персональных данных.	Контрольная работа №1.	6 неделя	5	Контрольная работа №1	Учебный сайт

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
5	Тема 3. Анализ объекта информатизации. Составление модели угроз.	Подведение итогов по контрольной работе №1. Работа над ошибками по контрольной работе №1.	7 неделя	5	Контрольная работа №1	Учебный сайт
5	Тема 4. Техническое задание на систему защиты ПДн.	Подготовка к контрольной работе №2	8-11 неделя	5	Контрольная работа №2	Учебный сайт
5	Тема 5. Стадия проектирования. Требования методических документов.	Контрольная работа №2.	12 неделя	5	Контрольная работа №2	Учебный сайт
5	Тема 6. Особенности защиты персональных данных при их обработке в государственных информационных системах.	Подведение итогов по контрольной работе №2. Работа над ошибками по контрольной работе №2.	13 неделя	5	Контрольная работа №2	Учебный сайт
Общий объем самостоятельной работы по дисциплине (час)				30		

4.3. Содержание учебного материала

Тема 1. Основы законодательства в области защиты персональных данных. Права субъекта ПДн и обязанности оператора.

Анализ международного и Российского законодательства по вопросам обработки ПДн и обеспечения безопасности ПДн. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Права субъекта персональных данных, обязанности оператора.

Работа в программе Консультант Плюс. Поиск правовых документов в программе Консультант Плюс. Изучение ФЗ № 152-ФЗ «О персональных данных».

Тема 2. Основные этапы обработки и защиты персональных данных.

Состав мероприятий по приведению информационных систем и процессов обработки персональных данных в соответствие с требованиями законодательства о персональных данных.

Тема 3. Анализ объекта информатизации. Составление модели угроз.

Стадия предпроектного обследования. Составление перечня ПДн, перечня сотрудников, работающих с ПДн. Описание ИСПДн. Выявление угроз безопасности персональных данных при их обработке в ИСПДн. Разработка частной модели угроз безопасности ПДн. Базовая модель угроз безопасности ПДн при их обработке в ИСПДн. Определение актуальности угроз в соответствии с методическими документами ФСТЭК России. Разработка модели нарушителя.

Тема 4. Техническое задание на систему защиты ПДн.

Составление частного технического задания на разработку системы защиты персональных данных. Обоснование разработки системы защиты ПДн. Требования методических документов ФСТЭК и ФСБ России к составу и содержанию организационных и технических мер по обеспечению безопасности

Тема 5. Стадия проектирования. Требования методических документов.

Разработка системы защиты ПДн. Выбор средств защиты информации. Программно-технические комплексы защиты информации от несанкционированного доступа. Технические средства перекрытия технических каналов утечки информации. Организационные мероприятия.

Тема 6.. Особенности защиты персональных данных при их обработке в государственных информационных системах.

Особенности защиты персональных данных при их обработке в государственных информационных системах. Подготовка объекта к аттестации. Типовые формы документов. Изучение методов обезличивания персональных данных.

Особенности организации обработки персональных данных в государственных информационных системах.

4.3.1. Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела и темы	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)		Оценочные средства	Формируемые компетенции
			Всего часов	Из них практическая подготовка		
1	2	3	4	5	6	7

1.	Тема 1	Практическое занятие №1	2		Тестовый контроль по теме	ОК-7 ПК-8
2.	Тема 2	Практическое занятие №2	4		Тестовый контроль по теме	ОК-7 ПК-10
3.	Тема 3	Практическое занятие №3	4		Тестовый контроль по теме	ОК-7 ПК-10
4.	Тема 4	Практическое занятие №4	4		Тестовый контроль по теме	ОК-7 ПК-8
5.	Тема 5	Практическое занятие №5	4		Тестовый контроль по теме	ОК-7 ПК-10
6.	Тема 6	Практическое занятие №6	4		Тестовый контроль по теме	ОК-7 ПК-8

4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы (СРС)

№ п/п	Тема	Задание	Формируемая компетенция
1	Тема 1	Контрольная работа №1.	ОК-7 ПК-8
2	Тема 2	Контрольная работа №1.	ОК-7 ПК-10
3	Тема 3	Контрольная работа №1.	ОК-7 ПК-10
4	Тема 4	Контрольная работа №2.	ОК-7 ПК-8
5	Тема 5	Контрольная работа №2.	ОК-7 ПК-10
6	Тема 6	Контрольная работа №2.	ОК-7 ПК-8

4.4. Методические указания по организации самостоятельной работы студентов

Текущая самостоятельная работа по дисциплине «Защита персональных данных», направленная на углубление и закрепление знаний студента, на развитие практических умений, включает в себя следующие виды работ:

- работа с лекционным материалом;
- подготовка к практическим занятиям;
- выполнение индивидуальных проектов;
- подготовка к контрольным работам;
- подготовка к зачету и экзамену.

Творческая проблемно-ориентированная самостоятельная работа по дисциплине «Защита персональных данных», направленная на развитие интеллектуальных умений, общекультурных и профессиональных компетенций, развитие творческого мышления у студентов, включает в себя следующие виды работ по основным проблемам курса:

- поиск, анализ, структурирование информации;
- выполнение графических работ, обработка и анализ данных;
- участие в конференциях, олимпиадах и конкурсах.

Оценка результатов самостоятельной работы организуется как единство двух форм: самоконтроль и контроль со стороны преподавателя.

Самоконтроль зависит от определенных качеств личности, ответственности за результаты своего обучения, заинтересованности в положительной оценке своего труда, материальных и моральных стимулов, от того насколько обучаемый мотивирован в достижении наилучших результатов. Задача преподавателя состоит в том, чтобы создать условия для выполнения самостоятельной работы (учебно-методическое обеспечение), правильно использовать различные стимулы для реализации этой работы (рейтинговая система), повышать её значимость, и грамотно осуществлять контроль самостоятельной деятельности студента (фонд оценочных средств).

4.5. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) учебным планом не предусмотрены.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) основная литература

1. Бычков, А. И. Проблемы защиты персональных данных / А. И. Бычков. — Москва : Infotropic Media, 2020. — 116 с. — ISBN 978-5-9998-0352-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/234317> (дата обращения: 20.12.2023). — Режим доступа: для авториз. пользователей.

б) базы данных, информационно-справочные и поисковые системы

2. Учебный сайт Лаборатории ТЗИ Физического факультета ИГУ - <https://sites.google.com/view/ltzi/>, – Режим доступа: свободный.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-лабораторное оборудование:

Компьютерная лаборатория 323б (16 серверов) и лекционная аудитория 225, оснащенные мультимедийными средствами, электронной базой знаний, системой тестирования, выходом в глобальную сеть Интернет. Технические характеристики серверов

обеспечивают возможность моделирования необходимого аппаратного обеспечения для работы с современными компьютерными системами хранения и обработки информации.

6.2. Программное обеспечение

Система тестирования и анализа программно-аппаратной платформы защиты информации.

6.3. Технические и электронные средства:

В ходе учебного процесса используются технические средства обучения и контроля знаний студентов (презентации, контролирующих программ, демонстрационных установок), использование которых предусмотрено методической концепцией преподавания.

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Для достижения планируемых результатов обучения, в дисциплине «Программно-аппаратные средства защиты информации» используются различные образовательные технологии:

Информационно-развивающие технологии, направленные на формирование системы знаний, запоминание и свободное оперирование ими.

Используется лекционно-семинарский метод, самостоятельное изучение литературы, применение новых информационных технологий для самостоятельного пополнения знаний, включая использование технических и электронных средств информации.

Деятельностные практико-ориентированные технологии, направленные на формирование системы профессиональных практических умений при проведении экспериментальных исследований, обеспечивающих возможность качественно выполнять профессиональную деятельность.

Используется анализ, сравнение методов проведения исследований, выбор метода, в зависимости от объекта исследования в конкретной производственной ситуации и его практическая реализация.

Развивающие проблемно-ориентированные технологии, направленные на формирование и развитие проблемного мышления, мыслительной активности, способности видеть и формулировать проблемы, выбирать способы и средства для их решения. Используются виды проблемного обучения: освещение основных проблем информационной безопасности, учебные дискуссии, коллективная деятельность в группах при выполнении лабораторных работ, решение задач повышенной сложности. При этом используются первые три уровня (из четырех) сложности и самостоятельности: проблемное изложение учебного материала преподавателем; создание преподавателем проблемных ситуаций, а обучаемые вместе с ним включаются в их разрешение; преподаватель создает проблемную ситуацию, а разрешают её обучаемые в ходе самостоятельной деятельности.

Личностно-ориентированные технологии обучения, обеспечивающие в ходе учебного процесса учет различных способностей обучаемых, создание необходимых условий для развития их индивидуальных способностей, развитие активности личности в учебном процессе. Личностно-ориентированные технологии обучения реализуются в результате индивидуального общения преподавателя и студента при защите лабораторных

работ, при выполнении домашних индивидуальных заданий, решении задач повышенной сложности, на еженедельных консультациях.

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.1. Оценочные средства для входного контроля

Входной контроль (25 вариантов, 7-й семестр), представляет собой перечень из 10-15 вопросов и заданий. Входной контроль проводится в письменном виде на первом практическом занятии в течение 15 минут. Проверяется уровень входных знаний.

8.2. Оценочные средства текущего контроля

Вопросы к практическим занятиям. Представляют собой перечень вопросов, проверяющих знание теоретического лекционного материала и тем, вынесенных на самостоятельную проработку.

8.3. Оценочные средства для промежуточной аттестации

(в форме экзамена).

Перечень вопросов к экзамену:

1. Информация, относящаяся к государственной тайне
2. Персональные данные
3. Информация, составляющая коммерческую тайну
4. Объекты информационной безопасности
5. Информационные системы и их классификация
6. Информационные процессы
7. Случайные и целенаправленные угрозы нарушения сохранности информации
8. Дезинформация
9. Риски ИБ
10. Информационное оружие
11. Информационные войны
12. Технические средства промышленного шпионажа
13. Критерии безопасности
14. “Оранжевая книга” США
15. Классы безопасности
16. Аудит информационной безопасности
17. История хакерства
18. Хакерство в России
19. Правовые механизмы защиты информации на разных уровнях
20. Понятие тайны, секрета и конфиденциальности
21. Задачи и способ функционирования межсетевое экрана
22. Политика безопасности администратора сети и брандмауэра

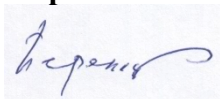
Оценивание ответа на экзамене

4-балльная шкала (уровень освоения)	Показатели	Критерии
Отлично		Студентом дан полный, в логической последовательности развернутый ответ

(повышенный уровень)	<ol style="list-style-type: none"> 1. Полнота изложения теоретического материала; 2. Полнота и правильность решения практического задания; 3. Правильность и/или аргументированность изложения (последовательность действий); 4. Самостоятельность ответа; 5. Культура речи; 6. и т.д. 	<p>на поставленный вопрос, где он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса, решил предложенные практические задания без ошибок.</p>
Хорошо (базовый уровень)		<p>Студентом дан развернутый ответ на поставленный вопрос, где студент демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, в ответе присутствует свободное владение монологической речью, логичность и последовательность ответа. Однако допускается неточность в ответе. Решил предложенные практические задания с небольшими неточностями.</p>
Удовлетворительно (пороговый уровень)		<p>Студентом дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа и решении практических заданий.</p>
Неудовлетворительно (уровень не сформирован)		<p>Студентом дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками</p>

		<p>анализа явлений, процессов, неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Выводы поверхностны. Решение практических заданий не выполнено. Т.е студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.</p>
--	--	---

Разработчик:



(подпись)

_____доцент_____

(занимаемая должность)

_____Ю.Н.Переляев_____

(инициалы, фамилия)

Программа составлена в соответствии с требованиями ФГОС ВО и учитывает рекомендации ПООП по направлению и профилю **10.03.01 Информационная безопасность**.

Программа рассмотрена на заседании кафедры радиопизики и радиоэлектроники «20» марта 2020 г.

Протокол № 8 И.О.Зав. кафедрой



Колесник С.Н.

способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

Настоящая программа, не может быть воспроизведена ни в какой форме без предварительного письменного разрешения кафедры-разработчика программы.