Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Структурное подразделение «Автоматизации и управления (132)»

УТВЕРЖДЕНА:
на заседании кафедры
Протокол №9 от 03 февраля 2026 г.

Рабочая программа дисциплины

«ЗАЩИТА ИНФОРМАЦИИ И БЕЗОПАСНОСТЬ БИЗНЕСА»

Направление: 27.04.05 Инноватика

Проектный инжиниринг в нефтегазохимической отрасли

Квалификация: Магистр

Форма обучения: очная

Документ подписан простой электронной подписью Составитель программы: Галяутдинов Ильдус Ильясович Дата подписания: 17.06.2026	Документ подписан простой электронной подписью Утвердил: Елшин Виктор Владимирович Дата подписания: 23.06.2026	Документ подписан простой электронной подписью Согласовал: Конюхов Владимир Юрьевич Дата подписания: 17.06.2026

Год набора – 2026

Иркутск, 2026 г.

1 Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

1.1 Дисциплина «Защита информации и безопасность бизнеса» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ОПК-5 Способен проводить патентные исследования, определять формы и методы правовой охраны и защиты прав на результат интеллектуальной деятельности, распоряжаться правами на них для решения задач в области развития науки, техники и технологии	ОПК-5.2

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ОПК-5.2	Способен использовать программные средства для защиты интеллектуальной собственности	**Знать** Основы авторского и патентного права, а также законы о коммерческой тайне, принципы депонирования , лицензирования и технического ограничения доступа, классификацию программных средств защиты от несанкционированного доступа, шифрования и управления доступом **Уметь** Настраивать программы контроля целостности данных, межсетевые экраны и антивирусные комплексы для предотвращения утечек исходных кодов и баз данных, работать с системами защиты от утечек **Владеть** Владение инструментами депонирования цифровых объектов для навыками получения правоподтверждающих документов, технологиями защиты мультимедиа, электронных книг и коммерческого ПО от копирования и нецелевого использования, навыками администрирования прав доступа сотрудников к критически важным элементам инфраструктуры и базам данных с целью соблюдения режима конфиденциальности

2 Место дисциплины в структуре ООП

Изучение дисциплины «Защита информации и безопасность бизнеса» базируется на результатах освоения следующих дисциплин/практик: «Компьютерные технологии в

инновационной деятельности», «Проектный инжиниринг и эксплуатация технических систем», «Экономическая теория»

Дисциплина является предшествующей для дисциплин/практик: «Управление проектами и процессами в промышленном производстве», «Креативный менеджмент»

3 Объем дисциплины

Объем дисциплины составляет – 2 ЗЕТ

Вид учебной работы	**Трудоемкость в академических часах** (Один академический час соответствует 45 минутам астрономического часа)	
	Всего	Семестр № 3
Общая трудоемкость дисциплины	72	72
Аудиторные занятия, в том числе:	26	26
лекции	13	13
лабораторные работы	0	0
практические/семинарские занятия	13	13
Самостоятельная работа (в т.ч. курсовое проектирование)	46	46
Трудоемкость промежуточной аттестации	0	0
Вид промежуточной аттестации (итогового контроля по дисциплине)	Зачет	Зачет

4 Структура и содержание дисциплины

4.1 Сводные данные по содержанию дисциплины

Семестр № 3

№ п/п	Наименование раздела и темы дисциплины	Виды контактной работы						СРС		Форма текущего контроля
		Лекции		ЛР		ПЗ(СЕМ)				
		№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	
1	2	3	4	5	6	7	8	9	10	11
1	Информационная безопасность как определяющий компонент национальной безопасности России	3	2			2, 3	6	3	10	Устный опрос
2	Угрозы информационной безопасности. Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере. Понятие и	6, 7	3			5	3	2, 5	18	Решение задач

	виды защищаемой информации.									
3	Общая характеристика способов и средств защиты информации. Криптографические методы защиты информации	4, 5	4			4	2	4	10	Тест
4	Защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программных средств	1, 2	4			1	2	1	8	Контрольная работа
	Промежуточная аттестация									Зачет
	Всего		13				13		46	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 3

№	Тема	Краткое содержание
1	Информационная безопасность как определяющий компонент национальной безопасности России	1. Место информационной безопасности в системе национальной безопасности России: понятие, структура и содержание. 2. Основные руководящие документы, регламентирующие вопросы информационной безопасности. 3. Современные угрозы информационной безопасности в России
2	Угрозы информационной безопасности. Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере. Понятие и виды защищаемой информации.	1. Информационные ресурсы и конфиденциальность информации. 2. Угрозы конфиденциальной информации организации. 3. Система защиты конфиденциальной информации.
3	Общая характеристика способов и средств защиты информации. Криптографические методы защиты информации	1. Анализ и типизация организационных и программно-аппаратных структур автоматизированных систем предприятия 2. Анализ возможных угроз и их специфика в различных типах АС. 3. Систематизация видов защиты информации

4	Защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программных средств	1. Юридические и организационные меры защиты. 2. Программно-аппаратные методы и средства защиты. 3. Защита программ и ценных баз данных от несанкционированного копирования и распространения

4.3 Перечень лабораторных работ

Лабораторных работ не предусмотрено

4.4 Перечень практических занятий

Семестр № 3

№	Темы практических (семинарских) занятий	Кол-во академических часов
1	Основные руководящие документы, регламентирующие вопросы информационной безопасности.	2
2	Угрозы конфиденциальной информации организации	2
3	Система защиты конфиденциальной информации.	4
4	. Систематизация видов защиты информации	2
5	Программно-аппаратные методы и средства защиты	3

4.5 Самостоятельная работа

Семестр № 3

№	Вид СРС	Кол-во академических часов
1	Выполнение тренировочных и обучающих тестов	8
2	Подготовка к зачёту	10
3	Подготовка к практическим занятиям	10
4	Проработка разделов теоретического материала	10
5	Решение специальных задач	8

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: Дискуссия, деловая игра, мозговой штурм

5 Перечень учебно-методического обеспечения дисциплины

5.1 Методические указания для обучающихся по освоению дисциплины

5.1.1 Методические указания для обучающихся по практическим занятиям

Цель подготовки к практическим (семинарским) занятиям предполагает усвоение теоретического материала к следующему практическому занятию, а также закрепление знаний, полученных на предыдущем практическом занятии.

Чтобы подготовиться к предстоящему практическому занятию, студент должен изучить конспект лекций, дополнить его материалом из соответствующего учебного пособия, ответить на вопросы для самоподготовки и контрольные вопросы по теме занятия.
Для закрепления материала по предыдущему практическому занятию студенту необходимо решить заданные на дом задачи.

5.1.2 Методические указания для обучающихся по самостоятельной работе:

Цель самостоятельного изучения теоретического материала — усвоить теоретический материал по некоторым вопросам отдельных тем, который преподаватель не раскрывает на лекции.
Для самостоятельного изучения теоретического материала необходимо ознакомиться с содержанием методических указаний по самостоятельной работе студентов. При этом целесообразно по всем изучаемым темам в разрезе предложенных вопросов для самостоятельной работы составить краткий конспект, который даст возможность более полного усвоения теоретических положений и систематизировать учебный материал, соответствующий программе курса

6 Фонд оценочных средств для контроля текущей успеваемости и проведения промежуточной аттестации по дисциплине

6.1 Оценочные средства для проведения текущего контроля

6.1.1 семестр 3 | Контрольная работа

Описание процедуры.

Суть контрольной работы заключается в том, чтобы проверить, насколько студент усвоил знания на протяжении конкретного времени. Контрольная работа состоит из нескольких вопросов. Студенту нужно письменно отвечать в развернутом виде, использовать методику сравнительного анализа.

Критерии оценивания.

Зачтено: тема раскрыта достаточно полно, логически выстроена, приведены примеры, оформление верное, плагиат в норме.
Не зачтено: тема не раскрыта, материал списан, множество грамматических или фактических ошибок, нет ссылок на источники
В случае отметки «не зачтено» за контрольную работу преподаватель в письменной форме должен дать комментарии по недочетам, допущенным студентом.

6.1.2 семестр 3 | Устный опрос

Описание процедуры.

Устный опрос требует устного изложения учеником изученного материала, связного ответа на поставленный вопрос. Такой опрос может строиться как беседа, рассказ ученика, объяснение, сообщение о наблюдении или опыте

Критерии оценивания.

Оценка «5» (Отлично)
Материал изложен в полном объеме. Даны точные определения основных понятий. Студент понимает суть, может обосновать суждения, применить знания на практике и привести самостоятельные примеры. Ответ логичен, изложен грамотным литературным языком без речевых и терминологических ошибок.
Оценка «4» (Хорошо)
Ответ удовлетворяет всем требованиям на «5», но может быть раскрыт не полностью. Допущено 1–2 недочета или небольшие ошибки в последовательности изложения. Ученик замечает и самостоятельно исправляет свои неточности.
Оценка «3» (Удовлетворительно)
Изложены только главные, базовые положения темы, но основные понятия раскрыты. Имеются существенные ошибки, студент неуверенно применяет знания, требуется наводящий вопрос преподавателя. Нарушена последовательность изложения, терминология используется с ошибками или неуверенно.
Оценка «2» (Неудовлетворительно) Материал не раскрыт, тема не усвоена. Непонимание основных понятий и принципов. Полное отсутствие логики в ответе, грубые речевые ошибки

6.1.3 семестр 3 | Тест

Описание процедуры.

Текущий контроль освоения дисциплины осуществляется в виде тестирования по изученным разделам дисциплины. Тестирование проводится в аудитории во время практического занятия

Критерии оценивания.

Раздел считается усвоенным при условии, что студент ответил правильно на все тестовые вопросы

6.1.4 семестр 3 | Решение задач

Описание процедуры.

Краткое напоминание предыдущего материала учебного курса.
Заявление темы, целей и задач практического задания.
Подробное объяснение практического задания.
Методические указания по его выполнению.
Ответы на дополнительные вопросы.
Постановка контрольных вопросов на практическое занятие.
Формирование команд, если это групповая форма работы.
Непосредственное выполнение задания.
Сдача готовых работ или презентация результатов.
Подведение финальных итогов.
Рекомендации преподавателя и дополнительные задания по теме, если это необходимо

Критерии оценивания.

Теоретическая обоснованность: Студент правильно определяет базовые формулы и законы, необходимые для решения.
Практическая применимость (алгоритм): Шаги решения логичны и приводят к

правильному ответу. Учитываются единицы измерения.
Анализ ответа: Оценивается умение интерпретировать полученный результат и проверять его на реалистичность

6.2 Оценочные средства для проведения промежуточной аттестации

6.2.1 Критерии и средства (методы) оценивания индикаторов достижения компетенции в рамках промежуточной аттестации

Индикатор достижения компетенции	Критерии оценивания	Средства (методы) оценивания промежуточной аттестации
ОПК-5.2	Уверенно демонстрирует навыки администрирования прав доступа сотрудников к критически важным элементам инфраструктуры и базам данных с целью соблюдения режима конфиденциальности. Умеет настраивать программы контроля целостности данных, межсетевые экраны и антивирусные комплексы для предотвращения утечек исходных кодов и баз данных, работать с системами защиты от утечек	Устный опрос/тестирование

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 3, Типовые оценочные средства для проведения зачета по дисциплине

6.2.2.1.1 Описание процедуры

Зачет проводится в формате контрольного тестирования по всем пройденным разделам дисциплины. Тестирование проводится в аудитории.

Пример задания:

1. Какая из следующих мер является основной для обеспечения физической безопасности бизнеса?
1. Установка системы биометрической идентификации.
2. Создание сложных паролей для сотрудников.
3. Ежемесячные обучающие курсы по кибербезопасности.
4. Использование защиты от вирусов на компьютерах.

2. Какая из нижеперечисленных атак направлена на обман сотрудников с целью получения конфиденциальной информации?
1. Фишинговая атака. DDoS-атака.
2. SQL-инъекция.
3. Социальная инженерия.

3. Что представляет собой двухфакторная аутентификация?

1. Использование двух различных компьютеров для входа в систему.
2. Внедрение двух видов антивирусного программного обеспечения.
3. Использование двух методов подтверждения личности для доступа.
4. Шифрование данных на двух уровнях.

4. Какова основная цель политики информационной безопасности в компании?

1. Максимизация прибыли.
2. Оптимизация производственных процессов.
3. Улучшение клиентского сервиса.
4. Защита конфиденциальности и целостности данных.

5. Какие меры следует предпринять для защиты от внутренних угроз в компании?

1. Установка современных брандмауэров.
2. Частая смена поставщиков оборудования.
3. Регулярная проверка прав доступа к данным.
4. Использование открытых сетей для обмена информацией.

6. Какие из нижеперечисленных действий сотрудников могут повысить уровень безопасности в компании?

1. Использование одного и того же пароля для различных аккаунтов.
2. Обход установленных правил безопасности для удобства работы.
3. Регулярное обновление программного обеспечения.
4. Отключение антивирусного ПО для улучшения производительности.

7. Какие из нижеперечисленных являются методами обеспечения конфиденциальности данных?

1. Открытое размещение информации на внутреннем сервере.
2. Публикация конфиденциальных отчетов в открытых источниках.
3. Шифрование передаваемых данных.
4. Использование общедоступных облачных хранилищ.

6.2.2.1.2 Критерии оценивания

Зачтено	Не зачтено
Обучающийся демонстрирует знание основного учебно-программного материала в объеме, необходимом для дальнейшей учебы предусмотренной программой дисциплины. Количество верных ответов при контрольном тестирование должно превышать 60%.	Обучающийся демонстрирует значительные пробелы в знаниях основного учебно-программного материала, допустил принципиальные ошибки в выполнении тестового задания предусмотренного программой и не способен продолжить обучение или приступить по окончании университета к профессиональной деятельности. Количество верных ответов при контрольном тестирование менее 60%.

7 Основная учебная литература

1. Прокофьев И.В. Защита информации в информационных интегрированных системах : учеб. для вузов по специальности "Управление качеством" / И.В. Прокофьев, 2002. - 137.

2. Попова Е. С. Информационная безопасность и защита информации [Электронный ресурс] : курс лекций / Е. С. Попова, 2009. - 68.

[Сайт] – URL: http://elib.istu.edu/viewer/view.php?file=/files/er-4183.pdf

3. Мельников В. П. Информационная безопасность и защита информации : учебное пособие для вузов по специальности 230201 "Информационные системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова, 2011. - 330.

4. Хорев П. Б. Программно-аппаратная защита информации : учебное пособие для вузов по направлениям "Информационная безопасность" и "Информатика и вычислительная техника" / П. Б. Хорев, 2012. - 351.

5. Нагаев И. В. Информационная безопасность и защита информации [Электронный ресурс] : учебно-методическое пособие для бакалавров технических вузов / И. В. Нагаев, 2012. - 213.

[Сайт] – URL: http://elib.istu.edu/viewer/view.php?file=/files/er-6789.pdf

8 Дополнительная учебная литература и справочная

1. Рудометов Евгений А. Электронные средства коммерческой разведки и защита информации / Евгений А. Рудометов, В. Е. Рудометов, 2000. - 218.

2. Мельников В. П. Информационная безопасность и защита информации : учебное пособие для вузов по специальности 230201 "Информационные системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова, 2009. - 330.

3. Коноплева И. А. Управление безопасностью и безопасность бизнеса : учебное пособие для вузов по специальности "Прикладная информатика (по областям)" / И. А. Коноплева, И. А. Богданов, 2014. - 446.

9 Ресурсы сети Интернет

1. http://library.istu.edu/
2. https://e.lanbook.com/

10 Профессиональные базы данных

1. http://new.fips.ru/
2. http://www1.fips.ru/

11 Перечень информационных технологий, лицензионных и свободно распространяемых специализированных программных средств, информационных справочных систем

1. Лицензионное программное обеспечение Системное программное обеспечение

2. Лицензионное программное обеспечение Пакет прикладных офисных программ

3. Лицензионное программное обеспечение Интернет-браузер

12 Материально-техническое обеспечение дисциплины

1. Учебная аудитория для проведения лекционных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Оснащение: комплект учебной мебели, рабочее место преподавателя, доска. Мультимедийное оборудование (в том числе переносное): мультимедийный проектор, экран, акустическая система, компьютер с выходом в интернет.

2. Учебная аудитория для проведения лабораторных/практических (семинарских) занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Оснащение: комплект учебной мебели, рабочее место преподавателя, доска. Мультимедийное оборудование (в том числе переносное): мультимедийный проектор, экран, акустическая система, компьютер с выходом в интернет.