Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Структурное подразделение «Городского строительства и хозяйства»

УТВЕРЖДЕНА:
на заседании кафедры
Протокол №8 от 28 февраля 2025 г.

Рабочая программа дисциплины

«БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ»

Направление: 08.04.01 Строительство

Цифровое управление объектами капитального строительства

Квалификация: Магистр

Форма обучения: очная

Документ подписан простой электронной подписью Составитель программы: Гребнева Оксана Александровна Дата подписания: 16.06.2025	Документ подписан простой электронной подписью Утвердил: Чупин Виктор Романович Дата подписания: 17.06.2025	Документ подписан простой электронной подписью Согласовал: Мелехов Евгений Сергеевич Дата подписания: 19.06.2025

Год набора – 2025

Иркутск, 2025 г.

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

1.1 Дисциплина «Безопасность информационных технологий и систем» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ПК-2 Способен организовать деятельность по созданию информационной модели ОКС для целей эксплуатации и применять информационные технологии для адаптации САПР и систем управления	ПК-2.2

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ПК-2.2	Способен определить уровень доступа участников процесса информационного моделирования ОКС к различным зонам среды общих данных	**Знать** современные информационные системы и технологии, используемые на разных этапах процессов Строительства; процессы анализа, передачи и хранения информации; методы обеспечения информационной безопасности и защиты данных для использования в профессиональной деятельности. **Уметь** применять методы информационной безопасности при решении поставленных задач с необходимостью обеспечения защиты данных в профессиональной деятельности. **Владеть** навыками и средствами для обеспечения защиты информации на этапах анализа, передачи и хранения информации.

2 Место дисциплины в структуре ООП

Изучение дисциплины «Безопасность информационных технологий и систем» базируется на результатах освоения следующих дисциплин/практик: «Геоинформационные системы в городском хозяйстве», «Проектирование и моделирование информационных систем и процессов ОКС», «Современные цифровые технологии при эксплуатации ОКС», «Управление цифровыми моделями ОКС»

Дисциплина является предшествующей для дисциплин/практик: «Интеграция цифровых технологий с процессами управления ОКС», «Цифровая трансформация процессов и технологий управления ОКС», «Производственная практика: практика по разработке виртуального симулятора узла управления системой жизнеобеспечения», «Производственная практика: преддипломная практика»

3 Объем дисциплины

Объем дисциплины составляет – 3 ЗЕТ

Вид учебной работы	**Трудоемкость в академических часах** (Один академический час соответствует 45 минутам астрономического часа)	
	Всего	Семестр № 3
Общая трудоемкость дисциплины	108	108
Аудиторные занятия, в том числе:	30	30
лекции	15	15
лабораторные работы	0	0
практические/семинарские занятия	15	15
Самостоятельная работа (в т.ч. курсовое проектирование)	78	78
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	Законодательная, нормативная, техническая документация и объекты защиты информации	1	4			1, 2	4	1, 2, 3	20	Устный опрос
2	Свойства информации: доступность, целостность и конфиденциальность.	2	6			3, 4, 5	6	1, 2, 3	26	Устный опрос
3	Средства обеспечения информационной безопасности.	3	5			6, 7	5	1, 2, 3	32	Проект
	Промежуточная аттестация									Зачет
	Всего		15				15		78	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 3

№	**Тема**	**Краткое содержание**

1	Законодательная, нормативная, техническая документация и объекты защиты информации	В данном разделе рассматривается российское законодательство, существующая нормативная и техническая литература в области защиты информации: федеральные законы, постановления, указы и т.д. Слушатели знакомятся с основными понятиями и решениями, предусмотренные в данных источниках. Внимание уделяется отношениям, возникающим в профессиональной деятельности при: 1) применении информационных технологий; 2) осуществлении права на поиск, получение, передачу, производство и распространение информации; 3) обеспечении информационной безопасности данных. Также в данном разделе рассматриваются основные объекты защиты при обеспечении информационной безопасности в сфере Строительства: 1)все виды информационных ресурсов профессиональной деятельности: документированная информация (документооборот предприятия); информация, зафиксированная на материальном носителе с параметрами, позволяющими ее идентифицировать; 2)права юридических лиц (предприятий и организаций в сфере Строительства) и государства на получение, распространение и использование информации; 3)системы формирования, распространения и использования информации: библиотеки, архивы, нормативные документы и т.д.
2	Свойства информации: доступность, целостность и конфиденциальность.	В данном разделе рассматривается свойства информационной системы, обеспечивающие: 1) своевременный беспрепятственный доступ субъектов к интересующей их информации; 2) возможность осуществлять своевременный информационный обмен; 3) устойчивость информации к случайному или преднамеренному разрушению или изменению; 4) быть известной (доступной) только субъектам, обладающими соответствующими правами. Рассматриваются сложности практической реализации мер по обеспечению данных свойств в современных информационных систем.
3	Средства обеспечения информационной безопасности.	В данном разделе рассматривается возможность получения прав и доступа к информации лицами или организациями в обход существующей системы защиты с помощью программных, технических и других средств, а также выход конфиденциальной информации за пределы организации. Кроме того, рассматриваются возможные средства защиты информации: 1) формальные; 2) физические; 3) аппаратные; 4)

		программные; 5) специфические; 6) неформальные.

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	Применение существующего законодательства при обеспечении информационной безопасности в области Строительства	2
2	Выбор субъектов Строительства (объектов или процессов) для организации защиты данных.	2
3	Средства обеспечения доступности информации на примере выбранного субъекта Строительства	2
4	Средства обеспечения целостности информации на примере выбранного субъекта Строительства	2
5	Средства обеспечения конфиденциальности информации на примере выбранного субъекта Строительства	2
6	Непосредственный исполнитель угрозы в плане ее негативного воздействия на информацию выбранного субъекта Строительства	2
7	Описание технологии защиты информации для конкретной информационной системы выбранного субъекта Строительства. Создание модели угроз.	3

4.5 Самостоятельная работа

Семестр № 3

№	Вид СРС	Кол-во академических часов
1	Подготовка к зачёту	14
2	Подготовка к практическим занятиям (лабораторным работам)	34
3	Проработка разделов теоретического материала	30

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: Кейс-технология, которая представляет собой работу обучающихся по решению задачи в виде описания проблемной ситуации.

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

Проектирование информационных систем [Электронный ресурс]: методические указания к лабораторным работам и курсовому проектированию / Иркут. гос. техн. ун-т, 2005. - 22 с.

5.1.2 Методические указания для обучающихся по самостоятельной работе:

Проектирование информационных систем [Электронный ресурс]: методические указания к лабораторным работам и курсовому проектированию / Иркут. гос. техн. ун-т, 2005. - 22 с.

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 | Устный опрос

Описание процедуры.

После изучения конкретный темы проводится устный опрос в соответствии с предложенным ниже перечнем вопросов. Магистранту предлагается ответить на три вопроса.
Вопросы для контроля:
1. Какие методы относятся к правовым методам, обеспечивающим информационную безопасность.
2. Основные источники угроз информационной безопасности.
3. Виды информационной безопасности.
и т.д.

Критерии оценивания.

Зачтено: даны верные, развернутые ответы на два и более вопроса, приведены примеры
Не зачтено: дан развернутый ответ на менее двух вопросов

6.1.2 семестр 3 | Проект

Описание процедуры.

Студент по заданию выполняет проект по описанию модели угроз для выбранного объекта Строительства и разрабатывает предложения с мероприятиями по ликвидации возможных угроз. Результаты оформляются в соответствии с требованиями в виде ПЗ. Защита проекта проводится в форме доклада по основным результатам, оформленным в виде презентации.
Пример задания:
Модель угроз проектной организации г. Иркутска

Критерии оценивания.

Зачтено: проект выполнен в полном объеме, даны верные, развернутые ответы не на все вопросы
Не зачтено: проект не выполнен или не даны ответы на вопросы

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
ПК-2.2	Демонстрирует знания методами и средствами защиты информационных процессов, технологий и систем в сфере строительства, умения применять существующие методы в профессиональной деятельности для объектов строительства и жилищно-коммунального хозяйства.	Сдает зачет.

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 форме устного опроса: магистранту задается три вопроса из перечня, приведенного ниже, на которые необходимо дать развернутый ответ. Время для подготовки составляет 20 минут. Во время зачета магистранту запрещено пользоваться конспектом лекций, литературой, гаджетами.
Вопросы к зачету:
1. Какие методы относятся к правовым методам, обеспечивающим информационную безопасность.
2. Основные источники угроз информационной безопасности.
3. Виды информационной безопасности.
4. Цели информационной безопасности.
5. Основные объекты информационной безопасности.
6. Основные риски информационной безопасности.
7. Основные принципы обеспечения информационной безопасности.
8. Основные субъекты информационной безопасности.
9. Негативные средства воздействия на компьютерную сеть.
10. Принцип Кирхгофа.
11. ЭЦП.
12. Угрозы информационной безопасности корпоративной системы.
13. Свойства информации.
14. Политика безопасности в системе.
15. Защитные меры политики безопасности.
16. Вирусы в сети, логические мины (закладки), информационный перехват.
17. Ошибки эксплуатации и неумышленного изменения режима работы системы.
18. Государственной системы защиты информации.
19. Задачи, методы и средства защиты информации.
20. Организация обеспечения режима конфиденциальности на объекте.

6.2.2.1.2 Критерии оценивания

Зачтено	Не зачтено

Магистрант раскрыл тему в полном объеме, посещал все лекции и практические занятия, защитил проект	Магистрант не раскрыл тему в полном объеме или посещал не все лекции и практические занятия, или не защитил проект

7 Основная учебная литература

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

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, 2011. - 330.

3. Глухих В. И. Информационная безопасность и защита данных : учебное пособие / В. И. Глухих, 2012. - 244.

8 Дополнительная учебная литература и справочная

1. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации : учеб. пособие для вузов по специальности 075400 "Комплекс. защита объектов информ." / А. А. Малюк, 2004. - 280.

2. Курушин Владимир Дмитриевич. Компьютерные преступления и информационная безопасность : справочник / Владимир Дмитриевич Курушин, Владимир Александрович Минаев, 1998. - 256.

3. Технологии Электронных Коммуникаций. Т. 45. Информационная безопасность компьютерных сетей/В. Ю. Гайкович, П. В. Дорошкевич, Е. А. Дуйков и др. / В. Ю. Гайкович, П. В. Дорошкевич, Е. А. Дуйков, Д. В. Ершов, 1993. - 122.

4. Родичев Ю. Информационная безопасность. Национальные стандарты Российской Федерации : учебное пособие / Ю. Родичев, 2023. - 384.

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. Microsoft Office Professional Plus 2013

2. Microsoft Visual ++

12 Материально-техническое обеспечение дисциплины

1. проектор LG DX125

2. Рулонный настенно-потолочный экран 244*244