Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Структурное подразделение «Институт информационных технологий и анализа данных (121)»

УТВЕРЖДЕНА:
на заседании совета института ИТиАД им. Е.И.Попова
Протокол №8 от 16 февраля 2026 г.

Рабочая программа практики

«ПРОИЗВОДСТВЕННАЯ ПРАКТИКА: ЭКСПЛУАТАЦИОННАЯ ПРАКТИКА»

Направление: 10.03.01 Информационная безопасность

Организация и технологии защиты информации (в сфере техники и технологии)

Квалификация: Бакалавр

Форма обучения: очная

Документ подписан простой электронной подписью Составитель программы: Маринов Александр Андреевич Дата подписания: 2026-06-18	Документ подписан простой электронной подписью Утвердил:Говорков Алексей Сергеевич Дата подписания: 2026-06-18

Год набора – 2026

Иркутск, 2026 г.

1 Вид практики, тип, способ и формы её поведения

Вид практики – Производственная практика

Тип практики – Производственная практика: эксплуатационная практика

Способ проведения – Стационарная, Выездная

Форма проведения – Дискретная

2 Перечень планируемых результатов обучения при прохождении практики

2.1 Вид и тип практики обеспечивает формирование следующих компетенций и индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ПКС-1 Способность анализировать функциональный процесс объекта информатизации, включая социотехнические системы с применением программных средств для определения возможных источников информационных угроз, их вероятных целей и тактики; организовывать и сопровождать аттестацию объекта защиты в соответствии с требованиями безопасности информации	ПКС-1.5, ПКС-1.6

2.2 В результате прохождения практики у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результаты обучения при прохождении практики
ПКС-1.5	Осмысливает результаты исследований учёных в области информационной безопасности и применяет полученные знания и методы на производстве под контролем уполномоченных федеральных органов исполнительной власти по защите информации	Опыт профессиональной деятельности: знать: ключевые концепции, модели и теории защиты информации (например, модели Белла–ЛаПадулы, Биба, Кларка–Уилсона), нормативно правовую базу РФ в сфере ИБ: ФЗ № 149 ФЗ, ФЗ № 152 ФЗ, ФЗ № 187 ФЗ, требования ФСТЭК и ФСБ России, современные методы и технологии защиты информации: криптография, аутентификация, авторизация, защита от НСД, DLP системы, SIEM системы; типовые угрозы и уязвимости информационных систем, методики их выявления и оценки (в т.ч. базы данных угроз ФСТЭК); стандарты ИБ (ISO/IEC 27000 серия, NIST SP 800 серии, PCI DSS и др.); порядок взаимодействия с уполномоченными органами

		(ФСТЭК, ФСБ) при реализации мер защиты информации; принципы контроля и надзора за соблюдением требований ИБ со стороны федеральных органов исполнительной власти. **Уметь:** анализировать научные публикации по ИБ, выделять ключевые идеи, методы и результаты исследований; сопоставлять научные подходы с практическими задачами защиты информации на производстве; адаптировать научные методы и алгоритмы к реальным условиям функционирования информационных систем организации; применять нормативные требования ФСТЭК и ФСБ при проектировании и внедрении мер защиты информации; разрабатывать или модифицировать регламенты, политики и инструкции по ИБ на основе актуальных научных и нормативных данных; оценивать эффективность реализованных мер защиты с учётом научных критериев и требований регуляторов. **Владеть:** навыками критического анализа научных статей, отчётов и технических документов в области ИБ, методами моделирования угроз и оценки рисков с применением научных подходов (количественных и качественных), способами верификации и валидации реализованных решений на соответствие научным и нормативным требованиям.
ПКС-1.6	Способен составлять и оформлять аналитический отчет по проведенным испытаниям, делать выводы по оценке защищенности на основании аналитического отчета, владеет навыками использования профиля защиты и задания по безопасности, а также	Опыт профессиональной деятельности: методики оценки защищённости информационных систем (в т.ч. методики ФСТЭК России), нормативные документы, регламентирующие требования к защищённости (ФЗ № 149 ФЗ, ФЗ № 152 ФЗ, приказы ФСТЭК, профили защиты, руководящие документы), понятия «профиль защиты»

	формулирования выводов по оценке защищенности	(ППЗ) и «задание по безопасности» (ЗБ) в соответствии с международными и российскими стандартами (ISO/IEC 15408 — «Общие критерии»),состав и содержание профиля защиты (классы, семейства, компоненты требований безопасности), порядок сопоставления фактических характеристик системы с требованиями профиля защиты и задания по безопасности, типовые уязвимости и угрозы, влияющие на защищённость информационных систем, методы и инструменты сбора данных для анализа защищённости (сканеры уязвимостей, SIEM системы, журналы аудита), правила формулирования выводов и рекомендаций по результатам оценки защищённости. **Уметь:** оформлять отчёт в соответствии с установленными шаблонами и требованиями регуляторов, анализировать полученные данные и сопоставлять их с требованиями профиля защиты и задания по безопасности, выявлять отклонения фактических параметров защищённости от нормативных требований, формулировать обоснованные выводы по оценке защищённости (уровень защищённости, соответствие классу защищённости, наличие критических уязвимостей), разрабатывать рекомендации по устранению выявленных недостатков и повышению уровня защищённости, использовать профили защиты и задания по безопасности для оценки соответствия информационных систем нормативным требованиям, интерпретировать результаты испытаний с учётом контекста эксплуатации системы (бизнес процессы, архитектура, угрозы). **Владеть:** методиками анализа

		защищённости на основе профилей защиты и заданий по безопасности, навыками составления карт уязвимостей и угроз на основе результатов испытаний, технологией документирования выявленных несоответствий требованиям ИБ, приёмами формулирования чётких и обоснованных выводов по оценке защищённости, включая количественные и качественные показатели, методами подготовки рекомендаций по устранению уязвимостей с учётом приоритетов и ресурсных ограничений.

3 Место практики в структуре ООП, её объём и продолжительность

Форма обучения	Период проведения (курс/семестр)	Объём практики (ЗЕТ)	Продолжительность практики (количество недель/ академических часов *(один академический час соответствует 45 минутам астрономического часа))*	Форма промежуточной аттестации
очная	3 курс / 6 семестр	6	4 недели / 216 часов	Зачет с оценкой
очная	4 курс / 8 семестр	6	4 недели / 216 часов	Зачет с оценкой

4 Содержание практики

Содержание этапов приведено в таблице ниже:

№ п/п	Этап	Содержание работ
1	Организационный	1. Оформление документов для прохождения эксплуатационной практики. 2. Прибытие на базу практики, согласование подразделения, в котором будет организовано рабочее место. 3. Прохождение вводного инструктажа. 4. Инструктаж по технике безопасности
2	Прохождение практики	1. Изучение деятельности организации. 2. Изучение подразделения организации (конкретного места прохождения практики). 3. Исследование информационной системы

		организации 4. Сбор материала для написания отчета по практике. 5. Сбор материала для написания выпускной квалификационной работы. 6. Участие в выполнении отдельных видов работ, а также разработке и реализации проектов в области искусственного интеллекта. 7. Самостоятельное выполнение отдельных видов работ в рамках обязанностей исполнителя или стажера (по заданию руководителя практикой от предприятия).
3	Заключительный этап	Обработка и анализ полученной в ходе прохождения практики информации; составление отчета о прохождении научно-исследовательской практики.
4	Отчетный	1. Презентация и ответы на вопросы по прохождению научно-исследовательской практики. 2. Оформление отчета о прохождении практики.

5 Форма отчетности по практике

По результатам прохождения практики обучающийся должен предоставить:

- Дневник прохождения практики;
- Отчет о прохождении практики;
- Характеристика;
- Отзыв с места практики;

Требования к содержанию и оформлению отчета о прохождении практики, учитывая специфику направления подготовки:

Отчет по практике должен включать:
- титульный лист (по форме 1 Приложения);
- индивидуальное задание;
- оглавление;
- термины и определения (при необходимости);
- введение;
- цели выполненной работы;
- описание задания;
- используемые технические и программные средства;
- описание основной части (содержания практики):
- заключение;
- список использованной литературы;
- приложения (при необходимости).

Текст отчета должен быть выполнен на одной стороне листа белой бумаги формата А4 с использованием электронных носителей. Размеры полей: верхнего – 20 мм, нижнего – 20 мм, левого – 30 мм, правого – 10 мм; размер шрифта 14 Times New Roman, междустрочный интервал «полуторный», выравнивание текста по ширине, абзацный отступ 1,25 см., «запрет висящих строк», «автоперенос».

При прохождении научно-исследовательской практики студенты должны руководствоваться положением «о порядке организации и проведения практики обучающихся, осваивающих образовательные программы высшего образования - программы бакалавриата, программы специалитета и программы магистратуры в ИРНИТУ».

6 Оценочные материалы по практике

6.1 Оценочные средства для проведения текущего контроля

В качестве оценочных средств для проведения текущего контроля успеваемости используется дневник прохождения практики и характеристика.

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
ПКС-1.5	Рассказал практическую часть (модель и методы) используемую на предприятии (производстве) по методикам	Устное собеседование по теоретическим вопросам и индивидуальные практические задания (зачет с оценкой).
ПКС-1.6	Составил и оформил аналитический отчет по проведенным испытаниям, сделал выводы по оценке защищенности на основании аналитического отчета	Устное собеседование по теоретическим вопросам и индивидуальные практические задания (зачет с оценкой).

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 6, дифференцированный зачет

Типовые оценочные средства: Промежуточная аттестация - рейтинг каждого обучающегося по дисциплине определяется от 0 до 100 баллов

6.2.2.1.1 Описание процедуры

Зачет проводится в форме Студент предоставляет оформленный отчет, дневник о прохождении практики, отвечает на вопросы, связанные с работой выполняемой входе прохождения практики.

Оценка знаний, умений, навыков осуществляется по компетенциям. Студент, полностью выполнивший программу производственной практики, получивший положительные отзывы от руководителя практики от организации, где он проходил практику, представляет отчет по производственной практике руководителю практики от университета.

Прием отчета по производственной практике производит комиссия по председательством руководителя производственной от университета или заведующего выпускающей кафедры.

Оценка выполненной работы производится по системе аттестации на основе ответов студента, отзывов руководителей от предприятия, содержания и качества оформления отчета.

Критериями оценки отчета являются:

- уровень теоретического осмысления студентом практической деятельности принимающей организации (ее целей, задач, содержания, методов);
- качество отчета по итогам практики;
- степень и качество приобретенных студентом профессиональных умений;
- уровень профессиональной направленности выводов и рекомендаций, сделанных студентом в ходе прохождения практики;
- качество доклада;
- качество оформления отчета;
- умение отвечать на вопросы и вести дискуссию.

Защита отчета по практике проходит в форме доклада с представлением результатов работы в виде презентации.

6.2.2.1.2 Критерии оценивания

Отлично	**Хорошо**	**Удовлетворительно**	**Неудовлетворительно**
От 87 до 100	От 73 до 87	От 60 до 73	Менее 60

6.2.2.2 Семестр 8, дифференцированный зачет

Типовые оценочные средства: Промежуточная аттестация - рейтинг каждого обучающегося по дисциплине определяется от 0 до 100 баллов

6.2.2.2.1 Описание процедуры

Зачет проводится в форме Студент предоставляет оформленный отчет, дневник о прохождении практики, отвечает на вопросы, связанные с работой выполняемой входе прохождения практики.

Оценка знаний, умений, навыков осуществляется по компетенциям. Студент, полностью выполнивший программу производственной практики, получивший положительные отзывы от руководителя практики от организации, где он проходил практику, представляет отчет по производственной практике руководителю практики от университета.

Прием отчета по производственной практике производит комиссия по председательством руководителя производственной от университета или заведующего выпускающей кафедры.

Оценка выполненной работы производится по системе аттестации на основе ответов студента, отзывов руководителей от предприятия, содержания и качества оформления отчета.

Критериями оценки отчета являются:

- уровень теоретического осмысления студентом практической деятельности принимающей организации (ее целей, задач, содержания, методов);
- качество отчета по итогам практики;
- степень и качество приобретенных студентом профессиональных умений;
- уровень профессиональной направленности выводов и рекомендаций, сделанных студентом в ходе прохождения практики;
- качество доклада;
- качество оформления отчета;
- умение отвечать на вопросы и вести дискуссию.

Защита отчета по практике проходит в форме доклада с представлением результатов работы в виде презентации.

6.2.2.2.2 Критерии оценивания

Отлично	Хорошо	Удовлетворительно	Неудовлетворительно

От 87 до 100	От 73 до 87	От 60 до 73	Менее 60

7 Основная учебная литература

1. 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

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

[Сайт] – URL: http://elib.istu.edu/viewer/view.php?file=/files/er-2623.pdf

3. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства : учебное пособие для студентов высш. учеб. заведений , обучающихся по направлению 230100 "Информатика и вычислительная техника" / В. Ф. Шаньгин, 2010. - 542.

4. Технические средства и методы защиты информации : учебное пособие для вузов / А. П. Зайцев [и др.], 2012. - 615.

5. 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.

6. Ищейнов В. Я. Защита конфиденциальной информации : учебное пособие для студентов направления 090103 "Организация и технология защиты информации" и 090104 "Комплексная защита объектов информации" / В. Я. Ищейнов, М. В. Мецатунян, 2011. - 254.

8 Дополнительная учебная литература и справочная

1. 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.

9 Ресурсы сети Интернет

1. http://library.istu.edu/
2. https://e.lanbook.com/
3. http://www.securitylab.ru/
4. http://www.intuit.ru/department/security/pki/
5. http://www.edu.ru

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. Свободно распространяемое программное обеспечение ОС Windows (версия 7 и выше)

2. Свободно распространяемое программное обеспечение MS Office (версия 2007 и выше)

3. Свободно распространяемое программное обеспечение Любая интегрированная среда разработки C/C++ приложений (Borland C++ Builder, Dev-C++, Codeblocks, Deductor Academic)

12 Материально-техническое обеспечение практики

1. Материально-техническое обеспечение научно-исследовательской практики соответствует направлению 10.04.01 «Информационная безопасность» и определяется условиями договора с предприятиями, учреждениями о прохождении научно-исследовательской практики.
Материально – техническое обеспечение лаборатории информационной безопасности ИРНИТУ:
Учебно – научные комплексы: «Обнаружение каналов утечки информации» (ОКУИ) и «Техническая защита от утечки информации по виброакустическим каналам (ТЗУИ), включающих
программно – аппаратные комплексы «Аврора –Т» и «Гриф- АЭ1001», «RS turbo», « RS turbo Mobile L» « RS turbo Mobile 7G», «Спрут – 7» и др., позволяющие осуществить оценку ограждающих конструкций помещения от утечки информации по акустическому, виброакустическому каналам и каналам электроакустических преобразований.