

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»**

**РАБОЧАЯ ПРОГРАММА ПРАКТИКИ
Б2.В.03(Пд) ПРОИЗВОДСТВЕННАЯ (ПРЕДДИПЛОМНАЯ)
ПРАКТИКА**

Направление подготовки: 100301 - Информационная безопасность

Профиль подготовки: Безопасность автоматизированных систем

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

1 АННОТАЦИЯ

1.1 производственная (преддипломная) практика входит в состав практики основной образовательной программы высшего профессионального образования и учебного плана подготовки бакалавров по направлению 100301 – Информационная безопасность, профиля – Информационная безопасность автоматизированных систем”.

Цели, объемы и виды практики определяются ФГОС ВО 10.03.01 «Информационная безопасность», а также Положением о порядке проведения практики студентов Оренбургского государственного аграрного университета.

1.2 Практика проходит в 8 семестре 4 курса и состоит из тесно взаимосвязанных этапов (подготовительного, аналитического, заключительного), предполагающих выдачу индивидуального задания студенту, инструктажа по технике безопасности, консультации научного руководителя, изучения методических рекомендательных материалов, нормативных документов.

2 ВИД ПРАКТИКИ, СПОСОБЫ И ФОРМЫ ЕЕ ПРОВЕДЕНИЯ

2.1 Вид практики: Производственная (преддипломная) практика входит в Блок 2 практики учебного плана.

Основной целью проведения производственной (преддипломной) практики являются закрепление и углубление знаний, полученных студентами в процессе теоретического обучения, получения профессиональных умений и навыков для работы по избранной специальности и защиты выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа бакалавра).

2.2 Проведение практики может осуществляться следующими способами: в качестве стационарной или выездной практики.

Стационарная практика проводится в образовательной организации или ее филиале, в котором обучающиеся осваивают образовательную программу, или в иных организациях, расположенных на территории населенного пункта, в котором расположена образовательная организация или филиал. Выездная практика проводится в том случае, если место ее проведения расположено вне населенного пункта, в котором расположена образовательная организация или филиал.

2.3 Организация проведения учебной практики осуществляется дискретно – по видам практик – путем выделения в календарном учебном графике непрерывного периода учебного времени для проведения каждого вида (совокупности видов) практики.

3 ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

3.1 Взаимосвязь планируемых результатов обучения при прохождении практики (знания, умения, навыки и (или) опыт деятельности) и планируемых результатов освоения образовательной программы (компетенций обучающегося) представлена в таблице 1.

Таблица 1. Взаимосвязь планируемых результатов обучения при прохождении практики и планируемых результатов освоения образовательной программы

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности
(ПК-1) способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	Этап1:- современные аппаратные средства вычислительной техники; Этап 2: современные инструментальные средства и технологии программирования	Этап 1: выполнять работы по настройке аппаратно - программных комплексов Этап 2: выполнять работы по настройке технических средств защиты информации	Этап 1: настройки и обслуживания аппаратно - программных комплексов Этап 2: настройки технических средств защиты информации
(ПК-2) способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Этап 1: основные программные средства для решения задач программирования Этап 2: современные специальные средства для решения задач программирования	Этап 1: разрабатывать программы прикладного значения Этап 2: разрабатывать программы специального значения	Этап 1: применения программных средств системного назначения Этап 2: применения программных средств специального назначения
(ПК-3) способностью администрировать подсистемы информационной безопасности объекта защиты	Этап 1: основные принципы администрирования Этап 2: современные инструментальные средства администрирования	Этап 1: проводить процедуру администрирования подсистемы безопасности Этап 2: уметь использовать инструментальные средства администрирования подсистемы безопасности	Этап 1: навыки администрирования подсистемы безопасности Этап 2: навыки применения инструментальных средств администрирования подсистемы безопасности
(ПК-4) способностью участвовать в работах по реализации политики информационной безопасности, применять	Этап 1основные составляющие политики безопасности Этап 2: принципы разработки политики безопасности	Этап 1: разрабатывать политику безопасности Этап 2: применять комплексный подход к обеспечению	Этап 1: навыки разработки политики безопасности Этап 2применения комплексного подхода к обеспечению

комплексный подход к обеспечению информационной безопасности объекта защиты		информационной безопасности	информационной безопасности
(ПК-5) способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	Этап 1: основные требования безопасности информации к объектам информатизации Этап 2: основные этапы аттестации объектов информатизации по требованиям безопасности информации	Этап 1: разрабатывать требования безопасности информации Этап 2: разрабатывать методику аттестации объектов информатизации	Этап 1: навыки в формировании требований безопасности информации Этап 2: навыки в проведении аттестации объектов информатизации
(ПК-6) способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	Этап 1: основные этапы контрольных проверок технических средств защиты информации Этап 2: основные принципы работы технических средств защиты информации	Этап 1: разрабатывать методику контрольных проверок технических средств защиты информации Этап 2: разрабатывать способы оценки эффективности применения программных, аппаратных средств защиты информации	Этап 1: навыки применения контрольных проверок Этап 2: навыки оценки эффективности применения аппаратно - программных комплексов
(ПК-7) способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Этап 1: основные этапы проектирования подсистемы информационной безопасности Этап 2: основные методы технико – экономического обоснования проектных решений	Этап 1: разрабатывать основные подсистемы безопасности информации Этап 2: проводить технико – экономическое обоснование проектных решений	Этап 1: навыки разработки подсистем информационной безопасности Этап 2: навыки технико - экономического обоснования проектных решений
(ПК-8) способностью оформлять рабочую техническую документацию с	Этап 1: основные этапы оформления рабочей документации	Этап 1: разрабатывать основные рабочие документы	Этап 1: навыки разработки рабочих документов Этап 2: навыки

учетом действующих нормативных и методических документов	Этап 2: основные нормативные и методические документы	Этап 2: применять нормативные документы в рабочей документации	применения нормативных документов
(ПК-9) способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	Этап 1: основные методы поиска научно – технической и нормативной литературы Этап 2: основные методические материалы по вопросам информационной безопасности	Этап 1: осуществлять подбор литературы по информационной безопасности Этап 2: уметь обобщать и составлять краткий обзор литературы по информационной безопасности	Этап 1: осуществления подбора литературы по информационной безопасности Этап 2: умения обобщения и составления обзора литературы по информационной безопасности
(ПК-10) способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Этап 1: методику анализа информационной безопасности Этап 2: современные стандарты в области информационной безопасности	Этап 1: разрабатывать методику анализа информационной безопасности Этап 2: использовать стандарты в области информационной безопасности	Этап 1: разработки анализа информационной безопасности Этап 2: использования стандартов в области информационной безопасности
(ПК-11) способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	Этап 1: методику проведения экспериментов Этап 2: методику обработки, оценки результатов экспериментов	Этап 1: разрабатывать методику проведения экспериментов Этап 2: разрабатывать методику обработки и оценки результатов эксперимента	Этап 1: разработки методики проведения экспериментов Этап 2: разработки методики обработки и оценки результатов эксперимента
(ПК-12) способностью принимать участие в проведении экспериментальных исследований системы защиты информации	Этап 1: методику проведения экспериментов Этап 2: методику обработки, оценки результатов экспериментов	Этап 1: разрабатывать методику проведения экспериментов Этап 2: разрабатывать методику обработки	Этап 1: разработки методики проведения экспериментов Этап 2: разработки методики обработки и оценки

		и оценки результатов эксперимента	результатов эксперимента
(ПК-13) способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Этап 1: основные меры по выполнению обеспечения информационной безопасности Этап 2: основные меры поддержки обеспечения информационной безопасности	Этап 1: разрабатывать меры по обеспечению информационной безопасности Этап 2: разрабатывать меры поддержки по обеспечению информационной безопасности	Этап 1: разработки мер по обеспечению информационной безопасности Этап 2: разработки мер поддержки обеспечения информационной безопасности
(ПК-14) способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	Этап 1: основные меры по выполнению обеспечения информационной безопасности Этап 2: основные меры поддержки обеспечения информационной безопасности	Этап 1: разрабатывать меры по обеспечению информационной безопасности Этап 2: разрабатывать меры поддержки по обеспечению информационной безопасности	Этап 1: разработки мер по обеспечению информационной безопасности Этап 2: разработки мер поддержки обеспечения информационной безопасности
(ПК-15) способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Этап 1: основные компоненты технологического процесса защиты информации Этап 2: современные нормативные и методические документы в области информационной безопасности	Этап 1: организовывать технологический процесс защиты информации Этап 2: применять нормативные и методические документы в области информационной безопасности	Этап 1: организации технологического процесса защиты информации Этап 2: применения нормативных и методических документов в области информационной безопасности
(ПСК4-1) способен	Этап 1: основные	Этап 1:	Этап 1:

учитывать и использовать особенности информационных технологий, применяемых в автоматизированных системах, при организации защиты обрабатываемой в них информации	информационные технологии Этап 2: автоматизированные системы, применяемые при организации защиты информации	разрабатывать и использовать особенности информационных технологий Этап 2: использовать особенности автоматизированных систем при организации системы защиты	использования информационных технологий при организации системы защиты Этап 2: навыки использования особенностей автоматизированных систем при организации системы защиты
(ПСК4-2) способен выполнять комплекс задач администрирования подсистем информационной безопасности операционных систем, систем управления базами данных, компьютерных сетей	Этап 1: основные операционные системы, системы управления базами данных Этап 2: комплекс задач при администрировании подсистем информационной безопасности	Этап 1: выполнять комплекс задач администрирования подсистемы безопасности Этап 2: выполнять комплекс задач по безопасности операционных систем и баз данных	Этап 1: выполнения комплекса задач администрирования подсистем безопасности Этап 2: выполнения администрирования компьютерных сетей по безопасности
(ПСК4-3) способен планировать и организовывать комплекс мероприятий по защите информации, связанных с обеспечением надежности функционирования и отказоустойчивости аппаратных и программных средств обработки информации	Этап 1: основные показатели надежности систем обеспечения информационной безопасности Этап 2: комплекс мер по обеспечению надежности систем обеспечения информационной безопасности	Этап 1: планировать комплекс мер по обеспечению надежности систем безопасности Этап 2: организовывать комплекс мер по обеспечению надежности подсистемы безопасности информации	Этап 1: планирования комплекса мер по обеспечению надежности систем безопасности Этап 2: организации комплекса мер по обеспечению надежности подсистемы безопасности информации
(ПСК4-4) способен участвовать в разработке аппаратных и программных средств в составе автоматизированных систем, связанных с обеспечением информационной безопасности	Этап 1: основные этапы проектирования подсистемы информационной безопасности Этап 2: основные методы технико – экономического обоснования проектных решений	Этап 1: разрабатывать основные подсистемы безопасности информации Этап 2: проводить технико – экономическое обоснование проектных решений	Этап 1: навыки разработки подсистем информационной безопасности Этап 2: навыки технико - экономического обоснования проектных решений

Общая трудоемкость по Учебному плану (пример)	6	216	144	72	24	<i>Дифференцированный зачет</i>	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-10; ПК-13; ПК-15; ПСК-4.1; ПСК-4.2; ПСК-4.3;
1. Подготовительный	1,2	18	12	6	2	-	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-11; ПК-12; ПК-13; ПК-14; ПК-15
2. Аналитический	3,6	180	120	60	20	-	ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-10; ПК-13; ПК-14; ПК-15
3. Заключительный	1,2	18	12	6	2	-	ПК-1; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-7; ПК-8; ПК-9; ПК-10; ПК-11; ПК-12; ПК-13; ПК-14; ПК-15; ПСК-4.1; ПСК-4.2; ПСК-4.3; ПСК-4.4
Вид контроля	дифференцированный зачет						

Примечания:

**Общая трудоемкость практики в зачетных единицах и часах с разделением на часы контактной и самостоятельной работы и заполняется из расчета: 1 зачетная единица включает в себя 24 часов контактной работы и 12 часов самостоятельной работы студента. Учитывать категории студентов.*

***Например: организация практики, подготовительный этап, включающий инструктаж по технике безопасности, производственный (экспериментальный исследовательский) этап, обработка и анализ полученной информации, подготовка отчета по практике.*

5.4 Самостоятельная работа студентов на практике.

Самостоятельная работа студентов на практике заключается в рассмотрении обязательных вопросов и выполнении индивидуального задания.

1. Изучить теоретические аспекты организации технической защиты конфиденциальной информации на объекте.

2. Рассмотреть методики определения эффективности технической защиты конфиденциальной информации.

3. Рассмотреть организационную структуру объекта.

4. Рассмотреть информационные потоки объекта.

5. Проанализировать возможные угрозы и каналы утечки конфиденциальной информации по техническим каналам.

6. Проанализировать существующую систему технической защиты конфиденциальной информации.

7. Провести оценку эффективности системы технической защиты конфиденциальной информации.

5.4.1. Примерный перечень вариантов индивидуальных заданий:

Индивидуальное задание определяется для студента исходя из направления деятельности объекта, на котором студент проходит производственную (преддипломную) практику, согласно договоров и приказов на прохождение производственной (преддипломной) практики.

6. ФОРМЫ ОТЧЕТНОСТИ ПО ПРАКТИКЕ

6.1 По окончании практики обучающийся должен предоставить на кафедру следующие документы не позднее 7 календарных дней с даты начала занятий или окончания практики:

- заполненный рабочий дневник с отзывом (оценкой работы практиканта администрацией и старшим специалистом предприятия). Дневник должен быть заверен подписью ответственного лица и круглой печатью организации;

- отчет по практике. Отчет по практике подписывается обучающимся, проверяется и визируется руководителем практики. Защита отчетов производится в соответствии с установленным графиком защиты отчетов, но не позднее трех месяцев с начала учебного процесса. Нарушение сроков прохождения практики и сроков защиты считается невыполнением учебного плана. По результатам защиты отчетов, а также отзыва с места прохождения практики обучающимся выставляется оценка по практике;

- индивидуальное задание.

7 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ПРАКТИКЕ

7.1 Форма аттестации практики зачет с оценкой.

7.2 Время проведения аттестации согласно графику Календарного учебного плана.

7.3 Зачет получает обучающийся, прошедший практику, представивший соответствующую документацию рабочий дневник с отзывом с места прохождения практики, отчет по практике и успешно защитивший его.

7.4 Описание системы оценок.

По итогам защиты отчета студенту выставляется дифференцированный зачет с учетом указанных ниже критериев.

По итогам защиты отчета студенту выставляется дифференцированный зачет с учетом указанных ниже критериев:

Общая оценка выставляется на титульном листе работы, в экзаменационной ведомости и зачетной книжке студента. Для студентов очного отделения критерием успешности освоения учебного материала является экспертная оценка преподавателя, учитывающая регулярность посещения учебных занятий, знаний теоретического раздела программы и выполнение установленных на данный семестр требований технической подготовки.

Итоговый контроль – дифференцированный зачет получает студент прошедший практику, имеющий отчет со всеми отметками о выполнении.

Студенты, не выполнившие программу практики по уважительной причине, направляются на практику вторично, в свободное от учебы время, либо практика переносится на следующий год с оформлением соответствующего приказа.

Студенты, не выполнившие программу практики без уважительной причины, или получившие отрицательный результат отчисляются из Университета, как имеющие академическую задолженность в порядке, предусмотренном Уставом ВУЗа.

7.4.1 По результатам прохождения практики начисляется максимум 100 баллов

7.4.2 Критерии балльно-рейтинговой оценки результатов прохождения обучающимися практики формируются на кафедре «Автоматизированные системы обработки информации и управления», за которой закреплена дисциплина. Перечень критериев зависит от специфики практики.

Основные критерии:

- полнота представленного материала, выполнение индивидуального задания, соответствующие программе практики – до 50 баллов;
- своевременное представление отчета, качество оформления – до 20 баллов;
- защита отчета, качество ответов на вопросы – до 30 баллов.

Форма фиксации с вариантом критериев представлена в таблице 4.

Таблица 4. Структура формирования балльно-рейтинговой оценки результатов прохождения обучающимися практики.

№	Критерии оценок	Баллы
1	полнота представленного материала, выполнение индивидуального задания	25
2	соответствие представленных результатов программе практики	25
3	своевременное представление отчета	10
4	качество оформления отчета	10
5	доклад по отчету	20
6	качество ответов на дополнительные вопросы	10
	ИТОГО	100

7.4.3 Структура формирования балльно-рейтинговой оценки прохождения обучающимися практики определяется ведущим преподавателем, рассматривается и одобряется на заседании кафедры, утверждается в установленном порядке в составе программы практики.

7.4.4 Система оценок представлена в таблице 5.

Таблица 5. Система оценок

Диапазон оценки в баллах	европейская шкала (ECTS)	традиционная шкала	Зачет
[95; 100]	A - (5+)	отлично – (5)	зачтено
[85; 95]	B - (5)		
[70; 85]	C – (4)	хорошо – (4)	
[60; 70]	D – (3+)	удовлетворительно – (3)	не зачтено
[50; 60]	E – (3)		
[33,3; 50]	FX – (2+)	неудовлетворительно – (2)	
[0; 33,3)	F – (2)		

7.4.5 Прохождение всех этапов практики (выполнение всех видов работ) является обязательным. Набранный высокий балл за один из этапов практики, обучающийся не освобождается от прохождения других этапов.

7.4.6 Оценочные материалы для проведения промежуточной аттестации обучающихся по практике (представлен в отдельном документе).

8 ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ И РЕСУРСОВ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

8.1.1 Основная литература

8.1.1 Основная литература

1. Назаров С.В. Современные операционные системы [Электронный ресурс]/ Назаров С.В., Широков А.И.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 351 с.

2. Сычев А.В. Перспективные технологии и языки веб-разработки [Электронный ресурс]/ Сычев А.В.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 493 с.

8.1.2 Дополнительная литература и Интернет-ресурсы

1. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2014.— 702 с.

2. Герасименко В.А., Малюк А.А. Основы защиты информации. [Электронный ресурс]/ Герасименко В.А М. .— Электрон. текстовые данные -: "Инкомбук", 1997. - 540с.

8.1.3 Методические указания и материалы по практике, в т. ч. методические материалы, в которых содержится форма отчетности по практике (указывать собственные кафедральные разработки).

1. Урбан В.А. Методические указания по подготовке и оформлению отчета по производственной (преддипломной) практике для студентов по направлению подготовки 10.03.01 «Информационная безопасность» профиля «Информационная безопасность автоматизированных систем».

8.1.4 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. <http://e.lanbook.com/> - ЭБС

2. <http://rucont.ru/> - ЭБС

3. <http://elibrary.ru/defaultx.asp> - ЭБС

4. <http://www.iprbookshop.ru>- ЭБС

5. <http://www.edu.ru/> - федеральный портал российского образования. Нормативные материалы по образованию, учебно-методические материалы и ресурсы по всем направлениям, специальностям.

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕДЕНИИ ПРАКТИКИ

MS Windows

MS Office

Open Office

Базы данных, информационно-справочные и поисковые системы:

1. Консультант плюс;

2. Гарант

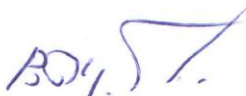
10 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

А Материально – техническое обеспечение преддипломной практики определяется местом, где она проходит и соответственно материально – технической обеспеченностью организации, где проходит практику студент.

Для материально - технического обеспечения производственной (преддипломной) практики студентов используется компьютерная техника, мультимедийное и копировально-множительное оборудование, библиотечно-информационные ресурсы, имеющиеся в распоряжении института управления рисками и комплексной безопасности.

Программа разработана в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденным приказом Министерства образования и науки РФ от 01.12.2016г. № 1515.

Разработал:



Урбан В.А.