ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА СВОЙ ПРАКТИКИ

Б2.В.01(ПД) ПРОИЗВОДСТВЕННАЯ (ПРЕДДИПЛОМНАЯ) ПРАКТИКА

Направление подготовки (специальность) 10.03.01 Информационная безопасность

Профиль подготовки (специализация) 10.03.01 Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)

Квалификация выпускника бакалавр

Форма обучения очная

1. АННОТАЦИЯ

1.1 Производственная (преддипломная) практика (далее по тексту – практика) входит в состав практики основной профессиональной образовательной программы высшего образования (далее по тексту ОПОП ВО) и учебного плана подготовки бакалавров по направлению подготовки/специальности 10.03.01 Информационная безопасность профилю подготовки/специализации Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности).

1.2 Практика проходит в 4 курсе(ах) в 8 семестре(ах). и состоит из:

1. Ознакомление со структурой и работой основных подразделений предприятия, лицензией и уставом, решаемыми задачами, наличием документов разрешающих основные виды деятельности

2. Ознакомление со структурой органов защиты информации. Ознакомление с видами угроз безопасности информации, характерными для предприятия

3. Ознакомление с видами, методами, средствами информационной защиты, применяемыми на предприятии

2. Вид и тип практики, способы и формы ее проведения

2.1 Тип практики: .

Основными целями 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 Способы проведения практики: выездная.

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. Выездная практика может проводится в полевой форме в случае необходимости создания специальных условий для ее проведения.

2.3 Формы проведения практики: непрерывно – путем выделения в календарном учебном графике непрерывного периода учебного времени для проведения всех видов практик, предусмотренных образовательной программой

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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине (модулю)

ПК-1 Способен составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	ПК-1.1 Разрабатывает предложения по совершенствованию системы управления защиты информации автоматизированных систем	*Знать:* основные меры по выполнения обеспечения информационной безопасности *Уметь:* разрабатывать меры по обеспечению информационной безопасности *Владеть:* навыками разработки мер поддержки обеспечения информационной безопасности
	ПК-1.2 Применяет технические средства контроля эффективности мер защиты информации	*Знать:* основные этапы контрольных проверок технических средств защиты информации *Уметь:* разрабатывать методику контрольных проверок технических средств защиты информации *Владеть:* навыками применения контрольных проверок

ПК-2 Способен администрировать средства защиты информации в компьютерных системах и сетях	ПК-2.1 Осуществляет выбор и настройку средств защиты информации в компьютерных системах и сетях	*Знать:* об установке, настройке, обслуживании, диагностике, эксплуатации подсистем управления информационной безопасностью объекта защиты *Уметь:* принимать участие в установке, настройке, обслуживании, диагностике, эксплуатации подсистем управления информационной безопасностью объекта защиты *Владеть:* способностью принимать участие в установке, настройке, обслуживании, диагностике, эксплуатации подсистем управления информационной безопасностью объекта защиты
ПК-3 Способен анализировать и противодействовать угрозам информации операционных систем, систем управления базами данных, вычислительных сетей	ПК-3.1 Выявляет потенциальные угрозы	*Знать:* источники угроз безопасности информации и меры по их предотвращению *Уметь:* классифицировать потенциальные угрозы безопасности информации *Владеть:* комплексом мер по информационной безопасности

ПК-3 Способен анализировать и противодействовать угрозам информации операционных систем, систем управления базами данных, вычислительных сетей	ПК-3.2 Разрабатывает меры противодействия потенциальным угрозам	*Знать:* источники угроз безопасности информации и меры по их предотвращению *Уметь:* классифицировать защищаемую информацию по видам тайны и степеням секретности *Владеть:* методами разработки компонентов по обеспечению информационной безопасности объекта защиты
ПК-4 Способен оценивать последствия от реализации угроз безопасности информации в автоматизированной системе	ПК-4.1 Оценивает информационные риски в автоматизированных системах	*Знать:* основные методики анализа угроз и рисков информационной безопасности *Уметь:* анализировать угрозы и проводить риск-анализ и реализовывать методики управления рисками с целью обеспечения безопасности объектов информатизации *Владеть:* технологиями обеспечения информационной безопасности в части проведения риск-анализа и управления риска
	ПК-4.2 Способен классифицировать и оценивать угрозы безопасности информации	*Знать:* источники и классификацию угроз информационной безопасности *Уметь:* классифицировать и оценивать угрозы информационной безопасности *Владеть:* способностью классифицировать и оценивать угрозы безопасности информации

ПК-4 Способен оценивать последствия от реализации угроз безопасности информации в автоматизированной системе	ПК-4.3 Определяет подлежащие защите информационные ресурсы автоматизированных систем	*Знать:* состав и принципы работы автоматизированных систем *Уметь:* осуществлять настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем *Владеть:* навыками определения и настройка компонентов систем защиты информации автоматизированных (информационных) систем
	ПК-4.4 Применяет нормативные документы по противодействию технической разведки	*Знать:* основные руководящие и нормативные документы в сфере инженерно-технической защите информации *Уметь:* использовать основные руководящие и нормативные документы в сфере инженерно-технической защите информации *Владеть:* навыками работы с профессиональными аппаратными средствами инженерно-технической защиты информации
ПК-5 Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	ПК-5.1 Применяет существующие методики для аттестации объектов информатизации	*Знать:* основные понятия информационной безопасности *Уметь:* разрабатывать политику информационной безопасности на аттестуемых объектах *Владеть:* методами разработки политики информационной безопасности на аттестуемых объектах

ПК-6 Способен проводить анализ рисков информационной безопасности автоматизированной системы	ПК-6.1 Проводит оценку рисков информационной безопасности на основе существующих методик	*Знать:* методики оценки риска и управления рисками, а также тестирования средств обеспечения информационной безопасности *Уметь:* анализировать угрозы и оценивать риски информационной безопасности с целью обеспечения безопасности объектов информатизации *Владеть:* средствами обеспечения информационной безопасности, анализа угроз, риск-анализа и управления рисками
ПК-7 Способен разрабатывать комплекс мероприятий по защите информации в автоматизированных системах финансовых и экономических структур	ПК-7.1 Учитывает и использует правовые нормы реализации профессиональной детельности в облсти обеспечения инфрмационной безопсности и защиты интересов личности , обества и государства	*Знать:* технологии и нормы обеспечения информационной безопасности *Уметь:* обеспечивать информационную безопасность при интеграции в государственную и международную информационную среду *Владеть:* способами практического обеспечения норм информационной безопасности при интеграции в государственную и международную информационную среду

ПК-7 Способен разрабатывать комплекс мероприятий по защите информации в автоматизированных системах финансовых и экономических структур	ПК-7.2 Реализует комплекс мероприятий по защите информации в автоматизированных системах финансовых и экономических структур	*Знать:* принципы организации информационных систем в соответствии с требованиями по защите информации *Уметь:* осуществлять меры противодействия нарушениям информационной безопасности *Владеть:* навыками безопасного использования технических сред
ПК-8 Способен проводить анализ информационной безопасности объектов и систем на соответсвие требований стандартов и нормативно-правовых актов в области информационной безопасности	ПК-8.1 Применяет стандарты и нормативно-правовые акты в области информационной безопасности	*Знать:* правила и нормативные требования к оформлению технической документации с учетом действующих методических документов *Уметь:* применять действующие нормативные и методические документы в области информационной безопасности *Владеть:* навыками оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов
ПК-9 Способен применять технические средства защиты информации на основе знаний физических законов	ПК-9.1 Выявляет технические каналы утечки на основе знаний физических законов	*Знать:* основные способы физической защиты объектов информатизации *Уметь:* применять инженерно-технические средства физической защиты объектов информатизации *Владеть:* навыками применения основных типов технических средств защиты информации

ПК-9 Способен применять технические средства защиты информации на основе знаний физических законов	ПК-9.2 Осуществляет сбор и анализ исходных данных для расчета и проектирования радиоэлектронных устройств и систем	*Знать:* принцип работы *Уметь:* самостоятельно проектировать *Владеть:* навыками осуществлять сбор и анализ исходных данных для расчета и проектирования
ПК-10 Способен разрабатывать компьютерные модели исследуемых процессов и систем и применять их для определения оптимальных вариантов проектных, конструкторских и технологических решений	ПК-10.1 Использует современное программное обеспечение в области разработки компьютерной графики	*Знать:* понятийный аппарат (используемые термины и определения) современной сферы компьютерной графики *Уметь:* создавать и редактировать изображения в специализированных программах обработки графической информации *Владеть:* методами использования информационных технологий для решения задач компьютерной графики
ПК-11 Способен участвовать в проектировании системы управления информационной безопасностью	ПК-11.1 Осуществляет проектирование средств защиты информации автоматизированных систем	*Знать:* методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации *Уметь:* применять программные и программно-аппаратные средства для защиты информации в базах данных *Владеть:* навыками обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами

4. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОПОП

Требования к предшествующим знаниям представлены в таблице 2. Перечень дисциплин, для которых практика «Производственная (преддипломная) практика» является основополагающей, представлен в табл. 3.

Таблица 2. – Требования к пререквизитам практики

Компетенция	Дисциплина/Практика
ПК-1	Основы защиты АИС КОИБАС Информационная безопасность значимых объектов критической информационной инфраструктуры (КИИ)
ПК-2	Основы защиты АИС Безопасность вычислительных сетей Безопасность информации в банковских системах
ПК-3	Безопасность вычислительных сетей Безопасность операционных систем КОИБАС Информационная безопасность значимых объектов критической информационной инфраструктуры (КИИ)
ПК-4	Аудит информационной безопасности КОИБАС Системы реального времени Маркетинг
ПК-5	Аудит информационной безопасности
ПК-6	Аудит информационной безопасности КОИБАС Информационная безопасность значимых объектов критической информационной инфраструктуры (КИИ) Системы реального времени Маркетинг
ПК-7	Безопасность информации в банковских системах
ПК-8	Стандарты информационной безопасности Основы защиты АИС
ПК-9	Безопасность информации в банковских системах
ПК-10	SQL-программирование Операционная система FreeBSD

Таблица 3 – Требования к постреквизитам практики

Компетенция	Дисциплина/Практика
ПК-1	Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра) Безопасность систем баз данных Информационная безопасность значимых объектов критической информационной инфраструктуры (КИИ) КОИБАС
ПК-2	Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра)

ПК-3	Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра) Безопасность систем баз данных Информационная безопасность значимых объектов критической информационной инфраструктуры (КИИ) КОИБАС
ПК-4	Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра) КОИБАС
ПК-5	Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра)
ПК-6	Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра) Информационная безопасность значимых объектов критической информационной инфраструктуры (КИИ) КОИБАС
ПК-7	Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра)
ПК-8	Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра)
ПК-9	Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра)
ПК-10	Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра)
ПК-11	Подготовка к процедуре защиты и защита выпускной квалификационной работы (работа бакалавра)

5. ОБЪЕМ, ПРОДОЛЖИТЕЛЬНОСТЬ И СОДЕРЖАНИЕ ПРАКТИКИ

5.1 Время проведения практики согласно - календарного учебного графика.

5.2 Продолжительность практики составляет 4 недель.

5.3 Общая трудоёмкость учебной/производственной практики составляет 6 зачетных единиц.

Распределение по разделам/этапам практики, видам работ, форм текущего контроля с указанием номера осваиваемой компетенции в соответствии с ОПОП приведено в таблице 4.

Таблица 4. Распределение по разделам/этапам практики, видам работ, форм текущего контроля

Разделы (этапы) практики	Трудоёмкость					Результаты	
	Зач.ед.	Часов			Кол-во дней	форма текущего контроля	Коды формируемых компетенций, код индикатора достижения компетенции
		всего	контактная работа	Выполнение инд. задания			
Общая трудоемкость по учебному плану	6	216	144	72			

1. Ознакомление со структурой и работой основных подразделений предприятия, лицензией и уставом, решаемыми задачами, наличием документов разрешающих основные виды деятельности		72	48	24			ПК-1.1, ПК-1.2, ПК-2.1, ПК-3.1, ПК-3.2, ПК-4.1, ПК-4.2, ПК-4.3, ПК-4.4, ПК-5.1, ПК-6.1, ПК-7.1, ПК-7.2, ПК-8.1, ПК-9.1, ПК-9.2, ПК-10.1, ПК-11.1
2. Ознакомление со структурой органов защиты информации. Ознакомление с видами угроз безопасности информации, характерными для предприятия		72	48	24			ПК-1.2, ПК-2.1, ПК-4.1, ПК-4.3, ПК-4.4, ПК-5.1, ПК-7.1, ПК-7.2, ПК-9.2, ПК-10.1, ПК-11.1
3. Ознакомление с видами, методами, средствами информационной защиты, применяемыми на предприятии		72	48	24			ПК-1.2, ПК-2.1, ПК-3.1, ПК-3.2, ПК-4.1, ПК-4.3, ПК-8.1, ПК-9.1, ПК-9.2, ПК-10.1, ПК-11.1, ПК-6.1
Вид контроля	Зачет с оценкой						

5.3 Выполнение индивидуального задания студентов на практике.

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.

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 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 практики 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 с 11.05.2022 г. по 31.05.2022 г.

7.3 Зачет получает обучающийся, прошедший практику, представивший Отчет, Рабочий дневник и успешно защитивший отчет по практике.

7.4 Описание системы оценок.

7.4.1 По результатам прохождения практики начисляется максимум 100 балов.

7.4.2 Критерии балльно-рейтинговой оценки результатов прохождения обучающимися практики формируются на кафедре, 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 возможным вариантом критериев представлена в таблице 5.

Таблица 5. 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 6.

Таблица 6. 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)	
[50; 60)	E– (3)		незачтено
[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. Набрав высокий балл за один из этапов практики, обучающийся не освобождается от прохождения других этапов.

7.4.6 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по практике.

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

8.1.1 Основная учебная литература, необходимая для освоения дисциплины

Преддипломная практика : методические указания / составители Н. А. Савельева, И. Ю. Столярова. — Сочи : СГУ, 2017. — 48 с. — Текст : электронный // Лань : электронно-библиотечная система.

8.1.2 Дополнительная учебная литература, необходимая для освоения дисциплины

1. Андреев, Н. Н. Методические указания по прохождению производственной (преддипломной) практики для студентов, обучающихся по специальности СПО 35.02.06 Технология производства и переработки сельскохозяйственной продукции : методические указания / Н. Н. Андреев. — Ульяновск : УлГАУ имени П. А. Столыпина, 2020. — 36 с. — Текст : электронный // Лань : электронно-библиотечная система.
2. Прока, Н. И. Учебно-методическое пособие по организации и проведению производственной преддипломной практики для обучающихся направления подготовки 38.04.02 Менеджмент профиль подготовки «Управление человеческими ресурсами» : учебно-методическое пособие / Н. И. Прока, Е. И. Ловчикова. — Орел : ОрелГАУ, 2021. — 66 с. — Текст : электронный // Лань : электронно-библиотечная система.
3. Шуткина, Ж. А. Учебно-методические рекомендации по организации практик : учебно-методическое пособие / Ж. А. Шуткина, Т. В. Маркелова, А. В. Барсуков. — Нижний Новгород : ННГУ им. Н. И. Лобачевского, 2018. — 81 с. — Текст : электронный // Лань : электронно-библиотечная система.

8.1.3 Методические материалы для обучающихся по освоению дисциплины

Тематическое содержание дисциплины

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕДЕНИИ ПРАКТИКИ

9.1 Комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

1. JoliTest (JTRun, JTEditor, TestRun)
2. MS Office

9.2 Современные профессиональные базы данных и информационно-справочные системы

1. Консультант+

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

- нормативно-правовая документация
- комплект бланков проектной документации;
- комплект учебно-методической документации;
- наглядные пособия.
- компьютер,
- принтер,
- сканер,
- модем (спутниковая система),
- программное обеспечение общего и профессионального назначения

Программа разработана в соответствии с Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

Разработал(и):

Заведующий кафедрой,к.т.н. _____ Урбан Владимир Александрович

Рабочая программа рассмотрена и одобрена на заседании кафедры Техносферной и информационной безопасности, протокол № 6 от 17.01.2021 г.

Зав. кафедрой _____ Урбан Владимир Александрович

Программа рассмотрена и утверждена на заседании Ученого совета Института управления рисками и комплексной безопасности, протокол № 7 от 22.02.2021 г.

Директор Института управления рисками и комплексной безопасности

_____ Яковлева Евгения Васильевна