ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМ. И.А. БУНИНА

«УТВЕРЖДАЮ»
Директор института математики, естествознания и техники
_____/Н.В.Черноусова/

ПРОГРАММА

Б2.О.01(П) ТЕХНОЛОГИЧЕСКАЯ ПРАКТИКА

Направление подготовки: *10.03.01 Информационная безопасность*
Направленность (профиль): *Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)*
Квалификация (степень): *бакалавр*
Форма обучения: *очная*

Институт: математики, естествознания и техники
Кафедра: математического моделирования, компьютерных технологий и информационной безопасности

Формы обучения	очная форма	очно-заочная форма	заочная форма
Курс	**4**		
Семестр / триместр	**7**		
Форма отчетности	***зачет с оценкой – 0,2***		
Контактная работа	**2**		
Самостоятельная работа	**322**		

Всего часов: 324
Трудоемкость: 9 зачетных единиц.

Разработчик программы:
к.т.н, доцент кафедры ММКТиИБ, Петров А.А.

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

1.1. Вид практики (в соответствии с ФГОС ВО):

Производственная

1.2. Тип практики:

Технологическая

1.3. Цель практики:

подготовка к решению производственных задач предприятия, закрепление и углубление теоретических знаний в области управления техническими системами на базе современных информационных технологий, программно-аппаратных средств защиты информации, приобретение практического опыта и навыков научной и производственной работы.

1.4. Задачи практики:

Ознакомление:

- со структурными и функциональными схемами предприятия, организацией деятельности подразделения;
- с организацией IT-инфраструктуры предприятия;
- с процессом проектирования и эксплуатации программно-технических комплексов в сфере информационной безопасности.

Изучение и приобретение практических навыков в области:

- порядка и методов ведения делопроизводства;
- методов проектирования и эксплуатации программно-технических комплексов и информационных систем в сфере информационной безопасности;
- методов организации мероприятий по защиты сетей и систем передачи данных.

Сбор материалов для написания выпускной квалификационной работы.

1.5. Способы проведения практики: стационарная.

1.6. Формы проведения практики: дискретная.

1.7. Перечень планируемых результатов обучения при прохождении практики, соотнесенных с планируемыми результатами освоения образовательной программы.

В результате прохождения практики у обучающихся формируются следующие компетенции:

универсальные (УК):

- способностью осуществлять социальное взаимодействие и реализовывать свою роль в команде (УК-3);

общепрофессиональные (ОПК):

- способностью применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности (ОПК-5, ОПК-10, ОПК-2.1).

Планируемые результаты прохождения практики

Код формируемой компетенции	Знать	Уметь	Владеть

по ОПОП ВО			
УК-3	- стратегии сотрудничества для достижения поставленной цели; - особенности поведения разных групп людей, с которыми работает/взаимодействует.	- определять свою роль в команде. - устанавливать разные виды коммуникации (учебную, деловую, неформальную и др.); - оценивать последствия личных действий и планировать последовательность шагов для достижения заданного результата.	- навыками эффективного взаимодействия с другими членами команды, в т.ч. участия в обмене информацией, знаниями и опытом, в презентации результатов работы команды.
ОПК-5	- основные нормативно-правовые акты и иные документы, регламентирующие деятельность по защите информации; - организационно-управленческие методы и инструментарий, обеспечивающие деятельность по защите информации в сфере профессиональной деятельности.	- использовать нормативно-правовые документы, связанные с обеспечением профессиональной деятельности на объектах защиты; - обосновывать организационно-управленческие решения в области обеспечения информационной безопасности систем, подлежащих информационной защите.	- навыками аналитической работы с нормативно-правовыми документами, в частности с нормативной базой РФ, в сфере профессиональной деятельности на конкретных объектах защиты; - методами разработки проектов нормативных и организационно-распорядительных документов для конкретных объектов защиты.
ОПК-10	- принципы реализации, развития и совершенствования систем обеспечения информационной безопасности предприятия в рамках комплексного подхода; - структуру политики информационной безопасности; - основные технические методы и принципы управления информационной безопасностью предприятий отрасли.	- определять комплекс мер (правила, процедуры, практические приемы, руководящие методы, принципы, средства) для обеспечения информационной безопасности информационных систем; - разрабатывать политику информационной безопасности объекта защиты; - применять на практике основные механизмы управления информационной безопасностью на объекте защиты.	- навыками планирования и организации системы защиты информации; - навыками реализации элементов политики информационной безопасности; - методами организации и управления деятельностью служб защиты информации на предприятии.

ОПК-2.1	- модели информационных угроз и нарушителей, методики оценки рисков реализации угроз при функционировании объекта защиты; - принципы обеспечения безопасности объекта защиты и его информационных составляющих, оценки предполагаемого ущерба.	- строить частные модели защиты от угроз информационной безопасности предприятия; - выстраивать траектории и определять необходимый инструментарий с целью выявления возможных источников информационных угроз и предполагаемого ущерба от них.	- способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; - методиками построения частной модели защиты от информационных угроз.

1.8. Место практики в структуре основной образовательной программы высшего образования (ОПОП ВО):

Шифр дисциплины в учебном плане Б2.О.01(П)

Технологическая практика для обучающихся направления 10.03.01 Информационная безопасность (профиль Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)) входит в вариативную часть блока Б2 Практика учебного плана и проходит в 7 семестре.

Технологическая практика базируется на знаниях, умениях и навыках обучающихся, полученных ими при изучении следующих дисциплин:

Введение в специальность
Архитектура электронно-вычислительных машин и систем
Безопасность операционных систем
Компьютерная графика
Техническая защита информации
Защита информации от утечки по техническим каналам
Теория информации и кодирования
Базы данных
Защита информации в компьютерных сетях
Информационная безопасность GPRS и IP телефонии
Защита и обработка конфиденциальных документов,

а также на знаниях, умениях и навыках, полученных в ходе учебной практики по получению первичных навыков научно-исследовательской работы.

Знания, умения и навыки, полученные в процессе технологической практики, являются необходимой основой для последующего прохождения преддипломной практики, а также успешного написания выпускной квалификационной работы.

1.9. Объем практики в зачетных единицах и ее продолжительность в неделях либо академических или астрономических часах:

Объем практики – 9 зачетных единиц.
Продолжительность практики – 6 недель.

1.10. Объем контактной работы в часах и её продолжительность в неделях:

Объем контактной работы – 2 ч.
Продолжительность контактной работы – 6 недель.
Контактная работа включает групповые консультации, а также проведение аттестации по практике.

II. СОДЕРЖАНИЕ ПРАКТИКИ

2.1. Содержание заданий, раскрывающих основные виды деятельности обучающихся во время прохождения практики:

При прохождении практики обучающиеся получают опыт проектирования информационных систем, технологий и их элементов, проводят анализ программных продуктов по обеспечению заданного уровня безопасности и требуемого качества обслуживания, разрабатывают техническую документацию с учетом действующих нормативных и методических документов.

Индивидуальные задания на весь период технологической практики предлагаются каждому студенту его научным руководителем и руководителем от предприятия, исходя из специфики деятельности предприятия, согласуются с руководителем практики от университета.

Перед прохождением практики студент заполняет календарный план, согласованный с групповым руководителем, с непосредственным руководителем практики от предприятия и руководителем ВКР. В течение практики учащийся обязан вести дневник, отражающий основные виды выполняемых работ с указанием времени.

Студенты в ходе технологической практики могут выполнять следующие виды деятельности:

1. *Проектно-конструкторская деятельность*: определение целей проектирования, критериев эффективности, ограничений применимости; системный анализ объекта проектирования; выбор исходных данных для проектирования; разработка обобщенных вариантов решения проблемы, прогнозирование последствий, нахождение компромиссных решений в условиях многокритериальности и неопределенности, планирование реализации проекта; оценка надежности и качества функционирования объекта проектирования; расчет экономической эффективности; разработка, согласование и выпуск всех видов проектной документации.
2. *Технологическая деятельность*: технология разработки объектов профессиональной деятельности, составление технологических программ и алгоритмов, технологическое обеспечение производственных процессов на предприятии, организации.
3. *Эксплуатационная деятельность:* организация внедрения объекта проектирования в опытную эксплуатацию; организация внедрения объекта проектирования в промышленную эксплуатацию.

По результатам производственной практики студент составляет отчет о прохождении практики в соответствии с планом-заданием, свидетельствующий о закреплении знаний, умений, приобретении практического опыта, освоении профессиональных компетенций.

III. ФОРМЫ ОТЧЕТНОСТИ ПО ПРАКТИКЕ

3.1. Формы отчетности по итогам практики:

Студенты обязаны пройти практику в сроки в соответствии с календарным учебным графиком, своевременно и полностью выполнить программу практики и сдать отчетные документы:

1. *Индивидуальное задание по технологической практике;*
2. *Дневник технологической практики;*

3. *Отчет по практике, имеющий следующую структуру:*

Титульный лист.

Содержание.

Введение. Во введении указывается наименование организации, где студент проходил практику, подразделение, выполняемая работа, руководитель практики от организации.

1. Описание предприятия (организации).

1.1. Описание деятельности предприятия (организации).

1.2. Организационная структура предприятия (организации) и описание деятельности отдела.

1.3. Особенности технологического процесса обработки информации.

1.4. Обоснование технологических решений.

2. Технологический раздел.

2.1. Техническое задание по проекту.

2.2. Описание проектируемого объекта и построение модели данных.

2.3. Функциональные характеристики проектируемого объекта.

2.4. Рекомендации по совершенствованию проекта.

Заключение. В заключении подводятся итоги технологической практики.

Список использованных источников.

Приложения.

4. *Отзыв руководителя практики от организации, подписанный и заверенный печатью;*
5. *Отзыв научного руководителя, составленный на основе данных о научно-исследовательской деятельности студента.*

IV. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ПРАКТИКЕ

4.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ №	Код контролируемой компетенции (или ее части) и ее формулировка	Контролируемые разделы (этапы) практики	Наименование оценочного средства
1	**Знать:** - стратегии сотрудничества для достижения поставленной цели; особенности поведения разных групп людей, с которыми работает/взаимодействует; основные нормативно-правовые акты и иные документы, регламентирующие деятельность по защите информации (УК-3); - основные нормативно-правовые акты и иные документы, регламентирующие деятельность по защите информации; организационно-управленческие методы и инструментарий, обеспечивающие деятельность по защите информации в сфере профессиональной деятельности (ОПК-5).	Подготовительный этап: установочная конференция, вводный инструктаж по месту проведения практики.	Рабочий план-график

	- принципы реализации, развития и совершенствования систем обеспечения информационной безопасности предприятия в рамках комплексного подхода; структуру политики информационной безопасности; основные технические методы и принципы управления информационной безопасностью предприятий отрасли (ОПК-10). - модели информационных угроз и нарушителей, методики оценки рисков реализации угроз при функционировании объекта защиты; принципы обеспечения безопасности объекта защиты и его информационных составляющих, оценки предполагаемого ущерба (ОПК-2.1).		
2	**Уметь:** - определять свою роль в команде; устанавливать разные виды коммуникации (учебную, деловую, неформальную и др.); оценивать последствия личных действий и планировать последовательность шагов для достижения заданного результата (УК-3); - использовать нормативно-правовые документы, связанные с обеспечением профессиональной деятельности на объектах защиты; обосновывать организационно-управленческие решения в области обеспечения информационной безопасности систем, подлежащих информационной защите (ОПК-5). - определять комплекс мер (правила, процедуры, практические приемы, руководящие методы, принципы, средства) для обеспечения информационной безопасности информационных систем; разрабатывать политику информационной безопасности объекта защиты; применять на практике основные механизмы управления информационной безопасностью на объекте защиты (ОПК-10). - определять комплекс мер (правила, процедуры, практические приемы, руководящие методы, принципы, средства) для обеспечения информационной безопасности информационных систем; разрабатывать политику информационной безопасности объекта защиты; применять на практике основ-	Основной этап: - выполнение индивидуального задания и поручений руководителя практики; - проведение работ по установке, настройке и испытаниям защищенных технических средств обработки информации; - проведение работ по техническому обслуживанию защищенных технических средств обработки информации; - сбор материалов, необходимых для выполнения выпускной квалификационной работы.	Выполненные типовые задания

	ные механизмы управления информационной безопасностью на объекте защиты (ОПК-2.1).		
3	**Владеть:** - навыками эффективного взаимодействия с другими членами команды, в т.ч. участия в обмене информацией, знаниями и опытом, в презентации результатов работы команды (УК-3). - навыками аналитической работы с нормативно-правовыми документами, в частности с нормативной базой РФ, в сфере профессиональной деятельности на конкретных объектах защиты; - методами разработки проектов нормативных и организационно-распорядительных документов для конкретных объектов защиты (ОПК-5). - навыками планирования и организации системы защиты информации; навыками реализации элементов политики информационной безопасности; методами организации и управления деятельностью служб защиты информации на предприятии (ОПК-10). - способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; методиками построения частной модели защиты от информационных угроз (ОПК-2.1).	Заключительный этап: - итоговая конференция; защита отчета по практике.	Дневник технологической практики. Отчет по практике. Отзыв руководителя практики от организации. Отзыв научного руководителя. Грамоты, сертификаты, патенты, тезисы выступлений на конференции, подготовленные к публикации статьи.

4.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Результаты (освоенные компетенции)	**Контролируемые разделы (этапы) практики**	**Основные показатели оценки результата**	**Критерии оценивания компетенций**
УК-3, ОПК-5, ОПК-10, ОПК-2.1	Подготовительный этап: установочная конференция, вводный инструктаж по месту проведения практики.	Оформление индивидуального плана-задания	**Знает:** - стратегии сотрудничества для достижения поставленной цели; особенности поведения разных групп людей, с которыми работает/взаимодействует; основные нормативно-правовые акты и иные документы, регламенти-

			рующие деятельность по защите информации (УК-3); - основные нормативно-правовые акты и иные документы, регламентирующие деятельность по защите информации; организационно-управленческие методы и инструментарий, обеспечивающие деятельность по защите информации в сфере профессиональной деятельности (ОПК-5). - принципы реализации, развития и совершенствования систем обеспечения информационной безопасности предприятия в рамках комплексного подхода; структуру политики информационной безопасности; основные технические методы и принципы управления информационной безопасностью предприятий отрасли (ОПК-10). - модели информационных угроз и нарушителей, методики оценки рисков реализации угроз при функционировании объекта защиты; принципы обеспечения безопасности объекта защиты и его информационных составляющих, оценки предполагаемого ущерба (ОПК-2.1).
УК-3, ОПК-5, ОПК-10, ОПК-2.1	Основной этап: - выполнение индивидуального задания и поручений руководителя практики; - проведение работ по установке, настройке и испытаниям защищенных технических средств обработки информации; - проведение работ по техническому обслуживанию защищенных технических средств обработки информации;	Выполнены типовые задания и поручения руководителя практики; осуществлен сбор материалов, необходимых для выполнения выпускной квалификационной работы.	**Умеет:** - определять свою роль в команде; устанавливать разные виды коммуникации (учебную, деловую, неформальную и др.); оценивать последствия личных действий и планировать последовательность шагов для достижения заданного результата (УК-3); - использовать нормативно-правовые документы, связанные с обеспечением профессиональной деятельности на объектах защиты; обосновывать организационно-управленческие решения в области обеспечения информационной безопасности систем, подлежащих информационной защите (ОПК-5).

	- сбор материалов, необходимых для выполнения выпускной квалификационной работы.		- определять комплекс мер (правила, процедуры, практические приемы, руководящие методы, принципы, средства) для обеспечения информационной безопасности информационных систем; разрабатывать политику информационной безопасности объекта защиты; применять на практике основные механизмы управления информационной безопасностью на объекте защиты (ОПК-10). - определять комплекс мер (правила, процедуры, практические приемы, руководящие методы, принципы, средства) для обеспечения информационной безопасности информационных систем; разрабатывать политику информационной безопасности объекта защиты; применять на практике основные механизмы управления информационной безопасностью на объекте защиты (ОПК-2.1).
УК-3, ОПК-5, ОПК-10, ОПК-2.1	Заключительный этап: - итоговая конференция; защита отчета по практике.	Оформлена отчетная документация (табл. 4.1.). Осуществлена защита отчета.	**Владеет:** - навыками эффективного взаимодействия с другими членами команды, в т.ч. участия в обмене информацией, знаниями и опытом, в презентации результатов работы команды (УК-3). - навыками аналитической работы с нормативно-правовыми документами, в частности с нормативной базой РФ, в сфере профессиональной деятельности на конкретных объектах защиты; - методами разработки проектов нормативных и организационно-распорядительных документов для конкретных объектов защиты (ОПК-5). - навыками планирования и организации системы защиты информации; навыками реализации элементов политики информационной безопасности; методами организации и управления деятельностью служб за-

			щиты информации на предприятии (ОПК-10). - способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты; методиками построения частной модели защиты от информационных угроз (ОПК-2.1).

Описание шкалы оценивания

«Зачтено (с оценкой «отлично»)» - обучающийся своевременно выполнил весь объем работы, требуемый программой практики, показал глубокую теоретическую, методическую, профессионально-прикладную подготовку; умело применил полученные знания во время прохождения практики, показал владение традиционными и альтернативными методами, современными приемами в рамках своей профессиональной деятельности, точно использовал профессиональную терминологию; ответственно и с интересом относился к своей работе, грамотно, в соответствии с требованиями сделал анализ проведенной работы; отчет о практике выполнил в полном объеме, результативность практики представлена в количественной и качественной обработке, продуктах деятельности, обучающийся показал сформированность профессиональных компетенций.

«Зачтено (с оценкой «хорошо»)» - обучающийся демонстрирует достаточно полные знания всех профессионально-прикладных и методических вопросов в объеме программы практики; полностью выполнил программу, но допустил незначительные ошибки при выполнении задания, владеет инструментарием методики в рамках своей профессиональной подготовки, умением использовать его; грамотно использует профессиональную терминологию при оформлении отчетной документации по практике.

«Зачтено (с оценкой «удовлетворительно»)» - обучающийся выполнил программу практики, однако в процессе работы не проявил достаточной самостоятельности, инициативы и заинтересованности, допустил существенные ошибки при выполнении заданий практики, демонстрирует недостаточный объем знаний и низкий уровень их применения на практике; неосознанное владение инструментарием, низкий уровень владения методической терминологией; низкий уровень владения профессиональным стилем речи; низкий уровень оформления документации по практике.

«Не зачтено» (с оценкой «неудовлетворительно») - обучающийся не выполнил программу практики и (или) не представил необходимую отчетную документацию в требуемой форме.

4.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Защита отчета по практике проводится в виде устной беседы руководителя и студента в соответствии с перечнем вопросов к зачету с оценкой, а также демонстрации студентом практических навыков выполнения описанных в отчете работ.

Примерный перечень вопросов к зачету с оценкой

1. Система информационной безопасности, направления защиты.
2. Технические средства обеспечения безопасности информации, их классификация.
3. Характеристика защитных средств.
4. Служба технической разведки, ее функции.
5. Характеристика физических и электрических полей.
6. Средства съема информации, порядок их применения.
7. Участие сотрудников службы безопасности в технической защите информации.
8. Акустические поля, их характеристика.
9. Утечка информации по ПЭМИН (побочное электромагнитное излучение и наводки).
10. Оптические поля, их характеристика.
11. Вибро-акустические каналы течки информации.
12. Технические средства несанкционированного доступа к информации.
13. Акустическая разведка, ее возможности и принципы работы технических средств.
14. Оптическая разведка, ее возможности и принципы работы технических средств.
15. Принципиальные схемы установки радио-микрофонов и радио закладок.
16. Проводная связь, ее слабые места.
17. Средства лазерной разведки, принцип работы.
18. Порядок съема информации с технических средств ее передачи и хранения.
19. Понятие ТКУИ (технические каналы утечки информации), классификация и факторы их возникновения.
20. Защищаемы объекты, их характеристика
21. Основные технические средства обработки информации, их характеристика.
22. Вспомогательные технические средства обработки информации, их характеристика.
23. Организационные мероприятия по защите информации по техническим каналам утечки информации.
24. Защита помещений и сетей от утечки по техническим каналам утечки информации.
25. Типы закладных устройств, порядок их применения
26. Физический поиск закладных устройств.
27. Индикаторы поля, порядок их применения.
28. Программные средства выявления каналов утечки информации.
29. Технические комплексы выявления каналов утечки информации.
30. Нелинейные радиолокаторы, порядок их применения.
31. Порядок применения аппаратуры контроля линий.
32. Средства защиты линий связи, их характеристика.
33. Средства зашумления, их характеристика.
34. Аппаратура измерения уровня сигнала в электрических цепях и сетях связи, порядок ее использования.
35. Степени защищенности помещений, порядок ее определения.
36. Порядок аттестации помещений
37. Лицензирование деятельности в области ИБ

38. Виды потенциально опасных воздействий на ЭВМ.
39. Виды потенциально опасных воздействий.
40. Защита от ошибок обслуживающего персонала.
41. Защита от заражений компьютерными вирусами.

4.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Контроль над ходом технологической практики имеет целью выявление и установление недостатков, оказание практической помощи студентам. Руководитель практики от организации ежедневно контролирует соблюдение студентами правил внутреннего распорядка и качественные результаты их работы. Руководитель практики от университета встречается со студентами не реже одного раза в две недели для беседы, в процессе которой проверяется ход выполнения задания по практике, выполнение индивидуальных заданий, а также ведение дневника практики. Руководитель должен принимать оперативные меры по устранению выявленных недостатков.

Оценка знаний, умений, навыков, характеризующая этапы формирования компетенций по практике, проводится в форме текущей и промежуточной аттестации.

К контролю текущей успеваемости относится проверка знаний, умений и сформированных компетенций, обучающихся при собеседовании по результатам выполнения заданий отчета обучающихся в ходе индивидуальной консультации с методистом от образовательной организации.

Промежуточная аттестация по практике осуществляется в форме зачета с оценкой. Для аттестации обучающийся представляет отчет, который выполняется по результатам прохождения практики с учетом (анализом) результатов проведенных работ и отзыва руководителя практики.

Зачет с оценкой проводится после завершения прохождения практики в объеме программы практики. Результаты аттестации практики фиксируются в зачетно-экзаменационных ведомостях. Получение обучающимся неудовлетворительной оценки за аттестацию является академической задолженностью.

V. ОРГАНИЗАЦИЯ ПРАКТИКИ

5.1. Этапы практики:

1. Подготовительный.

1) *Установочная конференция.*

На установочной конференции до студентов доводятся вопросы организации, содержания практики, выдается индивидуальное задание. Объясняются особенности прохождения практики в организациях и предприятиях, выполнения плана-графика, заполнения дневника практики, подготовки отчета о выполнении практики.

2) *Вводный инструктаж по месту проведения практики.*

Проводится специалистами по технике безопасности предприятий и организаций. Основное внимание уделяется вопросам распорядка дня работы, соблюдения мер производственной и противопожарной безопасности. По результатам инструктажа делается запись в книге проведения инструктажа с росписью студента.

2. **Основной.**

1) Ознакомление со структурой, лицензией и уставом организации, решаемыми задачами.

Студент в первые дни практики знакомится с организацией информационного обеспечения подразделения, с процессом проектирования и эксплуатации

информационных средств, с методами планирования и проведения мероприятий по созданию (разработке) проекта (подсистемы) информационной среды предприятия для решения конкретной задачи.

2) Ознакомление со структурой подразделений информационных технологий организации.

Изучаются:

- структурные и функциональные схемы предприятия, организация деятельности подразделения;
- порядок и методы ведения делопроизводства;
- требования к техническим, программным средствам, используемым на предприятии;
- методы проектирования и эксплуатации программно-технических комплексов;
- методы оптимизации и технической поддержки функционирования IT-инфраструктуры предприятия;
- методы организации внедрения ЛВС;
- сопровождение программных продуктов, вычислительных автоматизированных систем;
- методы анализа эксплуатационных характеристик, поддержание их на требуемом уровне;
- методы представления информационных сервисов.

3) Ознакомление с современными информационными технологиями, используемыми в организации в сфере ИБ.

Приобретение практических навыков:

- выполнение функциональных обязанностей;
- ведение в организации или предприятии типовых документов (стандартов, ГОСТов, руководящих документов и т.д.) регламентирующих вопросы разработки, внедрения и эксплуатации информационных технологий и применения современных методов защиты информации;
- знакомство с применяемыми в организации информационными технологиями;
- проведение работ по установке, настройке и испытаниям защищенных технических средств обработки информации;
- проведение работ по техническому обслуживанию защищенных технических средств обработки информации;
- практическая апробация и реализация предлагаемых проектных решений;
- сбор материалов, необходимых для выполнения выпускной квалификационной работы.

4) Разработка концепции проекта.

Изучение используемых технологий защиты информации. Анализ современных достижений и решений в предметной области. Выявление объекта автоматизации, постановка задачи и выбор способа реализации проекта решения. Анализ требований и разработка системной архитектуры проекта, моделирование функционирования объекта проектирования в сфере информационной безопасности.

3. **Заключительный.**

1) *Итоговая конференция.*

На итоговой конференции доводятся общие результаты выполнения студентами практики, заслушиваются студенты с наиболее содержательными результатами практики с применением слайдов и другой наглядной продукции. На итоговую конференцию приглашается преподавательский состав кафедры, представители директората, а также представители предприятий, на которых выполнялась практика.

2) *Защита отчета.*

В ходе практики обучающиеся обязаны:

- ознакомиться с организацией и управлением деятельностью организации (предприятия), видом работ и основными характеристиками продукции;
- изучить имеющееся техническое и программное обеспечение, относящееся к сфере профессиональной деятельности, действующие положения и инструкции, используемую техническую документацию;
- освоить используемое оборудование, аппаратуру;
- знать применяемую вычислительную технику и программы по защите информации;
- принимать непосредственное участие в деятельности организации (предприятия), выполняя технологическую разработку по теме индивидуального задания;
- проанализировать возможность и перспективы внедрения результатов собственных исследований в организации (на предприятии), где проводится практика;
- провести испытание собственной технологической разработки на базе организации (предприятия), где проводится практика.

Руководитель практики от университета:

- координирует организационные вопросы практики с дирекцией института;
- участвует в распределении обучающихся по местам практики и видам работ на предприятии;
- разрабатывает задания для обучающихся, выполняемые в период практики;
- участвует в разработке программ практики;
- организует и проводит установочную конференцию по практике;
- формирует (при необходимости) списки обучающихся для оформления требуемых пропусков и формы допусков на режимные предприятия и представляют данные списки в дирекцию института;
- контролирует заполнение обучающимися дневников прохождения практики;
- осуществляет контроль за соблюдением сроков проведения практики и соответствием её содержания требованиям, установленным ОПОП;
- проводит аттестацию и оценивает результаты прохождения практики обучающимися;
- представляет письменный отчет на выпускающую кафедру и в дирекцию института в течение двух недель после завершения практики с заключениями и предложениями по её совершенствованию.

Руководитель практики от предприятия:

- взаимодействует с руководителем практики от университета, согласовывает с ним задания, содержание и планируемые результаты практики;
- создает необходимые условия для выполнения программы практики, индивидуальных заданий;
- разъясняет обучающимся круг выполняемых в период практики задач;
- обеспечивает безопасные условия прохождения практики обучающимся, отвечающие санитарным правилам и требованиям охраны труда;
- контролирует выполнение обучающимися внутреннего трудового распорядка предприятия и дисциплины.

5.2. Базы практики

Производственная практика проходит на базе организаций, направленность деятельности которых соответствует профилю подготовки обучающихся.

Производственная практика организуется на основе договоров между Университетом и организациями, осуществляющими деятельность по образовательной

программе соответствующего профиля. В соответствии с договорами указанные организации независимо от их организационно-правовых форм обязаны предоставлять места для прохождения практики студентов образовательных организаций высшего образования, имеющих государственную аккредитацию и материалы для выполнения программы практики.

Предприятиями, с которыми заключены договоры о научно-практическом сотрудничестве и организации прохождения практик для обучающихся, являются:

1. ПАО «Елецгидроагрегат»;
2. ООО "Айти-Нэт»;
3. ООО «Базальт СПО»;
4. Сервисный центр «Все для оргтехники».

5.3. Особенности организации практики для инвалидов и лиц с ограниченными возможностями здоровья.

При выборе базы практики для лиц с ОВЗ и инвалидов учитывается не только возможность решения студентом (-ами) задач практики, но и его (их) ограниченные возможности здоровья. Порядок организации практики регламентирован соответствующим локальным актом.

VI. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ПРАКТИКИ

6.1. Перечень учебной литературы и ресурсов сети «Интернет», необходимых для проведения практики

Основная литература

1. *Астапчук, В. А.* Корпоративные информационные системы: требования при проектировании : учебное пособие для вузов / В. А. Астапчук, П. В. Терещенко. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 113 с. — (Высшее образование). — ISBN 978-5-534-08546-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/472111 (дата обращения: 01.09.2021).
2. *Кубашева, Е.С.* Информатика и вычислительная техника. Информационная безопасность автоматизированных систем : учебно-методическое пособие : / Е.С. Кубашева, И.А. Малашкевич, Е.Н. Чекулаева ; Поволжский государственный технологический университет. – Йошкар-Ола : Поволжский государственный технологический университет, 2019. – 66 с. : табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562246 (дата обращения: 01.09.2021). – Библиогр.: с. 45. – ISBN 978-5-8158-2081-4. – Текст : электронный.

Дополнительная литература

1. Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. : схем., табл., ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=480637 (дата обращения: 01.09.2021). – Библиогр. в кн. – Текст : электронный.
2. Голиков, А.М. Защита информации от утечки по техническим каналам : учебное пособие : [16+] / А.М. Голиков ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 256 с. : схем., табл., ил. – Режим до-

ступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=480636 (дата обращения: 01.09.2021). – Библиогр.: с. 213. – Текст : электронный.
3. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 253 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 01.09.2021). – Библиогр. в кн. – ISBN 978-5-4475-3946-7. – DOI 10.23681/276557. – Текст : электронный.
4. Сагдеев, К.М. Физические основы защиты информации : учебное пособие / К.М. Сагдеев, В.И. Петренко, А.Ф. Чипига ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2015. – 394 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=458285 (дата обращения: 01.09.2021). – Библиогр.: с. 387-388. – Текст : электронный.

Интернет-ресурсы

№ пп	Ссылка на информационный ресурс	Наименование разработки в электронной форме	Доступность
1	http://www.biblioclub.ru	Электронно-библиотечная система (ЭБС) Университетская библиотека онлайн	Регистрация через любой университетский компьютер. В дальнейшем неограниченный доступ из любой точки, в которой имеется доступ к сети Интернет
2	http://msdn.microsoft.com/ru-ru/vstudio	Программное обеспечение	Без регистрации свободный доступ из любой точки, в которой имеется доступ к сети Интернет
3	http://www.proklondike.com/	Бесплатная электронная библиотека	Без регистрации свободный доступ из любой точки, в которой имеется доступ к сети Интернет
4	http://www.coders-library.ru/	Библиотека программиста	Требуется только регистрация
6	http://www.edu.ru/	Федеральный портал Российское образование	Без регистрации свободный доступ из любой точки, в которой имеется доступ к сети Интернет
7	https://fstec.ru/	Федеральная служба по техническому и экспортному контролю	Без регистрации свободный доступ из любой точки, в которой имеется доступ к сети Интернет

6.2. Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

При реализации учебной дисциплины применяется следующее лицензионное и свободно распространяемое программное обеспечение:
- Microsoft Windows;
- Microsoft Office;
- Libre Office и др.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

Материально-техническая база организации, в которой проводится технологическая практика, помещения соответствуют действующим санитарным и противопожарным нормам, а также требованиям технической безопасности при осуществлении технологической деятельности.

VIII. ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ

В связи с утверждением и введением в действие Положения о практической подготовке обучающихся федерального государственного бюджетного образовательного учреждения высшего образования «Елецкий государственный университет им. И.А. Бунина» (приказ №169-а от 5 июля 2022 г.) внести следующие изменения в Раздел III. «Формы отчетности по практике»:

В результате прохождения практики обучающиеся предоставляют следующий пакет документов в печатном и электронном виде:

- задание на практику;
- дневник практики;
- отчет о прохождении практики;
- характеристику;
- аттестационный лист.

Учитывать внесенное изменение в остальных разделах программы практики.