1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Практика студентов образовательных организаций высшего профессионального образования является составной частью основной профессиональной образовательной программы высшего профессионального образования и представляет собой одну из форм организации учебного процесса, заключающуюся в профессионально-практической подготовке студентов на базах практики.

Программа практики – это нормативно-методический документ, определяющий содержание обучения студентов профессионально-практической деятельности в условиях реального производства. Представленная программа регулирует вопросы прохождения всех видов практики студентами высшего профессионального образования по направлению 590100 «Информационная безопасность».

Программа разработана в соответствии с:

- государственным образовательным стандартом высшего профессионального образования;
- учебным планом по направлению 590100 «Информационная безопасность»;
- профессиональными стандартами в области информационной безопасности и кибербезопасности;
- положение об организации практик студентов КГТУ им. И. Раззакова.

Цель, объем, и виды практики определяются Государственным образовательным стандартом высшего профессионального образования по соответствующей специальности подготовки студентов. С учетом изложенных в нем требований, учебным заведением разработаны документы, регламентирующие планирование, организацию и проведение практики. Прохождение практики осуществляется согласно рабочему учебному плану и утвержденной программой практики и завершается составлением отчета практики и его защитой.

В соответствии с государственным образовательным стандартом высшего профессионального образования и рабочим учебным планом по направлению 590100 «Информационная безопасность» предусмотрены следующие виды практик:

– учебная практика;

– производственная практика;

– предквалификационная практика.

Подготовка студентов в области информационной безопасности должна быть тесно связана с конкретными задачами его будущей практической деятельности. Решению этой задачи призваны способствовать предусмотренные настоящим документом виды практики.

Практика является неотъемлемой частью образовательного процесса и реализуется в форме учебной, производственной и предквалификационной практик, образующих единую сквозную систему практической подготовки. Сквозной характер практики обеспечивает поэтапное усложнение содержания, расширение круга профессиональных задач и рост самостоятельности обучающихся.

Целью практики является закрепление и углубление теоретических знаний, полученных в ходе освоения учебных дисциплин, а также формирование практических умений и навыков профессиональной деятельности в области кибербезопасности. В процессе практики обучающиеся осваивают методы и средства защиты информации, приобретают опыт работы с современными технологиями обеспечения кибербезопасности и учатся применять их в условиях реальной или моделируемой профессиональной среды.

Основными задачами практики являются:

•формирование представлений о профессиональной деятельности специалиста по кибербезопасности;
•изучение организационных и технических мер обеспечения информационной безопасности;
•освоение методов анализа киберугроз, уязвимостей и рисков;
•приобретение навыков эксплуатации и администрирования средств защиты информации;
•развитие умений реагирования на инциденты информационной безопасности;
•подготовка к самостоятельной профессиональной деятельности и выполнению выпускной квалификационной работы.

Практика проводится на базе профильных организаций, предприятий и учреждений, осуществляющих деятельность в области информационных технологий и информационной безопасности, а также в специализированных лабораториях и структурных подразделениях образовательной организации. В качестве баз практики могут выступать службы информационной безопасности, центры мониторинга и реагирования на инциденты (SOC), IT-подразделения, а также иные организации, соответствующие профилю подготовки.

В ходе практики у обучающихся формируются профессиональные компетенции, связанные с обеспечением кибербезопасности информационных систем, сетей и ресурсов, в том числе способность анализировать и классифицировать угрозы, проектировать и эксплуатировать защищённые системы, применять средства сетевой, программной и криптографической защиты, а также участвовать в расследовании инцидентов информационной безопасности.

Результаты прохождения практики подлежат обязательной оценке. Формами отчетности являются дневник практики, отчет по практике, а также отзыв (характеристика) руководителя практики от организации. Итоговая аттестация по практике проводится в форме зачета или дифференцированного зачета в соответствии с учебным планом.

Таким образом, практика по направлению 590100 «Информационная безопасность», профиль «Кибербезопасность», обеспечивает практико-ориентированную направленность подготовки обучающихся, способствует формированию профессиональной готовности выпускников к деятельности в сфере кибербезопасности и повышает их конкурентоспособность на рынке труда.

2. УЧЕБНАЯ ПРАКТИКА

2.1. Цель и задачи учебной практики

Цель учебной практики

Формирование у обучающихся первичных практических умений и навыков разработки программных и веб-приложений с учетом требований информационной и кибербезопасности.

Задачи учебной практики:

- закрепление теоретических знаний по программированию и основам информационной безопасности;
- освоение принципов алгоритмизации и структурирования программного кода;
- приобретение навыков разработки прикладных программ и веб-сайтов;
- изучение основ безопасной разработки программного обеспечения;
- формирование умений выявлять и устранять типовые уязвимости в программном коде;
- развитие навыков работы в учебной команде и оформления технической документации.

2.2. Место учебной практики в структуре ОПОП

Учебная практика проводится на начальных этапах обучения и базируется на дисциплинах:

- «Программирования»;
- «Алгоритмы и структуры данных»;
- «Введение в кибербезопасность»;
- «Веб-программирования».
- «Системы базы данных»

Практика является основой для последующего освоения дисциплин и практик, связанных с кибербезопасностью, безопасностью программных и сетевых систем.

2.3. Место и условия проведения практики

Учебная практика проводится в аудиториях и специализированных компьютерных классах университета, оснащенных:

- персональными компьютерами;
- средами разработки (IDE);
- средствами тестирования и отладки программ;
- локальной сетью и доступом к учебным серверным ресурсам.

Практика осуществляется под руководством преподавателей кафедры.

2.4. Содержание учебной практики

Раздел 1. Основы программирования

- разработка консольных приложений;
- работа с переменными, условиями, циклами, функциями;
- обработка данных и файлов;
- основы объектно-ориентированного программирования.

Раздел 2. Разработка прикладных приложений

- проектирование структуры приложения;
- разработка пользовательского интерфейса;
- реализация логики приложения;
- тестирование и отладка программ.

Раздел 3. Веб-разработка

- основы HTML, CSS, JavaScript;
- разработка статических и динамических веб-страниц;
- работа с формами и пользовательским вводом;
- основы клиент-серверного взаимодействия.

Раздел 4. Основы безопасной разработки

- принципы secure coding;
- типовые уязвимости программного обеспечения;
- защита пользовательского ввода;
- основы аутентификации и авторизации.

Раздел 5. Учебный проект

- разработка учебного программного или веб-приложения;
- реализация базовых механизмов защиты;
- подготовка отчётной и проектной документации.

2.5. Результаты освоения учебной практики

В результате прохождения учебной практики обучающийся должен:

знать:

- основы программирования и веб-разработки;
- принципы безопасной разработки программного обеспечения;
- типовые уязвимости программных и веб-приложений.

уметь:

- разрабатывать простые прикладные и веб-приложения;

•применять базовые методы защиты программного кода;

•тестировать и отлаживать программные продукты.

владеть:

•навыками работы в средах разработки;

•навыками командной разработки учебных проектов;

•навыками оформления технической документации.

2.6. Индивидуальные задания обучающихся

Индивидуальное задание предусматривает разработку программного или веб-приложения учебного назначения с реализацией базовых механизмов безопасности и подготовкой отчёта по практике.

2.7. Формы отчетности и контроль

Формами отчетности по учебной практике являются:

•отчет по практике;

•демонстрация разработанного программного или веб-приложения.

Итоговый контроль проводится в форме диф. зачета.

2.8. Учебно-методическое и материально-техническое обеспечение

Учебная практика обеспечивается методическими указаниями кафедры, программным обеспечением и вычислительной техникой университета.

3. ПРОИЗВОДСТВЕННАЯ ПРАКТИКА

3.1. Цель и задачи производственной практики

Цель производственной практики

Формирование и развитие профессиональных компетенций обучающихся в области кибербезопасности на основе практического участия в деятельности профильной организации.

Задачи производственной практики:

•закрепление и углубление теоретических знаний в области информационной и кибербезопасности;

•освоение практических методов защиты информации в корпоративных информационных системах;

•участие в администрировании и эксплуатации средств защиты информации;

•анализ уязвимостей и киберугроз;

•участие в мероприятиях по мониторингу и реагированию на инциденты информационной безопасности;

•приобретение навыков профессионального взаимодействия в коллективе.

3.2. Место производственной практики в структуре ОПОП

Производственная практика проводится после освоения обучающимися базовых и профессиональных дисциплин и опирается на знания и умения, полученные при изучении: Программирование, Основы информационной безопасности, Основы кибербезопасности, Криптографические методы защиты информации, Технические методы защиты информации. Практика является логическим этапом перехода от учебной деятельности к профессиональной.

3.3. Место и условия проведения практики

Производственная практика проводится в организациях различных форм собственности, деятельность которых связана с: эксплуатацией информационных систем и сетей, обеспечением информационной и кибербезопасности, разработкой и сопровождением программного обеспечения, оказанием услуг в сфере IT и информационной безопасности.

В качестве баз практики могут выступать IT-компании, государственные и коммерческие организации, банки, телекоммуникационные компании, центры обработки данных, подразделения информационной безопасности и SOC.

Практика осуществляется под руководством: руководителя практики от образовательной организации, руководителя практики от организации.

3.4. Содержание производственной практики

Раздел 1. Ознакомление с деятельностью организации

- изучение структуры организации и IT-инфраструктуры;
- знакомство с политикой информационной безопасности;
- изучение локальных нормативных документов.

Раздел 2. Эксплуатация информационных систем и сетей

- участие в администрировании серверов и рабочих станций;
- сопровождение корпоративных сетей;
- обеспечение резервного копирования и восстановления данных.

Раздел 3. Средства и методы кибербезопасности

- настройка и эксплуатация межсетевых экранов, VPN, IDS/IPS;
- использование антивирусных и анти-DLP решений;
- работа с системами мониторинга и журналирования событий безопасности.

Раздел 4. Анализ уязвимостей и киберугроз

- участие в проведении оценки уязвимостей;
- анализ рисков информационной безопасности;
- изучение типовых кибератак и методов противодействия.

Раздел 5. Реагирование на инциденты

- участие в выявлении и классификации инцидентов ИБ;
- первичные мероприятия по реагированию;
- документирование инцидентов и подготовка отчетов.

3.5. Результаты освоения производственной практики

В результате прохождения производственной практики обучающийся должен:

знать:

- принципы построения защищённых информационных систем;
- организационные и технические меры обеспечения кибербезопасности;
- порядок реагирования на инциденты информационной безопасности.

уметь:

- применять средства защиты информации в реальной инфраструктуре;
- анализировать уязвимости и угрозы;
- участвовать в администрировании и мониторинге систем безопасности.

владеть:

- практическими навыками работы с современными средствами киберзащиты;
- навыками документирования результатов работ;
- навыками профессионального взаимодействия.

3.6. Индивидуальные задания обучающихся

Индивидуальное задание определяется руководителем практики и может включать:

- участие в настройке средств защиты;
- анализ защищенности информационной системы;
- разработку предложений по повышению уровня кибербезопасности;

•участие в проектных или эксплуатационных работах.

3.7. Формы отчетности и контроль

Формами отчетности по производственной практике являются:

•дневник практики;

•отчет по практике;

•отзыв (характеристика) руководителя практики от организации.

Итоговая аттестация проводится в форме дифференцированного зачета.

3.8. Учебно-методическое и материально-техническое обеспечение

Производственная практика обеспечивается методическими указаниями образовательной организации, нормативной документацией организации-базы практики, а также техническими и программными средствами, используемыми в профессиональной деятельности.

4. ПРЕДКВАЛИФИКАЦИОННАЯ ПРАКТИКА

4.1. Цель и задачи предквалификационной практики

Цель предквалификационной практики

Формирование у обучающихся готовности к самостоятельному решению профессиональных задач в области кибербезопасности и сбор практического материала для выпускной квалификационной работы.

Задачи предквалификационной практики:

•закрепление и углубление профессиональных знаний и навыков в области кибербезопасности;

•изучение объекта профессиональной деятельности, выбранного для ВКР;

•анализ текущего уровня защищенности информационных систем организации;

•сбор, анализ и систематизация материалов для ВКР;

•разработка и обоснование технических и организационных мер обеспечения кибербезопасности;

•оценка эффективности предлагаемых решений;

•формирование навыков самостоятельной профессиональной деятельности.

4.1. Место практики в структуре ОПОП

Предквалификационная практика проводится на завершающем этапе обучения после освоения обучающимися учебной и производственной практик, а также основных профессиональных дисциплин. Практика является связующим звеном между образовательным процессом и итоговой государственной аттестацией.

4. Место и условия проведения практики

Предквалификационная практика проводится в организациях, деятельность которых связана с эксплуатацией, разработкой и защитой информационных систем и сетей.

Базами практики могут являться:

•IT-компании;

•банки и финансовые организации;

•государственные учреждения;

•телекоммуникационные компании;

•центры обработки данных;

•подразделения информационной безопасности и SOC.

Практика осуществляется под руководством руководителя от образовательной организации и руководителя от организации-базы практики.

5. Содержание предквалификационной практики

Раздел 1. Анализ деятельности организации и объекта исследования

- изучение структуры организации и IT-инфраструктуры;
- анализ политики и системы информационной безопасности;
- определение объекта и предмета исследования ВКР.

Раздел 2. Анализ угроз и уязвимостей

- моделирование угроз и нарушителя;
- анализ уязвимостей информационных систем;
- оценка рисков информационной и кибербезопасности.

Раздел 3. Разработка решений по обеспечению кибербезопасности

- выбор и обоснование средств защиты информации;
- разработка технических и организационных мер защиты;
- проектирование архитектуры защищенной системы.

Раздел 4. Оценка эффективности предлагаемых мер

- анализ соответствия решений нормативным требованиям;
- оценка эффективности и целесообразности внедрения;
- формирование рекомендаций по повышению уровня кибербезопасности.

Раздел 5. Подготовка материалов для ВКР

- систематизация собранных данных;
- оформление аналитических и проектных материалов;
- подготовка выводов и предложений для ВКР.

---

6. Результаты освоения предквалификационной практики

В результате прохождения предквалификационной практики обучающийся должен:

знать:

- современные подходы и технологии обеспечения кибербезопасности;
- нормативно-правовые и методические основы защиты информации;
- методы анализа и управления рисками.

уметь:

- самостоятельно анализировать защищенность информационных систем;
- разрабатывать и обосновывать решения по обеспечению кибербезопасности;
- применять профессиональные методы и инструменты в практической деятельности.

владеть:

- навыками самостоятельной профессиональной деятельности;
- методами подготовки аналитических и проектных материалов;
- навыками публичного и письменного представления результатов работы.

---

7. Индивидуальное задание обучающегося

Индивидуальное задание формируется с учетом темы выпускной квалификационной работы и включает анализ объекта исследования, разработку и обоснование решений в области кибербезопасности.

---

8. Формы отчетности и контроль

Формами отчетности по предквалификационной практике являются:

- дневник практики;
- отчет по практике;
- отзыв (характеристика) руководителя практики от организации;
- материалы, используемые при выполнении ВКР.

Итоговая аттестация проводится в форме дифференцированного зачета.

---

9. Учебно-методическое и материально-техническое обеспечение

Предквалификационная практика обеспечивается методическими рекомендациями образовательной организации, нормативной документацией организации-базы практики, а также техническими и программными средствами, используемыми в профессиональной деятельности.

---

10. Заключительные положения

Программа предквалификационной практики подлежит актуализации с учетом развития технологий кибербезопасности, изменений нормативно-правовой базы и требований рынка труда.