Учреждение образования «Полоцкий государственный университет»

УТВЕРЖДАЮ
Проректор по учебной работе
учреждения образования
«Полоцкий государственный университет»
_____ Д. В. Дук
«_01_» _____01_____ 2017 г.
Регистрационный № 264/980101-пр

ПРОГРАММА
преддипломной практики
для специальности:
1-98 01 01 Компьютерная безопасность (по направлениям)
направления специальности:
1-98 01 01-01 Компьютерная безопасность (математические методы и программные системы)
специализации:
1-98 01 01-01 03 Защищённые информационные системы

2017 г.

СОСТАВИТЕЛЬ:
О. В. Голубева, заведующий кафедрой технологий программирования, кандидат физико-математических наук, доцент

РАССМОТРЕНА И РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:
Кафедрой технологий программирования
(протокол № 14 от 12 декабря 2016 г.)

Заведующий кафедрой
_____ О. В. Голубева

ОДОБРЕНА И РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:
Советом факультета информационных технологий
(протокол № 1 от 10 января 2017 г.)

Председатель Совета факультета
_____ С. Г. Ехилевский

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1. ЦЕЛИ И ЗАДАЧИ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

Программа преддипломной практики разработана в соответствии с образовательным стандартом ОСВО 1-98 01 01-2013, типовым учебным планом по специальности 1–98 01 01 Компьютерная безопасность (математические методы и программные системы).

Преддипломная практика проводится в соответствии с Положением о практике студентов, курсантов, слушателей и является подготовительным этапом к выполнению дипломной работы и дальнейшей профессиональной деятельности.

Целями преддипломной практики являются:

– освоение в условиях производства принципов организации и управления производством, участие в работе над реальным проектом;

– освоение и участие в разработке промышленных программных систем, средств вычислительной техники и различных операционных приложений;

– изучение требований и разработки проектных решений, ознакомление с конкретными проектами различных системных программ и средств вычислительной техники;

– формирование и анализ материалов для выполнения дипломной работы.

Задачами преддипломной практики являются:

знакомство с

– организацией систем научно-технического и эксплуатационного обеспечения;

– формами организации производственного процесса и его технологическим обеспечением;

– организационной структурой подразделения по защите информации;

– составом и особенностями эксплуатации технических, программных, аппаратных средств защиты информации;

– методами проектирования и эксплуатации компьютерных систем передачи и обработки информации;

– подходами по разработке нормативно-методических документов по организационной защите информации.

Изучение:

– правил техники безопасности и порядка организации труда на рабочих местах;

– требований режима безопасности и делопроизводства;

– особенностей соблюдения специальных правил при работе с оперативно-технической и служебной документацией;

– основных обязанностей должностных лиц подразделения по защите информации;

– основных характеристик и возможностей используемых в подразделении технических, программных, аппаратных и криптографических средств защиты информации, методов и приемов их применения для решения задач по обеспечению информационной безопасности объекта;

– общих принципов существующего порядка использования технических и программных средств защиты информации;

– методов построения современных систем защиты информации, используемых подразделением;

– порядка использования подразделением руководящих документов по оценке защищенности компьютерных систем.

При прохождении преддипломной практики у студентов должны сформироваться следующие группы компетенций:

– АК-1. Уметь применять базовые научно-теоретические знания для решения теоретических и практических задач.

– АК-2. Владеть системным и сравнительным анализом.

– АК-3. Владеть исследовательскими навыками.

– АК-4. Уметь работать самостоятельно.

– АК-5. Быть способным вырабатывать новые идеи (креативность).

– АК-6. Владеть междисциплинарным подходом при решении проблем.

– АК-7. Иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером.

– АК-8. Иметь лингвистические навыки (устная и письменная коммуникация).

– АК-9. Уметь учиться, повышать свою квалификацию в течение всей жизни.

– СЛК-2. Быть способным к социальному взаимодействию.

– СЛК-3. Обладать способностью к межличностным коммуникациям.

– СЛК-4. Владеть навыками здорового образа жизни.

– СЛК-5. Быть способным к критике и самокритике (критическое мышление).

– СЛК-6. Уметь работать в команде.

– ПК-1. Работать с научной, нормативно-справочной и специальной литературой с целью получения последних сведений о новых методах защиты информации, о стойкости существующих систем защиты информации.

– ПК-3. Разрабатывать модели явлений, процессов или систем при организации защиты информации.

– ПК-8. Взаимодействовать со специалистами смежных профилей.

– ПК-9. Анализировать и оценивать собранные данные.

– ПК-10. Вести переговоры, разрабатывать контракты с другими заинтересованными участниками.

– ПК-15. Организовывать процесс создания, оценки и эксплуатации средств и систем защиты информации, поддерживать и повышать их безопасность; осуществлять контроль за их использованием.

– ПК-16. Разрабатывать техническое задание на разработку средств и систем защиты информации.

– ПК-17. Находить оптимальные проектные решения.

– ПК-18. Разрабатывать программные, аппаратно-программные и технические средства и системы защиты информации; разрабатывать необходимую документацию.

– ПК-19. Выполнять оценку безопасности реализации средств и систем защиты информации.

– ПК-20. Внедрять программные, аппаратно-программные и технические средства и системы защиты информации; разрабатывать необходимую для этого документацию.

– ПК-21. Эксплуатировать программные, аппаратно-программные и технические средства и системы защиты информации; осуществлять контроль за их использованием; вести необходимую для этого документацию.

– ПК-22. Осуществлять поддержку и повышать эффективность эксплуатируемых программных, аппаратно-программных и технических средств и систем защиты информации.

В результате прохождения преддипломной практики студент должен

знать:

– принципы и методы проектирования, внедрения, обслуживания систем информационной безопасности;

– обязанности должностных лиц предприятия, обеспечивающих решение задач защиты информации, формирование общего представления об информационной безопасности объекта защиты, методов и средств её обеспечения; изучение комплексного применения методов и средств обеспечения информационной безопасности объекта защиты;

– системы оценок эффективности применяемых мер обеспечения защиты информации.

уметь:

– проверять, настраивать, использовать технические и программные средства защиты информации;

– выполнять основные функциональные обязанности в соответствии с должностью;

– работать с технической и эксплуатационной документацией;

– использовать современные методы программирования и разработки эффективных алгоритмов решения прикладных задач;

– применять методы проведения анализа надежности системы защиты информации в компьютерных системах.

По окончании преддипломной практики должно быть сформулировано окончательное задание на дипломную работу.

1.2. БАЗЫ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

Преддипломная практика проводится на предприятиях (организациях, кафедрах), в деятельности которых необходимо обеспечивать информационную безопасность. Студенты, у которых дипломная работа связана с обеспечением учебного процесса или научно-исследовательской деятельностью кафедры технологий программирования, могут проходить преддипломную практику на кафедре технологий программирования.

Базами прохождения преддипломной практики могут служить следующие предприятия и организации:

- Отдел по раскрытию преступлений в сфере высоких технологий (отдел «К»), узел связи технической защиты информации УВД Витебской области
- Управление Следственного комитета Республики Беларусь по Витебской области
- Витебская таможня
- Филиал № 214 ОАО «АСБ Беларусбанк» в г. Новополоцк
- Филиал ОАО «Белагропромбанк» в г. Полоцк
- ОАО «Полоцктранснефть Дружба»
- ИООО «ЭПАМ Системз»
- ЗАО «ИТРАНЗИШЭН»
- ЗАО «БелХард Групп»
- ОАО «Нафтан»
- ИООО «Эксадел»
- ОАО «Полоцк-Стекловолокно»

1.3. ОРГАНИЗАЦИЯ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

Преддипломная практика проводится в соответствии с графиком образовательного процесса университета, составленным на основе учебного плана специальности, для студентов дневной формы получения высшего образования на четвёртом курсе в течение 6 недель из расчёта 5 дней в неделю по 6 часов каждый день.

За 10 дней до начала практики на базы практики высылаются списки студентов-практикантов.

Перед началом практики на кафедре технологий программирования проводится организационное собрание, инструктаж по охране труда в связи с прохождением преддипломной практики.

Общее руководство практикой на предприятии осуществляет руководитель предприятия или уполномоченный им сотрудник предприятия в соответствии с Положением о практике студентов, курсантов, слушателей.

Непосредственное руководство практикой студентов на объекте, в структурном подразделении предприятия осуществляет сотрудник предприятия, назначенный приказом руководителя предприятия.

По окончании преддипломной практики на кафедре технологий программирования проходит защита результатов.

На студентов в период практики распространяются законодательство об охране труда и правила внутреннего трудового распорядка предприятия, а на студентов, принятых на работу на вакантные должности, распространяется также законодательство о труде.

2. СОДЕРЖАНИЕ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

Этапы изучения технологии и организации производства, приобретения студентами производственных навыков по специальности, подбора материала для дипломной работы представлены в таблице 1.

Таблица 1

График проведения преддипломной практики

Номер недели	Выполняемая работа	Продолжительность, дни
1	2	3
1	Организационное собрание студентов в университете; разъяснение целей и задач практики; инструктаж по охране труда в связи с прохождением преддипломной практики	1
1	Прибытие студента в отдел кадров предприятия; представление документов, регламентирующих прохождение практики; распределение студентов по производствам, цехам, отделам; оформление пропусков на режимные предприятия; инструктаж по технике безопасности и промышленной санитарии, правилам внутреннего распорядка и особенностям режима работы на предприятии	1
1-2	Изучение литературы, отчётов, других материалов по теме работы, консультации с руководителем и специалистами подразделения. Результатом должен быть обзор литературы, обоснование математических методов, информационных технологий и аппаратных средств выбранных для решения задач. Изучение вопросов охраны труда на предприятии.	5
2-6	Выполнение производственных заданий, научных исследований, экспериментов.	20
6	Оформление отчёта по практике. Доклад руководителю практики от предприятия о проделанной работе	3
	Итого:	30

После закрепления студента за конкретной базой прохождения практики и по результатам консультаций с руководителем практики от предприятия студенту руководителем практики от университета выдается индивидуальное задание.

Все поставленные перед практикантом задания должны выполняться им самостоятельно в тесном взаимодействии с руководителем и сотрудниками подразделения. Помощь руководителя и сотрудников подразделения в ходе выполнения заданий может заключаться в консультациях, пояснениях и проверке выполненных работ.

Самостоятельная работа практиканта включает:

а) изучение информационных технологий, математических методов, программных и аппаратных средств по тематике практики;

б) исследования по совершенствованию технологий, поиск новых подходов и методов решения рассматриваемых задач;

в) проведение вычислительных экспериментов для сравнения эффективности используемых и предлагаемых информационных технологий, методов и алгоритмов.

3. ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

3.1. ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ СТУДЕНТАМ

При прохождении преддипломной практики студенты изучают:

– состояние информационной технологий и их использование в различных сферах деятельности предприятия;

– оборудование, аппаратуру, контрольно-измерительные приборы и инструменты, используемые в технологических процессах предприятия;

– организацию и результаты проектно-конструкторской, научно-исследовательской работы в области прикладной математики, информационной и компьютерной безопасности на предприятии;

– математические методы, используемые в обеспечении безопасности информации на предприятии;

– передовой опыт лучших специалистов предприятия;

– создание и обеспечение безопасных и здоровых условий труда при работе с вычислительной техникой;

– менеджмент и маркетинг в сфере производства программных продуктов.

При прохождении преддипломной практики студенты разрабатывают и исследуют:

– математические модели в системах безопасности, информационных, экономических системах;

– алгоритмы и методы решения задач в рамках полученных математических моделей;

– информационные технологии и программное обеспечение для решения полученных задач;

– информационные системы в целом и их отдельные модули;

– математические аспекты задач обеспечения компьютерной безопасности, основанные на теории вероятностей и математической статистике, вычислительной математике, дискретной математике и математической логики, математической физики;

– базы данных и системы управления базами данных;

– компьютерные сети, Internet-технологии.

После закрепления студента за конкретной базой прохождения практики и по результатам консультаций с руководителем практики от предприятия студенту руководителем практики от университета выдается индивидуальное задание.

Индивидуальное задание является конкретизацией работ по одному из нижеприведенных направлений.

ТИП Т (теоретический) – работа, ориентированная на построение математических моделей процессов, возникающих при защите информации.

ТИП АП (аппаратно-программный) – работа, ориентированная на разработку и (или) анализ аппаратуры и поддерживающего её программного обеспечения, создаваемых с целью защиты информации, хранящейся в ЭВМ, системах и компьютерных сетях.

ТИП С (сетевой) – работа, ориентированная на разработку и (или) анализ защиты вычислительных сетей.

ТИП П (программный) – работа, ориентированная на разработку и (или) анализ средств системного и прикладного программного обеспечения, создаваемых с целью защиты информации, хранящейся в ЭВМ, системах и компьютерных сетях.

Примерная тематика дипломных работ:

для ТИПА Т

– разработка криптографических систем защиты информации;

– разработка математических моделей безопасности компьютерных систем;

– разработка новых теоретических подходов к решению задач защиты информации и информационных ресурсов.

Для ТИПА АП

– разработка контроллеров различного назначения с поддерживающими драйверами и программами;

– разработка аппаратных устройств защиты информации с соответствующим поддерживающим программным обеспечением;

Для ТИПА С

– разработка и(или) анализ системы информационной безопасности однородных локальных вычислительных сетей для малых предприятий;

– разработка и(или) анализ системы информационной безопасности гетерогенных локальных вычислительных сетей для предприятий с развитой организационной структурой;

– разработка и(или) анализ системы информационной безопасности корпоративных вычислительных сетей для крупных предприятий с компактным размещением;

Для ТИПА П

– разработка драйверов для различного типа устройств;

– разработка и(или) анализ программного обеспечения для защиты информационных систем (ЭВМ, компьютерных сетей, баз данных);

– разработка и(или) анализ антивирусных программных систем;

– разработка и(или) анализ защищённых информационных систем.

Приведём **некоторые возможные темы** дипломных работ.

1. Разработка проекта и реализация защищенного мобильного приложения.

2. Исследование методов оценивания рисков, проектирование и разработка программного комплекса для оценивания.

3. Обеспечение безопасного авторизованного доступа к SOAP и REST сервисам в приложениях сервис-ориентированной архитектуры.

4. Проблемы безопасности при компоновке приложений сервис-ориентированной архитектуры.

5. Разработка программных средств защиты данных в локальных сетях Windows.

6. Методы и средства защиты данных от воздействия вредоносного программного обеспечения.

7. Разработка программного обеспечения криптографической защиты информации в соответствии со стандартами Республики Беларусь.

8. Обеспечение безопасности программных систем электронной коммерции.

9. Анализ текстов на естественном языке.

10. Проектирование и разработка защищенной распределенной системы управления группой отелей.

11. Разработка методики детектирования речи русскоязычного диктора.

12. Разработка средств контроля целостности программного обеспечения и данных в информационных системах.

13. Обеспечение безопасности виртуального хостинга с использованием двух-уровневой архитектуры Nginx/Apache.

14. Исследование влияния интенсивности звука на изоляцию воздушного шума интегральных панелей акустической защиты.

15. Обеспечение защиты служебной информации в многоаспектных корпоративных системах передачи извещений.

16. Исследование многослойных конструкций экранов при воздействии на них электромагнитного излучения оборудования активного зашумления.

17. Разработка средства активной защиты информации от утечки по цепям электропитания и заземления – генератора линейного зашумления.

18. Обеспечение комплексной безопасности электронной почты корпоративной сети на базе Postfix/Dovecot-сервера.

19. Квантовая система формирования ключевых последовательностей с повышенной криптостойкостью.

20. Безопасность связи в беспроводных сенсорных сетях.

21. Защита информации в сетях Ethernet.

22. Защита речевой информации от утечки за счет высокочастотного навязывания.

23. Аутентификация пользователя на основе клавиатурного почерка.

24. Обеспечение безопасности сети мобильного видеомониторинга распределенных динамических объектов.

25. Обеспечение процедуры аккредитации поставщика услуг в государственной системе управления открытыми ключами на примере негосударственного удостоверяющего центра.

26. Использование технологии VPN для построения корпоративных сетей.

27. Симметричная криптосистема на основе модели детерминированного хаоса.

28. Обеспечение защиты информации в локальной сети предприятия.

29. Методы и средства обнаружения компьютерных атак.

30. Исследование и математическое моделирование систем информационной безопасности на основе методов нелинейной динамики.

31. Исследование и математическое моделирование систем информационной безопасности на основе методов фрактального анализа.

32. Обеспечение информационной безопасности в автоматизированных системах контроля состояния сложных объектов.

33. Разработка методов и моделей защиты информации в виртуальном центре охраны здоровья.

34. Методы и средства искусственного интеллекта в сфере информационной защиты.

35. Применение методов реконструкции моделей систем для защиты конфиденциальных данных.

36. Комплексная защита информации в системах электронного обучения и документооборота.

37. Разработка моделей, методов и программных средств защиты от несанкционированного доступа к информации для автоматизированных рабочих мест.

38. Разработка межплатформенных инструментальных программных средств и веб-приложений имитационного моделирования систем массового обслуживания на основе языков программирования C++ и Java.

39. Оптимизационные модели и методы проектирования различных структур защищенных автоматизированных систем.

40. Имитационное моделирование функционирования элементов защищенных автоматизированных систем.

41. Исследование криптографических примитивов и протоколов с открытым ключом и их практическое применение в системах защиты информации.

42. Методы построения и анализ алгоритмов решения оптимизационных задач в условиях искаженной информации.

43. Формальные схемы построения систем информационной безопасности.

44. Обеспечение безопасности телефонных переговоров на каналах сотовой связи стандарта GSM.

45. Защита информации (факсимильной, речевой) на каналах связи сети общего пользования.

46. Разработка системы засекречивания нетекстовой информации на каналах Интернет.

47. Анализ фонограмм в прикладных задачах информационной безопасности.

48. Защита персональных данных в речевых биометрических комплексах и оценка защищенности помещений от утечки информации по вибрационному и акустическому каналам.

49. Мониторинг действий пользователей и групп при доступе к картографическим данным в географических информационных системах.

50. Применение стереомониторинга объекта в биометрических системах.

51. Идентификация просодических характеристик языка в речевом сигнале.

52. Методы построения и анализа алгоритмов блочного шифрования.

53. Методы построения и анализа алгоритмов поточного шифрования.

54. Конечные автоматы и их применение в построении и анализе криптографических алгоритмов.

55. Схемы из обратимых логических элементов и исследование эффекта однонаправленности криптопреобразований.

56. Разработка и анализ стеганографических алгоритмов для включения защищенной информации в аудио- и видеоданные.

57. Компараторные сети сортировки малой глубины.

58. Исследование низкоплотностных помехоустойчивых кодов.

59. Разработка методов защиты от сетевого червя, использующего для распространения уязвимости Windows.

60. Разработка методов противодействия несанкционированного удаленного управления компьютером.

61. Распознавание изображения инвариантного по отношению к афинным преобразованиям.

62. Сертификация программного обеспечения по требованиям безопасности информации.

63. Аудит информационной безопасности.

63. Анализ защищенности программного обеспечения.

64. Обеспечение информационной безопасности мобильных информационно-телекоммуникационных систем.

65. Разработка политики информационной безопасности машиностроительных и приборостроительных предприятий.

66. Создание автоматизированных систем в защищенном исполнении.

67. Методы защиты информации в электронном документообороте.

68. Влияние надежности устройств защиты информации на надежность вычислительных сетей.

69. Информационная безопасность паразитных каналов утечки информации.

70. Психологические и финансовые аспекты информационной безопасности.

71. Оптимальность выбора меток для защиты информации.

72. Автоматизация выявления программных закладок и не декларированных возможностей программного обеспечения.

73. Формальные модели и методы обеспечения информационной безопасности.

74. Моделирование и анализ fault-атак на аппаратные реализации криптосистем.

75. Анализ систем алгебраических уравнений, порождаемых упрощенными шифрами.

76. Методы сокрытия данных на различных носителях в стеганографии.

3.2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРОХОЖДЕНИЮ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

Основной формой обучения при прохождении преддипломной практики является самостоятельная работа студента, которая состоит из следующих элементов:

– изучение теоретического материала (полученные выводы оформляются в виде обзора с обязательными ссылками на источники информации);

– выполнение конкретных заданий (руководитель должен указать время на выполнение задания и вид требуемого результата);

– проведение исследований и вычислительных экспериментов (студент должен применить свои знания для впервые решаемых задач; руководителю нужно соотносить степень трудности задачи с возможностями практиканта; исследования и эксперименты должны завершатся выводами и рекомендациями по применению полученных результатов);

– формулировка выводов и рекомендаций.

Если в процессе работы у студента возникают вопросы, на которые он не может ответить самостоятельно, студент обращается к руководителю за консультацией. Студент должен точно указать, в чём он испытывает затруднение, характер затруднения и предполагаемый план действий.

Учебно-методическое и информационное обеспечение практики определяется на подготовительном этапе при составлении плана и зависит от базы прохождения практики.

Кроме этого студентам рекомендуется использовать следующие Internet-ресурсы:

1. http://www.cyberpolice.ru (Web-сервер подразделения по выявлению и пресечению преступлений, совершаемых с использованием поддельных кредитных карт, и преступлений, совершаемых путем несанкционированного доступа в компьютерные сети и базы данных)
2. http://www.infosecurity. report.ru/ (портал по информационной безопасности)
3. http://www.void.ru/ (портал по информационной безопасности)
4. http://www.infosec.ru/ (Сервер компании НИП «Информзащита»)
5. http://www.jetinfo.ru/ (Информационный бюллетень «Jet Info» с тематическим разделом по информационной безопасности)
6. http://www.bezpeka.com/ (Украинский Центр информационной безопасности)

3.3. ТРЕБОВАНИЯ К ОТЧЁТУ ПО ПРЕДДИПЛОМНОЙ ПРАКТИКЕ

Отчёт по преддипломной практике представляется для проверки в сброшюрованном виде (сшитым в папку или переплетённым). Отчёт оформляется в соответствии с требованиями технических нормативных правовых актов, предъявляемыми к текстовым документам.

Отчёт должен быть подписан руководителем практики от предприятия и заверен печатью. К отчёту прикладывается отзыв руководителя от предприятия о работе студента.

Содержание отчёта и рекомендуемый объём материалов:

– обложка-титульный лист (приложение 1);

– оглавление;

– раздел «Введение» (должен содержать краткую характеристику объекта практики; сведения о ведущих подразделениях и службах предприятия, о подразделении, где непосредственно проходила практика; описание технологии работ, выполняемых во время практики, перечень оборудования, технических средств, образцы нормативных документов, инструкций, используемых во время работы в подразделении; охрана труда и техники безопасности в организации);

– раздел «Постановка задачи» (задание на преддипломную практику);

– раздел «Обзор» (результаты ознакомительной части практики, обзор литературы, описание использованных аппаратных и программных средств, 1-2 стр.);

– раздел «Результаты» (структурированное изложение основных результатов и выводов по всем разделам задания, 5-8 стр.; задание на дипломную работу, 4-5 стр.);

– раздел «Рекомендации» (1 стр.);
– раздел «Список используемой литературы»
– приложения.

Отчёт должен содержать пояснительные иллюстрации, схемы, рисунки.

Рекомендуемое количество страниц отчёта 15-20.

Требования к оформлению отчета

1. Формат А4, шрифт Times New Roman, кегль шрифта – 14, интервал – одинарный.
2. Поля: левое – 2.5, верхнее, нижнее и правое – 2 см.
3. Абзацы в тексте начинаются с отступа.
4. Между заголовком и текстом межстрочный интервал должен составлять не менее двух.
5. Наименование структурных элементов отчета о практике следует печатать прописными буквами и располагать в начале строки, без точки в конце и без подчеркивания.
6. Форматирование основного текста – по ширине страницы.

3.4. ПОДВЕДЕНИЕ ИТОГОВ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

Текущий контроль за прохождением преддипломной практики осуществляется руководителями практики от предприятия и от кафедры.

В течение недели после окончания преддипломной практики в соответствии с графиком защиты студент сдаёт дифференцированный зачёт руководителю практики от университета. Критериями оценки результатов практики является актуальность тематики, достоверность полученных результатов, степень самостоятельности выполнения задания, объём проделанной работы, отзыв руководителей практики.

Для проверки на соответствие отчёта заданию и требованиям оформления, предварительной оценки и допуска к защите студент представляет отчёт о выполнении программы практики и письменный отзыв руководителя практики от предприятия о прохождении практики студентом.

Отзыв руководителя практики от предприятия должен содержать следующую информацию:

– сроки начала и окончания практики;
– название подразделения предприятия в котором работал студент;
– краткое описание работы, выполненной студентом;
– личностная характеристика студента-практиканта (профессиональная подготовка и отношение к работе);
– оценка, которую заслуживает студент.

Отзыв должен быть подписан руководителем практики от предприятия и заверен печатью с названием предприятия.

По результатам защиты отчёта студент получает оценку, которая выставляется в зачётную книжку. Положительная оценка позволяет студенту получить допуск к выполнению дипломной работы после успешной сдачи Государственного экзамена по специальности.

Сданный на кафедру отчёт и результат защиты, зафиксированный в ведомости и зачётной книжке студента, являются свидетельством успешного окончания преддипломной практики.

ПРИЛОЖЕНИЕ 1

Титульный лист отчёта по преддипломной практике

Министерство образования Республики Беларусь
Учреждение образования «Полоцкий государственный университет»

Факультет информационных технологий
Кафедра технологий программирования

ОТЧЁТ О ПРОХОЖДЕНИИ ПРЕДДИПЛОМНОЙ ПРАКТИКИ
на _____
(наименование предприятия)

в период с «_____» по «_____» _____ 20____г.

студента(ки) факультета информационных технологий 4 курса группы _____

_____ _____
(подпись) (Ф.И.О.)

Руководитель практики от кафедры технологий программирования

_____ _____
(подпись) (Ф.И.О.)

Руководитель практики от _____
(название организации)

_____ _____
(подпись) (Ф.И.О.)

ДОПОЛНЕНИЕ К ПРОГРАММЕ ПРЕДДИПЛОМНОЙ ПРАКТИКИ ДЛЯ СПЕЦИАЛЬНОСТИ 1-98 01 01 «Компьютерная безопасность»
(по направлениям)

№ пп	Дополнение	Основание
1.	Дополнить раздел 1.3 следующим содержанием: «При проведении организационного собрания студентов, руководитель практики от кафедры должен ознакомить студентов с Инструкцией по обеспечению безопасности обучающихся в период прохождения практики под роспись в Журнале регистрации инструктажа студентов по безопасному прохождению практики»	Приказ от 21.02.2018 № 103

Программа пересмотрена и одобрена на заседании кафедры технологий программирования
(протокол № № 3 от 1.03.2018 г.)

Заведующий кафедрой
Технологий программирования,
к.т.н., доцент О.В. Голубева

УТВЕРЖДАЮ

Декан факультета
информационных технологий,
д.т.н., доцент С.Г. Ехилевский