МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ПГТУ»)

РП СФОРМИРОВАНА, СОГЛАСОВАНА И УТВЕРЖДЕНА В ЭИОС

УТВЕРЖДАЮ
Декан ФИиВТ

УТВЕРЖДАЮ /А.А. Кречетов/
(Ф.И.О. декана (директора института))

31.01.2023 г.

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Направление подготовки (специальность): 10.05.03 Информационная безопасность автоматизированных систем

Квалификация выпускника: Специалист
(бакалавр/магистр/специалист)

Специализация: Анализ безопасности информационных систем

Распределение учебного времени

Трудоемкость по учебному плану	324 / 9	часов/зачетных единиц
Подготовка к сдаче и сдача государственного экзамена	108 / 3	часов/зачетных единиц
Подготовка к процедуре защиты и защита выпускной квалификационной работы	216 / 6	часов/зачетных единиц

(год)

Оборотная сторона титульного листа

Программа составлена в соответствии с требованиями ФГОС ВО направления подготовки (специальности) 10.05.03 Информационная безопасность автоматизированных систем

Программу составили:

заведующий кафедрой с ученой степенью доктора наук и ученым званием "профессор"	ИБ	СОГЛАСОВАНО	И.Г. Сидоркина
(должность)	(кафедра)		(И.О. Фамилия)

РАССМОТРЕНА и ОДОБРЕНА на заседании выпускающей кафедры

Кафедра информационной безопасности

(наименование кафедры)

31.01.2023 протокол № 10/1

(дата)

Заведующий кафедрой СОГЛАСОВАНО И.Г. Сидоркина

(подпись) (И.О. Фамилия)

Председатель методической комиссии факультета (института), в который входит выпускающая кафедра

СОГЛАСОВАНО А.А. Кречетов

(И.О. Фамилия)

Эксперт(ы): Зверева Екатерина Васильевна, Начальник отдела ПД ИТР ОАО ММЗ

Программа проверена и зарегистрирована в УМЦ 01.03.2023 г.
Специалист учебно-методического центра СОГЛАСОВАНО /И.Р. Валиева/

Раздел 1. ОБЩИЕ ПОЛОЖЕНИЯ

Программа ГИА включает:
1) методические материалы к:
- государственному экзамену: организация проведения, перечень дисциплин, фонд оценочных средств, методические указания по подготовке, перечень допускаемых материалов и средств;
- выпускной квалификационной работе (далее – ВКР): требования к ВКР и порядку её выполнения, перечень тематик ВКР;
- учебно-методическое обеспечение.
2) процедуры оценивания результатов освоения образовательной программы:
- государственный экзамен;
- выпускная квалификационная работа;
3) порядок подачи апелляции.
Программа государственной итоговой аттестации разрабатывается выпускающей кафедрой.

Раздел 2. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

2.1. Государственный экзамен

Государственный экзамен проводится в письменной форме по экзаменационным билетам. Экзаменационный билет включает 5 вопроса по 4 дисциплинам.

2.1.1. Перечень дисциплин (модулей), включенных в государственный экзамен

1. Анализ безопасности информационных систем

2. Разработка и эксплуатация автоматизированных систем в защищенном исполнении

3. Организационное и правовое обеспечение информационной безопасности

4. Программно-аппаратные средства защиты информации

2.1.2. Фонд оценочных средств. Пример оформления экзаменационного билета / теста

Дисциплина: Анализ безопасности информационных систем
1. Оценка за государственный экзамен выставляется по четырехбалльной шкале: 5 – «отлично», 4 – «хорошо», 3 – «удовлетворительно», 2 – «неудовлетворительно».
Дисциплина: Организационное и правовое обеспечение информационной безопасности
1. Оценка за государственный экзамен выставляется по четырехбалльной шкале: 5 – «отлично», 4 – «хорошо», 3 – «удовлетворительно», 2 – «неудовлетворительно».
Дисциплина: Программно-аппаратные средства защиты информации
1. Оценка за государственный экзамен выставляется по четырехбалльной шкале: 5 – «отлично», 4 – «хорошо», 3 – «удовлетворительно», 2 – «неудовлетворительно».
Дисциплина: Разработка и эксплуатация автоматизированных систем в защищенном исполнении
1. Оценка за государственный экзамен выставляется по четырехбалльной шкале: 5 – «отлично», 4 – «хорошо», 3 – «удовлетворительно», 2 – «неудовлетворительно».

2.1.3. Методические указания для обучающихся по подготовке к государственному экзамену

Поволжский государственный технологический университет

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Кафедра «Информационной безопасности»

ЭКЗАМЕНАЦИОННОЕ ЗАДАНИЕ

Итоговый междисциплинарный экзамен

по специальности 10.05.03

« Анализ безопасности информационных систем»

(2022/2023учебный год)

«УТВЕРЖДАЮ»

Декан ФИиВТ

_____Кречетов А.А.

«___»_____2023 г.

Поволжский государственный технологический университет

Зав.кафедрой «Информационной безопасности»

_____И.Г. Сидоркина

«___»_____2023 г.

Задание:

Необходимо предложить исходный алгоритм использования БД угроз ФСТЭК России для определения алгоритма действий по включению новой угрозы информационной безопасности информационных (автоматизированных) систем и их систем защиты

Выполнил:

Ст. гр. БИ 51

_____

Проверили:

_____

_____

_____

Йошкар-Ола

2023

Задача

Важным компонентом базы данных угроз (БДУ) Федеральной службы по техническому и экспортному контролю (ФСТЭК) является каталог уязвимостей. Данный каталог обновляется один раз в год или два. Каталог хорошо структурирован, имеет сквозную нотацию, а общее число описанных угроз постоянно увеличивается. Как указано в описании БДУ ФСТЭК: «Угрозы безопасности информации, включенные в состав банка данных угроз, не являются элементами иерархической классификационной системы угроз, а представляют собой обобщенный перечень

основных угроз безопасности информации, потенциально опасных для информационных систем».

Необходимо предложить исходный алгоритм использования БД угроз ФСТЭК России для определения алгоритма действий по включению новой угрозы информационной безопасности информационных (автоматизированных) систем и их систем защиты

Исходные данные

Краткое содержание информации

Имя файла

Формат файла

Регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России

K3_Pril1

PDF

DOC

Оценка уязвимостей CVSS 3.0

K3_Pril2

PDF

DOC

Подзадача 1

Банк данных угроз безопасности информации предназначен для заказчиков, операторов, разработчиков информационных (автоматизированных) систем и их систем защиты, разработчиков и производителей средств защиты информации, испытательных лабораторий и органов по сертификации средств защиты информации, а также иных заинтересованных организаций и лиц.

Банк данных угроз безопасности информации **содержит сведения о(об)…**

Решение

- основных угрозах безопасности информации и уязвимостях, в первую очередь, характерных для государственных информационных систем и автоматизированных систем управления производственными и технологическими процессами критически важных объектов.

- основных угрозах безопасности информации

- уязвимостях, в первую очередь, характерных для государственных информационных систем

- уязвимостях автоматизированных систем управления производственными и технологическими

процессами критически важных объектов.

не содержит сведения о(об)…

- рисках информационной безопасности критически важных объектов информационной инфраструктуры организации

- уязвимостях испытательных лабораторий и органов по сертификации средств защиты информации

Подзадача 2

Регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России определяет порядок взаимодействия ФАУ «ГНИИИ ПТЗИ ФСТЭК России», обеспечивающего функционирование банка данных угроз безопасности информации (далее – Оператор), с разработчиками и производителями программного обеспечения и программно-аппаратных средств (далее – изготовители), с организациями и специалистами, которые выявляют (обнаруживают) уязвимости программного обеспечения и программно -аппаратных средств (далее – исследователи), при включении информации об уязвимостях программного обеспечения и программно-аппаратных средств (далее – уязвимости) в банк данных угроз безопасности информации ФСТЭК России (далее – Банк данных угроз).

Сведения об уязвимостях могут быть получены Оператором…

При выполнении задания используйте данные из файла k1_Pril1

Решение

Сведения об уязвимостях могут быть получены Оператором:

- при поступлении информации об уязвимостях от изготовителей;
- при поступлении информации об уязвимостях от исследователей;
- при выполнении исследований по заданию ФСТЭК России.
    - **Сведения об уязвимостях не могут быть получены Оператором**
- при поступлении информации с критически важных объектов информационной инфраструктуры организации
- при поступлении информации о нарушениях регламентов испытательных лабораторий и органов по сертификации средств защиты информации
- при поступлении информации об уязвимостях, полученных в результате научных исследований, проводимых на объектах информатизации предприятий

Подзадача 3

Раскрытие информации об уязвимости осуществляется путем размещения описания уязвимости в Банке данных угроз. В соответствии с «Регламентом включения информации об уязвимостях программного обеспечения и программно-аппаратных средств» в банк данных угроз безопасности информации ФСТЭК России, информация об уязвимостях

может быть предоставлена в следующих случаях…

Решение

Раскрытие информации об уязвимости в Банке данных угроз осуществляется в случае, если:

- информация об уязвимости опубликована в иных общедоступных базах данных уязвимостей или источниках;

- информация об уязвимости и мерах по ее устранению получена от изготовителя в соответствии с Регламентом;

- изготовитель не принимает меры по устранению уязвимости в соответствии с Регламентом

информация об уязвимостях может не может быть предоставлена в следующих случаях

- изготовитель предпринял меры по устранению уязвимостей в соответствии с Регламентом

- информации об уязвимости и мерах по ее устранению получена от посторонних лиц

Подзадача 4

Показатель, характеризующий уровень опасности уязвимости определяется в соответствии с оценкой CVSS v.3.0. Установите соответствие между уровнем опасности уязвимости и ее числовым значением.

1. Критический - %place1%

2. Высокий - %place2%

3. Средний - %place3%

4. Низкий - %place4%

При выполнении задания используйте данные из файла k1_Pril2

Решение

Верно 10

Верно 8,1

Верно 4,2

Верно 0,5

Неверно 12

Подзадача 5

База данных угроз ФСТЭК – это самый большой каталог уязвимостей. Помимо важных и полезных Базы уязвимостей и Базы угроз, сайт БДУ ФСТЭК предлагает и дополнительные инструменты.

Решение

Каталог угроз в БДУ ФСТЭК **позволяет осуществлять контекстный поиск по**

- названию угрозы и применять фильтры по источнику угрозы и последствиям реализации угрозы

(нарушение конфиденциальности, целостности и/или доступности), как это представлено на рисунке

по

источникам реализации угрозы

по

последствиям реализации угрозы

не позволяет осуществлять контекстный поиск

по

критичности реализации угрозы

по

вероятности реализации угрозы

Исходные данные и источники

1. **РЕГЛАМЕНТ ВКЛЮЧЕНИЯ ИНФОРМАЦИИ ОБ УЯЗВИМОСТЯХ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ В БАНК ДАННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ФСТЭК РОССИИ**
2. **системе оценки уязвимости** Common Vulnerability Scoring System – CVSS
3. **и т.д.**

2.1.4. Перечень учебных, справочно-информационных и иных материалов, средств вычислительной техники и предметов, допускаемых к использованию обучающимися при сдаче государственного экзамена

Информационная безопасность автоматизированных систем: учебно- методическое пособие по подготовке и оформлению выпускных квалификационных работ для студентов специальности 10.05.03 / А.П. Александров, И.Г. Сидоркина, Ю.Ф. Гуринович, В.И. Смирнов. - Йошкар-Ола: Поволжский государственный технологический университет, 2021. - 40с.

2.2. Выпускная квалификационная работа

ВКР представляет собой выполненную обучающимся или совместно несколькими обучающимися работу, демонстрирующую уровень подготовленности выпускника (выпускников) к самостоятельной профессиональной деятельности. Защита ВКР является заключительным этапом проведения ГИА.

2.2.1. Требования к ВКР и порядку их выполнения.

Требования к ВКР и порядку их выполнения устанавливаются выпускающей кафедрой и определяют:

- форму ВКР;

- структуру ВКР, в том числе структуру пояснительной записки, состав графической части, состав и содержание презентационных материалов;

- содержание отдельных разделов ВКР;

- правила оформления текстовых и графических материалов.

Критерии оценки результатов защиты ВКР должны соответствовать критериям, принятым в р. 4 Фонд оценочных средств

Итоговая оценка выводится непосредственно после процедуры защиты ВКР на основе оценивания государственной экзаменационной комиссией компетенций выпускника и защиты выполненной им выпускной квалификационной работы.

Выпускная квалификационная работа оценивается по шкале: 5 – «отлично», 4 – «хорошо», 3 – «удовлетворительно», 2 – «неудовлетворительно».

2.2.2. Перечень тематик ВКР

1. Разработка фреймворка автоматизированного тестирования безопасности веб-приложений

2. Система управления информационной безопасностью в организации

3. Настройка механизмов защиты и блокировок в Astra linux (Смоленск)

4. Модернизация Системы Контроля и Управления Доступа на действующем объекте ООО «Специальное Конструкторно-Технологическое Бюро «Сатурн» с применением новых технологий идентификации

5.Разработка системы защиты данных в компании

2.3. Учебно-методическое обеспечение

№№ п/п	Список используемой литературы	Количество экземпляров печатных изданий, имеющихся в библиотеке, или электронный адрес издания (ресурса) в сети Интернет
УЧЕБНЫЕ, УЧЕБНО-МЕТОДИЧЕСКИЕ И НАУЧНЫЕ ИЗДАНИЯ		
1.	Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] / Нестеров С. А. Санкт-Петербург: Лань, 2023. - 324 с. ISBN 978-5-8114-6738-9.	https://e.lanbook.com/book/341267
2.	Прохорова, О. В. Информационная безопасность и защита информации [Электронный ресурс] : учебник для вузов / Прохорова О. В. 5-е изд., стер. Санкт-Петербург: Лань, 2023. - 124 с. ISBN 978-5-507-46010-6.	https://e.lanbook.com/book/293009
3.	Краковский, Ю. М. Методы защиты информации [Электронный ресурс] / Краковский Ю. М. 3-е изд., перераб. Санкт-Петербург: Лань, 2021. - 236 с. ISBN 978-5-8114-5632-1.	https://e.lanbook.com/book/156401
4.	Шаньгин, В. Ф. Информационная безопасность [Электронный ресурс] / В. Ф. Шаньгин. Москва: ДМК Пресс, 2014. - 702 с. ISBN 978-5-94074-768-0.	http://e.lanbook.com/books/element.php?pl1_id=50578
ЭЛЕКТРОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ		
1.	Научная электронная библиотека eLIBRARY.RU	http://elibrary.ru
2.	Научная электронная библиотека «Киберленинка»	http://cyberleninka.ru
ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ		
1.	Справочно-правовая система Консультант+	http://www.consultant.ru

2.	Информационно-правовой портал Гарант	http://www.garant.ru
3.	Профессиональные справочные системы Техэксперт	http://www.cntd.ru

РАЗДЕЛ 3. ПРОЦЕДУРА ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процедура оценивания результатов освоения ОПОП включает:
- перечень компетенций;
- критерии оценивания, шкалу оценивания;
- методические материалы, определяющие процедуры оценивания результатов освоения ОПОП.

3.1. Государственный экзамен

Перечень компетенций, оцениваемых при проведении государственного экзамена

Код компетенции	Наименование компетенции
УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий
УК-2	Способен управлять проектом на всех этапах его жизненного цикла
УК-3	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели
УК-4	Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия
УК-5	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия
УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни
УК-7	Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности
УК-8	Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов
УК-9	Способен принимать обоснованные экономические решения в различных областях жизнедеятельности
УК-10	Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности
ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства
ОПК-2	Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности
ОПК-3	Способен использовать математические методы, необходимые для решения задач профессиональной деятельности
ОПК-4	Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники,

	применять основные физические законы и модели для решения задач профессиональной деятельности
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
ОПК-7	Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ
ОПК-8	Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах
ОПК-9	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации
ОПК-10	Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности
ОПК-11	Способен разрабатывать компоненты систем защиты информации автоматизированных систем
ОПК-12	Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем
ОПК-13	Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем
ОПК-14	Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования проектных решений
ОПК-15	Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем
ОПК-16	Способен анализировать основные этапы и закономерности исторического развития России, её место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма
ОПК-17	Способен использовать программные и программно-аппаратные средства для моделирования и испытания систем защиты информационных
ОПК-18	Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы и её соответствия нормативным требованиям по зашите информации
ОПК-19	Способен проводить анализ защищенности и верификацию программного обеспечения информационных систем

ПК-1	Способен использовать языки, системы, инструментальные программные и аппаратные средства для моделирования информационных систем и испытаний систем защиты
ПК-2	Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы, соответствия нормативным требованиям по защите информации
ПК-3	Способен разрабатывать модели угроз и модели нарушителя информационной безопасности, планировать объем тестовых проверок
ПК-4	Способен применять инструментарий анализа безопасности программного обеспечения

Критерии оценивания компетенций, шкала оценивания

Шкала оценивания	Критерии оценивания компетенций, шкала оценивания
«отлично» / компетенции сформированы в полном объеме	В ответе на вопросы экзаменационного билета на отличном уровне продемонстрировано: - понимание исследуемого вопроса, уровень теоретической и научно-исследовательской проработки проблемы, качество анализа проблемы; - умение находить, отбирать, систематизировать, анализировать информацию, критическое использование рекомендуемой литературы (основной и дополнительной); - владение культурой мышления, продуманность, творческий подход к освещению вопроса, умение аргументировать, иллюстрировать ответ примерами, применять полученные знания при решении практических вопросов и задач. Приведены примеры
«хорошо» / компетенции сформированы в достаточном объеме	В ответе на вопросы экзаменационного билета на хорошем уровне продемонстрировано: - понимание исследуемого вопроса, уровень теоретической и научно-исследовательской проработки проблемы, качество анализа проблемы; - умение находить, отбирать, систематизировать, анализировать информацию, критическое использование рекомендуемой литературы (основной и дополнительной); - владение культурой мышления, продуманность, творческий подход к освещению вопроса, умение аргументировать, иллюстрировать ответ примерами, применять полученные знания при решении практических вопросов и задач. Приведены отдельные примеры
«удовлетворительно» / компетенции сформированы частично	В ответе на вопросы экзаменационного билета на удовлетворительном уровне продемонстрировано: - понимание исследуемого вопроса, уровень теоретической и научно-исследовательской проработки проблемы, качество анализа проблемы; - умение находить, отбирать, систематизировать, анализировать информацию, критическое использование рекомендуемой литературы (основной и дополнительной); - владение культурой мышления, продуманность, творческий подход к освещению вопроса, умение аргументировать, иллюстрировать ответ примерами, применять полученные знания при решении практических вопросов и задач. Примеры отсутствуют
«неудовлетворительно» / компетенции не сформированы	В ответе на вопросы экзаменационного билета не продемонстрировано: - понимание исследуемого вопроса, уровень теоретической и научно-исследовательской проработки проблемы, качество анализа проблемы; - умение находить, отбирать, систематизировать, анализировать информацию, критическое использование рекомендуемой литературы (основной и дополнительной); - владение культурой мышления, продуманность, творческий подход к освещению вопроса, умение аргументировать, иллюстрировать ответ примерами, применять полученные знания при решении практических вопросов и задач. Примеры отсутствуют

При проведении государственного экзамена члену ГЭК выдается бланк «Перечень компетенций, оцениваемых при проведении государственного экзамена» и «Бланк оценивания результатов сдачи государственного экзамена» (приложение 1).

Оценка ответа обучающегося проставляется членом комиссии в «Бланк оценивания

результатов сдачи государственного экзамена». При оценивании ответа член комиссии должен проставить баллы в разрезе каждой компетенции по установленной шкале.
Оценка за государственный экзамен выставляется по четырехбалльной шкале: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».
На основании «Бланк оценивания результатов сдачи государственного экзамена» секретарем ГЭК составляется протокол заседания ГЭК по приему государственного экзамена (по установленной форме) и производится анализ уровня освоения компетенции в целом группе.

3.2. Выпускная квалификационная работа

Перечень компетенций, оцениваемых при защите ВКР

Код компетенции	Наименование компетенции
ПК-1	Способен использовать языки, системы, инструментальные программные и аппаратные средства для моделирования информационных систем и испытаний систем защиты
ПК-2	Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы, соответствия нормативным требованиям по защите информации
ПК-3	Способен разрабатывать модели угроз и модели нарушителя информационной безопасности, планировать объем тестовых проверок
ПК-4	Способен применять инструментарий анализа безопасности программного обеспечения

Критерии оценивания компетенций, шкала оценивания

Шкала оценивания	Критерии оценивания компетенций, шкала оценивания
«отлично» / компетенции сформированы в полном объеме	При выполнении выпускной квалификационной работы и в ходе защиты выпускник продемонстрировал отличный: - уровень теоретической и научно-исследовательской проработки проблемы; - понимание исследуемого вопроса; - качество анализа проблемы; - самостоятельность разработки, обоснованность результатов и выводов; - степень владения современным математическим аппаратом, программными продуктами и компьютерными технологиями; - иллюстративность, качество презентации результатов работы; - навыки публичной дискуссии.
«хорошо» / компетенции сформированы в достаточном объеме	При выполнении выпускной квалификационной работы и в ходе защиты выпускник продемонстрировал хороший: - уровень теоретической и научно-исследовательской проработки проблемы; - понимание исследуемого вопроса; - качество анализа проблемы; - самостоятельность разработки, обоснованность результатов и выводов; - степень владения современным математическим аппаратом, программными продуктами и компьютерными технологиями; - иллюстративность, качество презентации результатов работы; - навыки публичной дискуссии.
«удовлетворительно» / компетенции сформированы	При выполнении выпускной квалификационной работы и в ходе защиты выпускник продемонстрировал удовлетворительный: - уровень теоретической и научно-исследовательской проработки

частично	проблемы; - понимание исследуемого вопроса; - качество анализа проблемы; - самостоятельность разработки, обоснованность результатов и выводов; - степень владения современным математическим аппаратом, программными продуктами и компьютерными технологиями; - иллюстративность, качество презентации результатов работы; - навыки публичной дискуссии.
«неудовлетворительно» / компетенции не сформированы	При выполнении выпускной квалификационной работы и в ходе защиты выпускник не продемонстрировал: - уровень теоретической и научно-исследовательской проработки проблемы; - понимание исследуемого вопроса; - качество анализа проблемы; - самостоятельность разработки, обоснованность результатов и выводов; - степень владения современным математическим аппаратом, программными продуктами и компьютерными технологиями; - иллюстративность, качество презентации результатов работы; - навыки публичной дискуссии.

Особое внимание при оценивании выпускной квалификационной работы обращается на возможность практического использования данных, полученных в работе. Должны учитываться также: уровень доклада на защите; соответствие оформления работы установленным требованиям; качество иллюстративного материала к докладу.

При проведении защиты выпускной квалификационной работы члену ГЭК выдается бланк «Перечень компетенций, оцениваемых при защите ВКР» и «Бланк оценивания защиты ВКР» (приложение 2).

Итоговая оценка выводится непосредственно после окончания защиты выпускных квалификационных работ на основе оценивания государственной экзаменационной комиссией компетенций обучающегося и защиты выполненной им выпускной квалификационной работы. Итоговая оценка выставляется по четырехбалльной шкале: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Секретарь ГЭК на основании «Бланк оценивания защиты ВКР» составляет Протокол заседания ГЭК по защите ВКР.

РАЗДЕЛ 4. ПОРЯДОК ПОДАЧИ АПЕЛЛЯЦИИ.

Порядок подачи апелляции установлен в СМК-ПИ-3.01-07 «Положение о государственной итоговой аттестации обучающихся ПГТУ».

Приложение 1

Бланк оценивания результатов сдачи государственного экзамена

Институт/Факультет/Центр Факультет информатики и вычислительной техники

Кафедра Кафедра информационной безопасности

Направление подготовки 10.05.03 (о) - ст. - БИ

Наименование ОП 32 - Анализ безопасности информационных систем

ФИО обучающегося	**Балл по компетенции в соответствии с критериями оценивания***																														**Средний балл**	**Оценка** («отлично», «хорошо», «удовлетворительно», «неудовлетворительно»)
	УК-1	**УК-2**	**УК-3**	**УК-4**	**УК-5**	**УК-6**	**УК-7**	**УК-8**	**УК-9**	**УК-10**	**ОПК-1**	**ОПК-2**	**ОПК-3**	**ОПК-4**	**ОПК-5**	**ОПК-6**	**ОПК-7**	**ОПК-8**	**ОПК-9**	**ОПК-10**	**ОПК-11**	**ОПК-12**	**ОПК-13**	**ОПК-14**	**ОПК-15**	**ОПК-16**	**ОПК-17**	**ОПК-18**	**ОПК-19**	**ПК-1**	**ПК-2**	**ПК-3**	**ПК-4**		
1.																																		
2.																																		
3.																																		

** Ответ обучающегося оценивается в разрезе компетенции, исходя из принятой шкалы оценивания*

Председатель ГЭК _____
(подпись)

Члены ГЭК _____
(подпись)

_____
(подпись)

_____
(подпись)

_____
(подпись)

(«отлично», «хорошо», «удовлетворительно», «неудовлетвор

Приложение 2

Бланк оценивания защиты ВКР

Институт/Факультет/Центр	Факультет информатики и вычислительной техники
Кафедра	Кафедра информационной безопасности
Направление подготовки	10.05.03 (о) - ст. - БИ
Наименование ОП	32 - Анализ безопасности информационных систем

ФИО обучающегося	**Балл по компетенции в соответствии с критериями оценивания***				**Средний балл**	**Оценка** («отлично», «хорошо», «удовлетворительно», «неудовлетворительно»)
	ПК-1	**ПК-2**	**ПК-3**	**ПК-4**		
1.						
2.						
3.						

** ВКР обучающегося оценивается в разрезе компетенции, исходя из принятой шкалы оценивания*

Председатель ГЭК _____ *(подпись)*

Члены ГЭК _____ *(подпись)*

_____ *(подпись)*

_____ *(подпись)*

(подпись)