



Федеральное государственное бюджетное образовательное  
учреждение  
высшего профессионально образования  
«Российский государственный социальный университет»

«УТВЕРЖДАЮ»

Декан факультета  
информационных технологий

/С.В.Крапивка/  
«01»\_июля\_2020

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ  
ДЛЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ (ИТОГОВОЙ) АТТЕСТАЦИИ  
ОБУЧАЮЩИХСЯ**

Наименование образовательной программы  
**Безопасность информационных технологий в правоохранительной сфере**

Специальность  
**10.05.05 Безопасность информационных технологий в правоохранительной сфере**

Специализация  
**Технологии защиты информации в правоохранительной сфере**

**ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА ВЫСШЕГО ОБРАЗОВАНИЯ - ПРОГРАММА  
СПЕЦИАЛИТЕТА**

Уровень профессионального образования  
**Высшее образование – специалитет**

Форма обучения  
**Очная**

Москва, 2022 г.

Основная профессиональная образовательная программа **высшего образования «Безопасность информационных технологий в правоохранительной сфере»** составлена на основании федерального государственного образовательного стандарта высшего образования по специальности **10.05.05 Безопасность информационных технологий в правоохранительной сфере**, утвержденного приказом Министерства образования и науки Российской Федерации от 26.11.2020 № 1461, профессионального стандарта «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 01.11.2016 №598н, профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15.09.2016 № 522н, профессионального стандарта «Специалист по технической защите информации», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 01.11.2016 № 599н, профессионального стандарта «Следователь-криминалист», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 23.03.2015 № 183н.

Фонд оценочных средств для государственной итоговой (итоговой) аттестации обучающихся по основной профессиональной образовательной программе разработан рабочей группой в составе: д.ф.-м.н, профессора Краснова А.Е., к.т.н., к.ф.-м.н., доцента Мельниковой Е.А.

Руководитель основной профессиональной образовательной программы  
к.ф.-м.н., доцент



Е.А. Мельникова

\_\_\_\_\_  
(подпись)

Фонд оценочных средств для государственной итоговой (итоговой) аттестации обучающихся по основной профессиональной образовательной программе обсужден и утвержден на Ученом совете факультета информационных технологий  
(наименование факультета)

Протокол № 10 от «06» июня 2022 года

Декан факультета  
к.п.н, доцент



С.В.Крапивка

\_\_\_\_\_  
(подпись)

Фонд оценочных средств для государственной итоговой (итоговой) аттестации обучающихся по основной профессиональной образовательной программе «Безопасность информационных технологий в правоохранительной сфере» рекомендован к утверждению представителями организаций-работодателей:

АО ПВП «Амулет»  
зам. ген. директора по науке,  
к.т.н., доцент



А.С.Мосолов

\_\_\_\_\_  
(подпись)

д.т.н. , доцент, профессор кафедры информационных технологий ,  
ГБОУВО Академия ГПС МЧС России)



С.Ю. Бутузов

\_\_\_\_\_  
(подпись)

## Содержание

1. Форма государственных аттестационных испытаний по основной профессиональной образовательной программе ..... **Ошибка! Закладка не определена.**

2. Перечень компетенций, которыми должны овладеть обучающиеся в результате освоения основной профессиональной образовательной программы **Ошибка! Закладка не определена.**

3. Описание показателей и критериев оценивания компетенций, а также шкал оценивания  
**Ошибка! Закладка не определена.**

4. Типовые контрольные задания или иные материалы, необходимые для оценки конкретных результатов освоения образовательной программы, перечень которых определяется образовательной организацией совместно с работодателями и (или) их объединениями. **Ошибка! Закладка не определена.**

## **1. Форма государственных аттестационных испытаний по основной профессиональной образовательной программе**

Государственная итоговая (итоговая) аттестация обучающихся по основной профессиональной образовательной программе высшего образования «**Безопасность информационных технологий в правоохранительной сфере**» включает в себя защиту выпускной квалификационной работы.

## **2. Перечень компетенций, которыми должны овладеть обучающиеся в результате освоения основной профессиональной образовательной программы**

<b>Категория универсальных компетенций</b>	<b>Код универсальной компетенции</b>	<b>Формулировка компетенции</b>	<b>Код и наименование индикатора достижения универсальной компетенции</b>
Системное и критическое мышление	УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Анализирует задачу, выделяя ее базовые составляющие
			УК-1.2. Определяет, интерпретирует и ранжирует информацию, требуемую для решения поставленной задачи
			УК-1.3. Осуществляет поиск информации для решения поставленной задачи по различным типам запросов
			УК-1.4. При обработке информации отличает факты от мнений, интерпретаций, оценок, формирует собственные мнения и суждения, аргументирует свои выводы и точку зрения
			УК-1.5. Рассматривает и предлагает возможные варианты решения поставленной задачи, оценивая их достоинства и недостатки
Разработка и реализация проектов	УК-2	Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Определяет круг задач в рамках поставленной цели, определяет связи между ними
			УК-2.2. Предлагает способы решения поставленных задач и ожидаемые результаты; оценивает предложенные способы с точки зрения соответствия цели проекта
			УК-2.3 Планирует реализацию задач в зоне своей ответственности с учетом имеющихся ресурсов и ограничений, действующих правовых норм
			УК-2.4 Выполняет задачи в зоне своей ответственности в соответствии с запланированными результатами и точками

			<p>контроля, при необходимости корректирует способы решения задач</p> <p>УК-2.5 Представляет результаты проекта, предлагает возможности их использования и/или совершенствования</p>
Командная работа и лидерство	УК-3	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.1 Определяет свою роль в социальном взаимодействии и командной работе, исходя из стратегии сотрудничества для достижения поставленной цели
			УК-3.2 При реализации своей роли в социальном взаимодействии и командной работе учитывает особенности поведения и интересы других участников
			УК-3.3. Анализирует возможные последствия личных действий в социальном взаимодействии и командной работе и строит продуктивное взаимодействие с учетом этого
			УК-3.4. Осуществляет обмен информацией, знаниями и опытом с членами команды; оценивает идеи других членов команды для достижения поставленной цели
			УК-3.5 Соблюдает нормы и установленные правила командной работы; несет личную ответственность за результат
Коммуникация	УК-4	Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК-4.1. Выбирает стиль общения на русском языке в зависимости от цели и условий партнерства; адаптирует речь, стиль общения и язык жестов к ситуациям взаимодействия
			УК-4.2. Ведет деловую переписку на русском языке с учетом особенностей стилистики официальных и неофициальных писем
			УК-4.3. Выполняет для личных целей перевод официальных и профессиональных текстов с иностранного языка на русский, с русского языка на иностранный
			УК-4.4. Публично выступает на русском языке, строит свое выступление с учетом аудитории и цели общения
			УК-4.5. Устно представляет результаты своей деятельности на иностранном

			языке, может поддержать разговор в ходе их обсуждения.
Межкультурное взаимодействие	УК-5	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК-5.1. Отмечает и анализирует особенности межкультурного взаимодействия (преимущества и возможные проблемные ситуации), обусловленные различием этических, религиозных и ценностных систем
			УК-5.2. Предлагает способы преодоления коммуникативных барьеров при межкультурном взаимодействии
			УК-5.3. Определяет условия интеграции участников межкультурного взаимодействия для достижения поставленной цели с учетом исторического наследия и социокультурных традиций различных социальных групп, этносов и конфессий.
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни	УК-6.1. Оценивает свои ресурсы и их пределы (личностные, ситуативные, временные), оптимально их использует для успешного выполнения порученного задания
			УК-6.2. Определяет приоритеты профессионального роста и способы совершенствования собственной деятельности на основе самооценки по выбранным критериям
			УК-6.3. Выстраивает гибкую профессиональную траекторию, используя инструменты непрерывного образования, с учетом накопленного опыта профессиональной деятельности и динамично изменяющихся требований рынка труда
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-7	Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	УК-7.1. Выбирает здоровьесберегающие технологии для поддержания здорового образа жизни с учетом физиологических особенностей организма и условий реализации профессиональной деятельности
			УК-7.2. Планирует свое рабочее и свободное время для оптимального сочетания

			<p>физической и умственной нагрузки и обеспечения работоспособности</p> <p>УК-7.3. Соблюдает и пропагандирует нормы здорового образа жизни в различных жизненных ситуациях и в профессиональной деятельности.</p>
Безопасность жизнедеятельности	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	<p>УК-8.1. Анализирует факторы вредного влияния элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений)</p> <p>УК-8.2. Идентифицирует опасные и вредные факторы в рамках осуществляемой деятельности</p> <p>УК-8.3. Выявляет проблемы, связанные с нарушениями техники безопасности на рабочем месте; предлагает мероприятия по предотвращению чрезвычайных ситуаций</p>
Экономическая культура, в том числе финансовая грамотность	УК-9	Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	<p>УК-9.1. Понимает базовые принципы функционирования экономики и экономического развития, цели формы участия государства в экономике</p> <p>УК-9.2. Применяет методы личного экономического и финансового планирования для достижения текущих и долгосрочных финансовых целей, использует финансовые инструменты для управления личными финансами (личным бюджетом), контролирует собственные экономические и финансовые риски</p>
Гражданская позиция	УК-10	Способен формировать нетерпимое отношение к коррупционному поведению	<p>УК-10.1. Анализирует действующие правовые нормы, обеспечивающие борьбу с коррупцией в различных областях жизнедеятельности, а также способы профилактики коррупции и формирования нетерпимого отношения к ней</p> <p>УК-10.2. Планирует, организует и проводит мероприятия, обеспечивающие формирование гражданской</p>

			позиции и предотвращение коррупции в обществе
			УК-10.3. Соблюдает правила общественного взаимодействия на основе нетерпимого отношения к коррупции

<b>Категория общепрофессиональных компетенций</b>	<b>Код общепрофессиональной компетенции</b>	<b>Формулировка компетенции</b>	<b>Код и наименование индикатора достижения общепрофессиональной компетенции</b>
Ценностно-мотивационная ориентация	ОПК-1	Способен на основе анализа основных этапов и закономерностей исторического развития российского государства, его места и роли в контексте всеобщей истории формировать устойчивые внутренние мотивы профессионально-служебной деятельности, базирующиеся на гражданской позиции, патриотизме, ответственном отношении к выполнению профессионального долга	ОПК-1.1. Знает основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире
			ОПК-1.2. Умеет формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории
			ОПК-1.3. Владеет навыками по соотнесению общих исторических процессов и отдельных фактов, выявлению существенных черт исторических процессов, явлений и событий
Ценностно-мотивационная ориентация	ОПК-2	Способен анализировать мировоззренческие, социальные и личностно-значимые проблемы в целях формирования ценностных, этических основ профессионально-служебной деятельности	ОПК-2.1. Знать: профессиональные задачи и принципы служебного этикета в соответствии с нормами морали
			ОПК-2.2. Уметь выполнять профессиональные задачи в соответствии с нормами морали, профессиональной этики и служебного этикета
			ОПК-2.3. Владеть навыками выполнять профессиональные задачи в соответствии с нормами морали и служебного этикета
Проектно-технологические	ОПК-3	Способен использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных	ОПК-3.1. Знает основы математики, законы физики, основные методы оптимального кодирования источников информации
			ОПК-3.2. Умеет исследовать функциональные зависимости, возникающие при решении стандартных прикладных задач



		задач	ОПК-3.3. Владеет навыками использования справочных материалов по математическому анализу, использования расчетных формул и таблиц при решении стандартных вероятностно-статистических задач, самостоятельного решения комбинированных задач
	ОПК-4	выполнять технико-экономическое обоснование проектных решений по созданию систем обеспечения информационной безопасности, разрабатывать рабочую техническую документацию в соответствии с действующими нормативными и методическими документами в области защиты информации	ОПК-4.1. Знает принципы формирования политики информационной безопасности в информационных системах; основные этапы процесса проектирования и общие требования к содержанию проекта
			ОПК-4.2. Умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащих защите; анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации
			ОПК-4.3. Владеет навыками по разработке основных показателей технико-экономического обоснования соответствующих проектных решений
	ОПК-5	Способен планировать проведение работ по комплексной защите информации на объекте информатизации	ОПК-5.1. Знает основные приемы планирования проведения работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации
			ОПК-5.2. Умеет планировать проведение работ по комплексной защите информации и сведений, составляющих государственную тайну, на объекте информатизации
			ОПК-5.3. Владеет методами теоретического и инструментального анализа выявления и предотвращения образования технических каналов утечки информации
Проектно-технологические	ОПК-6	Способен применять положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач в	ОПК-6.1. Знает положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи
			ОПК-6.2. Умеет применять знания о системах электрической связи для

			<p>решения задач по созданию защищенных телекоммуникационных систем; - анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи</p> <p>ОПК-6.3. Владеет навыками безопасного использования технических средств в профессиональной деятельности; навыками проведения контрольных проверок работоспособности и эффективности средств защиты информации.</p>
	ОПК-7	Способен применять в практической деятельности основные концепции, принципы, теории и факты, связанные с информатикой	<p>ОПК-7.1. Знает основные принципы построения компьютера, формы и способы представления данных; области и особенности применения языков программирования высокого уровня</p> <p>ОПК-7.2. Умеет работать с интегрированной средой разработки программного обеспечения; разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач</p> <p>ОПК-7.3. Владеет навыками разработки, документирования, тестирования и отладки программ; разработки алгоритмов решения типовых профессиональных задач</p>
Эксплуатационные	ОПК-8	Способен реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз	<p>ОПК-8.1. Знает основные технические каналы утечки информации, физические принципы их возникновения, методы и средства обнаружения технических каналов утечки информации</p> <p>ОПК-8.2. Умеет обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз</p> <p>ОПК-8.3. Владеет технологиями установки, настройки и обслуживания технических средств обеспечения безопасности современной электронной аппаратуры</p>
Аналитические	ОПК-9	Способен применять технологии получения, накопления, хранения,	ОПК-9.1. Знает классификацию современных компьютерных систем, типовые структуры и принципы

		<p>обработки, интерпретации и использования информации в ходе профессиональной деятельности</p>	<p>организации компьютерных сетей; назначение, функции и обобщенную структуру операционных систем; назначение и основные компоненты систем баз данных</p> <p>ОПК-9.2. Умеет применять типовые программные средства сервисного назначения и пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети Интернет</p> <p>ОПК-9.3. Владеет навыками поиска информации в глобальной информационной сети Интернет; применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности</p>
	ОПК-10	<p>Способен осуществлять аналитическую деятельность с последующим использованием данных при решении профессиональных задач</p>	<p>ОПК-10.1. Знает принципы и порядок работы информационно-справочных систем; способы поиска и обработки информации, методы работы с научной информацией</p> <p>ОПК-10.2. Умеет обобщать, анализировать и систематизировать научную информацию в области информационной безопасности; пользоваться информационно-справочными системами</p> <p>ОПК-10.3. Владеет навыком составления и оформления отчетных документов по результатам обзора научно-технической литературы, нормативных и методических документов</p>
	ОПК-11	<p>Способен использовать автоматизированные информационные системы в профессиональной деятельности</p>	<p>ОПК-11.1. Знает принципы построения систем защиты информации; критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем; основные угрозы безопасности информации и модели нарушителя</p> <p>ОПК-11.2. Умеет анализировать угрозы безопасности информации, оценивать информационные риски; применять аналитические и компьютерные модели автоматизированных систем и систем защиты информации; анализировать программные и программно-аппаратные решения при проектировании системы защиты информации с целью</p>

			<p>выявления уязвимостей</p> <p>ОПК-11.3 Владеет навыками расчета показателей эффективности защиты информации, обрабатываемой в автоматизированных системах; проведения анализа уязвимости программного и программно-аппаратных средств защиты информации</p>
Информационно-коммуникационные технологии для профессиональной деятельности	ОПК-12	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	<p>ОПК-12.1. Знает программно-аппаратные средства защиты информации в типовых операционных системах, системах управления базами данных, компьютерных сетях</p>
			<p>ОПК-12.2. Умеет конфигурировать программно-аппаратные средства защиты информации в соответствии с заданными политиками безопасности</p>
			<p>ОПК-12.3. Владеет методами оценки, тестирования, настройки на применение средств программно-аппаратного обеспечения защиты информации</p>

### **3. Описание показателей и критериев оценивания компетенций, а также шкал оценивания**

<b>Код(ы) компетенции (ий)</b>	<b>Показатели оценивания</b>	<b>Критерии и шкалы оценивания</b>
ОПК-3; ОПК-4; ОПК-6; ОПК-7; ОПК-9; ОПК-10; ОПК-11; ОПК-12; ПК-1; ПК-2; ПК-6; ПК-3; ПК-5; ПК-4; ПК-7; ПК-8	Содержание ВКР: актуальность, полнота раскрытия темы, научный аппарат ВКР, обоснованность, соответствие работы профилю направления подготовки / специальности, установленным методическим требованиям к	1) обучающийся продемонстрировал умение эффективно решать задачи, соответствующие квалификационной характеристике, высокий уровень практической и теоретической подготовленности, владеет профессиональными технологиями, разрабатывает новые подходы к решению профессиональных проблем; актуальность темы работы, широко использованы современные компьютерные технология, высокая

	<p>оформлению работы выводов и рекомендаций, отражение в работе прохождения обучающимся практик</p>	<p>корректность использования методов и моделей, ВКР отличается оригинальностью и новизной полученных результатов, высокой практикой значимостью состояние вопроса оценено максимально подробно, практическая значимость работы – уровень оценки «отлично»;</p> <p>2) обучающийся продемонстрировал умение решать задачи, соответствующие квалификационной характеристике, устойчивый уровень практической и теоретической подготовленности, владеет основными профессиональными технологиями, использует новые подходы к решению профессиональных проблем – уровень оценки «хорошо»;</p> <p>3) обучающийся решает типовые задачи, соответствующие квалификационной характеристике, практически и теоретически подготовлен к исполнению поставленных задач, владеет отдельными профессиональными технологиями, использует типовые подходы к решению профессиональных проблем – уровень оценки «удовлетворительно»;</p> <p>4) обучающийся продемонстрировал низкий уровень умения решать задачи, соответствующие квалификационной характеристике, низкую практическую и теоретическую подготовленность, не владеет профессиональными технологиями, не готов использовать типовые подходы к решению профессиональных проблем - уровень оценки «неудовлетворительно»;</p> <p>5) выпускная квалификационная работа не представлена</p>
<p>ОПК-3; ОПК-4; ОПК-6; ОПК-7; ОПК-9; ОПК-10; ОПК-11; ОПК-12; ПК-1; ПК-2; ПК-6; ПК-3; ПК-5; ПК-4; ПК-7; ПК-8</p>	<p>Защита ВКР: доклад обучающегося (в т.ч. наличие презентационного и раздаточного материала и т.д.), аргументированность ответа на вопросы членов ГЭК и замечания рецензента</p>	<p>1) доклад структурирован, раскрывает причины выбора темы и ее актуальность, цель, задачи, предмет, объект исследования, логику получения каждого вывода; в заключительной части доклада показаны перспективы и задачи дальнейшего исследования данной темы, освещены вопросы практического применения и внедрения результатов исследования в практику ВКР выполнена в соответствии с</p>

		<p>целевой установкой, отвечает предъявляемым требованиям и оформлена в соответствии со стандартом; представленный демонстрационный материал высокого качества в части оформления и полностью соответствует содержанию ВКР и доклада; ответы на вопросы членов ГЭК показывают глубокое знание исследуемой проблемы, подкрепляются ссылками на соответствующие литературные источники, выводами и расчетами из ВКР, демонстрируют самостоятельность и глубину изучения проблемы студентом; результат оценки уровня сформированности компетенций (в соответствии с оценочными листами руководителя, рецензента, членов ГЭК) составляет уровень оценки «отлично»</p> <p>2) доклад структурирован, допускаются одна-две неточности при раскрытии причин выбора и актуальности темы, цели, задач, предмета, объекта исследования, но эти неточности устраняются при ответах на дополнительные уточняющие вопросы. ВКР выполнена в соответствии с целевой установкой, отвечает предъявляемым требованиям и оформлена в соответствии со стандартом. представленный демонстрационный материал хорошего качества в части оформления и полностью соответствует содержанию ВКР и доклада; ответы на вопросы членов ГЭК показывают хорошее владение материалом, подкрепляются выводами и расчетами из ВКР, показывают самостоятельность и глубину изучения проблемы студентом; результат оценки уровня сформированности компетенций (в соответствии с оценочными листами руководителя, рецензента, членов ГЭК) составляет уровень оценки «хорошо»;</p> <p>3) доклад структурирован, допускаются неточности при раскрытии причин выбора и актуальности темы, цели, задач, предмета, объекта исследования, но эти неточности устраняются в ответах на дополнительные вопросы; ВКР выполнена в соответствии с</p>
--	--	--

		<p>целевой установкой, но не в полной мере отвечает предъявляемым требованиям; представленный демонстрационный материал удовлетворительного качества в части оформления и в целом соответствует содержанию ВКР и доклада; ответы на вопросы членов ГЭК носят недостаточно полный и аргументированный характер, не раскрывают до конца сущности вопроса, слабо подкрепляются выводами и расчетами из ВКР, показывают недостаточную самостоятельность и глубину изучения проблемы студентом; результат оценки уровня сформированности компетенций (в соответствии с оценочными листами руководителя, рецензента, членов ГЭК) составляет уровень оценки «удовлетворительно»;</p> <p>4) доклад недостаточно структурирован, допускаются существенные неточности при раскрытии причин выбора и актуальности темы, цели, задач, предмета, объекта исследования, эти неточности не устраняются в ответах на дополнительные вопросы; ВКР не отвечает предъявляемым требованиям; представленный демонстрационный материал низкого качества в части оформления и не соответствует содержанию ВКР и доклада; ответы на вопросы членов ГЭК носят неполный характер, не раскрывают сущности вопроса, не подкрепляются выводами и расчетами из ВКР, показывают недостаточную самостоятельность и глубину изучения проблемы студентом. результат оценки уровня сформированности компетенций (в соответствии с оценочными листами руководителя, рецензента, членов ГЭК) составляет уровень оценки «неудовлетворительно»;</p> <p>5) защита ВКР не проведена, на заданные вопросы обучающихся не представил ответы</p>
--	--	--

**4. Типовые контрольные задания или иные материалы, необходимые для оценки конкретных результатов освоения образовательной программы, перечень которых**

**определяется образовательной организацией совместно с работодателями и (или) их объединениями.**

### **Примерная тематика выпускных квалификационных работ**

1. Внедрение центра управления безопасностью (SOC) в коммерческом банке
2. Разработка комплекса защитных мер по обеспечению ИБ баз данных 1С на примере компании
3. Разработка комплексной системы защиты информации компании
4. Разработка комплекса мероприятий, позволяющих уменьшить вероятность реализации угроз информационной безопасности компании
5. Защита информации в локальной вычислительной сети на примере компании
6. Развертывание комплекса криптографической защиты корпоративных баз данных
7. Проектирование и внедрение комплексного обеспечения информационной безопасности и защиты конфиденциальной информации в подразделениях банка Сбербанк России
8. Разработка мероприятий по защите от несанкционированного доступа к информации в ЛВС медийной компании
9. Информационная и технологическая безопасность на производственном предприятии
10. Разработка предложений по созданию системы защиты информации в ЛВС компании
11. Разработка модели безопасности корпоративной вычислительной сети
12. Организация защиты информации центров авторизации карт платежной системы VISA
13. Предложения по совершенствованию защищенного документооборота в распределенных локально-вычислительных сетях
14. Разработка предложений по повышению защищенности сетей WiMax
15. Разработка системы информационной защиты распределенных баз данных банка
16. Автоматизация и обеспечение информационной безопасности системы Service Desk в страховой компании
17. Разработка комплексной системы защиты информации в кабинете руководителя компании
18. Разработка комплексной системы безопасности в телекоммуникационной компании
19. Разработка и внедрение системы защиты конфиденциальной информации в ГИС
20. Защита от внешних угроз информационной системы банка
21. Организация защиты конфиденциальной информации в банке
22. Разработка системы информационной безопасности ЛВС SEO-компании
23. Методы и средства защиты информации в Сетях
24. Разработка комплексной системы безопасности компании
25. Разработка и программная реализация методов защиты экономической информации
26. Исследование способов предотвращения атак со вставкой SQL
27. Разработка и нейтрализация модели угроз безопасности информации государственного предприятия
28. Разработка защищенной системы электронного документооборота организации
29. Разработка защищенной система электронного документооборота организации (версия 2)
30. Разработка КСЗИ и организационно-технических мероприятий по предотвращению утечки информации в ГУП
31. Разработка системы защиты информации с использованием СЭД
32. Организация защиты информации при построении межсетевых экранов
33. Разработка системы защиты электронного документооборота коммерческого предприятия
34. Разработка комплексной системы информационной безопасности и защиты информации в торговой организации
35. Разработка мероприятий по защите информации коммерческого банка от внешних угроз
36. Разработка комплексной системы безопасности в торговой компании
37. Разработка рекомендаций по минимизации рисков ИБ в условиях санкций против РФ.  
Разработка рекомендаций по импортозамещению
38. Построение модели ситуационного управления защищенности информации в коммерческой организации



39. Автоматизация систем обеспечения безопасности данных торгового предприятия
40. Разработка информационной системы комплексной защиты коммерческой информации
41. Организация защиты информации при использовании электронных платежных систем
42. Программные средства защиты информации от преднамеренных угроз в ЛВС под управлением WINDOWS
43. Защищенная система электронной почты
44. Анализ защищенности операционных систем
45. Защита от несанкционированного доступа к информации в ЛВС МОУ СОШ
46. Система защиты информации в локальной вычислительной сети компании
47. Разработка комплекса защитных мер по обеспечению информационной безопасности баз данных
48. Управление персоналом как средство защиты информации в организации
49. Защита информации в локальных вычислительных сетях на предприятии
50. Защита информации в локально-вычислительных сетях от преднамеренных угроз
51. Разработка комплексной системы безопасности браузерной онлайн игры
52. Организация защиты и функционирование электронной почты в сетях
53. Разработка комплексной системы защиты информации в научно-исследовательском центре
54. Совершенствование и развитие системы обеспечения ИБ и защиты информации
55. Организация информационной безопасности электронного архива регистра недвижимости в БТИ
56. Основные направления, принципы и методы обеспечения информационной безопасности компании
57. Разработка мероприятий по резервному копированию данных серверов для обеспечения их максимальной отказоустойчивости
58. Выбор технологии проектирования систем защиты информации
59. Разработка предложений по созданию системы защиты информации в полиграфической компании
60. Разработка программной системы защиты информации на производственном предприятии
61. Разработка регламента проведения аудита информационной безопасности государственного бюджетного учреждения
62. Обеспечение безопасности узлов связи аппаратными средствами в проектируемой ЛВС компании
63. Обеспечение информационной безопасности в инвестиционной компании
64. Организация защиты информации в локальных вычислительных сетях, построенных на базе оборудования фирмы CISCO
65. Разработка комплекса мероприятий информационной безопасности и ЗИ в подразделениях гос. учреждения
66. Внедрение системы обеспечения информационной безопасности в ФГУП
67. Защита информации при использовании электронной почты на примере предприятия
68. Проектирование системы обеспечения комплексной информационной безопасности в филиале компании
69. Разработка системы защиты от утечки данных в информационной системе банка
70. Организация использования средств межсетевое экранирования на базе серверных систем Windows
71. Оценка защиты информации в системах документооборота
72. Разработка метода выбора и обоснования средств защиты информации для функционирования в составе КСЗИ
73. Разработка специализированных мероприятий по защите IP-телефонии в компании
74. Организация СКС для офиса торговой компании и обеспечение защиты информации
75. Разработка системы обеспечения кибербезопасности в компании
76. Разработка системы защиты информационной безопасности баз данных
77. Анализ информационной безопасности локальной вычислительной сети (ЛВС)

78. Обеспечение комплексной безопасности баз данных компании
79. Разработка проекта комплексной системы информационной безопасности строительной компании
80. Разработка комплексной защиты информационной системы на базе безопасной компьютерной сети предприятия
81. Внедрение системы видеонаблюдения с возможностью трансляции видео через сеть интернет для компании
82. Разработка комплексной системы безопасности оптовой торговой компании
83. Разработка комплексной системы информационной безопасности компании
84. Комплексное обеспечение информационной безопасности консалтинговой компании
85. Модернизация комплекта антивирусной защиты компании по разработке технических средств
86. Разработка комплексной системы информационной безопасности компании по производству строительных материалов
87. Разработка и внедрение комплексной защиты информации в управляющей компании
88. Разработка комплексной защиты информации на предприятии
89. Проектирование системы защиты информации на предприятии
90. Организация защиты информации в локальных вычислительных сетях применением оборудования фирмы CISCO
91. Организация защиты информации в системе электронного документооборота компании
92. Разработка рекомендаций по созданию защищенной системы удаленного банковского обслуживания
93. Разработка комплексной системы информационной безопасности автомагазина
94. Проектирование защищенного беспроводного доступа к ресурсам корпоративной вычислительной сети предприятия
95. Защита информации при помощи Active Directory
96. Автоматизация процесса выявления инцидентов информационной безопасности в коммерческом банке на основе SIEM-системы
97. Автоматизация и обеспечение безопасности оптовой торговой компании
98. Разработка комплекса мероприятий по обеспечению конфиденциальных и деловых переговоров в защищаемом помещении компании
99. Организация безопасного обмена данными центрального офиса компании с филиалами
100. Разработка комплексной системы защиты информации в кафе
101. Разработка комплекса мер по защите информации для компаний, занимающихся аутсорсинговой разработкой
102. Система обеспечения информационной безопасности компании, анализ и разработка предложений по ее совершенствованию
103. Организация безопасного обмена данными центрального офиса ИТ-компании с филиалами
104. Защита информации в локальной вычислительной сети строительной компании
105. Организация безопасного обмена данными центрального офиса компании-поставщика ИТ-решений с филиалами
106. Организация безопасного обмена данными в фирме, занимающейся автоматизацией предприятий на базе 1С
107. Информационная безопасность на предприятии Военно-промышленного комплекса
108. Разработка комплекса мер по обеспечению информационной безопасности в системах дистанционного банковского обслуживания
109. Разработка системы защиты информации предприятия по разработке программных продуктов на заказ, диплом по информационной безопасности
110. Особенности защиты информации в сети Интернет, диплом информационная безопасность

111. Повышение уровня защищенности системы информационной безопасности в компании, диплом защита информации
112. Разработка мероприятий по защите информации от внешних угроз, диплом по защите информации
113. Построение защищенного электронного документооборота в организации, диплом по защите информации
114. Обеспечение комплексной системы защиты информационных ресурсов компании с проведением теста на проникновение, диплом защита информации
115. Обеспечение информационной безопасности при внедрении и эксплуатации систем обработки электронных платежей, диплом по защите информации
116. Проектирование корпоративной инфокоммуникационной сети на базе технологии VPN, диплом по защите информации
117. Разработка системы защиты информации в банке, диплом по информационной безопасности
118. Организация комплексной системы защиты информации по модели PDCA в соответствии с требованиями стандарта ISO/IEC 27001:2005, диплом по защите информации
119. Противодействие перехвату опасного сигнала за счёт инженерно-технических методов защиты информации, диплом информационная безопасность
120. Разработка комплексной системы защиты информационных ресурсов ВУЗа, используемых в электронном образовании, диплом защита информации
121. Сравнительный анализ современных подходов к выявлению инцидентов ИБ в организации, дипломная работа по защите информации
122. Проектирование комплексной системы защиты информации в соответствии со стандартом ISO 27001, диплом информационная безопасность
123. Модель системы защиты мультиагентной системы (МАС) на основе модели угроз, диплом защита информации
124. Повышение эффективности передачи информации и разработка системы защиты мобильных целевых сетей, диплом информационная безопасность
125. Разработка комплексной системы безопасности в компании, диплом защита информации
126. Выявление возможных уязвимостей точек доступа по каналу Wi-Fi и разработка комплекса мер и рекомендаций по их устранению, диплом защита информации
127. Защита персональных данных при передаче их через открытые точки беспроводного доступа (Wi-fi), диплом защита информации
128. Система безопасного обмена данными центрального офиса страховой компании с филиалами, диплом защита информации
129. Методика оценки соответствия требованиям защиты персональных данных в банковской структуре, диплом по защите информации
130. Система защиты информации в сети сотового оператора с каналом Wi-Fi, диплом информационная безопасность
131. Аппаратная защита информации в закрытом помещении для переговоров, диплом информационная безопасность
132. Технологии идентификации и аутентификации, диплом защита информации
133. Защита конфиденциальной речевой информации от утечки по техническим каналам на примере компании
134. Разработка и внедрение системы информационной безопасности в компании, диплом по защите информации
135. Проектирование систем обеспечения информационной безопасности и защиты информации в компании
136. Анализ и повышение информационной безопасности предприятия, диплом по защите информации

137. Разработка комплексной защиты информации на предприятии, диплом по информационной безопасности
138. Разработка комплекса мероприятий по повышению уровня защищенности ИС компании, диплом по защите информации
139. Разработка комплексной системы защиты информации (КСЗИ) в банке, диплом по защите информации
140. Разработка типового проекта комплексной системы защиты информации на предприятии, диплом по защите информации
141. Аудит в защищенной информационной системе организации (Аудит на соответствие стандартам)
142. Разработка алгоритма скрытия данных в цифровых изображениях
143. Разработка рекомендаций по защите значимых объектов критической информационной инфраструктуры Банковской организации
144. Микросхемы безопасности в современной электронике
145. Разработка программного комплекса для обучения алгоритмам симметричного шифрования
146. Проектирование корпоративной сети компании на базе технологии виртуальных частных сетей
147. Проект обеспечения информационной защиты комплекса бортового оборудования на пассажирском транспортном средстве
148. Разработка рекомендаций по обеспечению информационной безопасности киберфизической системы "Умный дом"
149. Биометрическая система контроля и управления доступом
150. Разработка интерактивного пособия по теме "Квантовое шифрование" для дисциплины Криптографические методы защиты информации
151. Сравнительный анализ алгоритмов внедрения цифровых водяных знаков в аудиофайлы
152. Настройка единой автоматизированной системы мониторинга в банке как контроль безопасности компьютерной сети, сетевого оборудования и серверов
153. Разработка интерактивного пособия по теме «Методы социальной инженерии» для дисциплины «Информационная безопасность»
154. Исследование рисков кражи файлов служебного типа с текстовой информацией
155. Разработка интерактивного пособия по теме «Технология блокчейн» для дисциплины Информационная безопасность
156. Управление цифровым профилем компании в глобальном информационном пространстве
157. Разработка программного комплекса для изучения криптографии на решетках на примере LLL-алгоритма
158. Проект структуры информационной безопасности на предприятии, занимающимся пассажирскими перевозками

### Лист регистрации изменений

№ п/п	Содержание изменения	Реквизиты документа об утверждении изменения	Дата введения изменения
	<p>Утверждена и введена в действие на основании решения Ученого совета РГСУ и Федерального государственного образовательного стандарта высшего образования по специальности <b>10.05.05 Безопасность информационных технологий в правоохранительной сфере</b>, утвержденного приказом Министерства образования и науки Российской Федерации от 26.11.2020 № 1461</p>	<p>Протокол заседания Ученого совета РГСУ № от « » июня 2022 года</p>	