Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
Государственной итоговой аттестации

10.04.01 Информационная безопасность

Безопасность киберфизических систем

очная

Год набора - 2026

Иркутск 2026

Программа ФОС ГИА разработана в соответствии с требованиями федерального государственного образовательного стандарта 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России № 1455 от 26 ноября 2020 г. (зарегистрировано в Минюсте России 18 февраля 2021 года, регистрационный номер 62549), нормативно-правовыми актами Министерства науки и высшего образования РФ в сфере высшего образования и локальными актами университета.

Разработано:

Председатель рабочей группы по разработке ООП: Говорков А.С., директор института ИТиАД, к.т.н., доцент
(ФИО, должность, ученая степень, ученое звание)

Руководитель ООП Маринов А.А., канд.экон.наук, доцент
(Ф.И.О, ученая степень и (или) ученое звание, должность)

Программа ФОС ГИА одобрена учебно-методической комиссией Института информационных технологий и анализа данных им. Е.И. Попова протокол от «16» февраля 2026 г. № 2.

Программа ФОС ГИА одобрена ученым советом Института информационных технологий и анализа данных им. Е.И. Попова протокол от «16» февраля 2026 г. №8

Получено положительное экспертное заключение от представителей работодателей, (экспертное заключение к программе ФОС ГИА прилагается).

1 ПЕРЕЧЕНЬ КОМПЕТЕНЦИЙ, КОТОРЫМИ ДОЛЖНЫ ОВЛАДЕТЬ ОБУЧАЮЩИЕСЯ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ «БЕЗОПАСНОСТЬ КИБЕРФИЗИЧЕСКИХ СИСТЕМ»

1.1 Перечень универсальных компетенций, подтверждающих наличие у выпускника общих знаний и социального опыта, которые должен продемонстрировать обучающийся в ходе ГИА.

- 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.

1.2 Перечень общепрофессиональных компетенций, владение которыми должен продемонстрировать обучающийся в ходе ГИА.

- ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.
- ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.
- ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности.
- ОПК-4. Способен осуществлять сбор, обработку и анализ научно- технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок.
- ОПК-5. Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.

1.3 Перечень профессиональных компетенций, владение которыми должен продемонстрировать обучающийся в ходе ГИА:

- ПК-1 Способность самостоятельно ставить конкретные задачи научных исследований в области информационной безопасности или информационно-аналитических систем безопасности и решать их с использованием новейшего отечественного и зарубежного опыта.
- ПК-2 Способность участвовать в планировании и реализации процессов контроля над информационной безопасностью или процессов информационно-аналитических систем безопасности.
- ПК-3 Способность использования навыков составления и оформления организационно-нормативных документов, научных отчетов, обзоров, докладов и статей в области информационной безопасности или в области информационно-аналитических систем безопасности.
- ПК-4 Способность использования навыков разработки эксплуатационной документации на объектах информации и проводить экспериментально-исследовательские работы при проведении сертификации средств защиты информации по требованиям безопасности информации.
- ПК-5 Способность принимать участие в разработке систем обеспечения информационной безопасности или информационно-аналитических систем безопасности.
- ПК-6 Способность разрабатывать технические задания на проектирование систем обеспечения информационной безопасности или информационно-аналитических систем безопасности.

2 ИНДИКАТОРЫ (ПОКАЗАТЕЛИ) И КРИТЕРИИ ОЦЕНИВАНИЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

2.1 Выпускная квалификационная работа

Код, наименование компетенции	Итоговый индикатор	Критерии оценивания	Способ/средство оценивания
Универсальные компетенции			
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Выполняет поиск информации о проблемной ситуации, проводит аргументированный критический анализ проблемной ситуации, предлагает стратегию.	Содержание ВКР основано результатах критического анализа фактов, полученных из различных источников, и изложено в логической последовательности. Выявленная проблема и предложенные решения основаны на системном анализе проблемной ситуации. Принятые решения аргументированы на основе критического анализа фактических данных.	Содержание ВКР, отзыв руководителя ВКР. Портфолио обучающегося: опубликованные статьи по тематике ВКР (при наличии), сертификаты участника научно-практических конференций (при наличии), дипломы олимпиад, профессиональных конкурсов (при наличии).
УК-2. Способен управлять проектом всех этапах его жизненного цикла	Планирует и организует реализацию проекта с учетом последовательности этапов жизненного цикла проекта, требований к результату и к реализации.	Работы по ВКР спланированы и выполнены в заданный срок, с соблюдением требований к реализации проекта и последовательности этапов жизненного цикла проекта. Результаты ВКР соответствуют предъявляемым требованиям и оформлены надлежащим образом. Предложенные решения учитывают имеющиеся ресурсы и ограничения. При обосновании принятых решений и в ответах на вопросы опирается на опыт, приобретенный в ходе обучения и при выполнении ВКР. На защите ВКР представляет и защищает самостоятельно разработанный проект с обоснованием ресурсов и ограничений при его разработке и реализации и фиксацией полученного опыта.	Содержание ВКР, доклад, ответы на вопросы ГЭК, отзыв руководителя ВКР. Портфолио обучающегося: опыт проектной деятельности в ходе обучения и во внеучебной деятельности (при наличии).
УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.	Организует и руководит работой в команде, вырабатывает командную стратегию достижения поставленной цели, и контролирует ее достижение, используя основные способы и нормы социального взаимодействия и организации командной работы.	Самостоятельно представляет и защищает результаты ВКР, используя принятые нормы и способы социального взаимодействия. При выполнении ВКР взаимодействовал с экспертами в соответствующей профессиональной сфере, выбирая соответствующую ролевую позицию для сбора и анализа необходимой информации, решения поставленных задач, экспертной оценки принятых решений.	Содержание ВКР, доклад, ответы на вопросы ГЭК, отзыв руководителя ВКР. Портфолио обучающегося: опыт командной работы в рамках проектной деятельности в ходе обучения и во внеучебной деятельности (при наличии).
УК-4. Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия.	Осуществляет коммуникацию в рамках академического и профессионального взаимодействия в устной и письменной формах на государственном языке Российской Федерации и на иностранном языке, используя современные коммуникативные технологии и приемы создания научного текста.	Содержание ВКР изложено грамотно и логически последовательно на государственном языке Российской Федерации, с соблюдением норм и правил деловой коммуникации в письменной форме. Использован один или несколько источников информации на иностранном языке и приведены корректные ссылки на них. В ответах на вопросы соблюдает нормы и правила деловой коммуникации в устной форме.	Содержание ВКР, доклад, ответы на вопросы ГЭК, отзыв руководителя ВКР. Портфолио обучающегося: сертификаты по владению иностранным языком (при наличии). Зачетная книжка: результаты сдачи квалификационного экзамена по иностранному языку.
УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия.	Понимает и адекватно воспринимает межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах, комплексно анализирует причины и последствия культурных различий, знает и учитывает особенности культур при межкультурном взаимодействии.		Портфолио обучающегося: опыт межкультурной коммуникации во внеучебной деятельности (при наличии). Зачетная книжка: результаты промежуточной аттестации по философии и истории.
УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	Ставит цели и задачи, обоснованно определяя их приоритетность, эффективно планирует и контролирует собственное время и организует свою деятельность для достижения поставленных целей, применяет на практике методики и принципы самооценки, саморазвития и самообразования.	Успешно спланировал и организовал свою деятельность по выполнению ВКР и выполнил ВКР в заданный срок. Обоснованно сформулировал цель ВКР, определил приоритетность задач по выполнению ВКР. Самостоятельно собрал информацию и решил задачи, необходимые для выполнения и представления результатов ВКР к защите, используя опыт, полученный в ходе обучения и при прохождении практик.	Содержание ВКР, доклад, ответы на вопросы ГЭК, отзыв руководителя ВКР. Портфолио обучающегося: опыт самоорганизации, саморазвития и самообразования в рамках проектной деятельности и во внеучебной деятельности (при наличии), сертификаты об освоении онлайн-курсов, программ дополнительного образования (при наличии).
Общепрофессиональные компетенции			
ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и	Использует на практике умения и навыки в организации научно-исследовательских и проектных работ в профессиональной	В ходе работы над ВКР Применяет законы, принципы и методы математических, естественных и	Содержание ВКР, доклад, ответы на вопросы ГЭК, отзыв руководителя ВКР.

разрабатывать проект технического задания на ее создание.	деятельности.	технических наук при решении задач профессиональной деятельности.	Портфолио обучающегося: опыт самоорганизации, саморазвития и самообразования в рамках проектной деятельности и во внеучебной деятельности (при наличии), сертификаты об освоении онлайн-курсов, программ дополнительного образования (при наличии).
ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.	Владеет методами проектирования сложных систем (подсистем, компонентов системы) и комплексов управления информационной безопасностью с учетом особенностей объектов защиты. Применяет современные интеллектуальные технологии для решения профессиональных задач.	В ходе работы над ВКР обоснованно выбирает соответствующие информационные технологии и применяет их при решении задач профессиональной деятельности.	Содержание ВКР, доклад, ответы на вопросы ГЭК, отзыв руководителя ВКР. Портфолио обучающегося: опыт самоорганизации, саморазвития и самообразования в рамках проектной деятельности и во внеучебной деятельности (при наличии), сертификаты об освоении онлайн-курсов, программ дополнительного образования (при наличии).
ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности.	Владеет методами организации работы по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России.	В ходе работы над ВКР Применяет информационно-коммуникационные технологии для поиска, анализа и переработки необходимой для решения практических задач информации на основе информационной и библиографической культуры с учетом основных требований информационной безопасности.	Содержание ВКР, доклад, ответы на вопросы ГЭК, отзыв руководителя ВКР. Портфолио обучающегося: опыт самоорганизации, саморазвития и самообразования в рамках проектной деятельности и во внеучебной деятельности (при наличии), сертификаты об освоении онлайн-курсов, программ дополнительного образования (при наличии).
ОПК-4. Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок	Способен проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента.	В ходе работы над ВКР применяет стандарты оформления технической документации на различных стадиях жизненного цикла объектов профессиональной деятельности.	Содержание ВКР, доклад, ответы на вопросы ГЭК, отзыв руководителя ВКР. Портфолио обучающегося: опыт самоорганизации, саморазвития и самообразования в рамках проектной деятельности и во внеучебной деятельности (при наличии), сертификаты об освоении

			онлайн-курсов, программ дополнительного образования (при наличии).
ОПК-5. Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.	Способен проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента.	В ходе работы над ВКР показывает навыки инсталляции и настройки программного и аппаратного обеспечения информационных и автоматизированных систем.	Содержание ВКР, доклад, ответы на вопросы ГЭК, отзыв руководителя ВКР. Портфолио обучающегося: опыт самоорганизации, саморазвития и самообразования в рамках проектной деятельности и во внеучебной деятельности (при наличии), сертификаты об освоении онлайн-курсов, программ дополнительного образования (при наличии).
Профессиональные компетенции / Тип задач профессиональной деятельности: научно-исследовательский			
ПК-1 Способность самостоятельно ставить конкретные задачи научных исследований в области информационной безопасности или информационно-аналитических систем безопасности и решать их с использованием новейшего отечественного и зарубежного опыта.	Способен определять задачи научных исследований в профильной области на основе анализа фундаментальных и прикладных проблем информационной безопасности в условиях становления современного информационного общества.	В ходе работы над ВКР демонстрирует навыки самостоятельные исследования в области искусственного интеллекта.	Содержание ВКР, доклад, ответы на вопросы ГЭК, отзыв руководителя ВКР. Портфолио обучающегося: опыт самоорганизации, саморазвития и самообразования в рамках проектной деятельности и во внеучебной деятельности (при наличии), сертификаты об освоении онлайн-курсов, программ дополнительного образования (при наличии).
ПК-2 Способность участвовать в планировании и реализации процессов контроля над информационной безопасностью или процессов информационно-аналитических систем безопасности.	Способен анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты.	В ходе работы над ВКР указывает, каким образом работа зависит от специфики научного знания, основанного на научно-обоснованных фактах.	Содержание ВКР, доклад, ответы на вопросы ГЭК, отзыв руководителя ВКР. Портфолио обучающегося: результаты учебной и внеучебной деятельности за пределами основной профессиональной сферы (при наличии). Зачетная книжка: результаты промежуточной аттестации по дисциплинам дополнительного модуля. *(включить при наличии)*

Профессиональные компетенции / Тип задач профессиональной деятельности: организационно-управленческий			
ПК-3 Способность использования навыков составления и оформления организационно-нормативных документов, научных отчетов, обзоров, докладов и статей в области информационной безопасности или в области информационно-аналитических систем безопасности.	Способен организовать выполнение работ, управлять коллективом исполнителей и принимать решения в проведении научно-исследовательских и опытно-конструкторских работ.	В ходе работы над ВКР использует современные технологии при разработке программных продуктов в области искусственного интеллекта.	Содержание ВКР, доклад, ответы на вопросы ГЭК, отзыв руководителя ВКР. Портфолио обучающегося: результаты учебной и внеучебной деятельности за пределами основной профессиональной сферы (при наличии). Зачетная книжка: результаты промежуточной аттестации по дисциплинам дополнительного модуля. *(включить при наличии)*
ПК-4 Способность использования навыков разработки эксплуатационной документации на объектах информации и проводить экспериментально-исследовательские работы при проведении сертификации средств защиты информации по требованиям безопасности информации.	Способен проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, средств и технологий обеспечения информационной безопасности, а также выполнение по вводу в эксплуатацию систем и средств обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России .	В ходе работы над ВКР показывает практические навыки по поиску, диагностике ошибок и оптимизации программного обеспечения в области искусственного интеллекта.	Содержание ВКР, доклад, ответы на вопросы ГЭК, отзыв руководителя ВКР. Портфолио обучающегося: результаты учебной и внеучебной деятельности за пределами основной профессиональной сферы (при наличии). Зачетная книжка: результаты промежуточной аттестации по дисциплинам дополнительного модуля. *(включить при наличии)*
Профессиональные компетенции / Тип задач профессиональной деятельности: проектный			
ПК-5 Способность принимать участие в разработке систем обеспечения информационной безопасности или информационно-аналитических систем безопасности.	Применяет информационные технологии в системе информационно-аналитического обеспечения безопасности с учетом угроз, возникающих в процессе развития современного информационного общества, и основных требований информационной безопасности.	В ходе работы над ВКР демонстрирует навыки реализации проекта в области искусственного интеллекта.	Содержание ВКР, доклад, ответы на вопросы ГЭК, отзыв руководителя ВКР. Портфолио обучающегося: результаты учебной и внеучебной деятельности за пределами основной профессиональной сферы (при наличии). Зачетная книжка: результаты промежуточной аттестации по дисциплинам дополнительного модуля. *(включить при наличии)*
ПК-6 Способность разрабатывать технические задания на проектирование систем обеспечения информационной безопасности или информационно-аналитических систем безопасности.	Разрабатывает технические задания на проектирование систем обеспечения информационной безопасности на основе анализа прикладной области, выявления угроз и оценки уязвимости информационных систем с учетом требований и критериев оценки информационной безопасности.	В ходе работы над ВКР показывает практические навыки по поиску, диагностике ошибок и оптимизации программного обеспечения в области искусственного интеллекта.	Содержание ВКР, доклад, ответы на вопросы ГЭК, отзыв руководителя ВКР. Портфолио обучающегося: результаты учебной и внеучебной деятельности за пределами основной профессиональной сферы (при наличии). Зачетная книжка: результаты промежуточной аттестации по дисциплинам дополнительного модуля. *(включить при наличии)*

3 ШКАЛЫ ОЦЕНИВАНИЯ

Для каждого аттестационного испытания отдельно описывается шкала оценивания, которая применяется при выставлении итоговой оценки за все виды заданий, выполнение которых предусмотрено в рамках аттестационного испытания.

3.1 Шкала оценивания результатов защиты ВКР

За основу принимаются следующие критерии, с учетом степени освоения компетенций:

1) актуальность темы;
2) научно-практическое значение темы;
3) качество выполнения работы;
4) содержательность доклада и ответов на дополнительные вопросы членов государственной экзаменационной комиссии;
5) наглядность представленных результатов исследования в форме презентации;
6) портфолио выпускника.

При выставлении оценки за выпускную квалификационную работу учитывается работа выпускника и портфолио. По пятибалльной шкале отдельно оценивается:

1) качество текста представленной выпускной квалификационной работы;
2) доклад выпускника и ответы на дополнительные вопросы членов государственной экзаменационной комиссии.

Портфолио (электронное портфолио обучающегося) предоставляется в ГЭК на защите ВКР и содержит дополнительную информацию об учебных и внеучебных достижениях выпускника за весь срок обучения по основной образовательной программе.

Критерии оценки	**Оценка**
Работа выполнена в срок, оформление, структура и стиль работы соответствуют требованиям. Работа выполнена самостоятельно, присутствуют собственные обобщения, заключения и выводы. Сделаны практические предложения, рассчитан эффект от рекомендуемых мероприятий. Использовано оптимальное количество литературы и источников по теме работы. Автор работы владеет методикой исследования. Тема работы раскрыта полностью. Выступление выстроено логично и последовательно, четко отражает результаты исследования. При защите студент дает правильные и обоснованные ответы на вопросы, свободно ориентируется в тексте работы, убедительно защищает свою точку зрения.	5 (отлично)
Работа выполнена в срок; в оформлении, структуре и стиле работы нет грубых ошибок. Работа выполнена самостоятельно, присутствуют собственные обобщения, заключения и выводы, даны практические рекомендации, указан предполагаемый эффект от их внедрения. Использованы основная литература и источники по теме работы, работа может иметь некоторые недостатки в проведенном исследовании в изучении источников. Тема работы в целом раскрыта. Выступление выстроено логично и последовательно, достаточно хорошо отражает результаты исследования. При защите студент дает правильные ответы на большинство вопросов, хорошо ориентируется в тексте работы, достаточно обосновано защищает свою точку зрения.	4 (хорошо)
Работа выполнена с нарушениями графика, в оформлении, структуре и стиле работы есть недостатки. Работа выполнена самостоятельно, присутствуют собственные обобщения, заключения и выводы, носящие общий характер. Даны практические рекомендации, но эффект от их внедрения не назван, либо не подкреплен расчетом. Литература и источники по теме работы использованы в недостаточном объеме, их анализ слабый или вовсе отсутствует. Тема работы раскрыта не полностью. Выступление выстроено не вполне последовательно, с нарушением логики, недостаточно четко отражает результаты исследования. При защите студент отвечает на вопросы неуверенно или допускает ошибки, не может убедительно защищать свою точку зрения.	3 (удовлетворительно)

Значительная часть работы является заимствованным текстом и носит несамостоятельный характер. Содержание работы не соответствует ее теме. При написании работы не были использованы современные источники и литература. Оформление работы не соответствует требованиям. В докладе студента отсутствует логика и последовательность, не приведены результаты исследования. Студент не ориентируется в тексте работы, при защите допускает грубые фактические ошибки при ответах на поставленные вопросы или вовсе не отвечает на них.	2 (неудовлетворительно)

4 ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ, НЕОБХОДИМЫЕ ДЛЯ ОЦЕНКИ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

4.1 Общая характеристика выпускной квалификационной работы

- ВКР выполняется обучающимся и представляет собой работу, демонстрирующую уровень его подготовленности к самостоятельной профессиональной деятельности.
- ВКР выполняется на тему, которая соответствует области, объектам и (или) видам профессиональной деятельности по направлению подготовки.
- ВКР выполняется в виде дипломной работы. Дипломная работа представляет собой логически завершенное исследование, в котором анализируется одна из теоретических и (или) практических проблем в области профессиональной деятельности. Дипломная работа может основываться на обобщении выполненных обучающимся курсовых работ и проектов.
- Тематика ВКР подлежит ежегодному обновлению и должна соответствовать современному уровню развития науки и современным потребностям общественной практики и формироваться с учетом предложений работодателей.
- В перечень тем ВКР могут быть включены темы, предложенные заинтересованными организациями, в том числе заказчиками целевого обучения (далее – организации-работодатели). Для включения предлагаемых тем ВКР в перечень тем ВКР организация-работодатель направляет в институт ИТиАД заявку, в которой указаны предлагаемые темы ВКР с обоснованием целесообразности их разработки и их соответствия направлению подготовки и направленности (профилю) образовательной программы. Организации, являющиеся заказчиком целевого обучения, могут предложить темы ВКР с указанием конкретных обучающихся.
- По решению отдела по работе со студентами института ИТиАД в перечне тем ВКР могут быть указаны руководители ВКР.
- Перечень тем ВКР размещается для ознакомления обучающихся на официальном сайте ИРНИТУ в разделе института и на информационном стенде института не позднее, чем за 6 месяцев до даты начала ГИА.
- Обучающийся имеет право предложить свою тему ВКР посредством подачи в дирекцию института ИТиАД заявления с указанием предлагаемой темы ВКР и обоснованием целесообразности ее разработки и ее соответствия направлению подготовки и направленности (профилю) образовательной программы.
- Обучающийся выбирает тему ВКР из перечня тем ВКР.
- По решению дирекции института формулировки тем ВКР в перечне тем ВКР могут иметь предварительный (примерный) характер. В этом случае обучающийся согласовывает с руководителем ВКР окончательную формулировку темы ВКР. После выбора темы ВКР из перечня тем ВКР и согласования с руководителем ВКР окончательной формулировки темы ВКР (при необходимости) обучающийся подает в отдел по работе со студентами института ИТиАД заявление о закреплении за ним темы ВКР. В заявлении может быть обоснована необходимость назначения консультанта по ВКР.

- Не позднее даты начала преддипломной практики за каждым обучающимся распоряжением директора института ИТиАД закрепляется тема ВКР и назначается руководитель ВКР, а также при необходимости назначается консультант (консультанты).
- Руководителем ВКР по программам магистратуры, как правило, является преподаватель, который ведет дисциплину профессионального цикла по соответствующей образовательной программе, имеет ученую степень и (или) ученое звание и (или) обладает практическим опытом работы по направленности темы ВКР.

Примерный перечень актуальных тем ВКР (магистерских) по информационной безопасности:

1. Оценка эффективности существующих подходов к идентификации пользователей в информационных системах.
2. Исследование вопроса применимости итерационных функций в системах информационной безопасности.
3. Методы управления защитой данных организации на основе анализа циркулирующей информации.
4. Исследование существующих методов повышения уровня безопасности каналов передачи данных.
5. Разработка методики и анализ существующих средства раннего выявления и противодействия угрозам информационной безопасности.
6. Разработка математической модели обеспечения безопасности видеоинформации от угроз нарушения целостности.
7. Исследование моделей, методов и алгоритмов защиты информации систем интеллектуальной поддержки принятия решений.
8. Риск-анализ и управление рисками нарушения информационной безопасности серверов территориально распределенных сетей.
9. Совершенствование моделей и методов обеспечения информационной безопасности от вредоносных программ на основе физической защиты.
10. Разработка методики проведения оценки рисков реализации деструктивных воздействий на системы распределенных удостоверяющих центров.
11. Изучение существующих алгоритмов оценки эффективности систем информационной безопасности в сетях LTE.
12. Исследование вопроса достаточности обеспечения защиты критически важных объектов информатизации.
13. Исследование деструктивного воздействия твитов в социальных сетях, разработка модели управления рисками распространения.
14. Разработка моделей и алгоритмов оценки эффективности систем информационной безопасности от несанкционированного доступа в ИС государственных служб.
15. Исследование вопроса обеспечения эффективности подходов к информационной безопасности от вирусных атак в автоматизированных информационных системах.
16. Разработка методики обеспечения информационной безопасности в рамках аутентификации пользователей на WEB – ресурсах.
17. Разработка методики узнавания Интернет-пользователей на базе стилистических и лингвистических характеристик публикуемой информации.
18. Разработка алгоритмов и методов повышения уровня информационной безопасности систем с архитектурой «тонкий клиент».
19. Исследования вопроса безопасности коммерческих предприятий в отношении использования сотрудниками мобильных устройств и других современных гаджетов.
20. Совершенствование методики повышения уровня информационной безопасности компьютерных сетей на основе вероятностной модели.

21. Методическое и алгоритмическое обеспечение проведения информационно-технических экспертиз.
22. Исследование технологий и подходов к оценке уровня защиты информации в государственных структурах.
23. Создание методологии оценки уровня информационной безопасности на базе комплексного подхода.
24. Разработка системы мониторинга действий пользователей сетей коммерческих предприятий на основе анализа поведенческих факторов.
25. Исследование методов повышения эффективности систем обнаружения злоумышленников в системах информационной безопасности защищаемых объектов
26. Разработка модели защищенности пользователей современных телекоммуникационных систем.
27. Исследование вопроса обеспечения защиты конфиденциальных данных в Интернет-пространстве.
28. Управление рисками информационной безопасности мультисерверных web-систем.
29. Автоматизация подхода к применению средств защиты персональных данных на основе анализа содержащейся информации.
30. Исследование эффективности работы средств противодействия скрытым угрозам информационной безопасности.
31. Разработка требований к системе автоматизированного обнаружения конфликтов в комплексе программных средств обеспечения информационной безопасности.
32. Оценка эффективности существующей методики снижения рисков реализации вредоносных воздействий в облачных сервисах с учетов классификации составляющих их ресурсов.
33. Разработка подхода к выявлению потенциально нежелательных файлов на основе интеллектуального анализа данных.
34. Формирование методики обеспечение информационной безопасности автоматизированных систем с учетом менеджмента инцидентов кибербезопасности.
35. Разработка современного подхода к обеспечению контроля и управления доступом в распределенных системах.
36. Исследование вопроса обеспечения аудита и мониторинга информационной безопасности открытых Интернет-ресурсов.
37. Разработка методики обеспечения и проведения аудита информационной безопасности предприятий на основе риск-ориентированного подхода.
38. Анализ методов обнаружения угроз информационной безопасности передачи данных по каналам газотранспортного предприятия.
39. Исследование методов и алгоритмов обеспечения безопасности данных для защиты от спама.
40. Исследование вопроса влияния резервированного копирования конфигураций вычислительных систем на уровень рисков информационной безопасности.
41. Разработка системы обнаружения и предупреждения атак информационной безопасности в банковской сфере.
42. Исследование вопроса обеспечения защиты автоматизированных систем на основе решений задач комбинаторной оптимизации.
43. Повышение уровня защиты сред облачных вычислений путём верификации пользователей на наличие факторов деструктивного поведения в открытых Интернет-источниках.
44. Разработка модели и алгоритма повышения уровня безопасности на основе внедрения биометрической аутентификации пользователей информационных систем.
45. Исследование вопроса совершенствования системы обеспечения информационной безопасности работы семантических баз данных.

46. Оценка возможности повышения безопасности систем удаленного администрирования средствами защиты информации.
47. Поиск современных способов повышения эффективности средств выявления зараженных файлов компьютерных систем.
48. Исследование статистических методов и средств оценки уровня информационной безопасности.

5 МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

Защита ВКР проводится на открытом заседании ГЭК (за исключением защиты ВКР по закрытой тематике).

Общая продолжительность защиты ВКР одним обучающимся не превышает 0,5 часа.

Процедура защиты ВКР предусматривает:

- выступление обучающегося по содержанию ВКР;
- вопросы членов ГЭК обучающемуся;
- оглашение отзыва руководителя;
- оглашение рецензий;
- ответы обучающегося на замечания, имеющиеся в отзыве и рецензиях (при необходимости, по желанию обучающегося);
- обсуждение ВКР;
- заключительное слово обучающегося (по желанию обучающегося).

Для выступления обучающегося по содержанию ВКР отводится, как правило, не более 10 минут. В ходе выступления обучающийся может представлять материалы, характеризующие научную и практическую ценность выполненной работы (печатные статьи, документы, указывающие на практическое применение результатов работы и т.п.), использовать технические средства для презентации материалов, связанных с выполнением ВКР.

Вопросы членов ГЭК обучающемуся соответствуют ее теме.

На открытой защите ВКР могут присутствовать все желающие, при этом они вправе задавать обучающемуся вопросы по теме ВКР.

Методические рекомендации по подготовке, оформлению и защите ВКР размещены на официальном сайте института ИТиАД www.istu.edu в разделе *«Деятельность» - «Образование» - «Структура» - «Институт информационных технологий и анализа данных»* подраздел *«Шаблоны и образцы документов»*