МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ

Проректор по ОД

_____ Е.В. Луков

«12» ноября 2025 г.

ПРОГРАММА

кандидатского экзамена по научной специальности
«2.3.6. Методы и системы защиты информации, информационная безопасность»

Томск – 2025

Программа кандидатского экзамена по научной специальности ***«2.3.6. Методы и системы защиты информации, информационная безопасность»*** рассмотрена и рекомендована к утверждению ученым советом *Института прикладной математики и компьютерных наук*

протокол № 11 от 29.10.2025г

Автор-разработчик:

Тренькаев Вадим Николаевич, канд. техн. наук, доцент, доцент кафедры компьютерной безопасности ТГУ

Согласовано:

Руководитель ОП
канд. техн. наук, доцент, доцент кафедры
компьютерной безопасности ТГУ — Тренькаев Вадим Николаевич

1. Общие положения

На основании постановления Правительства Российской Федерации от 23.09.2013 № 842 «О порядке присуждения ученых степеней» кандидатские экзамены сдаются в соответствии с научной специальностью (научными специальностями) и отраслью науки, предусмотренными номенклатурой научных специальностей, по которым присуждаются ученые степени, утверждаемой Министерством науки и высшего образования Российской Федерации (далее – Минобрнауки России), по которым осуществляется подготовка (подготовлена) диссертации.

Кандидатский экзамен по специальной дисциплине в соответствии с темой диссертации на соискание ученой степени кандидата наук представляет собой форму оценки степени подготовленности соискателя ученой степени к проведению научных исследований по научной специальности *«2.3.6. Методы и системы защиты информации, информационная безопасность»* и по соответствующей отрасли науки (далее – кандидатский экзамен).

Программа кандидатского экзамена разработана на основе Паспорта научной специальности *«2.3.6. Методы и системы защиты информации, информационная безопасность»*(далее – Программа), утвержденного ВАК при Минобрнауки России https://drive.google.com/drive/folders/1RNYkXhvAzaEF85GqxOH8HhbenJIoUMR7 .

Организация и проведение приема кандидатского экзамена осуществляется в соответствии с установленным в НИ ТГУ порядком.

Подготовка по Программе может осуществляться как самостоятельно, так и в рамках освоения соответствующей программы подготовки научных и научно-педагогических кадров в аспирантуре НИ ТГУ. Сдача аспирантом кандидатского экзамена является обязательным условием обучения и относится к оценке результатов освоения базовой дисциплины (модуля) образовательного компонента программы, осуществляемой в рамках промежуточной аттестации.

2. Структура кандидатского экзамена и шкала оценивания уровня знаний

Кандидатский экзамен проводится в форме устного экзамена по билетам продолжительностью один академический час и состоит из следующих частей:

1. Основные вопросы (три вопроса по содержанию курса «2.3.6. *Методы и системы защиты информации, информационная безопасность*»).
2. Дополнительные вопросы (три вопроса из 2-го раздела содержания Программы).
3. Реферат.

Оценка уровня знаний по каждому вопросу осуществляется по пятибалльной шкале со следующим принципом перерасчета:

«отлично» – 5 баллов;

«хорошо» – 4 балла;

«удовлетворительно» – 3 балла;

«неудовлетворительно» – 1-2 балла.

При оценивании ответов на каждый из вопросов экзаменационного билета учитываются следующие критерии:

Ответ на вопрос исчерпывающий, продемонстрировано понимание и знание сути вопроса в полном объеме. Замечаний нет.	5 баллов
Ответ на вопрос неполный, но раскрывающий основную суть вопроса, продемонстрировано понимание и знание вопроса в достаточном объеме. Замечания незначительные.	4 балла
Ответ неполный с существенными замечаниями, знания по вопросу фрагментарные и частичные, в том числе и по тематике диссертационного исследования.	3 балла
Ответ на вопрос отсутствует или дан неправильный	1-2 балла

Итоговая оценка за кандидатский экзамен выставляется решением экзаменационной комиссии:

«отлично» – при наличии не менее 80% 5-балльных ответов и отсутствии 3-2-1-балльных ответов;

«хорошо» – при наличии не менее 80% 4-балльных ответов и отсутствии 2-1-балльных ответов;

«удовлетворительно» – при наличии более 20% 3-балльных ответов и отсутствии 2-1-балльных ответов;

«неудовлетворительно» – при наличии 1-2 балльного ответа (или отказа отвечать на вопрос).

3. Перечень тем и вопросов для подготовки к сдаче экзамена

Раздел 1. Основные вопросы (по содержанию курса *«2.3.6.Методы и системы защиты информации, информационная безопасность»*).

1. Основы информационной безопасности.

1. Информация как объект защиты.
2. Понятийный аппарат информационной безопасности.
3. Государственная политика информационной безопасности.
4. Угрозы безопасности информации.
5. Меры противодействия угрозам безопасности.
6. Методы и средства защиты от несанкционированного доступа.

2. Криптографические методы защиты информации.

1. Блочные шифры.
2. Поточные шифры.
3. Ассиметричные шифры.
4. Цифровые подписи.

5. Функции хеширования.
6. Методы криптоанализа.

3. Криптографические протоколы.

1. Протоколы аутентификации сообщений.
2. Протоколы идентификации.
3. Протоколы с нулевым разглашением.
4. Протоколы распределения ключей
5. Прикладные криптографические протоколы.
6. Анализ безопасности криптографических протоколов.

4. Стандарты и нормативные документы информационной безопасности.

1. Международные стандарты.
2. Отечественные стандарты.
3. Руководящие документы.
4. Нормативные документы.
5. Методические документы.

5. Информационная безопасность компьютерных систем и сетей.

1. Классификация уязвимостей и атак.
2. Основные механизмы защиты.
3. Базовые средства защиты информации.
4. Модели безопасности компьютерных систем.
5. Инфраструктура открытых ключей.
6. Политика безопасности.

Рекомендуемая литература.

1. Нестеров С.А. Основы информационной безопасности: учебное пособие – Санкт-Петербург: Лань, 2019. – 324 с.
2. Бабаш А.В. Криптографические методы защиты информации. – М: Издательский Центр РИОР, 2019. – 413 с.
3. Лось А. Б., Нестеренко А. Ю., Рожков М. И. Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для вузов. – М.: Издательство Юрайт, 2025. – 424 с.
4. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. – М.: Академия, 2009, 271 с.
5. Запечников С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности: учеб. пособие. – М.: Горячая линия – Телеком, 2006. – 319 с.
6. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. – М.: ДМК-Пресс, 2012. – 592 с.
7. Бирюков А.А. Информационная безопасность: защита и нападение. – М.: ДМК Пресс, 2017. – 434 с.

8. Проскурин В.Г. Защита в операционных системах. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2014. – 192 с.
9. Хорев П.Б. Программно-аппаратная защита информации: учебное пособие. – М: ИНФРА-М, 2020. – 327 с.
10. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учебное пособие. – М.: Горячая линия-Телеком, 2017. – 338 с.
11. Проскурин В.Г. Защита программ и данных: учеб. пособие. – М.: Издательский центр «Академия», 2012. – 208 с.
12. Галатенко В.А. Стандарты информационной безопасности: учебное пособие. – Москва : ИНТУИТ, 2016. – 307 с.

Дополнительная литература

1. Галатенко В. А. Основы информационной безопасности: учебное пособие / В. А. Галатенко. – Москва : ИНТУИТ, 2016. – 266 с.
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие. – Москва: Гелиос АРВ, 2002. – 480 с.
3. Венбо Мао Современная криптография: теория и практика. – М.: Вильямс, 2005. – 768 с.
4. Шнайер Брюс Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 816 с.
5. Буренин П.В. и др. Безопасность операционной системы специального назначения Astra Linux Special Edition. – М.: Горячая линия – Телеком, 2019. – 404 с.
6. А.Ю. Щербаков. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. – М.: Книжный мир, 2009. – 352 с.
7. Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учебное пособие. – Саратов: Вузовское образование, 2018. – 195 с.
8. Горбатов В.С., Полянская О.Ю. Основы технологии PKI. – М.: Горячая линия - Телеком, 2004. – 248 с.
9. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия: учебное пособие. – СПб.: БХВ-Петербург, 2003. – 733с.
10. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия. – М.: Национальный Открытый Университет ИНТУИТ, 2024. – 461 с.

Раздел 2. Дополнительные вопросы (по области исследования паспорта научной специальности, в рамках которой определена тема подготавливаемой кандидатской диссертации).

1. Методы, модели и средства информационной безопасности

1. Методы, аппаратно-программные средства и организационные меры защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида.
2. Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса.
3. Системы документооборота (вне зависимости от степени их компьютеризации) и средства зашиты циркулирующей в них информации.
4. Методы, модели и средства (комплексы средств) противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет.
5. Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях.
6. Модели и методы формирования комплексов средств противодействия угрозам информационной безопасности для различного вида объектов защиты (систем, цепей поставки) вне зависимости от области их функционирования.
7. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющие получать оценки показателей информационной безопасности.
8. Модели и методы оценки защищенности информации и информационной безопасности объекта.
9. Модели и методы оценки эффективности систем (комплексов), средств и мер обеспечения информационной безопасности объектов защиты.
10. Методы и модели выявления и противодействия распространению ложной и вредоносной информации.
11. Модели, методы и средства обеспечения аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности, и расследования инцидентов информационной безопасности в автоматизированных информационных системах.
12. Методы, модели и средства разработки безопасного программного обеспечения, выявления в нем дефектов безопасности, противодействия скрытым каналам передачи данных и выявления уязвимостей в компьютерных системах и сетях.

13. Модели и методы управления информационной безопасностью, непрерывным функционированием и восстановлением систем, противодействия отказам в обслуживании.

Тема 2. Современные тенденции развития методов и систем защиты информации

1. Теория и методология обеспечения информационной безопасности и защиты информации.
2. Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации в информационных системах любого вида и области применения.
3. Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа.
4. Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления.
5. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.
6. Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов.

Рекомендуемая литература

1. Зегжда Д.П., Александрова Е.Б., Калинин М.О., и др. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / под ред. Д.П. Зегжды. – М.: Горячая линия – Телеком, 2021. – 560 с.
2. Барабанов А.В., Дорофеев А.В., Марков А.С., Цирлов В.Л. Семь безопасных информационных технологий / под. ред. А.С.Маркова. М.: ДМК Пресс, 2017. – 224 с.
3. Марков А. С., Цирлов В. Л., Барабанов А. В. Методы оценки несоответствия средств защиты информации / под ред. А. С.Маркова. – М.: Радио и связь, 2012. – 192 с.
4. Мартишин С.А., Храпченко М.В., Шокуров А.В. Исследование задачи обеспечения безопасности при хранении и обработке конфиденциальных данных // Труды ИСП РАН. Том 33. Вып. 2. 2021. С. 173-190
5. Бабенко Л.К. и др. Полностью гомоморфное шифрование (обзор) // Вопросы защиты информации. 2015. № 3. С. 3-26

6. Аракелов Г.Г. Вопросы применения прикладной гомоморфной криптографии // Вопросы кибербезопасности. 2019. № 5(33). С. 70–74.
7. Агибалов Г.П. Конечные автоматы в криптографии // Прикладная дискретная математика. Приложение. 2009. № 2. С. 43–73
8. Городилова А.А. От криптоанализа шифра к криптографическому свойству булевой функции // Прикладная дискретная математика. 2016. № 3(33). С. 16–44
9. Бабаш А.В. Теория автоматов. Синтез шифрующих автоматов: учебное пособие / А. В. Бабаш. – Москва : ФГБОУ ВО «РЭУ им. Г. В. Плеханова», 2020. – 348 с.
10. Бабаш А.В. Теория автоматов. Анализ шифрующих автоматов: учебное пособие / А. В. Бабаш. – Москва : ФГБОУ ВО «РЭУ им. Г. В. Плеханова», 2021. – 296 с.
11. Агибалов Г.П. Избранные теоремы начального курса криптографии. – Томск: НТЛ, 2005. – 112 с.
12. Панкратова И.А. Булевы функции в криптографии: учебное пособие. Томск: Изд. Дом ТГУ, 2014. – 88 с.
13. Логачев О.А. и др. Булевы функции в теории кодирования и криптологии. – М.: Изд-во МЦНМО, 2012. – 583 с.

Дополнительная литература

1. Варновский Н.П, Шокуров. А.В. Гомоморфное шифрование // Труды ИСП РАН. Том 12. 2007. С. 28-36
2. А.А. Гаража и др. Об использовании библиотек полностью гомоморфного шифрования // International Journal of Open Information Technologies. Vol. 9. №3. 2021. p.11-22
3. Popa R. et al. CryptDB: Protecting Confidentiality with Encrypted Query Processing // Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles. 2011. P. 85-100.
4. Poddar R. et al. Arx: an encrypted database using semantically secure encryption. // Proceedings of the VLDB Endowment. 2019. Vol. 12. P. 1664–1678
5. Arasu A. et al. Transaction processing on confidential data using cipherbase // 2015 IEEE 31st International Conference on Data Engineering. 2015. P. 435-446
6. Tu S. et al. Processing analytical queries over encrypted data // Proceedings of the VLDB Endowment. V.6. I5. 2013. P. 289–300
7. De Capitani Di Vimercati et al. Confidentiality Protection in Large Databases. In: S. Flesca et al. (eds.), A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years. Studies in Big Data. 2018. Vol. 31. P. 457-472

Раздел 3. Реферат по теме диссертационного исследования с обзором литературы, источников, авторов, достижений и проблем в выбранной аспирантом научной области, а также ролью и местом исследований аспиранта в этой области.

4. Пример экзаменационного билета

1. Основные вопросы
   1. Линейный криптоанализ.
   2. Схема Лэмпорта.
   3. Межсетевые экраны.
2. Дополнительные вопросы.
   1. Защищенные облачные СУБД.
   2. Криптографические свойства булевых функций.
   3. Автоматная модель симметричных криптосистем.