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

«_____»_____ 2022 г.

ПРОГРАММА

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

Томск – 2022

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 №____ от _____

Авторы-разработчики:

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

Останин Сергей Александрович, канд. техн. наук, доцент, заведующий кафедрой 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).

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. Основные понятия защиты информации и информационной безопасности.
2. Криптографические методы защиты информации.
    1. Блочные шифры.
    2. Поточные шифры.
    3. Ассиметричные шифры.
    4. Цифровые подписи.
    5. Функции хеширования.
    6. Криптоанализ.
3. Криптографические протоколы.
    1. Протоколы аутентификации сообщений.
    2. Протоколы идентификации.
    3. Протоколы с нулевым разглашением.
    4. Протоколы распределения ключей

5. Анализ безопасности криптографических протоколов.

4. Стандарты в области информационной безопасности.
   1. Международные стандарты.
   2. Отечественные стандарты.

5. Информационная безопасность компьютерных систем и сетей.
   1. Классификация уязвимостей и атак.
   2. Основные механизмы защиты.
   3. Базовые средства защиты.
   4. Политика безопасности.

Рекомендуемая литература.

1. Бабаш А.В. Криптографические методы защиты информации. – М: Издательский Центр РИОР, 2019. – 413 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. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости . – М.: Академия, 2009, 271 с.
4. Запечников С.В. Криптографические протоколы и их применение в финансовой и коммерческой деятельности: учеб. пособие. – М.: Горячая линия – Телеком, 2006. – 319 с.
5. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. – М.: ДМК-Пресс, 2012. – 592 с.
6. Проскурин В.Г. Защита в операционных системах. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2014. – 192 с.
7. Буренин П.В. и др. Безопасность операционной системы специального назначения Astra Linux Special Edition. М.: Горячая линия – Телеком, 2019. – 404 с.

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

Область исследования: Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

1. Архитектуры защищенных облачных СУБД.
2. Криптографические алгоритмы защиты облачных данных.
3. Схемы управления доступом к зашифрованным облачным данным.

Рекомендуемая литература.

1. Бабенко Л.К. и др. Полностью гомоморфное шифрование (обзор) // Вопросы защиты информации. 2015. № 3. С. 3-26.

2. Popa R., Redfield C., Zeldovich N., Balakrishnan H. CryptDB: Protecting Confidentiality with Encrypted Query Processing // Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles (SOSP‘11), 2011. P. 85-100.

3. Tu S., Kaashoek M.F., Madden S., Zeldovich N. Processing analytical queries over encrypted data // Proceedings of the VLDB Endowment 6(5), 2013. P. 289–300.

4. Shatilov K., Boiko V., Krendelev S., Anisutina D., Sumaneev A. Solution for secure private data storage in a cloud // Federated Conference on Computer Science and Information Systems (FedCSIS). IEEE, 2014. P. 885-889.5

5. Arasu A. et al. Transaction processing on confidential data using cipherbase // 2015 IEEE 31st International Conference on Data Engineering, Seoul, 2015, pp. 435-446.

Область исследования: Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов.

1. Корреляционная иммунность булевых функций.
2. Нелинейность булевых функций.
3. Лавинные характеристики булевых функций.
4. Алгебраическая иммунность булевых функций.
5. Запреты булевых функций.

Рекомендуемая литература.

1. Агибалов Г.П. Избранные теоремы начального курса криптографии. – Томск: НТЛ, 2005. – 112 с.

2. Бабаш А.В., Шанкин Г.П. Криптография. М.: СОЛОН-Р, 2002.

3. Логачев О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. – М: МНЦМО, 2004.

4. Панкратова И.А. Булевы функции в криптографии: учебное пособие. Томск: Изд. Дом ТГУ, 2014. – 88 с.

3. Пример экзаменационного билета

1. Основные вопросы
   1. Линейный криптоанализ.
   2. Схема Лэмпорта.
   3. Межсетевые экраны.
2. Дополнительные вопросы.
   1. Архитектура СУБД CryptDB.
   2. Гомоморфное шифрование.
   3. Шифрование, сохраняющее порядок.