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

УТВЕРЖДЕНО:
Директор ИПМКН
_____ А.В. Замятин
«_08_» _____мая_____ 2023 г.

Рабочая программа дисциплины (модуля)

«Методы и системы защиты информации, информационная безопасность»

для подготовки научных и научно-педагогических кадров в аспирантуре
по научной специальности:
«2.3.6. Методы и системы защиты информации, информационная безопасность»

Форма обучения
Очная

Томск – 2023

Рабочая программа дисциплины (модуля) «Методы и системы защиты информации, информационная безопасность» (далее – Рабочая программа) разработана и составлена в соответствии с:

Положением о подготовке научных и научно-педагогических кадров в аспирантуре Национального исследовательского Томского государственного университета (утв. Приказом ректора НИ ТГУ от 31.03.2022 № 250/ОД);

– самостоятельно устанавливаемыми требованиями к программам подготовки научных и научно-педагогических кадров в аспирантуре Национального исследовательского Томского государственного университета (далее – ОП аспирантуры) (утв. Приказом ректора НИ ТГУ от 31.03.2022 № 250/ОД);

для включения в учебный план ОП аспирантуры НИ ТГУ по научной специальности «2.3.6. Методы и системы защиты информации, информационная безопасность» в качестве обязательной дисциплины, направленной на подготовку к сдаче кандидатского экзамена.

Рабочая программа рассмотрена и рекомендована к утверждению учебно-методической комиссией наименование института прикладной математики и компьютерных наук, протокол № 2 от «08» июня 2023 года.

Курс: 2
Трудоёмкость в ЗЕТ – 3
Трудоёмкость в академических часах – 108

Авторы-разработчики:

Тренькаев В.Н., канд. техн. наук, доцент,
доцент кафедры компьютерной безопасности ТГУ,
руководитель ОП «2.3.6. Методы и системы защиты информации, информационная безопасность»

1. Цели и задачи освоения дисциплины (модуля)

Целью освоения дисциплины (модуля) «Методы и средства защиты информации, информационная безопасность» является формирование знаний, умений и навыков в сфере компьютерной и информационной безопасности, достаточных для подготовки к сдаче и сдачи кандидатского экзамена по научной специальности «2.3.6. Методы и средства защиты информации, информационная безопасность» в соответствии с Номенклатурой научных специальностей (приказ Минобрнауки России от 24.02.2021 № 118).

Основные задачи дисциплины (модуля):

– формирование основных понятий защиты информации и информационной безопасности;

– освоение методов и математических основ криптографической защиты информации;

– формирование знаний о криптографических протоколах и умений применения методов анализа безопасности криптографических протоколов;

– формирование знаний о стандартах в области информационной безопасности;

– формирование основных понятий информационной безопасности компьютерных систем и сетей;

– формирование знаний об архитектуре защищённых облачных СУБД, криптографических алгоритмах защиты облачных данных, схем управления доступом к зашифрованным облачным данным.

2. Место дисциплины (модуля) в структуре образовательной программы аспирантуры

Дисциплина (модуль) «Методы и средства защиты информации, информационная безопасность» относится к дисциплинам (модулям), направленным на сдачу кандидатских экзаменов, образовательного компонента программы аспирантуры по научной специальности, по которой осуществляется подготовка (подготовлена) диссертации.

В соответствии с учебным планом дисциплина (модуль) реализуется на втором году обучения.

В рамках данной дисциплины (модуля) обобщаются, систематизируются и углубляются знания о теоретико-методологических основах исследования в рамках соответствующей научной специальности, формируется необходимый уровень подготовленности к самостоятельной научно-исследовательской работе.

3. Планируемые результаты освоения дисциплины (модуля)

По окончании освоения дисциплины (модуля) аспирант должен:

Знать:

– основных понятия защиты информации и информационной безопасности;
– методы и инструменты обеспечения безопасного функционирования программного обеспечения;
– основы информационной безопасности компьютерных систем и сетей;
– методы и математические основы криптографической защиты информации и криптоанализа;
– криптографические протоколы;
– стандарты в области информационной безопасности;
– архитектуру защищённых облачных СУБД, криптографические алгоритмы защиты облачных данных, схемы управления доступом к зашифрованным облачным данным.

Уметь:
– обеспечивать безопасность программного обеспечения;
– выполнять мониторинг и обеспечивать безопасность компьютерных систем и сетей;
– использовать методы и инструменты криптографической защиты информации и криптоанализа;
– применять методы анализа безопасности криптографических протоколов;
– использовать стандарты в области информационной безопасности;
– работать с криптографическими алгоритмами защиты облачных данных.

Владеть:
– навыками обеспечения безопасность программного обеспечения;
– навыками обеспечения безопасности компьютерных систем и сетей;
– навыками работы с инструментами криптографической защиты информации и криптоанализа;
– навыками анализа безопасности криптографических протоколов;
– навыками работы с криптографическими алгоритмами защиты облачных данных;
– навыками управления доступом к зашифрованным облачным данным.

4. Язык реализации

Русский и(или) английский (в соответствии с языком освоения ОП аспирантуры и индивидуальным планом работы аспиранта).

5. Объём и структура дисциплины (модуля)

Общая трудоёмкость дисциплины (модуля) составляет 3 зачётные единицы, 108 академических часов:

№ п/п	Раздел дисциплины (модуля)	Период освоения	Виды учебной работы, включая самостоятельную работу аспирантов и трудоемкость (в часах)					Формы текущего контроля успеваемости и промежуточной аттестации
			Лекции	Лаб. работы	Прак-тика	Самост. работа	Всего	
1	Раздел 1. Основные вопросы	2	8			28	36	Аналитический обзор, реферат
2	Раздел 2. Дополнительные вопросы		8			28	36	Аналитический обзор, реферат
							36	Кандидатский экзамен
	ВСЕГО		16			54	108	

Самостоятельная работа аспирантов по темам дисциплины реализуется в форме подготовки аналитических обзоров и рефератов.

6. Содержание дисциплины (модуля)

№ п/п	Наименование раздела дисциплины (модуля)	Содержание раздела дисциплины (модуля)
1	**Раздел 1.** Основные вопросы	***Тема 1. Основные понятия защиты информации и информационной безопасности*** ***Тема 2. Криптографические методы защиты информации*** Блочные шифры. Поточные шифры. Ассиметричные шифры. Цифровые подписи. Функции хеширования. Криптоанализ. ***Тема 3. Криптографические протоколы*** Протоколы аутентификации сообщений. Протоколы идентификации. Протоколы с нулевым разглашением. Протоколы распределения ключей. Анализ безопасности криптографических протоколов. ***Тема 4. Стандарты в области информационной безопасности*** Международные стандарты. Отечественные стандарты. ***Тема 5. Информационная безопасность компьютерных систем и сетей*** Классификация уязвимостей и атак. Основные механизмы защиты. Базовые средства защиты. Политика безопасности.

2	**Раздел 2.** Дополнительные вопросы	***Тема 1. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности*** Архитектуры защищенных облачных СУБД. Криптографические алгоритмы защиты облачных данных. Схемы управления доступом к зашифрованным облачным данным. ***Тема 2. Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов.*** Корреляционная иммунность булевых функций. Нелинейность булевых функций. Лавинные характеристики булевых функций. Алгебраическая иммунность булевых функций. Запреты булевых функций.

7. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Освоение учебного материала дисциплины (модуля) запланировано в течение одного учебного года.

Текущий контроль знаний осуществляется на протяжении учебного года в ходе освоения дисциплины (модуля).

Промежуточная аттестация проводится в конце учебного года освоения дисциплины (модуля) в форме сдачи кандидатского экзамена (КЭ) комиссии, утверждаемой приказом ректора.

Сданный кандидатский экзамен является образовательным результатом выполнения индивидуального учебного плана аспиранта (ОР1).

Перечень тем с вопросами для подготовки к сдаче кандидатского экзамена:

Раздел 1. Основные вопросы

1. Основные понятия защиты информации и информационной безопасности.
2. Криптографические методы защиты информации.
   - 2.1. Блочные шифры.
   - 2.2. Поточные шифры.
   - 2.3. Ассиметричные шифры.
   - 2.4. Цифровые подписи.
   - 2.5. Функции хеширования.
   - 2.6. Криптоанализ.
3. Криптографические протоколы.
   - 3.1. Протоколы аутентификации сообщений.
   - 3.2. Протоколы идентификации.
   - 3.3. Протоколы с нулевым разглашением.
   - 3.4. Протоколы распределения ключей
   - 3.5. Анализ безопасности криптографических протоколов.

4. Стандарты в области информационной безопасности.
   4.1. Международные стандарты.
   4.2. Отечественные стандарты.
5. Информационная безопасность компьютерных систем и сетей.
   5.1. Классификация уязвимостей и атак.
   5.2. Основные механизмы защиты.
   5.3. Базовые средства защиты.
   5.4. Политика безопасности.

Раздел 2. Дополнительные вопросы

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.

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.

8. Критерии оценки знаний и навыков

Результаты освоения дисциплины (модуля) определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Итоговая оценка за кандидатский экзамен выставляется решением экзаменационной комиссии.

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

1. Основные вопросы.
2. Дополнительные вопросы.
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

Для сдачи кандидатского экзамена аспирант должен предварительно представить реферат по теме диссертационного исследования с обзором современных исследований по теме диссертации не менее 40 источников литературы.

Оценка «отлично» за реферат ставится, если:

– содержание реферата точно соответствует теме, отсутствуют ошибки в изложении и оформлении реферата;

– материал освещен в проблемном аспекте при достаточном фактологическом изложении;

– ссылки на работы известных ученых и новейшую литературу отличаются полнотой;

– изложено свое видение проблемы и аргументация своей позиции с помощью фактов;

– содержание связано с темой диссертационного исследования.

Оценка «хорошо» за реферат ставится, если:

– содержание реферата соответствует теме, допущены негрубые ошибки в изложении и оформлении реферата;

– обозначены основные проблемы изучения заявленного в теме вопроса при достаточном фактологическом изложении;

– даны ссылки на работы известных ученых и новейшую литературу;

– изложено свое видение проблемы и приведен ряд аргументов своей позиции с помощью фактов;

– содержание связано с темой диссертационного исследования.

Оценка «удовлетворительно» за реферат ставится, если:

– содержание реферата соответствует теме, допущены ошибки в изложении и оформлении реферата;

– поверхностное фактологическое изложение;
– даны ссылки на ряд работ известных ученых и новейшую литературу;
– содержание связано с темой диссертационного исследования.

Оценка «неудовлетворительно» за реферат ставится, если:

– содержание реферата не соответствует теме, допущены грубые ошибки в изложении и оформлении реферата;
– не изложено свое видение проблемы и не приведены аргументы своей позиции;
– содержание не связано с темой диссертационного исследования.

Пример экзаменационного билета:

Билет 1

Основные вопросы:

1. Линейный криптоанализ.
2. Схема Лэмпорта.
3. Межсетевые экраны.

Дополнительные вопросы.

1. Архитектура СУБД CryptDB.
2. Гомоморфное шифрование.
3. Шифрование, сохраняющее порядок.

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).

9. Учебно-методическое и информационное обеспечение дисциплины

Рекомендуемая литература по разделу 1

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие. – М.: Гелиос АРВ, 2002. – 480 с.
2. Бабаш А.В. Криптографические методы защиты информации. – М.: Издательский Центр РИОР, 2019. – 413 с.
3. Буренин П.В. и др. Безопасность операционной системы специального назначения Astra Linux Special Edition. – М.: Горячая линия – Телеком, 2019. – 404 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. Проскурин В.Г. Защита в операционных системах. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2014. – 192 с.
6. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. – М.: Академия, 2009. – 271 с.
7. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: ДМК-Пресс, 2012. – 592 с.

Рекомендуемая литература по разделу 2:

1. Arasu A. et al. Transaction processing on confidential data using cipherbase // 2015 IEEE 31st International Conference on Data Engineering, Seoul, 2015. P. 435-446.
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. 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.
4. 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.
5. Агибалов Г.П. Избранные теоремы начального курса криптографии. – Томск: НТЛ, 2005. – 112 с.
6. Бабаш А.В., Шанкин Г.П. Криптография. – М.: СОЛОН-Р, 2002.
7. Бабенко Л.К. и др. Полностью гомоморфное шифрование (обзор) // Вопросы защиты информации. 2015. – № 3. – С. 3-26.
8. Логачев О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. – М: МНЦМО, 2004.
9. Панкратова И.А. Булевы функции в криптографии: учебное пособие. Томск: Изд. Дом ТГУ, 2014. – 88 с.

Ресурсы информационно-телекоммуникационной сети «Интернет»:

1. Научная библиотека Томского государственного университета.

URL: http://www.lib.tsu.ru

Одна из крупнейших и старейших библиотек за Уралом, фонд которой составляет более 5 млн печатных изданий и электронных документов, в том числе 126,6 тыс. документов находится в отделе рукописей и книжных памятников (данные по состоянию на 01.01.2024). С 1998 года Научная библиотека в составе ТГУ имеет статус особо ценного объекта культурного наследия народов РФ.

2. Научная электронная библиотека eLIBRARY.RU

URL: http://elibrary.ru

Библиографическое описание, рефераты, полные тексты статей из российских и зарубежных журналов, а также доклады на конференциях монографии, учебные пособия, патенты, диссертации.

Российский индекс научного цитирования (РИНЦ) – национальная информационно-аналитическая система, аккумулирующая информацию о публикациях и цитированиях российских авторов, осуществляющая оценку результативности и эффективности деятельности научно-исследовательских организаций, уровень научных журналов.

3. Электронная библиотека диссертаций (РГБ)

URL: http://diss.rsl.ru/

Диссертации и авторефераты из фонда Российской государственной библиотеки (РГБ) по всем отраслям знания. Глубина полнотекстового доступа с 1998 года. Доступ к полным текстам только с компьютеров сети Научной библиотеки ТГУ по индивидуальному паролю. Пароль для работы можно получить в библиографическом информационном центре НБ ТГУ.

10. Материально-техническое обеспечение дисциплины

Материально-техническое оборудование, используемое при реализации дисциплины:

- аудитории для проведения занятий лекционного типа;
- аудитории для проведения занятий семинарского типа, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы, оснащённые компьютерной техникой с выходом в интернет, в электронную информационно-образовательную среду и к информационно-справочным системам;
- лаборатории, оборудованные компьютерной техникой со специализированным программным обеспечением;
- аудитории для проведения занятий лекционного и семинарского типа индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации в смешенном формате («Актру»).