АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «НАУЧНО-ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ «СИРИУС»
(АНОО ВО «УНИВЕРСИТЕТ «СИРИУС»)

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0208A68A00C9B29ABA45F7A10BC9735134
Владелец: Федоров Олег Дмитриевич
Действителен: с 24.04.2025 до 24.04.2026

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Шифр и наименование области науки:	2. Технические науки
Шифр и наименование группы научных специальностей:	2.3. Информационные технологии и телекоммуникации
Шифр и наименование научной специальности:	2.3.6. Методы и системы защиты информации, информационная безопасность
Форма обучения:	Очная
Срок освоения образовательной программы:	4 года
Год начала освоения образовательной программы:	2025
Структурное подразделение, ответственное за реализацию образовательной программы:	Научный центр информационных технологий и искусственного интеллекта

АННОТАЦИЯ
к рабочей программе дисциплины (модулю)

Дисциплина по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность, трудоемкость 4 з.е.

1.1. Цель освоения и краткое содержание дисциплины (модуля)

Цель: формирование у обучающихся системы основных понятий о современных проблемах в области систем защиты информации, информационной безопасности.

Краткое содержание (тематика):

Теоретические основы и методы систем защиты информации. Специальное математическое и алгоритмическое обеспечения систем анализа. Протоколы защиты информации. Алгоритмы информационной безопасности.

1.2. Планируемые результаты обучения по дисциплине (модулю)

1.2.1. Сдан кандидатский экзамен по специальной дисциплине по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

1.2.2. Расширение и углубление личностных компетенций, а также формирование профессиональных компетенций, необходимых для создания, внедрения и совершенствования технологий, обеспечивающих опережающее научно-технологическое развитие страны:

– применение инновационных инструментов и методов при определении путей решения научных задач в области системного анализа;

– осуществление поиска, обработки, систематизации цифровой информации, управление данными, информацией и цифровым контентом;

– умение анализировать и оценивать современные научные достижения, генерировать новые идеи при решении исследовательских и практических задач, в том числе в междисциплинарных областях;

– использование технических и инженерных решений основных задач исследовательской деятельности в области своих научных интересов;

– умение формулировать цели и задачи научных исследований на основе результатов поиска, обработки и анализа научно-технической информации.

1. Общая характеристика дисциплины

1.1. Цель дисциплины: формирование у аспирантов системы основных понятий о современных проблемах в области систем защиты информации, информационной безопасности.

1.2. Задачи дисциплины:

– применение инновационных инструментов и методов при определении путей решения научных задач в области системного анализа;

– осуществление поиска, обработки, систематизации цифровой информации, управление данными, информацией и цифровым контентом;

– умение анализировать и оценивать современные научные достижения, генерировать новые идеи при решении исследовательских и практических задач, в том числе в междисциплинарных областях;

– использование технических и инженерных решений основных задач исследовательской деятельности в области своих научных интересов;

- умение формулировать цели и задачи научных исследований на основе результатов поиска, обработки и анализа научно-технической информации.

1.3. Место дисциплины в структуре программы аспирантуры:

Дисциплина входит в образовательный компонент программы аспирантуры по научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Дисциплина является обязательной.

Дисциплина проводится в семестрах, установленных учебным планом и (или) индивидуальным учебным планом аспиранта.

1.4. Общая трудоемкость дисциплины: 4 з.е.

1.5. Планируемые результаты обучения по дисциплине:

1.5.1. Сдан кандидатский экзамен по специальной дисциплине по научной специальности 3.2.6. Методы и системы защиты информации, информационная безопасность.

1.5.2. Расширение и углубление личностных компетенций, а также на формирование профессиональных компетенций, необходимых для создания, внедрения и совершенствования технологий, обеспечивающих опережающее научно-технологическое развитие страны:

– умения применять инновационные инструменты и методы при определении путей решения научных задач в области системного анализа;

– способность осуществлять поиск, обработку, систематизацию цифровой информации, управления данными, информацией и цифровым контентом;

– умение анализировать и оценивать современные научные достижения, генерировать новые идеи при решении исследовательских и практических задач, в том числе в междисциплинарных областях;

– ориентация на использование технических и инженерных решений основных задач исследовательской деятельности в области своих научных интересов;

– умение формулировать цели и задачи научных исследований на основе результатов поиска, обработки и анализа научно-технической информации.

2. Структура и содержание дисциплины

2.1. Объем дисциплины и виды учебной деятельности:

Виды учебной деятельности	Всего
Контактная работа обучающихся с преподавателем, ч.	4
Самостоятельная работа обучающихся ч.	140
Промежуточная аттестация	4
Общая трудоемкость, ч.	**144**
Общая трудоемкость, з.е.	**4**

2.2. Структура дисциплины по разделам (темам) и видам учебной деятельности:

Наименования разделов (тем) дисциплины	Контактная работа, ч	Самостоятельная работа, ч	Форма текущего контроля / промежуточной аттестации
Раздел 1. Теоретические основы и методы системного анализа, оптимизации, управления, принятия решений, обработки информации и искусственного интеллекта.	0	28	Представление доклада
Раздел 2. Специальное математическое и алгоритмическое обеспечения систем анализа, оптимизации, управления, принятия решений, обработки информации и искусственного интеллекта.	0	28	
Раздел 3. Методы идентификации систем управления на основе ретроспективной, текущей и экспертной информации.	0	28	
Раздел 4. Методы и алгоритмы структурно-параметрического синтеза и идентификации сложных систем.	0	28	
Раздел 5. Методы и алгоритмы интеллектуальной поддержки при принятии управленческих решений в технических системах.	0	28	
Промежуточная аттестация	4	-	Кандидатский экзамен
Итого	4	140	

2.3. Содержание разделов (тем) дисциплины:

Наименования разделов (тем) дисциплины	Содержание разделов (тем) дисциплины
Раздел 1. Теория и методология обеспечения информационной безопасности и защиты информации.	Методы, аппаратно-программные средства и организационные меры защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида. Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса.
Раздел 2. Системы документооборота (вне зависимости от степени их компьютеризации) и средства зашиты циркулирующей в них информации.	Методы, модели и средства (комплексы средств) противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет. Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях. Модели и методы формирования комплексов средств противодействия угрозам информационной безопасности для различного вида объектов защиты (систем, цепей поставки) вне зависимости от области их функционирования.
Раздел 3. Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации в информационных системах любого вида и области применения.	Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющие получать оценки показателей информационной безопасности. Модели и методы оценки защищенности информации и информационной безопасности объекта. Модели и методы оценки эффективности систем (комплексов), средств и мер обеспечения информационной безопасности объектов защиты.
Раздел 4. Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа.	Методы и модели выявления и противодействия распространению ложной и вредоносной информации. Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

Раздел 5. Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов.	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. 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. Модели и методы управления информационной безопасностью, непрерывным функционированием и восстановлением систем, противодействия отказам в обслуживании.

2.4. Учебной программой дисциплины предусмотрена самостоятельная работа обучающихся в объеме 140 академических часа.

Самостоятельная работа проводится с целью углубления знаний по дисциплине и предусматривает:

– регулярную проработку пройденного на лекциях учебного материала по разделам курса;

– подготовку эссе по тематике курса, ознакомление с литературой в электронно-библиотечных системах, включая переводы публикаций из научных журналов, цитируемых в базах Scopus, Web of Science, РИНЦ;

– подготовку презентации результатов экспериментальной работы;

– участие в научных мероприятиях, а также дополнительных образовательных программах, проводимых на базе Научного центра генетики и наук о жизни АНОО ВО «Университет «Сириус»;

– знакомство с научными направлениями, реализуемыми на базе АНОО ВО «Университет «Сириус», в частности, с современным оборудованием и методиками для проведения биологических и междисциплинарных исследований.

3. Текущий контроль и промежуточная аттестация по дисциплине. Оценочные материалы

3.1. Текущий контроль успеваемости по дисциплине проводится в течение семестра в следующих формах:

Наименования разделов (тем) дисциплины	Форма текущего контроля	Оценочные материалы
Раздел 1. Теория и методология обеспечения информационной безопасности и защиты информации.	Представление доклада	Перечень вопросов для доклада
Раздел 2. Системы документооборота (вне зависимости от степени их компьютеризации) и	Представление доклада	Перечень тем для доклада

средства зашиты циркулирующей в них информации.		
Раздел 3. Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации в информационных системах любого вида и области применения.	Представление доклада	Перечень тем для доклада
Раздел 4. Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа.	Представление доклада	Перечень тем для доклада
Раздел 5. Исследования в области безопасности криптографических алгоритмов, криптографических примитивов, криптографических протоколов. Защита инфраструктуры обеспечения применения криптографических методов.	Устный доклад в виде презентации результатов экспериментальной работы	Перечень тем для выполнения экспериментальной работы

3.2. Оценочные материалы для текущего контроля:

3.2.1. Примерный перечень вопросов для собеседования:

1. Использование алгоритмов машинного обучения.
2. Методы, аппаратно-программные средства и организационные меры защиты систем.
3. Алгоритмы оптимизации, управления, принятия решений.
4. Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса.
5. Методы, модели и средства противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет.
6. Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях.
7. Модели и методы формирования комплексов средств противодействия угрозам информационной безопасности для различного вида объектов защиты (систем, цепей поставки) вне зависимости от области их функционирования.
8. Анализ рисков нарушения информационной безопасности и уязвимости процессов обработки, хранения и передачи информации в информационных системах любого вида и области применения.
9. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющие получать оценки показателей информационной безопасности.

10. Модели и методы оценки защищенности информации и информационной безопасности объекта.

Критерии оценивания доклада:

– полнота и правильность ответа;

– степень осознанности, понимания изученного;

– языковое оформление ответа.

«Отлично»	«Хорошо»	«Удовлетворительно»	«Неудовлетворительно»
– полно раскрыто содержание вопроса; – материал изложен грамотно, в определенной логической последовательности, точно используется терминология; – показано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации; – продемонстрировано усвоение ранее изученных сопутствующих вопросов.	– ответ удовлетворяет в основном требованиям на оценку «5» (отлично), но при этом имеет один из недостатков: в изложении допущены небольшие пробелы, не исказившие содержание ответа; – допущены один – два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя.	– неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала; – имеются затруднения или допущены ошибки в определении понятий, использовании терминологии, исправленные после нескольких наводящих вопросов преподавателя.	– не раскрыто основное содержание учебного материала; – обнаружено незнание или непонимание большей или наиболее важной части учебного материала; – допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов преподавателя; не сформированы компетенции, умения и навыки.

3.3. Формой промежуточной аттестации по дисциплине является кандидатский экзамен.

Результатом промежуточной аттестации в форме кандидатского экзамена являются оценки «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

Кандидатский экзамен проводится в соответствии с установленным в АНОО ВО «Университет «Сириус» порядком.

3.4. Примерный перечень тем для выполнения экспериментальной работы к кандидатскому экзамену:

1.Технологии идентификации и аутентификации пользователей и субъектов информационных процессов.

2. Системы разграничения доступа.

3. Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления.

4. Защита инфраструктуры обеспечения применения криптографических методов.

5. Метод управления информационной безопасностью, непрерывным функционированием и восстановлением систем, противодействия отказам в обслуживании.

Критерии оценки ответов на доклад кандидатского экзамена:

«Отлично»	«Хорошо»	«Удовлетворительно»	«Неудовлетворительно»
– обнаружил глубокое знание основного учебно-программного материала в соответствии с прослушанным лекционным курсом, основной и дополнительной литературой, в полном объеме, необходимом для предстоящей работы по специальности; – демонстрирует глубокое, всестороннее знание и понимание сущности рассматриваемых терминов, понятий, закономерностей и пр.; – свободно владеет научным стилем речи; его ответ характеризует точное, связное, последовательное, логичное, обоснованное и аргументированное изложение материала; – умеет формулировать обоснованные выводы.…	– обнаружил твердое знание основного учебно-программного материала в объеме, необходимом для предстоящей работы по специальности; – демонстрирует хорошее знание рассматриваемых терминов, понятий, закономерностей и пр.; – владеет научным стилем; его ответ характеризует точное, связное, последовательное, логичное изложение материала; – умеет формулировать выводы.	– обнаружил знание основного учебно-программного материала в объеме, необходимом для предстоящей работы по специальности; – демонстрирует нечеткое представление о сущности рассматриваемых терминов, понятий, закономерностей и пр.; – слабо владеет научным стилем; его ответ характеризует неточное изложение программного материала, – испытывает трудности с формулированием выводов. –	– обнаружил значительные пробелы в знаниях основного учебного материала; – демонстрирует непонимание сущности рассматриваемых терминов, понятий, закономерностей и пр.; – не владеет научным стилем речи; не умеет формулировать выводы.

4. Учебно-методическое и информационное обеспечение дисциплины

4.1. Перечень основной литературы:

1. Галатенко В.А. Основы информационной безопасности: учеб. пособие: для студентов вузов, обучающихся по специальности 351400 "Прикладная информатика" / В. А. Галатенко - 4-е изд. - М.: Интернет-Ун-т информ. технологий: БИНОМ, Лаб. знаний, 2008. - 205 с.

2. Коваленко Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности: учеб. пособие для слушателей, обучающихся по программе доп. проф. образования в области информ. безопасности "Основы лицензирования и сертификации в области защиты информации" / Ю. И. Коваленко. - Москв: Горячая линия-Телеком, 2012. - 138 с.

3. Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика».

4.2. Перечень дополнительной литературы:

1. Малюк, А. А. Теория защиты информации / А.А. Малюк. - Москва: Гор. линия-Телеком, 2012. - 184 с. - URL: https://new.znanium.com/catalog/product/367555

2.Ларин М.В., Янковая В.Ф. Организация хранения электронных документов // Современные технологии делопроизводства и документооборота. – 2013. - № 5. - С. 6-17.

Ресурсы информационно-телекоммуникационной сети Интернет:

1. Официальный интернет портал: http://www.rsreu.ru

2. Электронная библиотека: http://elib.rsreu.ru/The European Patent Office http://ep.espacenet.com

3. Электронно-библиотечная система IRPbooks: https://www.iprbookshop.ru/Ресурсы ELSEVIER: http://www.sciencedirect.com

5. Материально-техническое и программное обеспечение дисциплины

5.1. Материально-техническое обеспечение

Вид аудитории	Технические средства и оборудование
Учебная аудитория для проведения лекционных занятий	– Рабочее место преподавателя; – Компьютер / ноутбук; – Проектор; – Маркерная доска / флипчарт; маркеры; – Рабочие места для обучающихся; – Платформа для видеозвонков с полным доступом, позволяющая одновременное подключение не менее 40 человек, с доступными функциями демонстрации экрана, записи видеозвонка, разбиения участников по «комнатам»
Учебная аудитория для проведения практических занятий	– Рабочее место преподавателя; – Компьютер / ноутбук; – Проектор; – Маркерная доска / флипчарт; маркеры; – Рабочие места для обучающихся; – Платформа для видеозвонков с полным доступом, позволяющая одновременное подключение не менее 40 человек, с доступными функциями демонстрации экрана, записи видеозвонка, разбиения участников по «комнатам»

5.2. Учебно-наглядные пособия:

– Презентации лекций, электронные материалы и ресурсы сети «Интернет».

5.3. Информационные технологии, используемые в образовательном процессе

– Пакет программ Microsoft Office; Acrobat Reader.