Решение диссертационного совета Д 501.001.84 на базе ФГБОУ ВО «Московский государственный университет имени М.В.Ломоносова», о приеме к защите диссертации Грибова Алексея Викторовича «Алгебраические неассоциативные структуры и их приложения в криптографии» на соискание ученой степени **кандидата физико-математических наук** по специальности 01.01.06 – математическая логика, алгебра и теория чисел.

Диссертация **Грибова Алексея Викторовича** «Алгебраические неассоциативные структуры и их приложения в криптографии» на соискание ученой степени **кандидата физико-математических наук** по специальности 01.01.06 – математическая логика, алгебра и теория чисел поступила в совет **23 марта 2015 года** и размещена на сайте http://mech.math.msu.su/~snark/index.cgi , http://istina.msu.ru/dissertations/9607776/.

Рассмотрев заявление А.В. Грибова о принятии диссертации к защите, диссертационный совет **15 мая 2015 года протокол № 6** назначил комиссию для подготовки заключения о диссертации в составе д.ф.-м.н. профессор В.Н. Латышев, д.ф.-м.н., профессор В.А. Артамонов, член-корр. РАН, профессор Ю.В. Нестеренко.

Соискателем были представлены следующие документы:

1. Заявление соискателя на имя председателя диссертационного совета Д 501.001.84 на базе ФГБОУ ВО МГУ имени М.В. Ломоносова, д.ф.-м.н., профессора Чубарикова Владимира Николаевича — 1 экз.
2. Анкета с фотокарточкой, заверенная в установленном порядке – 2 экз.
3. Заверенная в установленном порядке копия документа государственного образца о высшем образовании – 2 экз.
4. Удостоверение о сдаче кандидатских экзаменов – 2 экз.
5. Диссертация – 6 экз. (один экз. не переплетён).
6. Автореферат диссертации.
7. Заключение кафедры высшей алгебры механико-математического факультета ФГБОУ ВПО «Московский государственный университет имени М. В. Ломоносова» от **2 марта 2015 года № 1025** – 2 экз.
8. Отзыв научного руководителя д.ф.-м.н., профессора Михалева Александра Васильевича (Московский государственный университет им. М.В. Ломоносова) — 2 экз.
9. 4 маркированных почтовых карточки с указанием адреса соискателя и адреса диссертационного совета.

Заключение комиссии о диссертации

Представленная диссертация является самостоятельно выполненной, законченной научно-исследовательской работой, посвященной решению актуальных задач в области неассоциативных колец и квазигрупп. В диссертации получены следующие основные результаты:

1. Развита теория первичного радикала лупы, исследованы его свойства, доказано его совпадение с множеством строго энгелевых элементов лупы.

2. Получено описание Ω-первичного радикала Ω-лупы, как множества Ω-строго энгелевых элементов.

3. Установлены связи первичного радикала лупы обратимых элементов альтернативного кольца и первичного радикала кольца.

4. Построены криптографические схемы над различными неассоциативными структурами:

- аналог схемы шифрования Эль-Гамаля над ПЛС-квазигруппой;
- схема выработки общего секретного ключа над лупами Пейджа;
- схема шифрования с открытым ключом на основе покрытий лупы Муфанг.

5. Рассмотрена схема шифрования с открытым ключом над луповым кольцом, проанализированы свойства данной схемы, доказана гомоморфность данной схемы относительно одной из операций.

Методы исследования: наряду с классическими методами и результатами теории неассоциативных колец и квазигрупп, используются так же методы криптографии с открытым ключом.

Результаты диссертации являются новыми и получены автором самостоятельно. Все результаты изложены с полными математическими доказательствами.

Основное содержание диссертации опубликовано в следующих работах автора:

1. А. В. Грибов, П. А. Золотых, А. В. Михалёв. Построение алгебраической криптосистемы над квазигрупповым кольцом, Математические вопросы криптографии т.1, N.4, 2010, с.23-33. А. В. Грибову принадлежат разделы 3 и 5.

2. А. В. Грибов, П. А. Золотых, В. Т. Марков, А. В. Михалёв, С. С. Скаженик. Квазигруппы и кольца в кодировании и построении криптосхем. Прикладная дискретная математика, т.4, 2012, с.31 — 52. А. В. Грибову принадлежат разделы 1 и 3.

3. А. В. Грибов, А. В. Михалёв, Первичный радикал для луп и Ω-луп: I. Фундамент. и прикл. мат. т.19, N.2, 2014, с. 25 — 42. А. В. Грибову принадлежат доказательства основных результататов работы. А.В. Михалёву принадлежит постановка задач и общая редакция работы.

4. А. В. Грибов, Первичный радикал для альтернативных колец и луп. Фундамент. и прикл. мат. т.20, N.1, 2015, с. 63– 82.

5. А. В. Грибов, Гомоморфность некоторых криптографических систем на основе неассоциативных структур. Фундамент. и прикл. мат. т.20, N.1, 2015, с. 55 – 62.

Апробация диссертации.

Результаты диссертации докладывались на всероссийских и международных конференциях:

- «Algebra and Cryptography», Нью-Йорк, США, 2013;
- «New directions in cryptography», Москва, 12 июня 2014;
- «Индо-российской конференций по алгебре, теории чисел, дискретной математике и их приложений», Москва, 15-17 октября 2014;
- «Non-associative algebra and Lie theory», Оахака, Мексика, 26-30 января 2015.

. а также на следующих семинарах кафедры высшей алгебры механико-математического факультета ФГБОУ ВО “Московский государственный университет имени М.В. Ломоносова”:

- научно-исследовательском семинаре кафедры Высшей алгебры;
- семинаре «Теория колец» под руководством профессора А.В. Михалева.

Диссертация соответствует профилю совета и специальности 01.01.06 – математическая логика, алгебра и теория чисел по физико-математическим наукам.

Основные результаты диссертации опубликованы в открытой печати в 5 работах, 2 из которых в изданиях, входящих в «Перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание учёных степеней доктора и кандидата наук». Представленные в диссертации материалы в надлежащей полноте отражены в работах, опубликованных диссертантом. Результаты других авторов, упомянутые в тексте диссертации, отмечены соответствующими ссылками.

Текст автореферата соответствует содержанию диссертации.

Диссертация к защите представляется впервые.

Вышесказанное даёт основание утверждать:

Диссертация удовлетворяет требованиям пункта 9 «Положения о порядке присуждения учёных степеней» ВАК РФ, а её автор заслуживает присуждения учёной степени кандидата физико-математических наук по специальности 01.01.06 – математическая логика, алгебра и теория чисел.

Рекомендуемые официальные оппоненты и ведущая организация:

Ведущая организация: ФГБОУ ВПО «Тульский государственный педагогический университет имени Л. Н. Толстого». Адрес: Россия, Тула, Тульская область, проспект Ленина, 125. Ректор: д. ф.-м. н., профессор Панин Владимир Алексеевич.

Официальные оппоненты:

Доктор физико-математических наук, профессор Кожухов Игорь Борисович. Место работы: ФГАОУ ВО Национальный исследовательский университет «МИЭТ», кафедра высшей математики №1. Специальность: 01.01.06.

Кандидат физико-математических наук, Голубков Артем Юрьевич. Место работы: ФГБОУ ВПО «Москвовский государственный технический университет имени Н.Э. Баумана». Специальность: 01.01.06.

ФГБОУ ВПО «Тульский государственный педагогический университет имени Л. Н. Толстого» – ведущий научно-исследовательский центр страны, в котором работают известные ученые по специальности рассматриваемой диссертации. Официальные оппоненты являются известными специалистами в области (имеются работы, близкие к теме диссертации соискателя).

Работы официальных оппонентов, близкие к теме диссертации:

Кожухов Игорь Борисович

1. Т. В. Апраксина, И. В. Барков, И. Б. Кожухов, Два примера диагональных биполигонов // Фундамент. и прикл. матем., 18:3 (2013), с. 3–9.
2. В. И. Ким, И. Б. Кожухов, В. А. Ярошевич, Слабо регулярные полугруппы изотонных преобразований // Фундамент. и прикл. матем., 17:4 (2012), с. 145–165.
3. И. Б. Кожухов, В. А. Ярошевич, О потенциальной делимости матриц над дистрибутивными решетками // Дискрет. Матем., 22:2 (2010), с. 148–159.

Голубков Артем Юрьевич

1. А.Ю. Голубков, Радикал RN и слабо разрешимый радикал линейных групп над ассоциативными кольцами // Фундамент. и прикл. матем., 13:2 (2007), с. 31–115
2. А.Ю. Голубков, Первичный радикал элементарной группы Шевалле (классические серии) // Фундамент. и прикл. матем., 6:4 (2000), с. 1023–1059
3. А.Ю. Голубков, Первичный (RI-разрешимый) радикал унитарной группы над кольцом с инволюцией // Фундамент. и прикл. Матем., 6:1 (2000), с. 93–119

Работы сотрудников ведущей организации, близкие к теме диссертации:

д.ф.-м.н., профессор Балаба Ирина Николаевна: имеет следующие работы, близкие к теме диссертации:

1. И.Н. Балаба, Е.Н. Краснова, Полупростые градуированные кольца // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика,13:4(2) (2013), с.23–28.
2. И.Н. Балаба, А.Л. Канунников, А.В. Михалёв, Кольца частных градуированных ассоциативных колец: I // Фундамент. и прикл. Матем., 17:2 (2012), с. 3–74.
3. И.Н. Балаба, Градуированные регулярные кольца и модули // Чебышевский сб., 11:3 (2010), с. 22–31
4. I.N. Balaba, Special radicals of graded rings // Bull. Academie de stinte a Republici Moldova. Matematica. - 2004. - V.44. - № 1. - P. 26-33.
5. И.Н. Балаба, С.А. Пихтильков, Первичный радикал специальных супералгебр Ли // Фундамент. и прикл. Матем., 9:1 (2003), с.51–60.

д.ф.-м.н., профессор Добровольский Николай Михайлович: имеет следующие работы, близкие к теме диссертации:

1. Н.М. Добровольский, Д.К. Соболев, В.Н. Соболева, О матричном разложении

приведенной кубической иррациональности // Чебышевский сб., 14:1 (2013), с. 34–55.

2. Л.П. Добровольская, М.Н. Добровольский, Н.М. Добровольский, Н.Н. Добровольский, Гиперболические дзета-функции сеток и решеток и вычисление оптимальных коэффициентов // Чебышевский сб., 13:4 (2012), с. 4–107.

3. Н.М. Добровольский, Н.Н. Добровольский, Е.И. Юшина, О матричной форме теоремы Галуа о чисто периодических цепных дробях // Чебышевский сб., 13:3 (2012), с. 47–52

Диссертационный совет Д 501.001.84 на базе ФГБОУ ВО МГУ имени М.В. Ломоносова, вынес **решение принять** диссертацию Грибова А.В. «Алгебраические неассоциативные структуры и их приложения в криптографии» **к защите** 29 мая, протокол № 8. Разместить текст диссертации, автореферата, отзыв научного руководителя и решение совета **на сайте ФГБОУ ВО МГУ имени М. В. Ломоносова** (http://mech.math.msu.su/~snark/index.cgi, http://istina.msu.ru/dissertations/9607776/) и **на сайте ВАК Минобрнауки РФ** разместить объявление о защите диссертации и автореферат.

Постановили.

1. Новизна и актуальность темы диссертации не вызывают сомнений. Она подтверждается экспертизой. Основные результаты диссертации опубликованы в полной мере. Результаты других авторов, упомянутые в тексте диссертации, отмечены соответствующими ссылками.

2. Назначить ведущую организацию:

ФГБОУ ВПО «Тульский государственный педагогический университет имени Л. Н. Толстого». Адрес: Россия, Тула, Тульская область, проспект Ленина, 125.

Назначить официальными оппонентами: д.ф.-м.н., профессора Кожухов Игоря Борисовича. ФГАОУ ВО Национальный исследовательский университет «МИЭТ», кафедра высшей математики №1; к.ф.-м.н. Голубкова Артема Юрьевича, ФГБОУ ВПО «Москвовский государственный технический университет имени Н.Э. Баумана».

3. Назначить дату защиты — **25 сентября 2015 года.**

4. Разрешить печатание автореферата диссертации на правах рукописи. Автореферат правильно отражает содержание диссертации.

5. Рассылку авторефератов произвести по «списку рассылки авторефератов диссертации» без изменений.

6. Поручить комиссии в составе: д.ф.-м.н. профессор В.Н. Латышев, д.ф.-м.н., профессор В.А. Артамонов, член-корр. РАН, профессор Ю.В. Нестеренко подготовку заключения по диссертации к защите по существующей форме ВАК Минобрнауки РФ.

Результаты голосования по вопросу принятия диссертации **Грибова Алексея Викторовича** «Алгебраические неассоциативные структуры и их приложения в криптографии» на соискание ученой степени **кандидата физико-математических наук** по специальности 01.01.06 – математическая логика, алгебра и теория чисел к защите: за — 20, против — нет, воздержавшихся — нет.

Председатель диссертационного совета
Д 501.001.84 на базе ФГБОУ ВО МГУ имени М.В. Ломоносова,
профессор В. Н. Чубариков

Учёный секретарь диссертационного совета
Д 501.001.84 на базе ФГБОУ ВО МГУ имени М.В. Ломоносова,
профессор А. О. Иванов