МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

Институт естественных наук и математики
Кафедра алгебры и фундаментальной информатики

УТВЕРЖДАЮ
Проректор по науке

_____ В.В. Кружаев

«___» _____ 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Рекомендована Учебно-методическим советом Института естественных наук и математики для направлений подготовки и направленностей:

Направление	**Направленность**	**Квалификация**
Информационная безопасность	Методы и системы защиты информации, информационная безопасность	Исследователь. Преподаватель-исследователь

Екатеринбург, 2017

Рабочая программа дисциплины составлена в соответствии с Федеральными государственными образовательными стандартами высшего образования

Код направления	**Название направления**	**Реквизиты приказа Министерства образования и науки Российской Федерации об утверждении и вводе в действие ФГОС ВО**	
		Дата	**Номер приказа**
10.06.01	Информационная безопасность	30.07.14 в ред. от 30.04.2015	874

с изменениями от 30.04.2015, приказ № 464

Рабочая программа дисциплины составлена авторами:

№	**ФИО**	**Ученая степень, ученое звание**	**Должность**	**Кафедра**	**Подпись**
1	Баранский Виталий Анатольевич	Доктор физ.-мат. наук, профессор	профессор	Алгебры и фундаментальной информатики	
2	Синадский Николай Игоревич	Кандидат тех. наук, доцент	доцент	Алгебры и фундаментальной информатики	

Рабочая программа дисциплины одобрена на заседании кафедр:

№	**Наименование кафедры (УМС)**	**Дата заседания**	**Номер протокола**	**ФИО зав. кафедрой (предс. УМС)**	**Подпись**
1	Читающая кафедра – кафедра алгебры и фундаментальной информатики	07.09.2017	1	М.В. Волков	
2	Выпускающая кафедра – кафедра алгебры и фундаментальной информатики	07.09.2017	1	М.В. Волков	

Согласовано:

Председатель учебно-методического совета
Института естественных наук и математики Е.С. Буянова

Протокол № 1 от 26.09.2017 г.

Начальник ОПНПК О.А. Неволина

1 ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ Стандартизация и управление качеством продукции

1. Пререквизиты	История науки Методология научных исследований Дополнительные главы программно-аппаратных средств обеспечения информационной безопасности
2. Кореквизиты	
3. Постреквизиты	Итоговая государственная аттестация
4. Трудоемкость дисциплины-модуля, з.е.	3

1.1. Цели дисциплины

Целью дисциплины «Методы и системы защиты информации, информационная безопасность» является изучение:

- основных направлений информационной защиты, взгляда на информацию, как объект защиты с выделением характерных свойств защищаемой информации, качественные модели информационной защиты, информационных преступлений и информационных войнам;
- технических средств и методов защиты информации;
- администрирования компьютерных систем и обеспечения защиты информации в компьютерных сетях под управлением ОС Windows NT/2000;
- организационных, технологических и программно-аппаратных мер защиты от опасной компьютерной информации, в первую очередь – от вредоносных программ для ЭВМ.

Изучение дисциплины направлено на формирование аспирантами компетенций:

– способностью к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях (УК-1);

– способностью проектировать и осуществлять комплексные исследования, в том числе междисциплинарные, на основе целостного системного научного мировоззрения с использованием знаний в области истории и философии науки (УК-2);

– способностью формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность (ОПК-1);

– способностью разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности (ОПК-2);

– способностью обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности (ОПК-3);

– способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности (ПК-1);

– способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники,

перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах (ПК-2);

– способностью использовать нормативные правовые документы в своей профессиональной деятельности (ПК-3);
– способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ПК-4);
– способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации (ПК-5);
– способностью организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов (ПК-6);
– способностью определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия (ПК-7);
– способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия (ПК-8);
– способностью администрировать подсистемы информационной безопасности объекта (ПК-9);
– способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации (ПК-10);
– способностью участвовать в разработке подсистемы управления информационной безопасностью (ПК-11);
– способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности (ПК-12);
– способностью оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности (ПК-13);
– способностью применять программные средства системного, прикладного и специального назначения (ПК-14);
– способностью использовать инструментальные средства и системы программирования для решения профессиональных задач (ПК-15);
– способностью к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности (ПК-16);
– способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПК-17);
– способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов (ПК-19);
– способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности (ПК-21);
– способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью (ПК-23);
– способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью (ПК-24);

– способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-25);
– способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации (ПК-26);
– способностью участвовать в работах по реализации политики информационной безопасности (ПК-27);
– способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности (ПК-28).

1.2. Требования к результатам освоения дисциплины

В результате изучения дисциплины аспиранты должны иметь представление:

- об основных направлениях информационной защиты,
- о защите информации от утечки по техническим каналам,
- о методах и системах обеспечения безопасности сетевых технологий,
- об организационных, технологических и программно-аппаратных мерах защиты от опасной компьютерной информации,

знать:

- модели информационной защиты,
- методы обнаружения и нейтрализации средств технической разведки,
- знать основные способы защиты компьютерных систем, построенных на базе ОС Windows NT/2000,
- основные приемы и способы несанкционированного распространения, внедрения и запуска вредоносных программ,

уметь:

- определить уголовно-правовую характеристику некоторых информационных преступных деяний,
- организовать инженерную защиту и техническую охрану объектов информатизации,
- обеспечивать защиту информации в компьютерных сетях под управлением ОС Windows NT/2000,
- применять на практике методы и технологии антивирусной защиты.

1.3. Краткое описание дисциплины

Дисциплина «Методы и системы защиты информации, информационная безопасность» предназначена для подготовки аспирантов к сдаче кандидатского экзамена по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

1.4. Удельный вес занятий, проводимых в интерактивных формах:

Удельный вес занятий, проводимых в интерактивной форме, составляет 100% объема аудиторной нагрузки по дисциплине.

1.5. Трудоемкость освоения дисциплины

Очная форма обучения

Виды учебной работы, формы контроля	**Всего, час.**	**Номер учебного семестра**

		6
Аудиторные занятия, час.	4	4
Лекции, час.	4	4
Практические занятия, час.		
Лабораторные работы, час.		
Самостоятельная работа студентов, час.	104	104
Вид промежуточной аттестации (зачет, экзамен)	Э	Э
Общая трудоемкость по учебному плану, час.	108	108
Общая трудоемкость по учебному плану, з.е.	3	3

2 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела	Раздел дисциплины	Содержание
Р1	**Основы информационной безопасности**	Свойства информации как объекта защиты. Содержание и анализ исторически сложившихся направлений информационной защиты. Принципы, стратегии и модели информационной защиты. Информационные и компьютерные преступления.
Р2	**Технические средства и методы защиты информации**	Защита информации от утечки по техническим каналам. Обнаружение и нейтрализация средств. технической разведки. Инженерная защита и техническая охрана объектов информатизации.
Р3	**Безопасность сетевых технологий**	Принципы построения составных сетей. Стек протоколов TCP/IP. Общая характеристика угроз безопасности в компьютерных сетях. Типовые задачи администрирования сетевых служб в ОС Windows 2000-XP. Обеспечение безопасности информации в компьютерных сетях. Протоколы аутентификации в компьютерных сетях. Виртуальные частные сети. Системы обнаружения сетевых атак.
Р4	**Защита от вредоносных программ**	Понятие об опасной компьютерной информации. Классификация вредоносных программ. Уязвимые места программного обеспечения

		ЭВМ, способствующие внедрению, сокрытию, распространению и запуску вредоносных программ. Изучение функциональных возможностей вредоносных программ.

3 РАСПРЕДЕЛЕНИЕ ТРУДОЕМКОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ПО РАЗДЕЛАМ И КОНТРОЛЬНЫМ МЕРОПРИЯТИЯМ
(по очной форме обучения)

Семестр обучения: 6 Объем дисциплины (зач.ед.): 3

Раздел дисциплины			Аудиторная нагрузка (час.)				Виды, количество и объемы мероприятий																				
							Подготовка к аудиторным занятиям (час.)						Выполнение самостоятельных внеаудиторных работ (колич.)										Подготовка к контрольным и аттестационным мероприятиям (колич.)				
Код раздела, темы	Наименование раздела, темы	Всего по разделу, теме (час.)	Всего	Лекции	Практические занятия	Лабораторные работы	Всего	Лекции	Практ., семинар. занятия	Лабораторные работы	Н/и семинары, семинар-конференции, коллоквиумы	Всего (час.)	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Инд. или групповой проект*	Перевод иноязыч. литературы*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Курсовая работа / Междисц. курсовая работа*	Курсовой проект / Междисц. курсовой проект*	Всего (час.)	Контрольная работа*	Коллоквиум*	Зачет* (при наличии экзамена)	Зачет* (дифференцированный или при отсутствии экзамена)	Экзамен*
Р1	**Основы информационной безопасности**	15	1	1			4	4				10	2														
Р2	**Технические средства и методы защиты информации**	21	1	1			4	4				16	3														
Р3	**Безопасность сетевых технологий**	36	1	1			4	4				31	3														
Р4	**Защита от вредоносных программ**	18	1	1			4	4				13	2														
Всего по дисциплине (час.):		**108**	90																								18

4 ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ И САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ

1.1. Лабораторный практикум

не предусмотрено

1.2. Практические занятия

не предусмотрено

1.3. Самостоятельная работа студентов

1.3.1. Примерный перечень тем рефератов

не предусмотрено

1.3.2. *Примерный перечень тем домашних работ*

1. Содержание и анализ исторически сложившихся направлений информационной защиты.
2. Принципы, стратегии и модели информационной защиты.
3. Информационные и компьютерные преступления..
4. Информационные войны и информационное оружие.
5. Защита информации от утечки по техническим каналам.
6. Обнаружение и нейтрализация средств технической разведки.
7. Инженерная защита и техническая охрана объектов информатизации.
8. Принципы построения составных сетей. Адресация в IP-сетях. Стек протоколов TCP/IP.
9. Общая характеристика угроз безопасности в компьютерных сетях. Типовые задачи администрирования сетевых служб в ОС Windows 2000-XP. Обеспечение безопасности информации в компьютерных сетях.
10. Системы обнаружения сетевых атак. Аудит безопасности компьютерных систем и сетей.
11. Классификация и технические возможности вредоносных программ.
12. Уязвимые места программного обеспечения ЭВМ, способствующие внедрению, сокрытию, распространению и запуску вредоносных программ.

1.3.3. Примерный перечень тем контрольных работ

Не предусмотрено

1.3.3. Примерный перечень тем расчетных работ

Не предусмотрено

1.3.4. Примерный перечень тем расчетно-графических работ

Не предусмотрено

1.3.5. Примерная тематика коллоквиумов

Не предусмотрено

1.3.6. Примерная тематика курсовых проектов (работ)

Не предусмотрено

1.4. Примерный перечень контрольных вопросов к промежуточной аттестации по дисциплине.

1. Вредная и опасная информация в Интернет.
2. Атаки на информационные системы путем перегрузки каналов связи и входных буферов памяти. Использование «протоколов вежливости» для реализации сетевых атак.
3. Формы незаконного использования информации. Законодательные меры против незаконного использования информации.
4. Виды и формы применения информационно-технологического оружия.
5. Доктрина информационной безопасности России и реальности ее осуществления.
6. Государственная система защиты граждан и общества от опасной информации (законодательство и практика).
7. Модель комплексной информационной защиты и ее элементы.
8. Модель информационной защиты каналов связи.
9. Угрозы скрытого информационного воздействия на пользователей Интернет.
10. Формы и методы защиты признаковой информации.
11. Угрозы конфиденциальности и формы их реализации.
12. Модель информационного нарушителя, посягающего на конфиденциальную информацию методами несанкционированного доступа.
13. Организационно-распорядительные меры информационной защиты.
14. Характеристики технических каналов утечки информации.
15. Защита линий связи от взаимного влияния.
16. Механизмы побочного электромагнитного излучения радиоэлектронной аппаратуры.
17. Спектры побочных излучений.
18. Оборудование заземляющих устройств.
19. Утечка информационных сигналов через источники питания.
20. Электромагнитное экранирование.
21. Сигналы и помехи, генераторы шума.
22. ЭВМ как источник утечки компьютерной информации.
23. Каналы утечки информации из компьютерных мониторов.
24. Иностранная техническая разведка, классификация по типу используемой аппаратуры.
25. Классификация акустических каналов утечки информации.
26. Электроакустические преобразователи.
27. Средства перехвата и противодействию перехвату речевой инфорсмации по воздушному каналу.
28. Программно-аппаратные методы и средства выделения речевого сигнала и акустического шума.
29. Обнаружение электронных средств подслушивания.
30. Защита акустической информации путем зашумления и экранирования.
31. Электромагнитное экранирование помещений.
32. Аналоговое и цифровое скремблирование.
33. Визуальный и инструментальный досмотр помещений.
34. Безопасность проводных телефонных коммуникаций.
35. Протоколы передачи данных и протоколы обмена маршрутной информацией. Структура стека TCP/IP. Характеристика протоколов. Адресация в IP-сетях.

36. Протокол межсетевого взаимодействия IP.
37. Протокол доставки пользовательских дейтаграмм UDP.
38. Протокол надежной доставки сообщений TCP.
39. Протокол обмена управляющими сообщениями ICMP.
40. Протоколы обмена маршрутной информацией стека TCP/IP.
41. Угрозы безопасности информации, ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию».
42. Классификация и характеристика основных видов атак на компьютерные системы и сети.
43. Настройка базовых сетевых служб и протоколов.
44. Управление рабочей средой пользователя.
45. Организация почтового, DNS и Web-серверов.
46. Межсетевые экраны.
47. Фильтрации пакетов.
48. Атаки на протоколы и службы Интернет.
49. Безопасная настройка клиентского программного обеспечения.
50. Анализатор сетевого трафика MS Network Monitor.
51. Протоколы аутентификации в компьютерных сетях.
52. Схема VPN. Варианты построения VPN.
53. Протоколы PPTP, L2TP. Шифрование в PPTP.
54. Протокол SKIP.
55. Протокол IPSec.
56. Инфраструктура открытых ключей.
57. Защита сетевого трафика с использованием протокола IPSec в Windows 2000-XP.
58. Принципы обнаружения атак. Сигнатуры атак.
59. Аудит безопасности. Средства активного аудита.
60. Методология обеспечения безопасности информационных технологий с применением ГОСТ Р ИСО/МЭК 15408-1-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».
61. Применение программных средств аудита информационной безопасности.
62. Вредоносный программный код документов офисных приложений и его возможности. Методы вирусного копирования.
63. Реализация защиты от вредоносного программного кода в приложениях офисного пакета. Нейтрализация вредоносных макросов с целью их исследования.
64. Механизм сетевых атак на Интернет-браузеры (на примере Microsoft Internet Explorer). Механизмы статического скрытия вредоносного программного кода.
65. Механизмы скрытности вредоносных программ на этапе их выполнения.
66. Механизмы скрытия, используемые современными макровирусами.
67. Классификация и основные особенности различных видов вредоносных программ.
68. Способы подготовки вредоносных программ к безусловному запуску. Несанкционированный характер запуска вредоносных программ.
69. Внедрение и запуск вредоносных программ на этапах самотестирования компьютера и загрузки операционной системы. Способы автоматического запуска вредоносных программ.
70. Возможности программных закладок. Виды и способы программного перехвата компьютерной информации.
71. Виды компьютерных инфекций. Сущность вирусного заражения и жизненный цикл компьютерного вируса.
72. Возможности и особенности сетевых вредоносных программ.
73. Понятие о «троянских» программах и их функциях. Программы-«джойнеры».
74. Виды несанкционированного копирования компьютерной информации.

75. Виды нарушений работы ЭВМ со стороны вредоносных программ.
76. Виды несанкционированного блокирования и модификации компьютерной информации вредоносными программами.
77. Традиционные способы антивирусной защиты и сравнительная оценка их эффективности.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Рекомендуемая литература

5.1.1. Основная литература

1. Бакланов В.В. Введение в информационную безопасность. Модели и стратегии информационной защиты : учеб. пособие. Екатеринбург: изд-во ФГАОУ ВПО УрФУ, 2013. 236 с.
2. Зайцев А. П. Технические средства и методы защиты информации: Учебное пособие для вузов / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков и др.; под ред. А. П. Зайцева и А. А. Шелупанова. – 4-е изд., испр. и доп. – М.: Горячая линия – Телеком, 2009. – 616 с.
3. Андрончик А. Н. и др. Защита информации в компьютерных сетях. Практический курс: Учебное пособие /А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский, А. С. Коллеров, Н. И. Синадский, Д. А. Хорьков, М. Ю. Щербаков; Под ред. Н. И. Синадского. — Екатеринбург: ФГАОУ ВПО УрФУ, 2012. — 248 с.
4. Бакланов В.В. Защита компьютерной информации в клиентских приложениях: учебное пособие / В.В. Бакланов. Екатеринбург: ГОУ ВПО УрФУ 2013. – 84 с.
5. Бакланов В.В., Пономарев М.Э. Опасная компьютерная информация: учеб. пособие. — Екатеринбург: ФГАОУ ВПО УрФУ, 2012. — 146 с.

5.2.1.Дополнительная литература

6. Андрончик А.Н., Бакланов В.В., Необутов С.А., Пономарев М.Э., Синадский Н.И., Соболев О.Н. Основы компьютерной и информационной безопасности. Часть 3. Проблемы защиты информации в компьютерных системах. Учебно-наглядное пособие. — Екатеринбург: УрГУ, 2002. — 124 с.
7. Бакланов В.В., Духан Е.И., Необутов С.А., Пономарев М.Э., Синадский Н.И. Основы компьютерной и информационной безопасности. Часть 4. Программно-аппаратные средства защиты компьютерных систем. Учебно-наглядное пособие. — Екатеринбург: УрГУ, 2002. — 76 с.
8. Расторгуев С. П. Основы информационной безопасности: Учебное пособие для студентов высших учебных заведений / С. П. Расторгуев. – М.: Академия, 2007. – 192 с.
9. Расторгуев С.П. Философия информационной войны. М.: 2000 г. – 446 с.
10. Мазуров В.А. Компьютерные преступления: классификация и способы противодействия: Учебно-практическое пособие. — М.: «Палеотип», «Логос», 2002. — 148 с.
11. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов : в 3 т. / А. А. Хорев – М.: НПЦ «Аналитика», 2008.
12. Торокин А. А. Основы инженерно-технической защиты информации. М: «Ось-89», 365 с.
13. Хорев А. А. Защита информации от утечки по техническим каналам утечки информации. Часть 1. Технические каналы утечки информации. М.: Гостехкомиссия России, 1998, 320 с.

14. Люцарев В.С., Ермаков К.В., Рудный Е.Б., Ермаков И.В. Безопасность компьютерных сетей на основе Windows NT. – М.: Издательский отдел «Русская Редакция» ТОО «Channel Trading Ltd.», 1998. – 304 с.
15. Проскурин В.Г., Крутов С.В., Мацкевич И.В. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. пособие для вузов. – М.: Радио и связь, 2000. – 168 с.
16. Касперский Е.В. Компьютерные вирусы: что это такое и как с ними бороться. – М.: СК Пресс, 1998. – 288 с., ил.
17. Касперский К. Техника и философия хакерских атак. - М.: «Солон - Р», 1999, 272с.
18. Крис Касперски. Укрощение Интернета. –М.: СОЛОН-Р, 2002. –288 с.
19. Скэмбрей Джоел, Мак-Клар Стюарт. Секреты хакеров. Безопасность Windows 2000 – готовые решения. Пер. с англ. –М.: Издательский дом «Вильямс», 2002. –464 с.
20. Стюарт Мак-Клар, Джоел Скембрей, Джордж Курц. Секреты хакеров. Безопасность сетей - готовые решения, 2-е изд.: Пер. с англ. - М.: Издательский дом "Вильямс", 2001. -656 с.

5.2. Программное обеспечение

1. MicrosoftWindows7
2. MicrosoftOffice 2010
3. Microsoft VISIO

5.3. Базы данных, информационно-справочные и поисковые системы

1. Официальный интернет-портал правовой информации. – Режим доступа : http://pravo.gov.ru/, свободный. – Загл. с экрана.
2. Портал информационно-образовательных ресурсов УрФУ. – Режим доступа: http://study.urfu.ru/info/, свободный. – Загл. с экрана.
3. Электронная база нормативных документов ГОСТЭКСПЕРТ. – Режим доступа : http://gostexpert.ru/ , свободный. – Загл. с экрана.
4. Поисковые системы: www.yandex.ru, google.ru www.rambler.ru,

5.4. Электронные образовательные ресурсы

1. Все студенты имеют полный доступ к перечисленным ресурсам, в т.ч. через авторизованный доступ из сети интернет:
2. ElsevierB.V. БД Reaxys Договор № 1-3839832505 от 20.02.2013;
3. ООО «Первое Независимое Рейтинговое Агентство» ИПС FIRAPRO Договор № 43-12/370-2013 от 23.05.2013;
4. EBSCO Industries, IncБД Business Source Complete Договор № 624 от 02.07.2013;
5. EBSCO Industries, IncБД EBSCO Discovery Service Договор № 625 от 02.07.2013;
6. Elsevier B.V. БД Freedom Collection Договор № 1-4412061361 от 26.04.2013;
7. НП «НЭИКОН», БДкомпании Thomson Reuters, Web of Science всоставе: БД Citation Index Expanded, БД Social Sciences Index, БДArt&Humanities Citation Index, Journal Citation Reports, Conference Proceedings Citation Index Договор № 43-12/456-2013 от 12.07.2013;
8. ЗАО «КОНЭК», БДкомпании ProQuest, БДдиссертаций ProQuest Didital Dissertations and Theses;
9. БДebrarукомпании ProQuest, БД Emerald Journals 95, Emerald eBooks Series, Emerald Engineering Договор № 43-12/761-2013 от 12.09.2013;
10. EBSCO Industries, Inc, БДInspec, БД Applied Science & Tech Source (upgrade CASC) Договор № 43-12/762-2013 от 30.08.2013;
11. ООО «Научная электронная библиотека» Система SCIENCEINDEX Договор № 43-12/615-2013 от 01.08.2013;

12. ООО «Издательство Лань» ЭБС Лань Договор № 43-12/808-2013 от 13.09.2013;
13. ООО «Директ-Медиа», ЭБС «Университетская библиотека онлайн» Договор № 167-07/13 от 13.09.2013;
14. НП «НЭИКОН» ЭР EBSCOPublishing Договор № 43-12/1176-2013 от 02.12.2013;
15. НО БФ «Фонд содействия развитию УГТУ-УПИ» ООО Компания «Кодекс-Люкс» Договор № 68/1354 от 25.11.2013;
16. НП «НЭИКОН» БД QuestelORBIT Договор № 43-12/1099-2013 от 06.11.2013;
17. НП «НЭИКОН» AIPNatureJournalsДоговор № 43-12/1354-2013 от 16.12.2013;
18. НП «НЭИКОН», ACS, CambridgeUniversityPressДоговор № 43-12/1474-2013 от 15.11.2013
19. ElsevierB.V. БДScopusДоговор № 1-5608083155 от 11.11.2013;
20. НП «НЭИКОН», БД JSTOR, БД ACM Договор № 43-12/1585-2013 от 25.12.2013;
21. НП «НЭИКОН», БДOXFORDREFERENCEONLINEДоговор № 43-12/1586-2013 от 26.12.2013;
22. ООО «НЭИКОН», ООО «Ивис», ООО «Твинком», ООО «Интегрум Медиа» Договор № 43-12/1226-2013 от 01.11.2013.

6. УЧЕБНО-МАТЕРИАЛЬНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Аспиранты кафедры алгебры и фундаментальной информатики обеспечены специальными помещениями для проведения занятий:

- лекционного типа с наборами демонстрационного оборудования и учебно-наглядных пособий, обеспечивающих тематические иллюстрации, соответствующие примерным программам дисциплин (модулей), рабочим учебным программам дисциплин (модулей) (общеинститутские лекционные аудитории Т.509, Т.621);
- занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации (общеинститутские аудитории Т.150, Т.602);
- лабораторных и научно-исследовательских работ (общеинститутские аудитории Т.150, Т.151).

7. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В РАБОЧЕЙ ПРОГРАММЕ

Номер листа изменений	Номер протокола заседания кафедры	Дата заседания кафедры	Всего листов в документе	Подпись ответственного за внесение изменений

Оглавление