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
ДОПОЛНИТЕЛЬНЫЕ ГЛАВЫ ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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
2. Кореквизиты	
3. Постреквизиты	Итоговая государственная аттестация
4. Трудоемкость дисциплины-модуля, з.е.	3

1.1. Цели дисциплины

Целью дисциплины «Дополнительные главы программно-аппаратных средств обеспечения информационной безопасности» является изучение:

- защитных механизмов, реализованных в операционных системах универсального назначения семейств Windows и Linux;
- защищенных файловых систем NTFS, UFS, EXT2FS, EXT3FS;
- используемых в многозадачных операционных системах механизмов разграничения доступа;
- реализации защиты от несанкционированного доступа в современных системах управления базами данных;
- защиты компьютерной информации на уровне клиентских приложений.
- 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);
– готовностью участвовать в работе российских и международных исследовательских коллективов по решению научных и научно-образовательных задач (УК-3);
– готовностью использовать современные методы и технологии научной коммуникации на государственном и иностранном языках (УК-4);
– 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);
– готовностью к преподавательской деятельности по основным образовательным программам высшего образования (ОПК-5).

– 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 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 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 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 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 проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов (ПК-20);
– 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 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 угрозах компьютерной информации, реализуемых на различных уровнях программной иерархии;
- об основных принципах защиты компьютерной информации в операционных системах и пользовательских программных приложениях;
- о перспективных программно-аппаратных средствах и методах защиты компьютерной информации.

знать:

- механизмы разграничения доступа к компьютерной информации, реализованные в универсальных многозадачных операционных системах;
- общую структуру и детальное построение основных защищенных файловых систем;
- методы защиты компьютерной информации на уровне систем управления базами данных;
- основные принципы защиты клиентских программ, предназначенных для обработки защищаемой информации;
- основные принципы администрирования операционных систем и баз данных;
- принципы функционирования основных типов вредоносных программ, способы их выявления и нейтрализации.

уметь:

- восстанавливать данные на поврежденных логических разделах с операционными системами FAT, NTFS, EXT2FS и др.;
- исследовать статический код интерпретируемых вредоносных программ;
- выполнять функции администратора операционных систем Windows и UNIX: регистрировать новых пользователей, предоставлять им права доступа к объектам операционных систем, настраивать политику аудита;
- организовывать защиту сегментов компьютерной сети с использованием межсетевых экранов;
- выполнять защиту рабочих мест с использованием программно-аппаратных средств защиты информации.

1.3. Краткое описание дисциплины

Дисциплина «Дополнительные главы программно-аппаратных средств обеспечения информационной безопасности» формирует у аспирантов знания, умения и навыки по защите компьютерной информации на уровне операционных систем, компьютерных сетей, баз данных и программных приложений, а также готовит аспиранта 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
		5
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)	3	3
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	**Системы управления доступом к информации**	Основные понятия и определения. Классификация СУД. Специальные режимы пропуска. Идентификация и аутентификация пользователей АИС. Биометрические системы аутентификации. Биометрическая аутентификация по статическим признакам. Принципы распознавания человека по дактилоскопическому узору пальцев и форме руки. Распознавание по радужной оболочке и сетчатке глаза. Распознавание по форме головы и лица. Использование тепловой карты лица. Сведения о распознающих приборах, их характеристика. Ошибки первого и второго рода. Хранение аутентифицирующей биометрической информации в базах данных СУД. Биометрическая аутентификация по динамическим признакам. Динамические признаки рукописного почерка. Принципы распознавания говорящего по голосу. Распознавание пользователя ЭВМ по клавиатурному почерку. Достоинства и недостатки биометрических систем. Перспективные способы аутентификации. Физические носители ключевой информации. Ключевые дискеты и оптические диски. Магнитные карты. Карты Виганда. Проксимити-карты. Устройства хранения и обработки

		идентифицирующей информации на основе смарт-карт. Исполнительные устройства управления доступом. Механические, электромеханические замки, автоматические шлагбаумы, турникеты, шлюзы. Методы и средства аутентификации пользователей ЭВМ. Идентификация и аутентификация пользователей ЭВМ. Парольные системы. Статистика применяемых пользователями паролей. Типовые атаки на парольные системы. Требования к выбору паролей, вводу и хранению парольной информации. Компьютерные варианты устройств аутентификации пользователей по биометрическим признакам и физическим носителям ключевой информации.
Р2	**Машинные носители компьютерной информации**	Понятия о физических принципах и стойкости запечатления компьютерной информации на внешних машинных носителях. Средства записи и считывания информации с машинных носителей. Параметры дисковых накопителей и магнитных носителей, особенности их эксплуатации. Оптические и магнитооптические носители информации. Внешняя память на полупроводниковых структурах. Механизмы копирования, модификации и удаления компьютерной информации на машинных носителях. Программные средства физического и логического удаления компьютерной информации, оценка их эффективности. Аппаратные средства мгновенного размагничивания магнитных носителей. Существующие способы реставрации удаленной компьютерной информации на машинных носителях. Регламентация порядка обращения с машинными носителями конфиденциальной информации. Основы эксплуатации вычислительной техники и профилактики носителей информации и файловой системы. Правила эксплуатации вычислительной техники. Использование общесистемных программных средств для профилактики магнитных носителей и файловой системы. Восстанавливаемые файловые системы. Резервирование компьютерной информации как основная мера обеспечения ее сохранности. Виды резервирования. Стратегия резервирования. Использование стандартных средств резервирования системной информации и данных, программ-архиваторов. Отказоустойчивые дисковые конфигурации (RAID).

		Методы и средства восстановления компьютерной информации. Автоматическое и ручное восстановление системной информации, удаленных и испорченных данных, дефектных носителей. Восстановление системной информации, данных и программного обеспечения с резервных копий.
Р3	**Защита компьютерной информации в операционных системах**	Ключевые элементы программной архитектуры ОС, влияющие на защиту информации. Базовые понятия. Основные отличия операционных систем клона UNIX. Архитектура операционной системы. Виртуальные файловые системы. Монтирование устройств с различными файловыми системами. Архитектура файловых систем EXT2FS, EXT3FS. Файл как универсальный объект ОС. Виды файлов. Права доступа к файлам. Основные команды, позволяющие работать с файлами и устройствами. Изменение разрешений на доступ к файлам. Размещение элементов файловой системы на дисковом пространстве. Структура и назначение суперблока, карт битовых полей, индексных дескрипторов. Структура индексного дескриптора. Использование утилит для работы с поврежденными файловыми системами типа EXT*FS. Работа с отладчиком файловой системы DebugFS. Возможности дисковых редакторов системы Linux. Механизмы образования технологического информационного мусора. Восстановление поврежденных файлов. Регистрация пользователей. Предоставление прав, объединение в группы. Процессы и их классификация. Атрибуты процесса. Средства межпроцессного взаимодействия. Создание и уничтожение процессов. Использование возможностей командных оболочек. Понятие политики разграничения доступа в компьютерных системах. Одноуровневая и многоуровневая модели разграничения доступа, достоинства и недостатки. Реализация технологии разграничения доступа в ОС Windows 2000-XP. Модель безопасности. Доменная модель. Архитектура модели безопасности. Администрирование учетных записей пользователей. Группы пользователей. Права и привилегии пользователей и групп. Управление системной политикой безопасности. Стратегия предоставления прав на доступ к ресурсам. Методы идентификации и аутентификации пользователей,

		применяемые в ОС Windows 2000-XP. Хранение парольной информации. Алгоритм сетевой аутентификации. Обеспечение безопасности при удаленном доступе. Механизмы защиты информации от несанкционированного доступа, встроенные в ОС Windows 2000-XP. Защита данных средствами разрешений файловой системы NTFS. Криптографическая защита пользовательских данных средствами шифрующей файловой системы (EFS). Понятие об EFS. Структура зашифрованного файла. Безопасность системных данных. Файлы конфигурации и инициализации. Структура системного реестра ОС Windows. Редактирование реестра. Критичные настройки системного реестра. Способы защиты реестра. Логическое удаление компьютерной информации. Последствия применения команд удаления файлов и каталогов. Автоматическое восстановление удаленной информации с помощью распространенных утилит для ОС Windows 95/98/Me. Программы и команды для «ручного» восстановления данных в файловых системах FAT-12, 16, 32. Работа с программами типа DiskEditor. Подключение носителей с NTFS-разделами. Приемы и программное обеспечение для «ручного» восстановления удаленных файлов на NTFS-разделах. Автоматизированное восстановление удаленных файлов.
Р4	**Защита компьютерной информации в базах данных**	Типовые модели организации данных. Запросы в базах данных. Средства и методы обеспечения безопасности баз данных. Журнализация. Защита от угроз целостности данных. Меры противодействия нарушениям целостности сущностей – требование уникальности ключевых полей, применение ограничений и «бизнес-правил» на значения полей. Защита от нарушения ссылочной целостности – контроль ссылок, каскадное удаление и обновление связанных полей. Транзакция, как механизм обеспечения целостности. Виды сбоев при выполнении транзакций: ошибки пользователей, ошибки в прикладном и системном ПО, отказы аппаратуры, сбой при совместном доступе. Виды сбоев при совместном доступе – потерянные изменения, «грязные» данные, неповторяющиеся чтения. Защита от сбоев при совместном доступе с помощью блокировки объектов базы данных, распознавание и разрешение тупиковых ситуаций при взаимных блокировках.

		Защита баз данных от несанкционированного доступа. Особенности реализации моделей разделения доступа в СУБД, виды субъектов и прав доступа. Применение представлений (view) для реализации дискретной и мандатной модели доступа. Основные способы реализации НСД в СУБД: расширение полномочий с помощью процедур и событий; возможность выполнять произвольные запросы (доступ к SQL); доступ к файлам данных в обход СУБД; получение информации путем логических выводов и «неправильных» условий запроса; защита учетных записей, наличие встроенных и стандартных учетных записей; проблема применения шифрования при обеспечении многопользовательского доступа к данным. Актуальность типов угроз НСД для различных схем построения СУБД (локальная БД, файл-сервер, клиент сервер). Организация Web-протоколов. Структура гипертекстовых документов формата html, htt, hta, chm. Основные тэги гипертекстового файла. Механизмы вызова программ с помощью гиперссылок. Запуск активных компонентов из HTML-файла. Реализация атак на отказ в обслуживании. Вызов компонентов ActiveX с помощью тэгов HTML-файла. Компоненты, безопасные для инициализации и использования. Подкачка компонентов ActiveX с Web-серверов. Цифровая подпись компонентов. Типовые атаки на браузеры, связанные с внедрением и удаленным запуском опасных программных компонентов. Возможности выявления вредоносных активных компонентов на Web-сайтах.

3 РАСПРЕДЕЛЕНИЕ ТРУДОЕМКОСТИ ОСВОЕНИЯ ДИСЦИПЛИНЫ ПО РАЗДЕЛАМ И КОНТРОЛЬНЫМ МЕРОПРИЯТИЯМ

(по очной форме обучения)

Семестр обучения: 5 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 инояз. 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	Системы управления доступом к информации	19	1	1			4	4				14	2														
Р2	Машинные носители компьютерной информации	19	1	1			4	4				14	2														
Р3	Защита компьютерной информации в операционных системах	25	1	1			4	4				20	3														
Р4	Защита компьютерной информации в базах данных	41	1	1			4	4				36	3														
Всего по дисциплине (час.):		**108**	104																						4		

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. Защита узлов и блоков стационарных компьютеров от НСД. Механические крепежные элементы. Средства, препятствующие хищению составных частей компьютера. Устройства, препятствующие несанкционированному доступу в аппаратные отсеки. Пломбы, печати, голографические наклейки. Защита дисководов и внешних интерфейсов.

2. Использование настроек BIOS для защиты от загрузки внешних программ со сменных машинных носителей. Использование сигнализационных датчиков для контроля вскрытия системного блока. Интеллектуальные возможности контроллеров жестких магнитных дисков с IDE-интерфейсом.

2. Использование сигнализационных датчиков для контроля доступа к рабочему месту пользователя. Контроль за рабочим местом с использованием Web-камер.

3. Возможности операционной системы и прикладных программ по отслеживанию фактов физического доступа к системному блоку и узлам компьютерной системы.

4. Характеристика офисного пакета как операционной среды для разработки текстовых, графических, табличных и иных документов. Изолирующие свойства приложений офисного пакета.

5. Механизмы образования технологического информационного мусора, способствующие утечке конфиденциальной информации (на примере текстового процессора Word). Информация, содержащаяся в «Свойствах» документа. Пользовательские словари, автозамена и автотекст.

6. Накопление «мусора» во фрагментах документов и шаблонов. Режим «быстрого сохранения» документов.

7. Защитные механизмы, реализованные в текстовом процессоре Word. Шифрование содержимого документа.

8. Возможности парольной защиты от изменения документа и доступа к встроенному программному коду.

9. Особенности встроенной среды программирования VBA. Программные проекты, модули, процедуры и функции. Событийные процедуры. Автоисполняемые макросы. Приоритет запуска событийных процедур из различных программных модулей в документах и шаблонах.

10. Реализация стандартной защиты от вирусов в макросах. Возможности использования офисных приложений для обработки конфиденциальной информации.

1.3.3. Примерный перечень тем контрольных работ
Не предусмотрено

1.3.4. Примерный перечень тем расчетных работ
Не предусмотрено

1.3.5. Примерный перечень тем расчетно-графических работ
Не предусмотрено

1.3.6. Примерная тематика коллоквиумов
Не предусмотрено

1.3.7. Примерная тематика курсовых проектов (работ)
Не предусмотрено

1.4. Примерный перечень контрольных вопросов к промежуточной аттестации по дисциплине

1. Работа с файловой системой EXT2FS.
2. Исследование файловой системы EXT2FS.
3. Администрирование операционной системы Linux.
4. Исследование процессов в операционной системе Linux.
5. Исследование защитных механизмов Microsoft Word.
6. Исследование защитных механизмов браузера Internet Explorer.
7. Основы администрирования ОС Windows 2000-XP.
8. Использование реестра для настройки параметров ОС Windows 2000-XP.
9. Ручное восстановление данных на разделах FAT и NTFS .
10. Настройка политики безопасности ОС Windows 2000-XP. Аудит событий безопасности
11. Противодействие угрозам безопасности информации в ОС Windows XP, связанным с физическим доступом к серверам и рабочим станциям.
12. Настройка защищенных рабочих станций под управлением ОС Windows 2000-XP и тестирование защиты.
13. Использование файловой системы с шифрованием (EFS) в ОС Windows XP. Работа с сертификатами.
14. Использование специализированных аппаратно-программных средств защиты информации от несанкционированного доступа. Создание защищенных виртуальных дисков средствами программно-аппаратных комплексов «StrongDisk» и «SecretDisk».
15. Защита информации от несанкционированного доступа средствами программно-аппаратного комплекса «Аппаратный модуль доверенной загрузки Аккорд-АМДЗ».
16. Защита информации от несанкционированного доступа средствами программно-аппаратного комплекса «Dallas Lock».
17. Реализация многоуровневой политики разграничения доступа средствами программно-аппаратного комплекса «Страж NT».
18. Организация защищенного документооборота с использованием криптографических средств, предоставляемых СКЗИ «КриптоПро».
19. Средства обеспечения защиты информации в системах управления базами данных (СУБД); средства контроля целостности информации, организация аудита; причины, виды, основные методы нарушения конфиденциальности в СУБД; совместное применение средств идентификации и аутентификации, встроенных в СУБД и в ОС. Реализация групповой политики доступа к данным средствами СУБД MS Access.

20. Мониторинг состояния элементов сети с использованием анализаторов сетевого трафика MS Network Monitor, Ethereal.
21. Создание защищенных сегментов при работе в сети Интернет с использованием межсетевых экранов. Применение фильтрующего маршрутизатора WinRoute.
22. Безопасная настройка клиентского программного обеспечения. Защита рабочих станций с использованием персональных сетевых фильтров. Конфигурирование персонального сетевого фильтра Agnitum OutPost Firewall.
23. Защита сетевого трафика с использованием протокола IPSec в Windows 2000-XP.
24. Применение программного комплекса ViPNet для организации виртуальной частной сети.
25. Защита сетевого трафика с использованием линейки программных продуктов «Застава».
26. Применение СОА Snort для обнаружения скрытого сканирования, атак, использующих преднамеренное нарушение структуры сетевых пакетов, атак вида «отказ в обслуживании».
27. Применение программных средств аудита информационной безопасности с целью тестирования состояния защищенности компьютерных систем от несанкционированного доступа и выработки мер защиты от выявленных угроз.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Рекомендуемая литература

5.1.1. Основная литература

1. Бакланов В.В. Защитные механизмы операционной системы Linux: учебное пособие. – Екатеринбург: ФГАОУ ВПО УрФУ, 2013. – 278 с.
2. Духан Е.И. Применение программно-аппаратных средств защиты компьютерной информации: учеб. пособие / Е.И. Духан, Н.И. Синадский, Д.А. Хорьков. – Екатеринбург: ФГАОУ ВПО УрФУ, 2013. — 182 с.
3. Синадский Н. И. Анализ и восстановление данных на носителях с файловой системой NTFS: учеб. пособие. – Екатеринбург: ФГАОУ ВПО УрФУ, 2012. – 136 с.

5.2.1.Дополнительная литература

4. Запечинков С.В., Милославская Н.Г., Толстой А.И. Основы построения виртуальных частных сетей: Учеб. пособие для вузов. — М.: Горячая линия – Телеком, 2003. — 249 с.
5. Гайдамакин Н.А. Автоматизированные информационные системы, базы и банки данных. Вводный курс: Учебное пособие. — М.: Гелиос АРВ, 2002. — 368 с.
6. Милославская Н.Г., Толстой А.И. Интрасети: доступ в Internet, защита: Учеб. пособие для вузов. — М.:ЮНИТИ-ДАНА, 2000. — 527 с.
7. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учеб. пособие для вузов / П.Ю.Белкин, О.О.Михальский, А.С.Першаков и др. – М.: Радио и связь, 1999. – 168 с.
8. 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.
9. Синадский Н.И., Соболев О.Н. Угрозы безопасности компьютерной информации: Учеб. пособие. — Екатеринбург: Изд-во Урал. ун-та, 2000. — 85 с.
10. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: Учеб. пособие для студ. высш. учеб. заведений / Павел Борисович Хорев. — М.: Издательский центр «Академия», 2005. — 256 с.
11. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. — СПб: Наука и Техника, 2004. — 384 с.: ил.

12. UNIX: руководство системного администратора. Для профессионалов. 3-е изд. /Э.Немет, Г.Снайдер, С.Сибасс, Т.Хейн. — К.: Издательская группа BHV, 2003. — 925 с.
13. Атака на Internet/Медведовский И.Д., Семьянов П.В., Леонов Д.Г. – 2-е изд., перераб. и доп. – М.: ДМК, 1999. – 336 с.
14. Ахметов К.С., Федоров А.Г. Microsoft Internet Explorer 4.0 для всех. – М.: КомпьютерПресс, 1997. – 336 с.
15. Б.Кришнамурти, Дж. Рексворд. Web-протоколы. Теория и практика. – М.: ЗАО «Издательство БИНОМ», 2002 г. – 592 с.
16. Барсуков В.С., Романцов А.П. Опасность и безопасность в сети INTERNET//Специальная техника – 1999, № 1-2, С. 74-83.
17. Борн Г. Руководство разработчика на Microsoft Windows Script Host 2.0 Мастер-класс/Пер. с англ. – СПб.: Питер; М.: Издательско-торговый дом «Русская редакция», 2001. – 480 с.
18. Бэндл Д. Защита и безопасность в сетях Linux. Для профессионалов. — СПб.: Питер, 2002. — 480 с.
19. В.А.Костромин. ОС Linux на вашем персональном компьютере (электронный вариант книги).
20. Дарахвелидзе П.Г., Марков Е.П. Разработка Web-служб средствами Delphi. – СПб.: БХВ-Петербург, 2003. – 672 с.
21. Дунаев С.Б. Технологии Интернет-программирования. – СПб.: БХВ-Петербург, 2001. – 480 с.
22. Елманова Н.З., Трепалин С.В. Delphi 4: технология COM. OLE, ActiveX, Автоматизация MIDAS, Microsoft Transaction Server. — М.: Диалог-МИФИ, 1999 г. — 320 с.
23. Зегжда Д.П., Ивашко А.М. Как построить защищённую информационную систему. — Санкт - Петербург, НПО «Мир и семья - 95» 1997, — 286с.
24. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. — М.: Горячая линия — Телеком, 2002. — 336 с.
25. Крис Касперски. Укрощение Интернета. – М.: СОЛОН-Р, 2002. – 288 с.
Лукацкий А.В. Вопросы информационной безопасности, возникающие при использовании технологий Java и ActiveX. Тематический выпуск № 2. – Москва, 1998.
26. Матросов А.В., Сергеев А.О., Чаунин М.П. HTML 4.0. — СПб.: БХВ-Петербург, 2001. —672 с.
27. Мельников В.В. «Защита информации в компьютерных системах», — М.: «Финансы и статистика», «Электронинформ», 1997. — 364 с.
28. Митчелл М., Оулдем Дж., Самьюэл А. Программирование для Linux. Профессиональный подход.: Пер. с англ. – М.: Издательский дом «Вильямс», 2003. — 288 с.
29. Попов А.В. Командные файлы и сценарии Windows Script Host. – СПб.: БХВ-Петербург, 2002. – 320 с.
30. Расторгуев С.П. «Программные методы защиты информации в компьютерах и сетях», — М.: «Яхтсмен», 1993. — 187с.
31. Робачевский А.М. Операционная система UNIX. — СПб.: БХВ-Санкт-Петербург, 2000. —528 с.
32. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. «Защита информации в компьютерных системах и сетях». — М.: «Радио и связь», 1999. — 328с.
33. С.Мак-Клар, С.Скембрей, Д.Курц. Секреты хакеров. Безопасность сетей-готовые решения, 2-е изд.: Пер. с англ. — М.: Изд.дом “Вильямс”, 2001. — 656 с.
34. Скэмбрей Джоел, Мак-Клар Стюарт. Секреты хакеров. Безопасность Windows 2000 – готовые решения. Пер. с англ. – М.: Издательский дом «Вильямс», 2002. – 464 с.

35. Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма. Справочное пособие — СПб.: БХВ - Петербург, Арлит 2002. — 496 с.
36. 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.
37. Таненбаум Э. Современные операционные системы. 2-е изд. — СПб.: Питер, 2002. — 1040 с.
38. Торрес Дж. Скрипты для администратора Windows. Специальный справочник. – СПб.: Питер, 2002. – 336 с.
39. Фридл Дж. Регулярные выражения. Библиотека программиста. – СПб.: Питер, 2001. — 352 с.
40. Хоникатт Джерри. Реестр Windows 2000. Пер. с англ. Уч. пос. – М.: Издательский дом «Вильямс», 2000. – 320 с.
41. Шрайбер С. Недокументированные возможности Windows 2000. Библиотека программиста. – СПб.: Питер, 2002. – 544 с.
42. Шураков В.В. «Обеспечение сохранности информации в системах обработки данных», — М.: «Финансы и статистика», 1985. — 223 с.
43. Эш Рофэйл, Яссер Шохауд. COM и COM+. Полное руководство: Пер. с англ. — К.: ВЕК+, К.: НТИ, М.: Энтроп, 2000. — 560 с.
44. Ярочкин В.И. «Безопасность информационных систем». — М.: «Ось-89», 1996. — 318с.

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