ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.15 Программно-аппаратные средства защиты информации

Направление подготовки 10.03.01 Информационная безопасность

Профиль подготовки Безопасность автоматизированных систем

Квалификация выпускника бакалавр

Форма обучения очная

1. Цели освоения дисциплины:

- изучение программно-аппаратных средств защиты информации на объектах информатизации.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Программно–аппаратные средства защиты информации» относится к базовой части. Требования к предшествующим знаниям представлены в таблице 2.1. Перечень дисциплин, для которых дисциплина «Программно – аппаратные средства защиты информации» является основополагающей, представлен в табл. 2.2.

Таблица 2.1 – Требования к пререквизитам дисциплины

Компетенции	Дисциплина
ОК-5	Учебная практика по получению первичных профессиональных умений и навыков
ПК-2	Языки программирования
ПК-2	Операционные системы
ПК-2	Программирование на языках высокого уровня
ПК-2	Сетевые технологии
ПК-2	Базы данных
ПК-2	Основы защиты АИС
ПК-2	Безопасность операционных систем
ПК-2	Теория функции комплексного переменного
ПК-2	Системы реального времени
ПК-2	Прикладные компьютерные программы
ПК-2	Учебная практика по получению первичных профессиональных умений и навыков
ПК-3	Сети и системы передачи информации
ПК-3	Основы защиты АИС
ПК-8	Русский язык и культура речи
ПК-8	Психология и педагогика
ПК-8	Инженерная графика
ПК-8	Компьютерная графика

Таблица 2.2 – Требования к постреквизитам дисциплины

Компетенции	Дисциплина
ОК-5	Производственная эксплуатационная практика
	Производственная (преддипломная) практика
	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа бакалавра)
ПК-2	Безопасность систем баз данных
ПК-2	Производственная эксплуатационная практика
ПК-2	Производственная (преддипломная) практика
ПК-2	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа бакалавра)
ПК-3	Производственная эксплуатационная практика
ПК-3	Производственная (преддипломная) практика
ПК-3	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа бакалавра)
ПК-8	КОИБАС
ПК-8	Производственная эксплуатационная практика
ПК-8	Производственная (преддипломная) практика
ПК-8	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты (работа бакалавра)

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Таблица 3.1 – Взаимосвязь планируемых результатов обучения по дисциплине и планируемых результатов освоения образовательной программы

Индекс и содержание компетенции	Знания	Умения	Навыки и (или) опыт деятельности

ОК-5 - способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Этап 1: о нормах профессиональной этики	Этап 1: соблюдать нормы профессиональной этики	Этап 1: навыки применения профессиональной этики при коллективной работе
ОК-5 - способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Этап 2: о социальной значимости своей будущей профессии при выполнении профессиональной деятельности в области обеспечения информационной безопасности, законодательство РФ о государственной гражданской службе	Этап 2: ориентироваться в законодательстве РФ о государственной гражданской службе, нормативных-правовых актах в области информационной безопасности	Этап 2: навыки анализа эффективности профессиональной деятельности в области обеспечения информационной безопасности
ПК-2 - способностью применять программные средства системного, прикладного и специального назначения, инструментальны е средства, языки и системы программирования для решения профессиональны х задач	Этап 1: основные программные средства для решения задач программировани я	Этап 1: разрабатывать программы прикладного значения	Этап 1: применения программных средств системного назначения
ПК-2 - способностью применять программные средства системного,	Этап 2: современные специальные средства для решения задач программировани	Этап 2: разрабатывать программы специального значения	Этап 2: применения программных средств специального назначения

прикладного и специального назначения, инструментальны е средства, языки и системы программирования для решения профессиональны х задач	я		
ПК-3 - способностью администрировать подсис темы информационной безопасности объекта защиты	Этап 1: основные принципы администрирова ния	Этап 1: проводить процедуру администрирова ния подсистемы безопасности	Этап 1: навыки администрирова ния подсистемы безопасности
ПК-3 - способностью администрировать подсистемы информационной безопасности объекта защиты подсистемы информационной безопасности объекта защ иты	Этап 2: современные инструментальные средства администрировани я	Этап 2:уметь использовать инструментальны е средства администрирован ия подсистемы безопасности	Этап 2: навыки применения инструментальн ых средств администрирова ния подсистемы безопасности
ПК-8 - способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Этап 1: Основные этапы оформления рабочей документации	Этап 1: Разрабатывать основные рабочие документы	Этап 1: Навыки разработки рабочих документов
ПК-8 - способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	Этап 2: Основные нормативные и методические документы	Этап 2: Применять нормативные документы в рабочей документации	Этап 2: Навыки применения нормативных документов

4. Объем дисциплины

Объем дисциплины «Программно – аппаратные средства защиты информации» составляет 5 зачетных единиц (180 академических часов), распределение объема дисциплины на контактную работу обучающихся с преподавателем (КР) и на

самостоятельную работу обучающихся (СР) по видам учебных занятий и по периодам обучения представлено в таблице 4.1.

Таблица 4.1 – Распределение объема дисциплины по видам учебных занятий и по периодам обучения, академические часы

№ п/п	Вид учебных занятий	Итого КР	Итого СР	Семестр № 6		Семестр № 7	
				КР	СР	КР	СР
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	Лекции (Л)	50	-	16	-	34	-
2	Лабораторные работы (ЛР)	32	-	16	-	16	-
3	Практические занятия (ПЗ)	30	-	14	-	16	-
4	Семинары(С)	-	-	-	-	-	-
5	Курсовое проектирование (КП)	2	20	-	-	2	20
6	Рефераты (Р)	-	-	-	-	-	-
7	Эссе (Э)	-	-	-	-	-	-
8	Индивидуальные домашние задания (ИДЗ)	-	-	-	-	-	-
9	Самостоятельное изучение вопросов (СИВ)	-	22	-	14	-	8
10	Подготовка к занятиям (ПкЗ)	-	18	-	10	-	8
11	Промежуточная аттестация	6	-	2	-	4	-
12	Наименование вида промежуточной аттестации	х	х	Зачет		Экзамен	
13	Всего	120	60	48	24	72	36

5. Структура и содержание дисциплины

Структура дисциплины представлена в таблице 5.1.

Таблица 5.1 – Структура дисциплины

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1.	**Раздел 1 Программно-аппаратная защита информации**	6	16	16	14	-	-	x	-	14	10	x	ОК-5, ПК-2, ПК-3, ПК-8
1.1.	**Тема 1** Основные понятия программно-аппаратной защиты информации.	6	8	8	8	-	-	x	-	6	6	x	ОК-5, ПК-2, ПК-3, ПК-8
1.2.	**Тема 2** Идентификация пользователей КС-субъектов доступа к данным.	6	8	8	6	-	-	x	-	8	4	x	ОК-5, ПК-2, ПК-3, ПК-8
2.	**Контактная работа**	6	16	16	14	-	-	x	-	-	-	2	
3.	**Самостоятельная работа**	6	-	-	-	-	-	x	-	14	10	-	x
4.	**Объем дисциплины в семестре**	6	16	16	14	-	-	x	-	14	10	2	x
5.	**Раздел 2**	7	34	16	16	-	22	x	-	8	8	x	ОК-5,

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
	Средства ограниченного доступа												ПК-2, ПК-3, ПК-8
5.1	**Тема 3** Средства и методы ограничения доступа к файлам.	7	8	4	4	-	6	х	-	2	2	х	ОК-5, ПК-2, ПК-3, ПК-8
5.2	**Тема 4** Методы и средства ограничения доступа к компонентам ЭВМ.	7	10	4	4	-	6	х	-	2	2	х	ОК-5, ПК-2, ПК-3, ПК-8
5.3	**Тема 5** Защита программ и данных от несанкционированного копирования.	7	8	4	4	-	6	х	-	2	2	х	ОК-5, ПК-2, ПК-3, ПК-8
5.4	**Тема 6** Управление криптографическими ключами.	7	8	4	4	-	4	х	-	2	2	х	ОК-5, ПК-2, ПК-3, ПК-8
6.	**Контактная работа**	7	16	16	16	-	2	х	-	-	-	4	

№ п/п	Наименования разделов и тем	Семестр	Объем работы по видам учебных занятий, академические часы										Коды формируемых компетенций
			лекции	лабораторная работа	практические занятия	семинары	курсовое проектирование	рефераты (эссе)	индивидуальные домашние задания	самостоятельное изучение вопросов	подготовка к занятиям	промежуточная аттестация	
1	2	3	4	5	6	7	8	9	10	11	12	13	14
7.	**Самостоятельная работа**	7	-	-	-	-	20	x	-	8	8	-	x
8.	**Объем дисциплины в семестре**	7	16	16	16	-	22	x	-	8	8	4	x
9.	**Всего по дисциплине**	x	50	32	30	-	22	x	-	22	18	6	x

5.2. Содержание дисциплины

5.2.1 – Темы лекций

№ п.п.	Наименование темы лекции	Объем, академические часы
Семестр №6		
Л-1	Предмет и задачи программно-аппаратной защиты информации	**2**
Л-2	Политика безопасности в компьютерных системах. Оценка защищенности	**2**
Л-3	Нормативно-методическое обеспечение создания АС	**2**
Л-4	Основные понятия и концепции	**2**
Л-5	Взаимная проверка подлинности пользователей	**2**
Л-6	Схема идентификации гиллоу-куискуотера	**2**
Л-7	Защита информации в кс от несанкционированного доступа	**2**
Л-8	Концепция построения систем разграничения доступа	**2**
Семестр №7		
Л-9-10	Защита информации, обрабатываемой пэвм и лвс, от утечки по сети электропитания	**4**
Л-11-12	Защита программ и данных от несанкционированного копировани	**4**
Л-13-14	Особенности проектирования на современном уровне и синтез	**4**
Л-15-16	Методы и методики проектирования КСИБ от НСД	**4**
Л-17-18	Методы и методики оценки КСИБ	**4**
Л-19-20	Генерация ключей	**4**
Л-21-22	Особенности эксплуатации КСИБ на объекте защиты	**4**
Л-23-24	Модели защиты информации	**4**
Л-25-26	Реализация системы управления доступом	**4**
Итого по дисциплине		**50**

5.2.2 – Темы лабораторных работ

№ п.п.	Наименование темы лабораторной работы	Объем, академические часы
Семестр №6		
ЛР-1-2	Защита информации в пэвм	**4**
ЛР-3-4	Виды мероприятий по защите информации	**4**
ЛР-5-6	Современные системы защиты пэвм от несанкционированного доступа к информации	**4**
ЛР-7-8	Методы, затрудняющие считывание скопированной информации	**4**
Семестр №7		
ЛР-9-10	Методы, препятствующие использованию скопированной информации	**4**
ЛР-11-12	«Основные функции средств защиты от	**4**

	копирования	
ЛР-13-14	Хранение ключей	**4**
ЛР-15-16	Распределение ключей	**4**
Итого по дисциплине		**32**

5.2.3 – Темы практических занятий

№ п.п.	Наименование темы занятия	Объем, академические часы
Семестр №6		
ПЗ-1	Основные понятия	**2**
ПЗ-2	Уязвимость компьютерных систем	**2**
ПЗ-3	Механизмы защиты	**2**
ПЗ-4	Идентификация и аутентификация пользователя	**2**
ПЗ-5	Протоколы идентификации с нулевой передачей знаний	**2**
ПЗ-6	Биометрическая идентификация и аутентификация пользователя	**2**
ПЗ-7	Парольная аутентификация	**2**
Семестр №7		
ПЗ-8	Система разграничения доступа к информации в кс	**2**
ПЗ-9	Методы разграничения доступа	**2**
ПЗ-10	Организация доступа к ресурсам кс	**2**
ПЗ-11	Обеспечение целостности и доступности информации в кс	**2**
ПЗ-12	Защита информации в пэвм	**2**
ПЗ-13	Виды мероприятий по защите информации	**2**
ПЗ-14-15	Современные системы защиты пэвм от несанкционированного доступа к информации	**4**
Итого по дисциплине		**30**

5.2.5 Темы курсовых работ (проектов)

1. Анализ аппаратных средств защиты ПК
2. Разработка ПС на основе асимметричного шифрования для защиты ОС.
3. Разработка ПС для защиты ОС с помощью цветовой схемы.
4. Разработка программно-аппаратного комплекса для защиты ОС.
5. Разработка электронного ключа для защиты от несанкционированного доступа к ПК
6. Разработка ПС для защиты от спама
7. Разработка ПС для защиты ПК от несанкционированного сканирования портов.
8. Анализ существующих методов защиты ОС
9. Разработка ПС для защиты от фишинговых атак
10. Разработка ПС для защиты ПК от несанкционированного сканирования портов.
11. Разработка электронного ключа для доступа к ПК
12. Разработка межсетевого экрана
13. Создание системы защиты локальной сети от несанкционированного доступа
14. Разработка системы управления сайтом с дополнительной аутентификацией пользователя

15. Разработка ПС для аутентификации пользователя с помощью графического изображения.

16. Разработка аппаратно-программного комплекса защиты ПК

17. Анализ существующих ПС по защите локальных сетей от внешних атак

18. Анализ существующих методов защиты ОС Linux

19. Разработка программного средства защиты ОС Linux

20. Разработка комплексной системы защиты серверной ОС

5.2.6 – Вопросы для самостоятельного изучения

№ п.п.	Наименования темы	Наименование вопроса	Объем, академические часы
1.	Основные понятия программно-аппаратной защиты информации	Основные процессы жизненного цикла АС. Оценка защищенности КС. Взаимосвязь между стандартными процессами и стадиями.	4
2.	Идентификация пользователей КС-субъектов доступа к данным	Идентификация объекта. Защита при обмене. Сведения о системе защиты информации. Знания о КС и умения работать с ней.	4
3.	Средства и методы ограничения доступа к файлам.	Идентификация и аутентификация субъекта доступа Проверка прав доступа субъекта к объекту	4
4.	Методы и средства ограничения доступа к компонентам ЭВМ	Обеспечение некопируемости дистрибутивных дисков стандартными средствами. Обеспечение некорректного дисассемблирования машинного кода программы стандартными средствами	4
5.	Защита программ и данных от несанкционированного копирования	Использование типовых СЗИ. Использование типовых структурно-ориентированных компонентов СЗИ	4
6.	Управление криптографическими ключами	Криптографические методы. Метод привязки к идентификатору	2
Итого по дисциплине			**22**

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная учебная литература, необходимая для освоения дисциплины

1. Методы и средства инженерно-технической защиты информации [Электронный ресурс]: учебное пособие/ В.И. Аверченков [и др.].— Электрон. текстовые данные.— Брянск: Брянский государственный технический университет, 2012.— 187 c.

2. Помешкин А.А. Система защиты информации от несанкционированного доступа на основе программно-аппаратного комплекса «SECRET NET 5.0» [Электронный ресурс]: учебно-методическое пособие/ Помешкин А.А., Коротких И.В.— Электрон. текстовые данные.— Новосибирск: Новосибирский государственный технический университет, 2012.— 47 c.

6.2 Дополнительная учебная литература, необходимая для освоения дисциплины

1. Аверченков В.И. Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - М.: ФЛИНТА, 2011 г. - 224 с.

2. Аверченков В.И. Аудит информационной безопасности органов исполнительной власти: учебное пособие / В.И. Аверченков, М.Ю. Рытов, М.В. Рудановский, А.В. Кувыклин. - М.: ФЛИНТА, 2011 г. - 100 с.

3. Аверченков В.И. Методы и средства инженерно-технической защиты информации: учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Кувыклин, Т.Р. Гайнулин . - М.: ФЛИНТА, 2011 г. - 187 с.

6.3 Методические указания для обучающихся по освоению дисциплины и другие материалы к занятиям

Электронное учебное пособие, включающее:

- конспект лекций;
- методические указания по выполнению лабораторных работ;
- методические указания по выполнению практических (семинарских) работ.

6.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Электронное учебное пособие, включающее:

- методические рекомендации для студентов по самостоятельному изучению вопросов;
-методические рекомендации по подготовке к занятиям;
- методические рекомендации по выполнению курсовой работы (проекта).

6.5 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

1. Open Office
2. JoliTest

6.6 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://www.intuit.ru/studies/courses/1162/285/lecture/7164?page=2

7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Занятия лекционного типа проводятся в аудитории, оборудованной мультимедиапроектором, компьютером, учебной доской.

Таблица 7.1 – Материально-техническое обеспечение лабораторных работ

Номер ЛР	Тема лабораторной работы	Название лаборатории	Название спецоборудования	Название технических и электронных средств обучения и контроля знаний
ЛР-1-2	Защита информации в пэвм	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Офисный пакет OpenOffice Операционные системы Windows XP/7; Интегрированный пакет MS Office Standard;
ЛР-3-4	Виды мероприятий по защите информации	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Офисный пакет OpenOffice
ЛР-5-6	Современные системы защиты пэвм от несанкционированного доступа к информации	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Операционные системы Windows XP/7;
ЛР-7-8	Методы, затрудняющие считывание скопированной информации	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Интегрированный пакет MS Office Standard;
ЛР-9-10	Методы, препятствующие использованию скопированной информации	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Офисный пакет OpenOffice

ЛР-11-12	«Основные функции средств защиты от копирования	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Операционные системы Windows XP/7;
ЛР-13-14	Хранение ключей	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Интегрированный пакет MS Office Standard;
ЛР-15-16	Распределение ключей	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Офисный пакет OpenOffice

Таблица 7.2 – Материально-техническое обеспечение практических занятий

Номер ПЗ	Тема занятия	Название аудитории	Название спецоборудования	Название технических и электронных средств обучения и контроля знаний
ПЗ-1	Основные понятия	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Офисный пакет OpenOffice
ПЗ-2	Уязвимость компьютерных систем	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Операционные системы Windows XP/7;
ПЗ-3	Механизмы защиты	941 аудитория – лаборатория программно-аппаратных средств защиты	ПЭВМ	Интегрированный пакет MS Office Standard;

		информации		
ПЗ-4	Идентификация и аутентификация пользователя	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Офисный пакет OpenOffice
ПЗ-5	Протоколы идентификации с нулевой передачей знаний	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Операционные системы Windows XP/7;
ПЗ-6	Биометрическая идентификация и аутентификация пользователя	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Интегрированный пакет MS Office Standard;
ПЗ-7	Парольная аутентификация	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Офисный пакет OpenOffice
ПЗ-8	Система разграничения доступа к информации в кс	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Операционные системы Windows XP/7;
ПЗ-9	Методы разграничения доступа	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Интегрированный пакет MS Office Standard;
ПЗ-10	Организация доступа к ресурсам кс	941 аудитория – лаборатория программно-аппаратных	ПЭВМ	Офисный пакет OpenOffice

		средств защиты информации		
ПЗ-11	Обеспечение целостности и доступности информации в кс	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Операционные системы Windows XP/7;
ПЗ-12	Защита информации в пэвм	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Интегрированный пакет MS Office Standard;
ПЗ-13	Виды мероприятий по защите информации	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Офисный пакет OpenOffice
ПЗ-14-15	Современные системы защиты пэвм от несанкционированного доступа к информации	941 аудитория – лаборатория программно-аппаратных средств защиты информации	ПЭВМ	Операционные системы Windows XP/7;

Занятия семинарского (практического) типа проводятся в аудиториях, оборудованных учебной доской, рабочим местом преподавателя (стол, стул), а также посадочными местами для обучающихся, число которых соответствует численности обучающихся в группе.

Текущий контроль и промежуточная аттестация проводится в учебных аудиториях для текущего контроля и промежуточной аттестации, укомплектованных специализированной мебелью и техническими средствами обучения.

Самостоятельная работа студентов проводится в помещениях для самостоятельной работы, укомплектованном специализированной мебелью и техническими средствами обучения. Учебное оборудование хранится и обслуживается в помещениях для хранения и профилактического обслуживания учебного оборудования.

Оценочный материал для проведения промежуточной аттестации обучающихся по дисциплине представлен в Приложении 6.

Программа разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 10.03.01

Информационная безопасность, утвержденным приказом Министерства образования и науки РФ № 1515 от 01.12.2016 г.

Разработал (и): _____ В.А. Урбан