Экз. № 1

Министерство образования и науки Российской Федерации

ГОУВПО «Сыктывкарский государственный университет»

«СОГЛАСОВАНО»

Начальник отдела по техническому и экспортному контролю Управления ФСТЭК России по Северо-Западному федеральному округу

_____ Назаров

«9» 11 2010 г.

«УТВЕРЖДАЮ»

Ректор ГОУВПО «Сыктывкарский государственный университет»

_____ В.Н.Задорожный

«18» 11 2010 г.

Инв. № 326
«18» 11 2010 г.
Сыктывкарский госуниверситет

УЧЕБНАЯ ПРОГРАММА

курса повышения квалификации

«Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»

г. Сыктывкар

2010

Приложение к Вход. № 180 дсп 18.11.10 г.
Сыктывкарский госуниверситет

«40» листов к Вх. № 1441
«22» 09 2010 г.
Управление ФСТЭК России по Северо-Западному федеральному округу

1. ВВЕДЕНИЕ

Образовательная программа «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных» разработана в соответствии с правовыми и нормативными документами в области информационной безопасности, введенными в действие указами Президента Российской Федерации и Постановлениями Правительства Российской Федерации. Основой для разработки программы являются документы, регламентирующие вопросы защиты персональных данных: «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные 15.02.2008 ФСТЭК России, Приказ ФСТЭК России от 5 февраля 2010 г. N 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных».

При разработке программы выполнены требования к содержанию дополнительных профессиональных образовательных программ, утвержденные приказом Министерства образования России от 18.06.1997 № 1221.

Программа рассмотрена и обсуждена на заседаниях учебно-методической комиссии факультета информационных систем и технологий с участием кафедры защиты информации 16.02.2010 (Протокол № УМК-05-09/10) и научно-методического совета ГОУВПО «Сыктывкарский государственный университет» с участием ведущих преподавателей и специалистов данного направления 17 февраля 2010 года (Протокол № 6).

Цель обучения по программе: обеспечить слушателей теоретическими знаниями и практическими навыками планирования, организации и проведения работ по обеспечению безопасности персональных данных (далее - ПДн) при их обработке в информационных системах персональных данных (далее - ИСПДн) в условиях существования угроз безопасности информации.

Поставленная цель обучения достигается решением следующих задач:

- изучением правовых и организационных основ обеспечения безопасности ПДн в ИСПДн;
- изучением методов и процедур выявления угроз безопасности ПДн в ИСПДн и оценке степени их опасности;
- практической отработкой способов и порядка проведения работ по обеспечению безопасности ПДн при их обработке в ИСПДн.

Категория слушателей: специалисты органов государственной власти, местного самоуправления, организаций и предприятий, осуществляющих разработку и эксплуатацию автоматизированных информационных систем, обеспечивающих обработку, хранение и передачу ПДн.

Срок обучения: 72 часа аудиторных учебных занятий.

Форма обучения: очная (с отрывом от работы).

Режим занятий: 36 часов аудиторной учебной и самостоятельной работы под руководством преподавателя в неделю.

В результате изучения курса слушатели должны:

быть ознакомленными:

- с концептуальными основами защиты информации в стране;
- с лицензированием деятельности в области защиты информации;
- с документами национальной системы стандартизации, действующими в области защиты информации.

знать:

- основные виды угроз безопасности ПДн;
- физическую природу и причины возникновения технических каналов утечки информации при ее обработке в ИСПДн;
- содержание основных нормативных актов, регламентирующих порядок организации работ по обеспечению безопасности ПДн;
- основные положения по категорированию и обоснованию требований по защите информации в ИСПДн;
- методы и процедуры выявления угроз безопасности ПДн;

- содержание и порядок организации работ по выявлению угроз безопасности ПДн;
- организацию контроля и оценки степени безопасности ПДн при их обработке в ИСПДн.

уметь:

- планировать организацию мероприятий по обеспечению защиты ПДн;
- разрабатывать необходимые документы в интересах организации работ по защите ПДн;
- производить категорирование ПДн и обосновывать требования по защите информации в ИСПДн;
- использовать методики оценки актуальных угроз безопасности ПДн при их обработке в ИСПДн.

иметь навык:

- применения организационных мер и программно-аппаратных средств обеспечения безопасности ПДн при их обработке в ИСПДн от несанкционированного доступа (далее - НСД).

2. Перечень тем

№	Наименование тем
1	**Раздел № 1. Общие вопросы технической защиты информации**
2	**Тема № 1.** Правовые и организационно-распорядительные документы в области технической защиты информации
3	**Тема № 2.** Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от НСД
4	**Тема № 3.** Основные организационные меры и технические средства защиты информации от утечки по техническим каналам на объектах информатизации ~~и в защищаемых помещениях~~
5	**Раздел № 2. Организация обеспечения защиты персональных данных в информационных системах персональных данных**
6	**Тема № 4.** Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных
7	**Тема № 5.** Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных
8	**Тема № 6.** Рекомендации по обеспечению безопасности и контролю безопасности персональных данных при их обработке в информационных системах персональных данных

3. РЕФЕРАТИВНОЕ ОПИСАНИЕ ТЕМ

Раздел № 1. Общие вопросы технической защиты информации

Тема № 1. Правовые и организационно-распорядительные документы в области технической защиты информации

Основные понятия в области технической защиты информации (ТЗИ). Стратегия ~~Концепция~~ национальной безопасности Российской Федерации до 2020 года. Доктрина информационной безопасности Российской Федерации. Концептуальные основы ТЗИ. Законодательные и иные правовые акты, регулирующие вопросы ТЗИ. Система документов по ТЗИ и краткая характеристика ее основных составляющих.

Основные положения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Принципы обработки персональных данных и права субъекта персональных данных.

Структура и направления деятельности системы ТЗИ в субъектах Российской Федерации. Система органов по ТЗИ в Российской Федерации, их задачи, распределение полномочий по обеспечению ТЗИ. Задачи и функции Федеральной службы по техническому и экспортному контролю (ФСТЭК России). Задачи и функции управлений ФСТЭК России по федеральным округам.

Системы лицензирования и сертификации ФСТЭК России. Аттестация объектов информатизации по требованиям безопасности информации. Документы национальной системы стандартизации в области ТЗИ.

Тема № 2. Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от несанкционированного доступа

Понятие «безопасности информации», «угрозы безопасности информации», «уязвимости», «источника угрозы». Целостность, конфиденциальность

и доступность информации. Классификационная схема угроз безопасности информации и их общая характеристика. Особенности проведения комплексного исследования объектов информатизации на наличие угроз безопасности информации. Методы оценки опасности угроз.

Классификация объектов информатизации. Методические рекомендации по классификации и категорированию объектов ~~защиты~~ информатизации.

Характеристика основных угроз НСД и моделей нарушителя безопасности информации, а также способов реализации этих угроз. Характеристика основных классов атак, реализуемых в сетях общего пользования, функционирующих с использованием стека протоколов TCP/IP. Понятие программно-математического воздействия и вредоносной программы. Классификация вредоносных программ, основных деструктивных функций вредоносных программ и способов их реализации. Особенности программно-математического воздействия в сетях общего пользования. Методы и средства выявления угроз НСД к информации и специальных воздействий на нее. Порядок обеспечения защиты информации при эксплуатации автоматизированных систем.

Требования и рекомендации по защите информации, обрабатываемой средствами вычислительной техники. Основные требования и рекомендации по защите ПДн. Основные рекомендации по защите информации, составляющей коммерческую тайну.

Содержание и порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Структура, содержание и порядок подготовки документов при аттестации объектов информатизации по требованиям безопасности информации.

Тема № 3. Основные организационные меры и технические средства защиты информации от утечки по техническим каналам на объектах информатизации ~~и в защищаемых помещениях~~

Причины и физические явления, порождающие технические каналы утечки информации (ТКУИ) при эксплуатации объектов информатизации и защищаемых помещений. Классификация ТКУИ. Характеристики информа-

ционных сигналов, определяющих степень их опасности. Методы и средства выявления ТКУИ на типовом объекте информатизации ~~и в защищаемом помещении~~.

Основные требования и рекомендации по защите речевой информации, циркулирующей в защищаемых помещениях. Защита информации, циркулирующей в системах звукоусиления и звукового сопровождения видеокинофильмов. Защита информации при проведении магнитной звукозаписи. Защита речевой информации при ее передаче по каналам связи.

Содержание и порядок организации и проведения специальных исследований технических средств обработки информации.

Оценка защищенности помещений от утечки речевой информации по акустическому и виброакустическому каналам и по каналу электроакустических преобразований во вспомогательных технических средствах и системах.

Оценка защищенности информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации.

Раздел № 2. Организация обеспечения защиты персональных данных в информационных системах персональных данных

Тема № 4. Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных

Основное содержание «Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного Постановлением Правительства Российской Федерации от 17.11.2007 № 781.

Особенности информационного элемента ИСПДн. Основные принципы обеспечения безопасности ПДн при их обработке: законности, превентивности, адекватности, непрерывности, адаптивности, самозащиты, многоуровневости, персональной ответственности и минимизации привилегий, разделения полномочий и их характеристика. Основные направления деятельности по обеспечению безопасности ПДн при их обработке в ИСПДн.

Общая характеристика уязвимостей информационной системы персональных данных. Определение актуальных угроз безопасности персональных данных в ИСПДн на основании «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной 15.02.2008 ФСТЭК России.

Типовые модели угроз безопасности персональных данных, обрабатываемых в ИСПДн. Порядок разработки частных моделей угроз безопасности ПДн в конкретных ИСПДн с учетом их назначения, условий и особенностей функционирования на основе «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной 15.02.2008 ФСТЭК России. Проведение анализа защищенности ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн.

Методы и способы защиты информации от несанкционированного доступа. Методы и способы защиты информации от утечки по техническим каналам. Разработка системы защиты ПДн с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн, на основании «Положения о методах и способах защиты информации в информационных системах персональных данных», утвержденного Приказом ФСТЭК России от 05.02.2010 № 58.

Тема № 5. Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Классификация информационных систем персональных данных в соответствии с «Порядком проведения классификации информационных систем персональных данных», утвержденных Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20.

Организация обеспечения безопасности ПДн в деятельности служб безопасности организаций при защите ПДн. Перечень основных этапов при организации работ по обеспечению безопасности ПДн. Реализация разреши-

тельной системы допуска пользователей. Разграничение доступа пользователей в помещения, где осуществляется обработка и хранение персональных данных. Организация учета, хранения и обращения носителей информации, содержащих охраняемые сведения. Рекомендации по применению мер и средств обеспечения безопасности ПДн от физического доступа.

Состав, содержание и порядок разработки организационных распорядительных документов для формирования и функционирования системы обеспечения безопасности ПДн в органах власти и организациях.

Тема № 6. Рекомендации по обеспечению безопасности и контролю безопасности персональных данных при их обработке в информационных системах персональных данных

Реализация функций управления доступом, регистрации и учета, обеспечения целостности, анализа защищенности, обеспечения безопасного межсетевого взаимодействия и обнаружения вторжений. Возможные варианты реализации мероприятий по защите ПДн с использованием существующих сертифицированных средств защиты информации.

Аналитические исследования (аудит) защиты информации в организации. Организация контроля за обеспечением уровня защищенности информации. Виды, формы и способы контроля защиты ПДн в ИСПДн. Планирование работ по контролю состояния защиты ПДн в ИСПДн. Основные вопросы, подлежащие проверке (анализу) при контроле состояния организации защиты ПДн.

4. НАИМЕНОВАНИЕ ВИДОВ ЗАНЯТИЙ ПО ТЕМАМ

№	Наименование тем	Всего часов	Лекции	Практические занятия	Семинары	Самост. работа	Зачет
1.	**Раздел № 1. Общие вопросы технической защиты информации**	**26**	**20**	**6**			
2.	**Тема № 1.** Правовые и организационно-распорядительные документы в области технической защиты информации	8	8				
3.	**Тема № 2.** Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от НСД	8	6	2			
4.	**Тема № 3.** Основные организационные меры и технические средства защиты информации от утечки по техническим каналам на объектах информатизации ~~и в защищаемых помещениях~~	10	6	4			
5.	**Раздел № 2. Организация обеспечения защиты ПДн в ИСПДн**	**42**	**20**	**10**	**8**	**4**	
6.	**Тема № 4.** Угрозы безопасности персональных данных при их обработке в информационных системах персональных данных	16	6	4	4	2	
7.	**Тема № 5.** Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	18	10	4	2	2	
8.	**Тема № 6.** Рекомендации по обеспечению безопасности и контролю безопасности персональных данных при их обработке в информационных системах персональных данных	8	4	2	2		
9.	**Итого по видам занятий**	**68**	**40**	**16**	**8**	**4**	
10.	**Всего**	**72**	**40**	**16**	**8**	**4**	**4**

5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО РЕАЛИЗАЦИИ УЧЕБНОЙ ПРОГРАММЫ

В процессе изучения данной программы необходимо использовать действующие законодательные акты в области защиты ПДн в ИСПДн, технической защиты информации, документы национальной системы стандартизации, организационно-распорядительные и нормативные документы ФСТЭК (Гостехкомиссии) России, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий по защите ПДн в ИСПДн. Часть лекций может излагаться проблемным методом с привлечением слушателей для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приемы тестирования.

На практические занятия выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл практических занятий по применению программно-аппаратных средств защиты ПДн при их обработке в ИСПДн (Темы № 2, 6) проводится в компьютерном классе с предварительной установкой необходимого программного обеспечения в компьютерной сети. Для проведения цикла практических занятий выделяются два преподавателя: ведущий преподаватель (лектор) и преподаватель для привития практических навыков. При проведении практических занятий необходимо отрабатывать задания, учитывающие специфику выполняемых функциональных обязанностей слушателями курсов по своему профессиональному предназначению, в том числе предусматривать задания с проведением деловых игр (эпизодов).

Практические занятия по обнаружению ТКУИ и отработке методического аппарата технического контроля (Тема № 3) проводятся по циклам на четырех-шести рабочих местах (количество рабочих мест зависит от количества обучаемых в учебной группе) в учебной лаборатории. На каждом рабочем месте должен быть преподаватель, развернуто необходимое оборудование технического контроля и средства имитации ТКУИ.

На практических занятиях по Теме № 4 слушатели определяют актуальные угрозы безопасности персональных данных и разрабатывают проект модели угроз безопасности ПДн в ИСПДн своей организации под контролем преподавателя.

На практических занятиях по Теме № 5 слушатели готовят проекты организационных распорядительных документов для формирования и функционирования системы обеспечения безопасности ПДн своей организации под контролем преподавателя.

Для проведения практических занятий должны использоваться методические разработки, позволяющие индивидуализировать задания обучаемым в зависимости от их должностных категорий. Такие задания представляют собой проблемные ситуационные варианты, различающиеся моделями ИСПДн и набором конкретных действий, существенных для определенных категорий обучаемых, объединенных в соответствующую подгруппу.

Теоретические вопросы по тематике курса, наиболее важные в профессиональной деятельности слушателей, выносятся для обсуждения на семинары. При подготовке к семинарам слушателям заранее выдаются вопросы, подготовка к которым требует самостоятельной работы с использованием рекомендованной литературы.

Примерные темы семинарских занятий:

- Классификация ИСПДн;

- Модель угроз ИСПДн;

- Проектирование системы защиты персональных данных;

- Мероприятия по техническому обеспечению безопасности ПДн при их обработке в ИСПДн и особенности их реализации;

- Организационные мероприятия по обеспечению безопасности ПДн при их обработке в ИСПДн.

В качестве формы итогового контроля полученных знаний выбран зачет, в процессе проведения которого применяются методы тестирования с использованием компьютерных технологий.

6. СПИСОК ОСНОВНОЙ ЛИТЕРАТУРЫ

6.1. Закон Российской Федерации от 05.03.1992 № 2446-1 «О безопасности».

6.2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите ~~и~~ информации».

6.3. Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании» (в ред. Федерального закона от 09.05.2005 № 45-ФЗ)

6.4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (в ред. Федеральных законов от 25.11.2009 № 266-ФЗ, от 27.12.2009 № 363-ФЗ)

6.5. Указ Президента Российской Федерации от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» (в ред. Указов Президента РФ от 22.03.2005 № 330, от 20.07.2005 № 846, от 30.11.2006 № 1321; от 23.10.2008 № 1517, от 17.11.2008 № 1625).

6.6. Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» (в ред. Указа Президента РФ от 21.10.2008 № 1510).

6.7. ~~Концепция~~ Стратегия национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от ~~17.12.1997~~ 12.05.2009 ~~№ 1300 (в ред. Указа Президента РФ от 10.01.2000 № 24).~~ 537 до 2020 года

6.8. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 09.09.2000 № Пр-1895.

6.9. Постановление Правительства Российской Федерации от 26.01.2006 № 45 «Об организации лицензирования отдельных видов деятельности» (в ред. Постановлений Правительства РФ от 05.05.2007 № 269, от 03.09.2007 № 556, от 02.10.2007 № 634, от 07.04.2008 № 241, от 12.06.2008 № 452, от 27.06.2008 № 478, от 12.08.2008 № 599, от 07.11.2008 № 821, от 27.01.2009 № 50)

6.10. Постановление Правительства Российской Федерации от 01.02.2006 № 54 «Об утверждении Положения об осуществлении государственного строительного надзора в Российской Федерации».

6.11. Постановление Правительства Российской Федерации от 15.08.2006 № 504 «О лицензировании деятельности по технической защите конфиденциальной информации».

6.12. Постановление Правительства Российской Федерации от 31.08.2006 № 532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации».

6.13. Постановление Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

6.14. Постановление Правительства Российской Федерации от 06.07.2006 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

6.15. Постановление Правительства Российской Федерации от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

6.16. Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

6.17. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Гостехкомиссия России, 1992.

6.18. Положение о сертификации средств защиты информации по требованиям безопасности информации. Утверждено приказом Гостехкомиссии России от 27.10.1995 № 199.

6.19. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30.08.2002 № 282.

6.20. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Гостехкомиссия России, 2002.

6.21. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Утвержден приказом председателя Гостехкомиссии России от 19.06.2002 № 187.

6.22. Приказ ФСТЭК России, ФСБ России и Минпромсвязи России от 13.02.2008 № 55/86/20 «Порядок проведения классификации информационных систем персональных данных».

6.23. Базовая модель угроз безопасности персональным данным при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15.02.2008.

6.24. Методика определения актуальных угроз безопасности персональным данным при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15.02.2008.

6.25. Приказ ФСТЭК России от 5 февраля 2010 г. N 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных». Зарегистрирован в Минюсте РФ 19 февраля 2010 г. N 16456.

6.26. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утвержден решением председателя Гостехкомиссия России от 30.03.1992.

6.27. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утвержден решением председателя Гостехкомиссии России от 30.03.1992.

6.28. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкционированного доступа к информации. Утвержден решением председателя Гостехкомиссии России от 25.07.1997.

6.29. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. Утвержден решением председателя Гостехкомиссии России от 30.03.1992.

6.30. Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования. Утвержден решением председателя Гостехкомиссии России от 25.07.1997.

6.31. Руководящий документ. Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден приказом председателя Гостехкомиссии России от 04.06.1999 №114.

6.32. ГОСТ Р52069.0-2003 Защита информации. Система стандартов. Основные положения.

6.33. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества.

6.34. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

6.35. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы воздействующие на информацию. Общие положения.

6.36. ГОСТ Р 52863-2007. Защита информации. Автоматизированные системы в защищённом исполнении. Испытания на устойчивость к намеренным силовым электромагнитным воздействиям. Общие требования.

6.37. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель (на основе прямого применения международного стандарта ИСО/МЭК 15408:99).

6.38. ГОСТ Р ИСО/МЭК 15408-2-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий Часть 2. Функциональные требования безопасности (на основе прямого применения международного стандарта ИСО/МЭК 15408:99).

6.39. ГОСТ Р ИСО/МЭК 15408-3-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности (на основе прямого применения международного стандарта ИСО/МЭК 15408:99).

7. СПИСОК ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ

7.1. Белов Е.Б., Основы информационной безопасности: Учебное пособие./Белов Е.Б., Лось В.П., Мещеряков Р.В. Шелупанов А.А.- М.: Горячая линия - Телеком, 2005.

7.2. Бузов Г.А. Защита от утечки информации по техническим каналам: Учебное пособие./Бузов Г.А., Калинин С.В., Кондратьев А.В.- М.: Горячая линия – Телеком, 2005.

7.3. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994.-Книга 1 и 2.

7.4. Герасименко В.А., Основы защиты информации. -/Герасименко В.А., Малюк А.А., М.:МОПО РФ-МИФИ, 1997.

7.5. Запечников С.В. Информационная безопасность открытых систем. Часть 1: Учебник для вузов /Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. – М.: Горячая линия – Телеком, 2004.

7.6. Малюк А.А. Введение в защиту информации в автоматизированных системах: Учебное пособие для вузов / Малюк А.А., Пазизин С.В., Погожин Н.С.- М.: Горячая линия – Телеком, 2004.

7.7. Снытников А.А. Лицензирование и сертификация в области защиты информации. -М.: Гелиос АРВ, 2003.

7.8. Стрельцов А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы. - Минск, 2005.

7.9. Хорев А.А. Защита информации от утечки по техническим каналам: Учеб. Пособие. М.: МО РФ, 2006.

7.10. Язов Ю.К. Основы методологии количественной оценки эффективности защиты информации в компьютерных сетях.- Ростов на Дону: Издательство СКНЦ ВШ, 2006.

7.11. Язов Ю.К. Основы технологий проектирования систем защиты информации в информационно-телекоммуникационных системах: Монография /Аграновский А.В., Мамай В.И., Назаров И.Г., Язов Ю.К.- Издательство СКНЦ ВШ, 2006.

7.12. Будников С.А., Паршин Н.В. Информационная безопасность автоматизированных систем: Учебное пособие – Воронеж, ЦПКС ТЗИ, 2009.

7.13. Мельников В.В. Защита информации в компьютерных системах. - М.,1997.

7.14. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа.- С.-П.,2004.

7.15. Петраков А.В. Основы практической защиты информации. Учебное пособие.- М.,2005.

7.16. Девянин П.Н., Садернинов А.А., Трайнев В.А. и др. Учебное пособие. Информационная безопасность предприятия. - М.,2006.

7.17. Некраха А.В., Шевцова Г.А.Организация конфиденциального делопроизводства и защита информации. Учебное пособие.- М.: Академический Проект, 2007.

Приложение № 1

СВЕДЕНИЯ

о педагогических кадрах и укомплектованности штатов

(в части обеспечения учебного процесса по программе повышения квалификации

«Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»)

№ п/п	Наименование дисциплин в соответствии с учебным планом	Обеспеченность педагогическими работниками							Основное место работы, должность	Условия привлечения к трудовой деятельности (штатный, совмест.)
		Фамилия И.О. должность по штатному расписанию	Какое образоват. учреждение профессионального образования окончил, специальность	Ученая степень и ученое (почетное) звание	Сведения о повышении квалификации	Стаж научно- педагогической работы				
						Всего	В т.ч. педагогической			
							Всего	В т.ч. по препод. дисципл.		
1	2	3	4	5	6	7	8	9	10	11
1.	**Тема №1.** Правовые и организационно - распорядительные документы в области ТЗИ	Оленева Наталья Рудольфовна преподаватель кафедры защиты информации	Сыктывкарский государственный университет Специальность: комплексная защита объектов информатизации	-	2009 г. Курсы повышения квалификации «Организация и технология технической защиты конфиденциальной информации, в т.ч. персональных данных» в ГОУВПО «СыктГУ»	2 г.	2 г.	1 год	ГОУВПО «Сыктывкарский государственный университет», преподаватель кафедры защиты информации	Штатный
2.	**Тема №2.** Выявление угроз безопасности информации на объектах информатизации, основные организационные меры, технические и программные средства защиты информации от НСД	Миронов Владимир Валерьевич, доцент кафедры защиты информации	Сыктывкарский государственный университет Специальность: математика	Кандидат физико-математических наук	2009 г. Курсы повышения квалификации «Безопасность информационных технологий» в Учебном центре «Информзащита», г. Москва	8 лет	8 лет	1 год	ГОУВПО «Сыктывкарский государственный университет», доцент кафедры математического моделирования и кибернетики	Штатный

1	2	3	4	5	6	7	8	9	10	11
	Тема №6. Рекомендации по обеспечению безопасности и контролю безопасности ПДн при их обработке в ИСПДн	Мищенко Юрий Владимирович, ассистент кафедры защиты информации	Сыктывкарский государственный университет Специальность: комплексная защита объектов информатизации	-		2 г.	2 г.	2 года	Отделение пенсионного фонда Российской Федерации по Республике Коми, Специалист по защите информации	Совместитель
		Митрюшин Даниил Алексеевич, ассистент кафедры защиты информации	Сыктывкарский государственный университет Специальность: комплексная защита объектов информатизации	-		2 г.	2 г.	2 года	ГУРК «Центр информационных технологий» Ведущий специалист отдела информационной безопасности	Совместитель
3.	**Тема №3.** Основные организационные меры и технические средства защиты информации от утечки по техническим каналам на объектах информатизации	Носов Леонид Сергеевич, заведующий кафедрой защиты информации	Сыктывкарский государственный университет Специальность: физика	Кандидат физико-математических наук	Курсы повышения квалификации: 2006 г. «Компьютерная безопасность» в ГОУВПО «СыктГУ» 2007г. «Техническая защита конфиденциальной информации» в Учебном центре ЦБИ, г. Москва	8 лет	6 лет	2 года	ГОУВПО «Сыктывкарский государственный университет», заведующий кафедрой защиты информации	Штатный
		Миронов Владимир Валерьевич, доцент кафедры защиты информации	Сыктывкарский государственный университет Специальность: математика	Кандидат физико-математических наук	2009 г. Курсы повышения квалификации «Безопасность информационных технологий» в Учебном центре «Информзащита», г. Москва	8 лет	8 лет	1 год	ГОУВПО «СыктГУ», доцент кафедры математического моделирования и кибернетики	Штатный

1	2	3	4	5	6	7	8	9	10	11
4.	**Тема №4.** Угрозы безопасности ПДн при их обработке в ИСПДн	Носов Леонид Сергеевич, заведующий кафедрой защиты информации	Сыктывкарский государственный университет Специальность: физика	Кандидат физико-математических наук	2006 г. Курсы повышения квалификации «Компьютерная безопасность» в ГОУВПО «СыктГУ» 2007г. Курсы повышения квалификации «Техническая защита конфиденциальной информации» в Учебном центре ЦБИ, г. Москва	8 лет	6 лет	2 года	ГОУВПО «Сыктывкарский государственный университет», заведующий кафедрой защиты информации	Штатный
5.	**Тема №5.** Основы организации и ведения работ по обеспечению безопасности ПДн при их обработке в ИСПДн **Тема №6.** Рекомендации по обеспечению безопасности и контролю безопасности ПДн при их обработке в ИСПДн	Едомский Дмитрий Николаевич, старший преподаватель кафедры защиты информации	Уральский политехнический институт Специальность: электропривод и автоматизация промышленных установок Академия государственной службы г. Сыктывкар Специальность: юриспруденция	-	1997 г. Курсы повышения квалификации «Защита информации, содержащей сведения, составляющие государственную тайну» в Межотраслевом специальном учебном центр г.Обнинск	3 г.	3 г.	3 г.	Управление ФСБ РФ по РК	Совместитель
		Носаль Елена Юрьевна, руководитель Регионального аттеста-	Киевский технологический институт легкой промышленности Специальность:	-	Курсы повышения квалификации: 2006 г. «Защита информации, содержащей сведения, составляющие государст-	1 год	1 год	1 год	ГОУВПО «Сыктывкарский государственный университет», Руководитель	Штатный

		ционного центра	конструирование изделий из кожи		венную тайну» в ГОУВПО «СыктГУ» 2010 г. «Организация и технология технической защиты конфиденциальной информации, в т.ч. персональных данных» в ГОУВПО «СыктГУ», г. Сыктывкар				Регионального аттестационного центра СыктГУ	

Ректор ГОУ ВПО «СыктГУ» В.Н.Задорожный

«19» апреля 2010 г.

М.П.

Приложение № 2

Сведения о материально-технической базе и оснащенности образовательного процесса ГОУВПО «Сыктывкарский государственный университет»

(в части обеспечения учебного процесса по программе повышения квалификации **«Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»**)

№ п.п.	Перечень оборудования, технических средств, компьютерной техники	Наименование оборудования, технических средств, их количество	Примечание
1	2	3	4
1.	Лаборатория программно-аппаратных средств защиты информации на 11 учебных мест и 1 сервером с выходом в Интернет (компьютеры класса Pentium – IV и выше) «Аудитория № 416»	Лекционная аудитория с ЛВС	Оперативное управление на основании Свидетельства о государственной регистрации права, выданного Управлением Федеральной регистрационной службы по Республике Коми 07.07.2009, регистрационный номер 11АА№ 627344
		Ноутбук Samsung P28, зав. № Y80493DX800157H	Собственность, счет-фактура № 056 от 29.04.2005
		Проектор BENQ MP611, зав. № PD42701037U0	Собственность, счет-фактура № 4483 от 10.05.2007
		Программа Secret Net 5.1 класса С сетевой на 11 клиентских мест и 1 сервер доступа	Собственность, счет-фактура № 1106 от 28.12.2009
		СЗИ от НСД Аккорд 9 шт.	Собственность, счет-фактура № 0216 от 15.06.2006
		СЗИ от НСД Secret Net 5.0 (автономный вариант) 1 шт.	Собственность, счет-фактура № 0002 от 15.01.2008
		СЗИ от НСД «Щит РЖД» 11 шт.	Собственность, счет-фактура № 0002 от 15.01.2008
2.	Выделенное помещение «Аудитория № 421»	Лекционная аудитория на 48 учебных мест Аттестат соответствия требованиям по безопасности информации № 73/2010, уч.№ 83с, выдан 05.07.2010, действителен до 05.07.2013	Оперативное управление на основании Свидетельства о государственной регистрации права, выданного Управлением Федеральной регистрационной службы по Республике Коми 07.07.2009, регистрационный номер 11АА№ 627344

1	2	3	4
3.	Защищаемое помещение «Аудитория № 422»	Лекционная аудитория на 24 учебных мест Аттестат соответствия № 427/2009 требованиям безопасности информации, уч.№ 581дсп от 29.07.2009, действителен до 12.09.2012	Оперативное управление на основании Свидетельства о государственной регистрации права, выданного Управлением Федеральной регистрационной службы по Республике Коми 07.07.2009, регистрационный номер 11АА№ 627344
		Ноутбук Samsung P28, зав. № Y80493DX800157H	Собственность, счет-фактура № 056 от 29.04.2005
		Проектор BENQ MP611, зав. № PD42701037U0	Собственность, счет-фактура № 4483 от 10.05.2007
4.	Автоматизированное рабочее место «АРМ-1» РАЦ, находящееся в ЗП «Аудитория № 422»	«АРМ-1» РАЦ	Аттестат соответствия № 363/2009 требованиям безопасности информации, уч.№ 486с от 02.07.2009, действителен до 02.07.2012
		Системный блок «Конком», зав. № 27150 с монитором Samsung Sync Master 740N зав. № HA17HMCP508142M	Собственность, счет-фактура № 1358 от 15.06.2007
		Принтер Canon LBP 2900, зав. № L11121E	Собственность, счет-фактура № 1358 от 15.06.2007
5.	Автоматизированное рабочее место «АРМ-2» РАЦ, находящееся в ЗП «Аудитория № 422»	«АРМ-2» РАЦ	Аттестат соответствия № 364/2009 требованиям безопасности информации, уч.№ 487с от 02.07.2009, действителен до 02.07.2012
		Системный блок «Конком», зав. № 23887 с монитором Samsung Sync Master 740N зав. № HA17HMCYA42556J	Собственность, счет-фактура № 172506 от 20.12.2005
		МФУ Canon Laser Base MF3228 зав. № NBA35549	Собственность, счет-фактура № 191721 от 10.11.2006
6.	Лаборатория инженерно-технической защиты «Аудитория № 423»	Лекционная аудитория на 24 учебных мест	Оперативное управление на основании Свидетельства о государственной регистрации права, выданного Управлением Федеральной регистрационной службы по Республике Коми 07.07.2009, регистрационный номер 11АА№ 627344

2	3	4
	Генератор виброакустический «Соната - АВ»	Собственность, счет-фактура № 011 от 22.02.2005
	Генератор шума «Соната-РС1»	Собственность, счет-фактура № 011 от 22.02.2005
	Генератор шума «Соната РК-1»	Собственность, счет-фактура № 62 от 18.06.2007
	Генератор виброакустического зашумления «Шорох-1»	Собственность, счет-фактура № 416 от 07.10.2005
	Генератор электромагнитного зашумления «Гном-3»	Собственность, счет-фактура № 011 от 22.02.2005
	Генератор электромагнитного зашумления ЛГШ-701	Собственность, счет-фактура № 45 от 06.12.2007
	Генератор шума ЛГШ-501	Собственность, счет-фактура № 011 от 22.02.2005
	Аудиоизлучатель АИ-65	Собственность, счет-фактура № 011 от 22.02.2005
	Виброизлучатель ВИ-45	Собственность, счет-фактура № 011 от 22.02.2005
	Виброизлучатель ПИ-45	Собственность, счет-фактура № 011 от 22.02.2005
	Фильтр сетевой помехоподав-ляющий ФСП-1Ф-7А	Собственность, счет-фактура № 011 от 22.02.2005
	Фильтр сетевой ФСП-1Ф-7А	Собственность, счет-фактура № 011 от 22.02.2005
	Фильтр телефонный Гранит-8	Собственность, счет-фактура № 011 от 22.02.2005
	Нелинейный локатор «Катран»	Собственность, счет-фактура № 20 от 18.10.2005
	Приемник сканирующий AR 8200	Собственность, товарный чек от 05.10.2004
	Адаптер ДАПЛ031	Собственность, счет-фактура № 19 от 18.10.2005

1	2	3	4
		Микровольтметр селективный с антеннами SMV 11	Собственность, счет-фактура № 16 от 26.02.2008
		Микровольтметр селективный с антеннами SMV 8,5	Собственность, счет-фактура № 95 от 11.04.2008
		Телефонное проверочное устройство «Улан-2»	Собственность, счет-фактура № 22 от 18.10.2005
		Детектор поля ST006	Собственность, счет-фактура № 21 от 18.10.2005
		Прибор «Тест»	Собственность, счет-фактура № 19 от 18.10.2005
		Универсальный прибор STO031 - Пиранья	Собственность, счет-фактура № 20 от 18.10.2005
		Телевизор Samsung	Собственность, счет № 20 от 19.10.2006
		Компьютер Celeron 1200	Собственность, счет-фактура № 46812 от 27.11.2002
		Компьютер Pentium 4-2000	Собственность, счет-фактура № 46812 от 27.11.2002

Обучающиеся имеют доступ к библиотеке ГОУВПО «СыктГУ». В библиотеке имеется более 20000 экземпляров современной учебной и практической литературы. Имеется читальный зал на 50 посадочных мест.

Для самостоятельной работы слушателям могут быть предоставлены нормативно-методические и методические документы ФСТЭК России.

Слушатели могут бесплатно пользоваться Интернет и системами «Консультант-Плюс», «ФСО России. Законодательство России».

Ректор ГОУ ВПО «СыктГУ» В.Н.Задорожный

«19» апреля 2010 г.

М.П.

Приложение № 3

Перечень раздаточного материала,

выдаваемого слушателям курса повышения квалификации по программе «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных»

Раздаточный материал для слушателей курса повышения квалификации по программе «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных» подготовлен в целях более глубокого освоения учебного материала и сформирован по следующим блокам:

1. Диск № 1. Нормативные правовые акты, нормативно-методические и методические документы по обеспечению безопасности ПДн.

1.1. Нормативные правовые акты

1.	Закон Российской Федерации от 5 марта 1992 г. № 2446-1 «О безопасности»
2.	Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации»
3.	Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»
4.	Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи»
5.	Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»
6.	Федеральный закон от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности»
7.	Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»
8.	Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю»
9.	Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»
10.	Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти»
11.	Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных"
12.	Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»

Постановление Правительства Российской Федерации от 26 января 2006 г. № 45 « Об организации лицензирования отдельных видов деятельности»
Постановление Правительства Российской Федерации от 15 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»
Постановление Правительства Российской Федерации от 31 августа 2006 г. № 532 «О лицензировании деятельности но разработке и (или) производству средств защиты конфиденциальной информации»
Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.2. Нормативно-методические и методические документы

Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895
Приказ ФСТЭК России от 28 августа 2007 г. № 181 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по лицензированию деятельности по технической защите конфиденциальной информации». Зарегистрирован в Минюсте РФ 3 октября 2007 г. № 10232
Приказ ФСТЭК России от 28 августа 2007 г. № 182 «Об утверждении Административного регламента Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по лицензированию деятельности по разработке и (или) производству средств защиты конфиденциальной информации». Зарегистрирован в Минюсте РФ 27 сентября 2007 г. № 10193
Приказ ФСТЭК России от 5 февраля 2010 г. N 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных». Зарегистрирован в Минюсте РФ 19 февраля 2010 г. N 16456
Положение о сертификации средств защиты информации по требованиям безопасности информации, утвержденное приказом Гостехкомиссии России от 27 октября 1995 г. № 199
Положение по аттестации объектов информатизации по требованиям безопасности информации, утвержденное председателем Гостехкомиссии России 25 ноября 1994 г.
Положение об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации, утвержденное председателем Гостехкомиссии России 25 ноября 1994 г.
Типовое положение об испытательной лаборатории, утвержденное председателем Гостехкомиссии России 25 ноября 1994 г.
Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации. утвержденное председателем Гостехкомиссии России 25 ноября 1994 г.
Типовое положение об органе по сертификации средств защиты информации по требованиям безопасности информации, утвержденное председателем Гостехкомиссии России 25 ноября 1994 г.

11.	Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Гостехкомиссия России, 1992
12.	Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. Гостехкомиссия России, 1992
13.	Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Гостехкомиссия России, 1992
14.	Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Гостехкомиссия России, 1992
15.	Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Гостехкомиссия России, 1992
16.	Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Гостехкомиссия России, 1997
17.	Руководящий документ. Защита информации. Специальные защитные знаки. Классификация и общие требования. Гостехкомиссия России, 1997
18.	Руководящий документ. Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден приказом Гостехкомиссии России от 4 июня 1999 г. № 114
19.	Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Утвержден приказом Гостехкомиссии России от 19 июня 2002 г. № 187 (часть 1, часть 2, часть 3)
20.	Приказ Минэнерго России от 13 января 2003 г. № 6 «Об утверждении Правил технической эксплуатации электроустановок потребителей» (зарегистрирован Минюстом России 22 января 2003 г., регистрационный № 4145, введен в действие с 1 июля 2003 г.)
21.	Порядок проведения классификации информационных систем персональных данных. Утвержден приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20
22.	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Выписка). Утверждена Заместителем директора ФСТЭК России 15.02.2008.
23.	Методика определения актуальных угроз безопасности персональным данным при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15.02.2008.

2. Диск № 2. Презентации по темам лекций в соответствии с учебной программой курса повышения квалификации «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных».

3. Методическое пособие по программе повышения квалификации «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных».

Ректор ГОУ ВПО «СыктГУ» В.Н.Задорожный

«19» апреля 2010 г.

М.П.