Государственное бюджетное образовательное учреждение высшего образования
Московской области

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

«УТВЕРЖДАЮ»
Проректор по учебно-методической работе
_____ Н.В. Бабина
«28» апреля 2020 г.

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ

«ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ПРЕДПРИЯТИИ»

Направление подготовки: 10.03.01 Информационная безопасность
Профиль: Информационно-аналитические системы финансового мониторинга
Квалификация (степень) выпускника: бакалавр
Форма обучения: очная

Королев
2020

Автор: к.в.н., доцент Воронов А.Н. Рабочая программа дисциплины: «Организация защиты персональных данных на предприятии». – Королев МО: «Технологический университет», 2020.

Рецензент: **к.в.н., доцент Соляной В.Н.**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 28.04.2020 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	к.в.н., доцент Соляной В.Н.			
Год утверждения (переутверждения)	2020	2021	2022	2023
Номер и дата протокола заседания кафедры	Протокол № 8 от 26.03.2020			

Рабочая программа согласована:
Руководитель ОПОП ВО к.в.н., доцент Воронов А.Н.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2020	2021	2022	2023
Номер и дата протокола заседания УМС	№ 7 от 28.04.2020			

2

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП ВО

Целью изучения дисциплины является:

1. Формирование у студентов специализированной базы знаний по системам защиты персональных данных на предприятиях;
2. Получение первичных навыков по применению подобных систем защиты.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

Общепрофессиональные компетенции:

- (ОПК-4) способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.

Профессиональные компетенции:

- (ПК-4) способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;
- (ПК-15) способность организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Основными **задачами** дисциплины являются:

1. Ознакомление студентов с методологическими подходами применения и эксплуатации систем защиты персональных данных на предприятии, а также с основными методами определения параметров, характеристик и условий применения данных систем;
2. Формирование у студентов способности самостоятельно решать поставленные задачи в области применения систем защиты персональных данных с помощью современных принципов, методов и сил в различных организационных структурах, по базовым направлениям и применительно к типовым информационным объектам.

После завершения освоения данной дисциплины студент должен:

Знать:

- основные методологические принципы теории защиты персональных данных;
- предполагаемые источники угроз информационным объектам персональных данных и порядок их выявления;
- возможные каналы утечки информации и предполагаемые информационные атаки на системы защиты персональных данных;
- постановления распоряжения и приказы руководящих государственных органов и другие руководящие, нормативно-технические и методические

документы по защите персональных данных, а также стандарты по информатизации и защите информации;

- порядок моделирования мер защиты информации и системы защиты персональных данных от различных видов угроз;
- методы и средства защиты персональных данных, основные мероприятия по защите информации в системах обработки персональных данных;
- основные направлений обеспечения безопасности персональных данных с помощью средств защиты;

особенности защиты персональных данных на предприятиях различного профиля и различных форм собственности.

Уметь:

- правильно производить анализ угроз информационной безопасности и определять факторы, влияющие на требуемый уровень их защиты;
- осуществлять классификацию объектов и средств защиты персональных данных и требований к системе защиты;
- проводить анализ защищённости информационных объектов и определять классы защиты персональных данных;
- использовать гипотетические модели защиты персональных данных при выборе соответствующих способов и средств защиты информации и объектов;
- использовать зарубежный и отечественный опыт в области защиты персональных данных в своей профессиональной деятельности;

формулировать рекомендации по совершенствованию уровня защищённости персональных данных.

Владеть:

- навыками выявления и анализа потенциально существующих угроз безопасности информации и защиты персональных данных;
- навыками применения основных методов анализа и оценки рисков, методов определения размеров возможного ущерба защищаемым информационным объектам;
- навыками грамотного применения на практике требований основных руководящих документов по защите персональных данных, основными методами и средствами их защиты;
- навыками применения методики организации и управления системой защиты персональных данных.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Организация защиты персональных данных на предприятии» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению

10.03.01 «Информационная безопасность», профиль: «Информационно-аналитические системы финансового мониторинга».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности», «Информационная безопасность кредитно-финансовых операций», «Информационно-психологическая безопасность персонала предприятия», «Финансовые институты» и компетенциях: ОК-5,6, ОПК-2,4,6, ПК-4,7,9,11,14,15 и ПСК-3.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Защищённые информационные системы банковской деятельности», «Основы расследования нарушений в финансовой сфере», «Стандарты информационной безопасности в банковской сфере», «Организация информационно-аналитического обеспечения финансового мониторинга», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы обучения составляет 4 зачетные единицы, 144 часа.

Таблица 1

Виды занятий	Всего часов	Семестр седьмой	Семестр …	Семестр …	Семестр …
Общая трудоемкость	144	144			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	48	48			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	32	32			
Лабораторные работы (ЛР)	-	-			
Самостоятельная работа	96	96			
Курсовые работы	-	-			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели)	Тест	Тест			
Вид итогового контроля	Экзамен	Экзамен			

4. Содержание дисциплины
4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. очное	Практические занятия, час очное	Занятия в интерактивной форме, час очное	Код компетенций
Седьмой семестр				
Тема 1. Законодательные основы и нормативно-методическое обеспечение безопасности персональных данных.	2	4	-	ОПК-4
Тема 2. Организация обработки персональных данных с помощью информационных систем.	2	4	4	ОПК-4
Тема 3. Характеристика угроз безопасности персональным данным при их обработке в информационных системах.	2	4	4	ОПК-4; ПК-4
Тема 4. Особенности построения систем защиты персональных данных в различных организациях.	2	4	4	ОПК-4; ПК-4
Тема 5. Организация работы по защите персональных данных государственных гражданских служащих.	2	4	4	ОПК-4; ПК-4; ПК-15
Тема 6. Особенности защиты персональных данных в медицинских учреждениях.	2	4	4	ОПК-4; ПК-4; ПК-15
Тема 7. Методика построения систем защиты персональных данных в медицинских учреждениях.	2	4	4	ОПК-4; ПК-4; ПК-15
Тема 8. Перспективы развития систем защиты персональных данных в современном обществе.	2	4	4	ОПК-4; ПК-4 ПК-15
Итого:	**16**	**32**	**18**	

4.2. Содержание тем дисциплины

Тема 1. Законодательные основы и нормативно-методическое обеспечение безопасности персональных данных

Международные акты о защите персональных данных и их роль в развитии российского законодательства. Место персональных данных в системе российского законодательства. Уровни обеспечения безопасности персональных дан-

ных и их характеристика. Государственная политика в области обеспечения защиты персональных данных. Уполномоченные государственные органы в области защиты персональных данных, их права и основные функции. Понятие персональных данных и право работника на их защиту.

Тема 2. Организация обработки персональных данных с помощью информационных систем

Основные понятия и определения обработки персональных данных работников, служащих. Особенности сбора и накопления персональных данных в различных организациях. Особенности хранения и использования персональных данных работников, служащих. Основания для осуществления классификации информационных систем обработки персональных данных. Типы информационных систем, подлежащих классификации и их особенности. Основные этапы классификации информационных систем, классы систем и их характеристика. Порядок проведения классификации информационных систем для обработки персональных данных. Особенности передачи персональных данных.

Тема 3. Характеристика угроз безопасности персональным данным при их обработке в информационных системах

Классификация угроз безопасности при обработке персональных данных. Основные источники угроз персональным данным. Содержание модели угроз верхнего уровня. Характеристика базовой модели угроз безопасности персональных данных при их обработке в информационных системах и порядок её формирования. Характеристика первичных и вторичных носителей защищаемой речевой информации о персональных данных. Статистика проявления угроз безопасности персональным данным. Потенциальные технические каналы утечки персональных данных и их характеристика. Категории и возможности нарушителей. Определение уровня исходной защищённости объектов обработки персональных данных.

Тема 4. Особенности построения систем защиты персональных данных в различных организациях

Основные требования к построению системы защиты персональных данных в организации. Требования к локальному нормативному регулированию защиты персональных данных в организации. Требования к назначению работников, ответственных за организацию обработки персональных данных в учреждениях, фирмах, на предприятиях. Требования к построению информационной системы обработки персональных данных организации. Требования к защите персональных данных при неавтоматизированной обработке информации.

Тема 5. Организация работы по защите персональных данных государственных гражданских служащих

Основные мероприятия по организации и техническому обеспечению безопасности персональных данных при их обработке в информационных системах. Замысел обеспечения безопасности персональных данных и его реализация. Стадии создания системы защиты персональных данных и их особенности. Дифференцированный подход к обеспечению безопасности персональных данных. Какие сведения запрещено указывать в средствах массовой информации. Основные

меры и средства защиты от несанкционированных действий с применением программных и программно-аппаратных средств. Характеристика средств защиты информационных систем обработки персональных данных.

Тема 6. Особенности защиты персональных данных в медицинских учреждениях

Краткая история развития информатизации медицинских учреждений. Виды медицинских информационных систем и их особенности. Электронная медицинская карта и электронная история болезни в медицинских информационных системах. Основные источники медицинской информации как информации ограниченного доступа. Виды конфиденциальной информации в типовом лечебно-профилактическом учреждении и требования по защите персональных данных.

Тема 7. Методика построения систем защиты персональных данных в медицинских учреждениях

Выделение основных потоков информации, в которой проявляются персональные данные и другие виды конфиденциальной информации. Основной объект защиты персональных данных в типовом медицинском учреждении. Типовой состав системы защиты персональных данных и его особенности. Роль руководства лечебно-профилактического учреждения и кадровые вопросы при организации защиты информации в типовом медицинском учреждении. Использование типовых решений по защите информационных систем обработки персональных данных в медицинских учреждениях. Защита баз данных, содержащих персональные данные, по опыту типовых лечебно-профилактических учреждений.

Тема 8. Перспективы развития систем защиты персональных данных в современном обществе

Проблемы информационной безопасности в «облаках» и пути их решения. Вопросы перспективной архитектуры и состава средств защиты персональных данных для систем обработки и «облачных» вычислений. Насущные вопросы обеспечения юридической значимости первичных документов и другой важной информации, а также процессов их защиты, обработки, хранения и обмена с применением перспективных информационных систем и новых информационных технологий.

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине

«Методические указания для обучающихся по освоению дисциплины» приведены в приложении 2.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Структура фонда оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине «Организация защиты персональных данных на предприятии» приведена в Приложении 1.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Васильков А.В., Васильков А.А., Васильков И.А. Информационные системы и их безопасность. Учебное пособие. – М.: «ФОРУМ», 2011.
2. Вихорев С. В. О защите персональных данных» под редакцией А. Бражникова. – М.: «Авангард центр», 2014.
3. Сабанов А.Г., Зыков В.Д., Мещеряков Р.В., Рылов С.П., Шелупанов А.А. Защита персональных данных в организациях здравоохранения. – М.: «Горячая линия-Телеком», 2012.

Дополнительная литература:

1. Анисимов А.А. Менеджмент в сфере информационной безопасности. Учебное пособие. – М.: Интернет – Университет информационных технологий / БИНОМ. Лаборатория знаний, 2010.
2. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. – М.: «Горячая Линия - Телеком», 2010.
3. Зайцев А. П., Шелупанов А. А., Мещеряков Р. В. И др. Технические средства и методы защиты информации. Учебное пособие для вузов. – М.: «Горячая линия – Телеком», 2012.

Рекомендуемая литература:

1. Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. Учебное пособие. – М.: Книжный дом «ЛИБРОКОМ», 2012.
2. Кузнецов П.П., Столбов А.П. Автоматизированная обработка и защита персональных данных в медицинских учреждениях. – М.: ИД «Менеджер здравоохранения», 2010.
3. Просветова О.Б., Федотов И.С. Персональные данные. Учебное пособие. – Воронеж: Воронежский институт МВД России, 2005.
4. Тихомирова Л.В. Защита персональных данных работника. Учебно-практическое пособие. – М.: Издательство Тихомирова М.Ю., 2002.
5. Шеломов Б.А. Защита персональных данных работника. Справочник кадровика. – М.: «Гелиос АРВ», 2003.

Электронные книги:

1. Обеспечение безопасности персональных данных. Методическое пособие. Издательский дом «Афина», 2010: **www.inside-zi.ru**
2. Спицын В. Г. Информационная безопасность вычислительной техники. Учебное пособие. Издатель: Эль Контент, 2011: **www.biblioclub.ru**
3. Краткий энциклопедический словарь информационной безопасности. Издатель: Энергия, 2010: **www.biblioclub.ru**
4. ЭБС «Руконт»: **www.rucont.ru**

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

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp** – Научно-образовательный портал;
2. **www.wikIsec.ru** – Энциклопедия информационной безопасности. – Публикации, статьи;
3. **http://www.fsb.ru/** – Официальный сайт Федеральной службы безопасности РФ;
4. **http://www.fstec.ru/** – Официальный сайт Федеральной службы по техническому экспортному контролю РФ.

9. Методические указания для обучающихся по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины, приведены в Приложении 2.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения: MS Office.

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды МГОТУ
2. Рабочая программа и методическое обеспечение по дисциплине «Организация защиты персональных данных на предприятии».
3. Информационно – справочные (правовые) системы:
   – «Гарант» (**garantcenter.ru**);
   – «Кодекс» (**doskainfo.ru/advert/64804/**);
   – «Консультант +» (**artiks.ru**).

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

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций/слайдов.

Практические занятия:

- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MS Office;
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Приложение 1

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

«ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ПРЕДПРИЯТИИ»

(Приложение 1 к рабочей программе)

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компетенции	Содержание компетенции (или ее части)*	Раздел дисциплины, обеспечивающий формирование компетенции (или ее части)	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции (или ее части), обучающийся должен:		
				Знать	уметь	владеть
1.	ОПК-4	способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	**Тема 1. Законодательные основы и нормативно-методическое обеспечение безопасности персональных данных.** **Тема 2. Организация обработки персональных данных с помощью информационных систем.** **Тема 3. Характеристика угроз безопасности персональным данным при их обработке в информационных системах.** **Тема 4. Особенности построения систем защиты персональных данных в различных организациях.** **Тема 5. Организация работы по защите персональных данных государственных гражданских служащих.** Основные мероприятия по организации и техническому обеспечению безопасности персональных данных при их	Особенности защиты персональных данных на предприятиях различного профиля и различных форм собственности.	Проводить анализ защищённости информационных объектов и определять классы защиты персональных данных;	Навыками грамотного применения на практике требований основных руководящих документов по защите персональных данных, основными методами и средствами их защиты;

			обработке в информационных системах. Замысел обеспечения безопасности персональных данных и его реализация. Стадии создания системы защиты персональных данных и их особенности. Дифференцированный подход к обеспечению безопасности персональных данных. Основные меры и средства защиты от несанкционированных действий с применением программных и программно-аппаратных средств. **Тема 8. Перспективы развития систем защиты персональных данных в современном обществе.**			
2.	ПК-4	способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	**Тема 3. Характеристика угроз безопасности персональным данным при их обработке в информационных системах.** Содержание модели угроз верхнего уровня. Характеристика базовой модели угроз безопасности персональных данных при их обработке в информационных системах и порядок её	Предполагаемые источники угроз информационным объектам персональных данных и порядок их выявления; возможные каналы утечки информации и предполагаемые информационные атаки на системы защиты персональных данных;	Использовать гипотетические модели защиты персональных данных при выборе соответствующих способов и средств защиты информации и объектов	Навыками выявления и анализа потенциально существующих угроз безопасности информации и защиты персональных данных;

			формирования. Потенциальные технические каналы утечки персональных данных и их характеристика. Категории и возможности нарушителей. Определение уровня исходной защищённости объектов обработки персональных данных. **Тема 4. Особенности построения систем защиты персональных данных в различных организациях. Тема 5. Организация работы по защите персональных данных государственных гражданских служащих. Тема 6. Особенности защиты персональных данных в медицинских учреждениях. Тема 7. Методика построения систем защиты персональных данных в медицинских учреждениях. Тема 8. Перспективы развития систем защиты персональных данных в современном обществе.**			
3.	ПК-15	способность организовывать технологический процесс защиты информации ограниченного доступа в соот-	**Тема 5. Организация работы по защите персональных данных государственных гражданских**	Порядок моделирования мер защиты информации и системы защиты персональных данных от	Правильно производить анализ угроз информационной безопасности и определять факторы,	Навыками применения основных методов анализа и оценки рисков, методов определения размеров возможного ущерба защищае-

		ветствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	**служащих. Тема 6. Особенности защиты персональных данных в медицинских учреждениях.** Виды медицинских информационных систем и их особенности. Электронная медицинская карта и электронная история болезни в медицинских информационных системах. Основные источники медицинской информации как информации ограниченного доступа. Виды конфиденциальной информации в типовом лечебно-профилактическом учреждении и требования по защите персональных данных. **Тема 7. Методика построения систем защиты персональных данных в медицинских учреждениях. Тема 8. Перспективы развития систем защиты персональных данных в современном обществе.**	различных видов угроз; методы и средства защиты персональных данных, основные мероприятия по защите информации в системах обработки персональных данных	влияющие на требуемый уровень их защиты	мым информационным объектам;

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Инструменты, оценивающие сформированность компетенции	Показатель оценивания компетенции	Критерии оценки
ОПК- 4	Письменное задание / Реферат	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	1. Проводится в форме письменной работы 2.Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие ответа заявленной тематике (0-5 баллов). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-4	Доклад в форме презентации	А) полностью сформирована **5 баллов** В) частично сформирована **3-4 балла** С) не сформирована **2 балла**	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-15	Контрольная работа	А) полностью сформирована **5 баллов** В) частично сформиро-	Проводится письменно с использованием мультимедийных систем, а также с использованием технических средств

		вана **3-4 балла** С) не сформирована **2 балла**	Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал.

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерная тематика докладов в презентационной форме:

1. Анализ законодательной и нормативной базы обеспечения безопасности при использовании персональных данных.
2. Характеристика ключевых моментов типового порядка реализации программы построения систем защиты персональных данных.
3. Обзор и характеристика передовых методов организации защиты персональных данных в информационных системах.
4. Анализ опыта и перспектив развития систем защиты персональных данных граждан, работников и служащих в РФ и за рубежом.
5. Обобщение и анализ основных моментов положения о разрешительной системе допуска к работе с персональными данными.

Примерная тематика реферата:

1. Обзор и характеристика способов перехвата конфиденциальной коммерческой информации, обрабатываемой техническими средствами.
2. Рейтинговый подход к защите коммерческой тайны и персональных данных, характеристика и особенности его применения.

3. Характеристика типовых преступлений, связанных с неправомерным использованием персональных данных и ответственность по ним.

4. Систематика ущерба информационным ресурсам организации, связанного с обработкой персональных данных.

5. Выявление, обзор и анализ основных противоречий в нормативных и правовых документах, регулирующих защиту персональных данных.

6. Революция или эволюция в сертификации средств защиты персональных данных.

Примерная тематика контрольной работы / письменного задания:

1. Характеристика основных проблем по защите персональных данных и пути их разрешения.

2. Актуальность и безопасность электронных документов в корпоративных сетях при обработке персональных данных.

3. Обеспечение защиты персональных данных в СУБД “Oracle”, методика и особенности применения основных процедур и функций.

4. Динамика обеспечения безопасности в обработке персональных данных при следовании от внешних угроз к внутренним.

5. Правовое исследование целесообразности создания и ведения автоматизированных баз данных при обработке персональных сведений.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Организация защиты персональных данных на предприятии» являются две текущие аттестации в виде тестов и одна итоговая аттестация в виде экзамена.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Согласно учебному плану	тестирование	ОПК-4 ПК-4 ПК-15	25 вопросов	Компьютерное тестирование; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка - 0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.

Согласно учебному плану	тестирование	ОПК-4 ПК-4 ПК-15	25 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	Критерии оценки определяются процентным соотношением. Не явка - 0 Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%. Максимальная оценка – 5 баллов.
Согласно учебному плану	Экзамен	ОПК-4 ПК-4 ПК-15	3 вопроса	Экзамен проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения экзамена	Критерии оценки: «**Отлично**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на большинство вопросов билета «У**довлетворительно**»: • демонстрирует частичные знания по темам дисциплин; • незнание не-

						умение использовать и применять полученные знания на практике; • не работал на практических занятиях; • ответил не на все вопросы билета «**Неудовлетворительно**»: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • не отвечает на вопросы.

4.1. Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один или несколько вариантов ответа.

1-е тестирование по дисциплине

1. В каком году была принята Директива Европейского Союза и Парламентской ассамблеи совета Европы № 95/46/ЕС «О защите прав частных лиц, применительно к обработке персональных данных и свободном их движении»?

– в 1970 г;
– в 1980 г;
– в 1995 г;
– в 1997 г.

2. Выберите основные международные акты по защите персональных данных, которые появились в Европе и стали основой законодательной базы для других стран:

– Конвенция Совета Европы «О защите прав личности в связи с автоматической обработкой персональных данных» (ETS №108);

– Директива Европейского Союза и Парламентской ассамблеи совета Европы № 95/46/ЕС «О защите прав частных лиц, применительно к обработке персональных данных и свободном их движении»;

– Кодекс практики по защите личных данных о работнике, утверждённый Административным советом Международной организации труда;

– Окинавская хартия глобального информационного общества.

3. На какие виды делится информация в соответствии с ч. 3 ст. 5 федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации»?

– на открытую;

– на общедоступную;

– на секретную;

– на информацию ограниченного доступа;

4. К какой категории информации относятся сами персональные данные?

– к секретной информации;

– к открытой информации;

– к коммерческой информации;

– к конфиденциальной информации.

5. Что понимается под персональными данными согласно ст. 3 федерального закона № 152-ФЗ «О персональных данных»?

– это информация, касающаяся конкретного лица или могущего быть идентифицированным лица;

– это разновидность информации о конкретном субъекте, представляющая собой сведения (сообщения, данные) независимо от формы их представления;

– это любая информация, относящаяся к определённому или определяемому на основании такой информации физическому лицу (субъекту персональных данных);

– это информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника;

6. Выберите разновидности, на которые делят персональные данные исходя из правового режима:

– общедоступные;

– биометрические;

– секретные;

– специальные.

7. В соответствии с какими документами предусмотрено деление персональных данных на категории?

– Постановление Правительства РФ № 781 от 2007 г;

– Приказ ФСТЭК РФ № 55 от 2008 г;

– Приказ ФСБ РФ № 86 от 2008 г;

– Госстандарт РФ.

8. К какой категории относят персональные данные, позволяющие идентифицировать субъекта персональных данных?

– 4-я категория;
– 3-я категория;
– 2-я категория;
– 1-я категория.

9. Федеральная служба по труду и занятости РФ (Роструд) входит в число контрольно-надзорных органов в сфере защиты персональных данных, определённых Правительством РФ?

– да;
– нет;

10. В какие сроки должен проводить плановые проверки деятельности предприятий (фирм) по защите персональных данных Роскомнадзор РФ?

– не чаще чем 1 раз в месяц;
– не реже 1 раза в год;
– не реже 1 раза в 3 года;
– не реже 1 раза в 5 лет.

11. Какие виды дисциплинарной ответственности выделяют согласно Трудовому кодексу РФ?

– общая;
– специальная;
– персональная;
– коллективная.

12. Какие наказания могут быть применены к лицу за дисциплинарный проступок в соответствии с Трудовым кодексом РФ?

– замечание;
– порицание;
– выговор;
– увольнение по соответствующим основаниям.

13. Отличается ли материальная ответственность работника от гражданско-правовой?

– да;
– нет;

14. Какие виды материальной ответственности выделяют?

– специальная;
– полная;
– универсальная;
– ограниченная;

15. Сбор или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну без его согласия подпадает под административное правонарушение согласно КОАП РФ?

– да;
– нет;

16. Выберите допустимые меры юридической ответственности работников и должностных лиц организаций за совершённые административные правонарушения?

– предупреждение;

– приостановление деятельности на срок до 90 суток;

– конфискация средств, с помощью которых было совершено правонарушение;

– заключение под стражу на срок до 10 суток.

17. Занятие видами деятельности по защите персональных данных без получения специального разрешения (лицензии) способствует уголовной ответственности должностных лиц, участвующих в обработке персональных данных?

– да;

– нет.

18. Персональные данные не должны быть избыточными по отношению к целям их обработки – это принцип обрабатываемых персональных данных согласно ст. 5 закона № 152-ФЗ?

– да;

– нет;

19. Письменное согласие субъекта персональных данных на их обработку должно содержать цель обработки персональных данных согласно ст. 9 закона № 152-ФЗ?

– да;

– нет;

20. Обязан ли работник (служащий) при предоставлении персональных данных работодателю предоставлять свой ИНН?

– да;

– нет.

21. Имеет ли право работник (служащий) запрашивать у работодателя порядок хранения, обработки и защиты персональных данных предприятия?

– да;

– нет.

22. Какой срок должны храниться персональные данные на предприятии согласно ст. 5 закона № 152-ФЗ?

– 1 год;

– 30 лет;

– 75 лет;

– не дольше чем этого требуют цели их обработки.

23. Предусмотрено ли создание электронного архива для хранения персональных данных?

– да;

– нет.

24. Каким классом взломостойкости должны обладать сейфы и запирающиеся шкафы для хранения в них персональных данных?

– Н0 или Н1;

– Н2 или Н3;

– Н4 или Н5;.

– свыше Н5.

25. Разрешается хранить в сейфах вместе с персональными данными другие документы, деньги и материальные ценности?

– да;

– нет.

26. Разрешается хранить документы с персональными данными в государственных архивных организациях?

– да;

– нет.

2-е тестирование по дисциплине

1. Как делят информацию на предприятии (в фирме) с точки зрения обращения персональных данных?

– внешняя;

– внутренняя;

– личная.

– универсальная.

2. Что понимают под трансграничной передачей персональных данных работников?

– это передача персональных данных третьим лицам;

– это передача персональных данных на хранение в государственные архивные органы;

– это передача персональных данных на территорию иностранного государства физическому или юридическому лицу;

– это передача персональных данных в сети Интернет и других ЛВС.

3. В каких случаях осуществляется блокирование обработки персональных данных согласно ст. 21 закона № 152-ФЗ?

– в случае выявления фактов неправомерной обработки персональных данных;

– в случае выявления неточных персональных данных, либо при обращении субъекта персональных данных или его представителя;

– в случае окончания сроков обработки персональных данных и невозможности их уничтожения;

– в случае их проверки надзорными органами власти.

4. В какой срок работодатель обязан прекратить обработку персональных данных работника и уничтожить его персональные данные в случае отзыва работником разрешения на обработку своих персональных данных?

– в течение текущих суток;

– в течение 3-х рабочих дней;
– в течение срока не более 30 суток;
– в течение срока не более 6 месяцев.

5. Какой орган вправе осуществлять уничтожение персональных данных работников на предприятии (в фирме)?

– отдел кадров предприятия (фирмы);
– комиссия в составе не менее чем из 3-х человек, созданная на основании приказа работодателя;
– специальные органы по защите персональных данных на предприятии (в фирме);
– руководитель предприятия (фирмы) или его заместители.

6. В какой срок работодатель обязан заблокировать обработку персональных данных работника с момента поступления его обращения?

– немедленно;
– в срок не более 3-х рабочих дней;
– в течение недели;
– в течение 10 календарных дней.

7. Устройство “Acronis” относится к спецсредствам гарантированного удаления информации с электронных носителей?

– да;
– нет.

8. Что такое шредер?

– устройство автоматизированной обработки персональных данных;
– устройство измельчения носителей информации при гарантированном уничтожении документов;
– устройство аппаратно-программной защиты персональных данных при их обработке;
– протокол для передачи защищённой информации по телекоммуникационной сети.

9. Выберите приемлемые исходные данные для проведения классификации информационных систем обработки персональных данных согласно постановлению Правительства РФ № 781 от 17.11.2007 г?

– категория обрабатываемых персональных данных;
– гриф секретности обрабатываемых персональных данных;
– объём обрабатываемых персональных данных;
– степень защищённости персональных данных от НСД.

10. К какому классу относят информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных?

– класс 1;
– класс 2;
– класс 3;
– класс 4.

11. Каким документом оформляется класс информационной системы по обработке персональных данных, присвоенный ей в результате классификации?

– приказом работодателя;

– актом назначенной комиссии;

– актом оператора;

– алгоритмом проведения классификации информационных систем.

12. Какие объёмы обрабатываемых персональных данных в информационных системах выделяют при их классификации?

– Хнпд =1 если в информационной системе одновременно обрабатываются персональные данные более чем 10 000 субъектов ПД;

– Хнпд =2 если в информационной системе одновременно обрабатываются персональные данные от 1000 до 10 000 субъектов ПД;

– Хнпд =3 если в информационной системе одновременно обрабатываются персональные данные менее чем 1000 субъектов ПД;

– Хнпд =4 если в информационной системе одновременно обрабатываются персональные данные от 1 до 10 субъектов ПД;

13. Определение уровня исходной защищённости информационной системы обработки персональных данных входит в перечень основных этапов разработки модели угроз безопасности персональных данных для информационных систем, в которых не используют криптосредства?

– да;

– нет.

14. Множество путей распространения персональных данных относят к признакам классификации угроз безопасности персональных данных в информационных системах?

– да;

– нет.

15. Что понимается под безопасностью персональных данных?

– это недостаток или слабое место в системном или прикладном программно-аппаратном обеспечении информационной системы, которое может быть использовано для реализации угроз безопасности персональным данным;

– состояние защищённости персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационной системе;

– это отношение государства к вопросам обеспечения безопасности персональных данных с целью защиты конституционных прав, нравственности, здоровья и законных интересов граждан страны и их безопасности;

– любое действие (операция) или совокупность действий, совершённых с использованием средств автоматизации или без них с персональными данными, включая их сбор, запись, систематизацию, накопление, хранение, уточнение, передачу, обезличивание, блокирование, удаление, уничтожение и защиту персональных данных.

16. Какова максимальная дальность перехвата акустической информации при использовании лазерных каналов утечки сведений?

– до 10 м;
– до 100 м;
– до 300 м;
– до 500 м.

17. К какой категории нарушителей по классификации ФСБ РФ относятся администраторы информационных систем или баз данных, нарушающие свои обязанности при обработке персональных данных с использованием криптосредств?

– Н1;
– Н2;
– Н3;
– Н4.

18. Объём персональных данных, которые предоставляются сторонним пользователям без предварительной обработки учитывается при определении уровня исходной защищённости объектов обработки персональных данных?

– да;
– нет.

19. Какому вербальному уровню исходной защищённости информационных систем обработки персональных данных соответствует коэффициент защищенности Y1 =0?

– «высокий»;
– «средний»;
– «низкий»;
– «очень низкий».

20. Какому значению вербального показателя реализации угроз безопасности персональным данным соответствует ситуация когда объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности персональных данных не приняты?

– маловероятно (Y2=0);
– низкая вероятность (Y2=2);
– средняя вероятность (Y2=5);
– высокая вероятность (Y2=10).

21. Какой уровень угрозы соответствует коэффициенту реализуемости угроз, находящемуся в пределах: 0,3 < Y < 0,6 согласно методики выявления актуальных угроз безопасности персональным данным:

– низкий;
– средний;
– высокий;
– очень высокий.

22. Выберите правильные критерии, по которым формируют группу экспертов для оценки угроз безопасности персональным данным?

– компетентность;

– креативность;
– антиконформизм;
– гомоморфизм.

23. Журнал учёта обращений субъектов персональных данных о выполнении их законных прав входит в необходимый перечень организационно-распорядительных документов на предприятии (в фирме) при организации обработки и защите персональных данных?

– да;
– нет.

24. Магнитофоны и диктофоны относятся к «вторичным» носителям защищаемой речевой информации о персональных данных?

– да;
– нет.

4.2. Типовые вопросы, выносимые на экзамен

1. Обработка и защита персональных данных как отдельный вид трудовых отношений при исполнении обязанностей государственной гражданской службы.
2. Характеристика международных актов по защите персональных данных и их роль в развитии российского законодательства.
3. Место персональных данных в системе российского законодательства.
4. Уровни обеспечения безопасности персональных данных и их характеристика.
5. Государственная политика в области обеспечения защиты персональных данных и основные направления деятельности государства по этим вопросам.
6. Уполномоченные государственные органы в области защиты персональных данных, их права и основные функции.
7. Основные понятия и определения обработки персональных данных и право работника на их защиту.
8. Организация контроля и надзора за обработкой персональных данных.
9. Дисциплинарная и материальная ответственность за нарушение норм, регулирующих защиту персональных данных.
10. Административная и уголовная ответственность за нарушение норм, регулирующих защиту персональных данных.
11. Особенности сбора, накопления хранения и использования персональных данных работников, служащих в различных организациях.
12. Основания для осуществления классификации информационных систем обработки персональных данных.
13. Типы информационных систем, подлежащих классификации и их особенности.
14. Основные этапы классификайии информационных систем, классы систем и их характеристика.
15. Порядок проведения классификации информационных систем для обра-

ботки персональных данных.
16. Основные особенности передачи и обмена персональными данными.
17. Особенности блокирования, прекращения обработки и уничтожения персональных данных работников, служащих.
18. Характеристика категорий, обрабатываемых в информационных системах персональных данных и их объёмы.
19. Алгоритм проведения классификации информационных систем, связанных с обработкой персональных данных и порядок его построения.
20. Основные источники и классификация угроз безопасности при обработке персональных данных.
21. Содержание модели угроз верхнего уровня и характеристика её элементов.
22. Характеристика базовой модели угроз безопасности персональных данных при их обработке в информационных системах и порядок её формирования.
23. Характеристика первичных и вторичных носителей защищаемой речевой информации о персональных данных.
24. Потенциальные технические каналы утечки персональных данных и их характеристика.
25. Основные категории нарушителей при обработке персональных данных, и их характерные возможности.
26. Определение уровня исходной защищённости объектов обработки персональных данных.
27. Порядок определения вероятности реализации, коэффициентов реализуемости и показателей опасности угроз при обработке персональных данных.
28. Методика выявления актуальных угроз безопасности персональных данных при их обработке в информационных системах.
29. Методика по приведению информационных систем, связанных с обработкой персональных данных к требованиям законодательства.
30. Основные требования к построению системы защиты персональных данных в типовой организации и их характеристика.
31. Требования к локальному нормативному регулированию защиты персональных данных в организации и их характеристика.
32. Требования к назначению работников, ответственных за организацию обработки персональных данных в учреждениях, фирмах, на предприятиях.
33. Порядок построения и требования к информационной системе обработки персональных данных типовой организации.
34. Требования к защите персональных данных при неавтоматизированной обработке информации и их характеристика.
35. Особенности обработки и защиты персональных данных в государственных или муниципальных информационных системах.
36. Характеристика основных понятий, определений и требований Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, введенного постановлением Правительства РФ № 781.
37. Характеристика положений и требований основных методических документов ФСТЭК России в области обеспечения безопасности персональных

данных при их обработке в информационных системах.
38. Характеристика основных мероприятий по организации и техническому обеспечению безопасности персональных данных при их обработке в информационных системах.
39. Замысел обеспечения безопасности персональных данных и его реализация на предприятии, в фирме, учреждении.
40. Дифференцированный подход к обеспечению безопасности персональных данных и основные стадии создания систем защиты персональных данных, их характеристика.
41. Основные меры и средства защиты от несанкционированных действий при обработке персональных данных с применением программных и программно-аппаратных средств.
42. Характеристика средств защиты информационных систем обработки персональных данных, применяемых на рынке современной продукции.
43. Требования, предъявляемые к кадровой службе типового учреждения, при получении, обработке, хранении и передаче персональных данных.
44. Виды медицинских информационных систем и их особенности применения при обработке персональных данных.
45. Основные источники медицинской информации и их особенности, электронная медицинская карта и электронная история болезни как объект защиты в медицинских информационных системах.
46. Виды конфиденциальной информации в типовом лечебно-профилактическом учреждении и требования по защите персональных данных в нём.
47. Особенности обработки информации о пациентах и сотрудниках типового лечебно-профилактического учреждения с точки зрения обеспечения информационной безопасности.
48. Особенности применения современных информационных технологий в медицинских учреждениях и требования к ним.
49. Типовой состав системы защиты персональных данных в медицинском учреждении и его особенности построения.
50. Роль руководства лечебно-профилактического учреждения и кадровые вопросы при организации защиты персональных данных в типовом медицинском учреждении.
51. Использование типовых решений по защите информационных систем обработки персональных данных в медицинских учреждениях.
52. Организация защиты баз данных, содержащих персональные данные, по опыту типовых лечебно-профилактических учреждений.
53. Методика по приведению медицинских информационных систем к требованиям законодательства по защите персональных данных.
54. Определение основных мероприятий по защите персональных данных в медицинской информационной системе.
55. Организационные мероприятия по защите персональных медицинских данных в медицинской информационной системе и их характеристика.
56. Основные проблемы информационной безопасности в «облаках» и пути их решения.

57. Вопросы перспективной архитектуры и состава средств защиты персональных данных для систем обработки и «облачных» вычислений.
58. Насущные вопросы обеспечения юридической значимости первичных документов и другой важной информации, а также процессов их защиты, обработки, хранения и обмена с применением перспективных информационных систем и новых информационных технологий.
59. Правовые аспекты электронного взаимодействия при обработке и защите персональных данных.
60. Насущные вопросы современной идентификации и аутентификации при обработке и защите персональных данных в перспективных информационных системах.

Приложение 2

ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

«ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ПРЕДПРИЯТИИ»

(Приложение 2 к рабочей программе)

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Информационно-аналитические системы финансового мониторинга

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Королев
2020

1. Общие положения

Цель дисциплины:

– приобретение студентами знаний и представлений по системам защиты персональных данных на предприятиях;

– приобретение студентами теоретических сведений и практических навыков по применению систем защиты персональных данных.

Задачи дисциплины:

– Ознакомление студентов с методологическими подходами применения и эксплуатации систем защиты персональных данных на предприятии;

– освоение студентами основных методов определения параметров, характеристик и условий применения систем защиты персональных данных;

– формирование у студентов способности самостоятельно решать поставленные задачи в области применения систем защиты персональных данных с помощью современных принципов, методов и сил в различных организационных структурах, по базовым направлениям и применительно к типовым информационным объектам.

2. Указания по проведению практических занятий

Тема: Законодательные основы и нормативно-методическое обеспечение безопасности персональных данных.

Практическое занятие 1.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания по организации контроля и надзора за обработкой персональных данных.

Основные положения темы занятия:

1. Место персональных данных в системе российского законодательства. Уровни обеспечения безопасности персональных данных и их характеристика.

2. Государственная политика в области обеспечения защиты персональных данных.

Вопросы для обсуждения:

1. Организация контроля и надзора за обработкой персональных данных.
2. Дисциплинарная и материальная ответственность за нарушение норм, регулирующих защиту персональных данных.
3. Административная и уголовная ответственность за нарушение норм, регулирующих защиту персональных данных.

Продолжительность занятия – 4 ч.

Тема: Организация обработки персональных данных с помощью информационных систем.

Практическое занятие 2.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания по особенностям классификации информационных систем и обработки персональных данных.

Основные положения темы занятия:

1. Особенности сбора и накопления персональных данных в различных организациях.
2. Основания для осуществления классификации информационных систем обработки персональных данных.

Вопросы для обсуждения:

1. Особенности блокирования, прекращения обработки и уничтожения персональных данных работников, служащих.
2. Характеристика категорий, обрабатываемых в информационных системах персональных данных и их объёмы.
3. Алгоритм проведения классификации информационных систем, связанных с обработкой персональных данных.

Продолжительность занятия – 4 ч.

Тема: Характеристика угроз безопасности персональным данным при их обработке в информационных системах.

Практическое занятие 3.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания по определению перечня актуальных угроз безопасности персональных данных.

Основные положения темы занятия:

1. Классификация угроз безопасности при обработке персональных данных.
2. Характеристика базовой модели угроз безопасности персональных данных при их обработке в информационных системах и порядок её формирования.

Вопросы для обсуждения:

1. Порядок определения вероятности реализации, коэффициентов реализуемости и показателей опасности угроз.
2. Определение перечня актуальных угроз безопасности персональных данных.
3. Методика выявления актуальных угроз безопасности персональных данных при их обработке в информационных системах.
4. Методика по приведению информационных систем, связанных с обработкой персональных данных к требованиям законодательства.

Продолжительность занятия – 4 ч.

Тема: Особенности построения систем защиты персональных данных в различных организациях.

Практическое занятие 4.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания по обработке и защите персональных данных в государственных или муниципальных информационных системах.

Основные положения темы занятия:

1. Требования к локальному нормативному регулированию защиты персональных данных в организации.
2. Требования к построению информационной системы обработки персональных данных организации.

Вопросы для обсуждения:

1. Особенности обработки и защиты персональных данных в государственных или муниципальных информационных системах.
2. Обзор положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, введенного постановлением Правительства РФ № 781.
3. Обзор методических документов ФСТЭК России в области обеспечения безопасности персональных данных при их обработке в информационных системах.

Продолжительность занятия – 4 ч.

Тема: Организация работы по защите персональных данных государственных гражданских служащих.

Практическое занятие 5.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания по требованиям, предъявляемым к кадровой службе, при получении, обработке, хранении и передаче персональных данных.

Основные положения темы занятия:

1. Основные мероприятия по организации и техническому обеспечению безопасности персональных данных при их обработке в информационных системах.
2. Основные меры и средства защиты от несанкционированных действий с применением программных и программно-аппаратных средств.

Вопросы для обсуждения:

1. Перечень документов государственного учреждения, содержащих персональные данные и их характеристика.
2. Обязанности кадровой службы государственного органа при ведении личных дел гражданских служащих.
3. Требования, предъявляемые к кадровой службе, при получении, обработке, хранении и передаче персональных данных.

Продолжительность занятия – 4 ч.

Тема: Особенности защиты персональных данных в медицинских учреждениях.

Практическое занятие 6.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания по особенностям обработки информации о пациентах и сотрудниках типового лечебно-профилактического учреждения.

Основные положения темы занятия:

1. Виды медицинских информационных систем и их особенности.
2. Виды конфиденциальной информации в типовом лечебно-профилактическом учреждении и требования по защите персональных данных.

Вопросы для обсуждения:

1. Классификация типов обрабатываемой информации в медицинских информационных системах с точки зрения информационной безопасности.
2. Особенности обработки информации о пациентах и сотрудниках типового лечебно-профилактического учреждения.
3. Особенности применения современных информационных технологий в медицинских учреждениях и требования к ним.

Продолжительность занятия – 4 ч.

Тема: Методика построения систем защиты персональных данных в медицинских учреждениях.

Практическое занятие 7.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания по определению основных мероприятий по защите персональных данных в медицинской информационной системе.

Основные положения темы занятия:

1. Выделение основных потоков информации, в которой проявляются персональные данные и другие виды конфиденциальной информации.
2. Роль руководства лечебно-профилактического учреждения и кадровые вопросы при организации защиты информации в типовом медицинском учреждении.

Вопросы для обсуждения:

1. Методика по приведению медицинских информационных систем к требованиям законодательства по защите персональных данных.
2. Определение основных мероприятий по защите персональных данных в медицинской информационной системе.
3. Организационные мероприятия по защите персональных медицинских данных в медицинской информационной системе.

Продолжительность занятия – 4 ч.

Тема: Перспективы развития систем защиты персональных данных в современном обществе.

Практическое занятие 8.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические знания по отдельным компонентам правовых аспектов электронного взаимодействия при обработке и защите персональных данных.

Основные положения темы занятия:

1. Проблемы информационной безопасности в «облаках» и пути их решения.

2. Вопросы перспективной архитектуры и состава средств защиты персональных данных для систем обработки и «облачных» вычислений.

Вопросы для обсуждения:

1. Юридическая значимость бумажного документооборота при обработке и защите персональных данных.

2. Правовые аспекты электронного взаимодействия при обработке и защите персональных данных.

3. Некоторые вопросы идентификации и аутентификации при обработке и защите персональных данных.

Продолжительность занятия – 4 ч.

3. Указания по проведению лабораторного практикума

Не предусмотрен учебным планом.

4. Указания по проведению самостоятельной работы студентов

Цель самостоятельной работы: подготовить бакалавров к самостоятельному научному творчеству.

Задачи самостоятельной работы:

– расширить представление в области защиты персональных данных работников (служащих) предприятий;

– систематизировать знания в области оценки предварительной защищённости информационных систем по обработке и хранению персональных данных и методике их защиты;

– овладеть некоторыми навыками решения нетривиальных задач в области организации защиты персональных данных на предприятии.

Объём времени на самостоятельную работу, и виды самостоятельной работы представлены в таблице 1.

Таблица 1

Объем времени и виды самостоятельной работы

Виды самостоятельной работы	**Очная форма обучения**
	Всего академических часов
Всего часов на самостоятельную работу	**96**
Вопросы, выносимые на самостоятельное изучение	28
Подготовка к практическим занятиям	32
Подготовка докладов	16
Выполнение практических заданий	20

Вопросы, выносимые на самостоятельное изучение:

1. Характеристика программы действий по приведению организаций банковской системы РФ в соответствие с требованиями федерального закона «О персональных данных».
2. Классификация информационных систем обработки персональных данных, применяемых в банковской системе РФ и их особенности, типовой перечень и характеристика персональных данных, обрабатываемых в банковских системах.
3. Формирование частной модели угроз и основные мероприятия по защите персональных данных в банковской системе РФ.
4. Общие принципы обеспечения безопасности персональных данных в информационных системах оператора связи.
5. Характеристика основных методов обеспечения безопасности персональных данных и особенности защиты информационных систем персональных данных оператора связи.
6. Модели угроз и нарушителей безопасности при обработке персональных данных, основные мероприятия по защите персональных данных в информационных системах оператора связи.
7. Порядок контроля и оценки эффективности системы защиты персональных данных оператора связи.
8. Основные проблемы информационной безопасности и защиты персональных данных в медицинских учреждениях и их характеристика.
9. Программа мер по внедрению новой архитектуры и состава средств защиты персональных данных в типовых медицинских учреждениях.
10. Основные направления развития методов и средств защиты персональных данных в медицинских учреждениях.
11. Обзор современного международного сотрудничества в области защиты персональных данных.
12. Системы защиты персональных данных информационных систем и сетей и особенности их применения.
13. Основные перспективы развития систем защиты персональных данных в развитых зарубежных странах.

Тематическое содержание самостоятельной работы представлено в таблице 2.

Таблица 2

Тематическое содержание самостоятельной работы

№ п/п	Виды самостоятельной работы	Количество часов	Перечень заданий
1.	Вопросы, выносимые на самостоятельное изучение	28	Изучение открытых источников
2.	Подготовка к практическим занятиям	32	Изучение открытых источников при подготовке доклада на выбранную тему.
3.	Тематика докладов	16	1. Обеспечение информационной безопасности и защиты персональных данных в организациях банковской системы Российской Федерации. 2. Характеристика концепции защиты персональных данных в информационных системах оператора связи и анализ её основных положений. 3. Перспективы и пути интеграции информационных медицинских систем, особенности защиты персональных данных в них. 4. Обзор современных методов и технических средств защиты персональных данных ведущих зарубежных стран, основные подходы по их использованию.
4.	Выполнение практических заданий	20	1. Характеристика способов перехвата конфиденциальной коммерческой информации, обрабатываемой техническими средствами. 2. Рейтинговый подход к защите коммерческой тайны и персональных данных, характеристика и особенности его применения. 3. Систематика ущерба информационным ресурсам организации, связанного с обработкой персональных данных. 4. Динамика обеспечения безопасности в обработке персональных данных при следовании от внешних угроз к внутренним.

Примерные темы докладов

1. Обеспечение защиты персональных данных в СУБД “Oracle”, методика и особенности применения основных процедур и функций.

2. Анализ законодательной и нормативной базы обеспечения безопасности при использовании персональных данных.
3. Правовое исследование целесообразности создания и ведения автоматизированных баз данных при обработке персональных сведений.
4. Обзор и характеристика передовых методов организации защиты персональных данных в информационных системах.
5. Анализ опыта и перспектив развития систем защиты персональных данных граждан, работников и служащих в РФ и за рубежом.
6. Обобщение и анализ основных моментов положения о разрешительной системе допуска к работе с персональными данными.
7. Выявление, обзор и анализ основных противоречий в нормативных и правовых документах, регулирующих защиту персональных данных.
8. Характеристика ключевых моментов типового порядка реализации программы построения систем защиты персональных данных.
9. Анализ ключевых моментов положения о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в организации.
10. Анализ опыта лицензирования деятельности операторов по обработке персональных данных.

5. Указания по проведению контрольных работ

5.1. Требования к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

5.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.

2. При определении целей и задач работы необходимо правильно их формулировать. Так, в качестве цели не следует употреблять глагол «сделать». Правильно будет использовать глаголы: «раскрыть», «определить», «установить», «показать», «выявить» и т.д.

3. Основная часть работы включает 2 - 4 вопроса, каждый из которых посвящается решению задач, сформулированных во введении, и заканчивается констатацией итогов и выводами.

4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).

5. Необходимо давать ссылки на используемую Вами литературу.

6. Заключение должно содержать сделанные автором работы общие выводы по итогам исследования и рекомендации по применению работы.

7. Вслед за заключением идёт список литературы, который должен быть составлен в соответствии с установленными требованиями.

8. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3. Требования к оформлению

Объём контрольной работы – 20 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

6. Указания по проведению курсовых работ

Не предусмотрены учебным планом.

7. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Васильков А.В., Васильков А.А., Васильков И.А. Информационные системы и их безопасность. Учебное пособие. – М.: «ФОРУМ», 2011.
2. Вихорев С. В. О защите персональных данных» под редакцией А. Бражникова. – М.: «Авангард центр», 2014.
3. Сабанов А.Г., Зыков В.Д., Мещеряков Р.В., Рылов С.П., Шелупанов А.А. Защита персональных данных в организациях здравоохранения. – М.: «Горячая линия-Телеком», 2012.

Дополнительная литература:

1. Анисимов А.А. Менеджмент в сфере информационной безопасности. Учебное пособие. – М.: Интернет – Университет информационных технологий / БИНОМ. Лаборатория знаний, 2010.
2. Зайцев А. П., Шелупанов А. А., Мещеряков Р. В. И др. Технические средства и методы защиты информации. Учебное пособие для вузов. – М.: «Горячая линия – Телеком», 2012.

Рекомендуемая литература:

1. Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. Учебное пособие. – М.: Книжный дом «ЛИБРОКОМ», 2012.
2. Кузнецов П.П., Столбов А.П. Автоматизированная обработка и защита персональных данных в медицинских учреждениях. – М.: ИД «Менеджер здравоохранения», 2010.
3. Тихомирова Л.В. Защита персональных данных работника. Учебно-практическое пособие. – М.: Издательство Тихомирова М.Ю., 2002.

Электронные книги:

1. Обеспечение безопасности персональных данных. Методическое пособие. Издательский дом «Афина», 2010: **www.inside-zi.ru**
2. Краткий энциклопедический словарь информационной безопасности. Издатель: Энергия, 2010: **www.biblioclub.ru**

3. ЭБС «Руконт»: **www.rucont.ru**

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp** – Научно-образовательный портал;
2. **www.wikIsec.ru** – Энциклопедия информационной безопасности. – Публикации, статьи;
3. **http://www.fsb.ru/** – Официальный сайт Федеральной службы безопасности РФ;
4. **http://www.fstec.ru/** – Официальный сайт Федеральной службы по техническому экспортному контролю РФ.

9. Перечень информационных технологий

Перечень программного обеспечения: *MSOffice*.

Информационные справочные системы:

1. Ресурсы информационно-образовательной среды МГОТУ
2. Рабочая программа и методическое обеспечение по дисциплине «Организация защиты персональных данных на предприятии».
3. Информационно – справочные (правовые) системы:
   – «Гарант» (**garantcenter.ru**);
   – «Кодекс» (**doskainfo.ru/advert/64804/**);
   – «Консультант +» (**artiks.ru**).