Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

**«УТВЕРЖДАЮ»**
**И.о. проректора**
**_____ А.В. Троицкий**
**_____ 2023 г.**

***ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ***

***КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ***

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

**«КАДРОВАЯ БЕЗОПАСНОСТЬ»**

**Специальность: 38.05.01 «Экономическая безопасность»**
**Специализация: «Экономико-правовое обеспечение экономической безопасности»**
**Уровень высшего образования: специалитет**
**Квалификация (степень) выпускника: экономист**
**Форма обучения: очная, заочная**

Королев
2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

**Автор: к.т.н., доцент Вихров А.П., Рабочая программа дисциплины: «Кадровая безопасность». – Королев МО: «Технологический университет», 2023.**

**Рецензент: к.в.н., доцент Воронов А.Н.**

Программа составлена в соответствии с требованиями федерального Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по специальности 38.05.01 «Экономическая безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол **№ 9 от 11 апреля 2023 г.**

**Рабочая программа рассмотрена и одобрена на заседании кафедры:**

| | | | | | |
|---|---|---|---|---|---|
| Заведующий кафедрой (ФИО, ученая степень, звание, подпись) | Сапнай В.Н. к.в.н., доцент | | | | |
| Год утверждения (переутверждения) | 2023 | 2024 | 2025 | 2026 | 2027 |
| Номер и дата протокола заседания кафедры | № 8 от 29.03.2023 г. | | | | |

**Рабочая программа согласована:**
**Руководитель ОПОП _____ к.э.н., доцент Коба Е.Е.**

**Рабочая программа рекомендована на заседании УМС:**

| | | | | | |
|---|---|---|---|---|---|
| Год утверждения (переутверждения) | 2023 | 2024 | 2025 | 2026 | 2027 |
| Номер и дата протокола заседания УМС | № 5 от 11.04.2023 г. | | | | |

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

**Целью** изучения дисциплины является:

1. Формирование у студентов специализированной базы знаний по кадровой безопасности в стране и на предприятиях;
2. Получение представления о понятийном аппарате, законах и закономерностях функционирования и развития процесса обеспечения кадровой безопасности, а так же об особенностях защиты персональных данных в современных условиях.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

**Универсальные компетенции**:

УК-1 - Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий;

УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия

**Профессиональные компетенции**

ПК-5 Способен принимать оптимальные управленческие решения, осуществлять управление кадровым составом, обеспечивать эффективные коммуникации, осуществлять мотивацию и контроль эффективности работы сотрудников и подразделений в сфере управления рисками.

**Основными задачами дисциплины являются:**

1. Ознакомление студентов с методологическими подходами применения и эксплуатации систем кадровой безопасности 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 кадровой безопасности с помощью современных принципов, методов и сил в различных организационных структурах, по базовым направлениям и применительно к типовым информационным объектам.

Показатели освоения компетенций отражают следующие индикаторы:

**Трудовые действия:**

УК-1. И-1. Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними.

УК-1. И-2. Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению.

УК-1. И-3. Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников.

УК-5. И-2. Выстраивает социальное профессиональное взаимодействие с учетом особенностей основных форм научного и религиозного сознания,

деловой и общей культуры представителей других этносов и конфессий, различных социальных групп;

УК-5. И-3. Обеспечивает создание недискриминационной среды взаимодействия при выполнении профессиональных задач

ПК-5. И-1. Анализирует кадровый потенциал организации, формулирует требования к специалистам по управлению рисками, организует разработку должностных инструкций, подбирает руководящие кадры управления рисками в организации.

ПК-5. И-2. Создает систему мотивации и развития персонала, отвечающего за процесс управления рисками

ПК-5. И-3. Управляет штатом риск-менеджеров всех бизнес-единиц и подразделений организации, контролирует деятельности отдела и работников, отвечающих за процесс управления рисками в организации, определяет процедуры контроля деятельности работников и подразделения, координирует выполнение работ и должностных обязанностей, выполнение оперативного и тактического плана работ, соблюдение корпоративных правил и норм работы в организации

**Необходимые умения:**

УК-1. И-1. У-1. Умеет проводить анализ проблемной ситуации как системы, выявляя ее составляющие и связи между ними

УК-1. И-2. У-1. Умеет определять пробелы в информации, необходимой для решения проблемной ситуации;

УК-1. И-2. У-2. Умеет проектировать процессы по устранению пробелов в информации;

УК-5. И-2. У-1.Умеет выстраивать социальное профессиональное взаимодействие с учетом особенностей основных форм научного и религиозного сознания, деловой и общей культуры представителей других этносов и конфессий, различных социальных групп;

УК-5. И-3. У-1 Умеет создавать недискриминационную среду взаимодействия при выполнении профессиональных задач

ПК-5. И-1. У-1 Умеет анализировать кадровый потенциал организации, формулировать требования к специалистам по управлению рисками, организовывать разработку должностных инструкций, подбирать руководящие кадры управления рисками в организации

ПК-5. И-2. У-1 Умеет определять ключевые показатели эффективности деятельности работников на основе стратегических задач в области риск-менеджмента;

ПК-5. И-2. У-2 Умеет составлять и анализировать мотивационные профили работников подразделения;

ПК-5. И-2. У-3 Умеет разрабатывать мероприятия по мотивированию и стимулированию работников, программы обучения работников подразделения, формировать кадровый резерв, применять методы поддержания позитивного социально-психологического климата в подразделении

ПК-5. И-3. У-1 Умеет управлять штатом риск-менеджеров всех бизнес-единиц и подразделений организации;

ПК-5. И-3. У-2 Умеет разрабатывать процедуры контроля деятельности работников и подразделения, координировать и контролировать выполнение
УК-5.И-1. З-1. Знает методику анализа важнейших идеологических и ценностных систем, сформировавшихся в ходе исторического развития;
работ и должностных обязанностей, выполнение оперативного и тактического плана работ, соблюдение корпоративных правил и норм работы в организации

**Необходимые знания:**

УК-1. И-1. З-1 Знает методику проведения анализа проблемной ситуации как системы, знает ее составляющие и связи между ними

УК-1. И-2. З-1. Знает способы определения пробелов в информации, необходимой для решения проблемной ситуации;

УК-1. И-2. З-2 Знает алгоритм проектирования процессов по устранению пробелов в информации, необходимой для решения проблемной ситуации;

УК-1. И-3. З-1 Знает методы оценки надежности источников информации, порядок работы с противоречивой информацией из различных источников.

УК-5. И-2. З-1. Знает способы социального профессионального взаимодействия с учетом особенностей основных форм научного и религиозного сознания, деловой и общей культуры представителей других этносов и конфессий, различных социальных групп;

УК-5. И-3. З-1 Знает способы обеспечения недискриминационной среды взаимодействия при выполнении профессиональных задач

ПК-5. И-1. З-1. Знает кадровый потенциал организации, требования к специалистам по управлению рисками, должностные инструкции;

ПК-5. И-1. З-2 Знает требования к обеспечению сохранения коммерческой тайны

ПК-5. И-2. З-1. Знает ключевые показатели эффективности деятельности работников;

ПК-5. И-2. З-2. Знает принципы создания мотивационных профилей работников подразделения;

ПК-5. И-2. З-3. Знает методы поддержания позитивного социально-психологического климата в подразделении

ПК-5. И-2. З-4. Знает алгоритм разработки мероприятий по мотивированию и стимулированию работников

ПК-5. И-3. З-1. Знает бизнес-процессы в сфере управления персоналом в организации;

ПК-5. И-3. З-2. Знает роль и место управления персоналом в общеорганизационном управлении и его связь со стратегическими задачами организации;

ПК-5. И-3. З-3. Знает нормы профессиональной этики, нормы корпоративного управления и корпоративной культуры

## 2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Кадровая безопасность» относится к части, формируемой участниками образовательных отношений дисциплин по выбору Блока 1

основной профессиональной образовательной программы подготовки специалистов по направлению 38.05.01 «Экономическая безопасность». Дисциплина реализуется кафедрой информационной безопасности

Данная дисциплина органически связана с дисциплинами общенаучной подготовки, а также с дисциплинами, определяющими специальную подготовку студентов и базируется на знании следующих учебных курсов: «Психология в профессиональной деятельности», «Менеджмент», «Экономика организации (предприятия)», «Этика деловых отношений», «Коммуникационный менеджмент», «Культурология» и компетенциях УК-1; УК-2; УК-3; УК-5; УК-6; УК-10; ОПК-3; ПК-5 ПК-9

Знания и компетенции, полученные при освоении дисциплины, являются значимыми для изучения дисциплины «Антикризисное управление», а также выполнения выпускной квалификационной работы.

## 3. Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 часов.

**Таблица 1 - Объем дисциплины (модуля) и виды учебной работы**

| Виды занятий | Всего часов | Семестр 7 | Семестр 8 | Семестр … | Семестр … |
|---|---|---|---|---|---|
| **Общая трудоемкость** | 108 | 108 | | | |
| **ОЧНАЯ ФОРМА ОБУЧЕНИЯ** | | | | | |
| **Аудиторные занятия** | 32 | 32 | | | |
| Лекции (Л) | 16 | 16 | | | |
| Практические занятия (ПЗ) | 16 | 16 | | | |
| Лабораторные работы (ЛР) | - | - | | | |
| Практическая подготовка | | | | | |
| **Самостоятельная работа** | 76 | 76 | | | |
| **Контрольная работа** | + | + | | | |
| **Текущий контроль знаний** | Тесты | Тесты | | | |
| **Вид итогового контроля** | Зачёт с оценкой | Зачет с оценкой | | | |
| **ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ** | | | | | |
| **Аудиторные занятия** | 8 | | 8 | | |
| Лекции (Л) | 4 | | 4 | | |
| Практические занятия (ПЗ) | 8 | | 8 | | |
| Лабораторные работы (ЛР) | - | | - | | |
| Практическая подготовка | - | | - | | |
| **Самостоятельная работа** | 96 | | 96 | | |
| **Курсовые работы (проекты)** | - | | - | | |
| **Расчетно-графические работы** | - | | - | | |
| **Контрольная работа** | + | | + | | |
| **Вид итогового контроля** | Зачет с оценкой | | Зачет с оценкой | | |

## 4. Содержание дисциплины

### 4.1. Темы дисциплины и виды занятий

**Таблица 2- Темы дисциплины и виды занятий**

| Наименование тем | Лекции, час. очн/заоч | Практические занятия, час очн/заоч | Занятия в интерактивной форме, час очн/заоч | Код компетенций |
|---|---|---|---|---|
| Тема 1. Законодательные основы и нормативно-методи-ческое обеспечение кадровой безопасности РФ. | 2/0,5 | 2/1 | 4/0,5 | УК-1, УК-5, ПК-5 |
| Тема 2. Организация обработки персональных данных с помощью информационных систем. | 2/0,5 | 2/1 | 2/0,5 | УК-1, УК-5, ПК-5 |
| Тема 3. Характеристика угроз кадровой безопасности и персональным данным при их обработке в информационных системах. | 2/0,5 | 2/1 | 2/0,5 | УК-1, УК-5, ПК-5 |
| Тема 4. Особенности построения систем защиты персональных данных в различных организациях. | 2/0,5 | 2/1 | 2/0,5 | УК-1, УК-5, ПК-5 |
| Тема 5. Организация работы по защите персональных данных государственных гражданских служащих. | 2/0,5 | 2/1 | 4/0,5 | УК-1, УК-5, ПК-5 |
| Тема 6. Особенности защиты персональных данных в медицинских учреждениях. | 2/0,5 | 2/1 | 2/0,5 | УК-1, УК-5, ПК-5 |
| Тема 7. Методика построения систем защиты персональных данных в медицинских учреждениях. | 2/0,5 | 2/1 | 2/0,5 | УК-1, УК-5, ПК-5 |
| Тема 8. Перспективы развития кадровой безопасности и систем защиты персональных данных в современном обществе. | 2/0,5 | 2/1 | 4/0,5 | УК-1, УК-5, ПК-5 |
| **Итого:** | **16/4** | **16/8** | **22/4** | |

### 4.2. Содержание тем дисциплины

#### Тема 1. Законодательные основы и нормативно-методическое обеспечение кадровой безопасности РФ

Понятие кадровой безопасности в международном и Российском законодательстве. Международные акты о защите персональных данных и их

роль в развитии российского законодательства. Место персональных данных в системе российского законодательства. Уровни обеспечения безопасности персональных данных и их характеристика. Государственная политика в области кадровой безопасности и 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 кадровой безопасности и персональным данным при их обработке в информационных системах**

Классификация угроз безопасности при обработке персональных данных. Основные источники угроз кадровой безопасности и 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 кадровой безопасности и 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

1. «Методические указания для обучающихся по освоению дисциплины».

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

Структура фонда оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине «Кадровая безопасность» приведена в Приложении 1.

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

**Основная литература:**

1. Кадровая безопасность компании : учеб. пособие / Т.О. Соломанидина, В.Г. Соломанидин. — 2-е изд., перераб. и доп. — М. : ИНФРА-М, 2021. — 559 с. + Доп. материалы [Электронный ресурс; Режим доступа http://www.znanium.com]. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/23580. http://znanium.com/bookread2.php?book=753429

2. Кадровая безопасность организации : учебник и практикум для академического бакалавриата / С. В. Духновский. — Москва : Издательство Юрайт, 2019. — 245 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-09266-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/427522

**Дополнительная литература:**

1. Карзаева Н.Н. Основы экономической безопасности : учебник / Н.Н. Карзаева. — М. : ИНФРА-М, 2017. — 275 с. — (Высшее образование: Специалитет). — www.dx.doi.org/10.12737/20854.http://znanium.com/bookread2.php?book=561349

2. Бабковская, В.Н. Розничный персонал от А до Я / В.Н. Бабковская. - 2-е изд. - Москва-Вологда : Инфра-Инженерия, 2016. - 352 с. : ил., табл., схем. - ISBN 978-5-9729-0129-6 ; То же [Электронный ресурс]. - URL://biblioclub.ru/index.php?page=book&id=444426

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

**Интернет-ресурсы**:

1. ЭБС «Университетская библиотека on-line»
2. www. consultant. ru
3. www.qarant. Ru
4. **www.biblioclub.ru**
5. **http://eup.ru/catalog/all-all.asp** – Научно-образовательный портал;
6. **www.wikIsec.ru** – Энциклопедия информационной безопасности. – Публикации, статьи;
7. **http://www.fsb.ru/** – Официальный сайт Федеральной службы безопасности РФ;

8. **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)Электронные ресурсы образовательной среды Университета.**

1.Учебный портал с электронно-методическими комплексами(do.kimes)

**2) Информационно-справочные системы:**

**СПС «Консультант Плюс»**

«Гарант» (**garantcenter.ru**);

«Кодекс» (**doskainfo.ru/advert/64804/**);

**3)Электронные ресурсы:**

*2.Университетская библиотека онлайн(*www.biblioclub.ru*).*

*3.Библиотека диссертаций РГБ(*www.diss.ru*)*

*4.Polpred.com(www.polpred.com)*

*5.Единое окно доступа(*www.window.edu.ru*).*

*6.Универсальная библиотека ИстВью(online.ebiblioteka.ru).*

*7.Издательский дом «Гребенников»(htth/grebennikon.ru)/*

**Информационные справочные системы:** «*Электронные ресурсы образовательной среды Университета*»

*1.Учебный портал с электронно-методическими комплексами(do.kimes)*

*2.Университетская библиотека онлайн(*www.biblioclub.ru*).*

*3.Библиотека диссертаций РГБ(*www.diss.ru*)*

*4.Polpred.com(www.polpred.com)*

*5.Единое окно доступа(*www.window.edu.ru*).*

*6.Универсальная библиотека ИстВью(online.ebiblioteka.ru).*

*7.Издательский дом «Гребенников»(htth/grebennikon.ru)/*

**2. СПС «Консультант Плюс».**

## 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 Windows; 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 ИНФОКОММУНИКАНИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ**

***КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ***

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

# «КАДРОВАЯ БЕЗОПАСНОСТЬ»

**(Приложение 1 к рабочей программе)**

**Специальность: 38.05.01 «Экономическая безопасность»**
**Специализация: «Экономико-правовое обеспечение экономической безопасности»**
**Квалификация (степень) выпускника: экономист**
**Форма обучения: очная, заочная**

Королев
2023

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

| № п/п | Индекс компетенции | Содержание компетенции | **Раздел дисциплины, обеспечивающий формирование компетенции** | **В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:** | | |
|---|---|---|---|---|---|---|
| | | | | **Трудовые действия** | **Необходимые умения** | **Необходимые знания** |
| 1 | УК-1 | Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий | Темы 1-8 | УК-1.1<br>Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними | УК-1. И-1. У-1<br>Умеет проводить анализ проблемной ситуации как системы, выявляя ее составляющие и связи между ними | УК-1. И-1. З-1<br>Знает методику проведения анализа проблемной ситуации как системы, знает ее составляющие и связи между ними |
| | | | | УК-1. И-2. Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению | УК-1. И-2. У-1<br>Умеет определять пробелы в информации, необходимой для решения проблемной ситуации;<br>УК-1. И-2. У-2<br>умеет проектировать процессы по устранению пробелов в информации; | УК-1. И-2. З-1<br>Знает способы определения пробелов в информации, необходимой для решения проблемной ситуации;<br>УК-1. И-2. З-2<br>Знает алгоритм проектирования процессов по устранению пробелов в информации, необходимой для решения проблемной ситуации; |
| | | | | УК-1. И-3. Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников. | УК-1. И-3. У-1<br>Умеет критически оценивать надежность источников информации, работать с противоречивой информацией из разных источников | УК-1. И-3. З-1<br>Знает методы оценки надежности источников информации, порядок работы с противоречивой информацией из различных источников. |
| 2 | УК-5 | Способен анализировать и учитывать разнообразие культур в процессе межкультурного | Темы 1-8 | УК-5. И-2. Выстраивает социальное профессиональное взаимодействие с учетом особенностей основных форм научного и религиозного сознания, деловой и общей культуры представителей других этносов и | УК-5. И-2. У-1.Умеет выстраивать социальное профессиональное взаимодействие с учетом особенностей основных форм научного и религиозного сознания, деловой и общей культуры представителей других этносов и | УК-5. И-2. З-1. Знает способы социального профессионального взаимодействия с учетом особенностей основных форм научного и религиозного сознания, деловой и общей культуры представителей других этносов и конфессий, различных социальных |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | взаимодействия | | конфессий, различных социальных групп; | конфессий, различных социальных групп; | групп; |
| | | | | УК-5. И-3. Обеспечивает создание недискриминационной среды взаимодействия при выполнении профессиональных задач | УК-5. И-3. У-1 Умеет создавать недискриминационную среду взаимодействия при выполнении профессиональных задач | УК-5. И-3. З-1 Знает способы обеспечения недискриминационной среды взаимодействия при выполнении профессиональных задач |
| 3 | ПК-5 | Способен принимать оптимальные управленческие решения, осуществлять управление кадровым составом, обеспечивать эффективные коммуникации, осуществлять мотивацию и контроль эффективности работы сотрудников и подразделений в сфере управления рисками | Темы 1-8 | ПК-5. И-1<br>Анализирует кадровый потенциал организации, формулирует требования к специалистам по управлению рисками, организует разработку должностных инструкций, подбирает руководящие кадры управления рисками в организации | ПК-5. И-1. У-1<br>Умеет анализировать кадровый потенциал организации, формулировать требования к специалистам по управлению рисками, организовывать разработку должностных инструкций, подбирать руководящие кадры управления рисками в организации | ПК-5. И-1. З-1<br>Знает кадровый потенциал организации, требования к специалистам по управлению рисками, должностные инструкции;<br>ПК-5. И-1. З-2<br>Требования к обеспечению сохранения коммерческой тайны |
| | | | | ПК-5. И-2.<br>Создает систему мотивации и развития персонала, отвечающего за процесс управления рисками | ПК-5. И-2. У-1<br>Умеет определять ключевые показатели эффективности деятельности работников на основе стратегических задач в области риск-менеджмента;<br>ПК-5. И-2. У-2<br>Умеет составлять и анализировать мотивационные профили работников подразделения;<br>ПК-5. И-2. У-3<br>Умеет разрабатывать мероприятия по мотивированию и стимулированию работников, программы обучения работников подразделения, формировать кадровый резерв, применять методы поддержания позитивного социально-психологического климата в подразделении | ПК-5. И-2. З-1<br>Знает ключевые показатели эффективности деятельности работников;<br>ПК-5. И-2. З-2<br>Знает принципы создания мотивационных профилей работников подразделения;<br>ПК-5. И-2. З-3<br>Знает методы поддержания позитивного социально-психологического климата в подразделении<br>ПК-5. И-2. З-4<br>Знает алгоритм разработки мероприятий по мотивированию и стимулированию работников |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | ПК-5. И-3<br>Управляет штатом риск-менеджеров всех бизнес-единиц и подразделений организации, контролирует деятельности отдела и работников, отвечающих за процесс управления рисками в организации, определяет процедуры контроля деятельности работников и подразделения, координирует выполнение работ и должностных обязанностей, выполнение оперативного и тактического плана работ, соблюдение корпоративных правил и норм работы в организации | ПК-5. И-3. У-1<br>Умеет управлять штатом риск-менеджеров всех бизнес-единиц и подразделений организации;<br>ПК-5. И-3. У-2<br>Умеет разрабатывать процедуры контроля деятельности работников и подразделения, координировать и контролировать выполнение работ и должностных обязанностей, выполнение оперативного и тактического плана работ, соблюдение корпоративных правил и норм работы в организации | ПК-5. И-3. З-1<br>Знает бизнес-процессы в сфере управления персоналом в организации;<br>ПК-5. И-3. З-2<br>Знает роль и место управления персоналом в общеорганизационном управлении и его связь со стратегическими задачами организации;<br>ПК-5. И-3. З-3<br>Знает нормы профессиональной этики, нормы корпоративного управления и корпоративной культуры<br>ПК-5. И-3. З-4<br>Современные теории и концепции взаимодействия работников в организации, включая вопросы мотивации, групповой динамики, командообразования, коммуникаций, лидерства и управления конфликтами |

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

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

| | | | |
|---|---|---|---|
| | | B) частично сформирована<br>**3-4 балла**<br>C) не сформирована<br>**2 балла** | 1.Соответствие содержания реферата заявленной тематике (1 балл).<br>2.Качество источников и их количество при подготовке работы (1 балл).<br>3.Владение информацией и способность отвечать на вопросы аудитории (1 балл).<br>4.Качество самой представленной работы (1 балл).<br>5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).<br>Максимальная сумма баллов - 5 баллов.<br>Результаты оценочной процедуры представляются обучающимся в срок не позднее 1 недели после проведения процедуры – для текущего контроля. Оценка проставляется в электронный журнал. |
| УК-1, УК-5, ПК-5 | Письменное задание | A) полностью сформирована<br>**5 баллов**<br>B) частично сформирована<br>**3-4 балла**<br>C) не сформирована<br>**2 балла** | 1. Проводится в форме письменной работы<br>2.Время, отведенное на процедуру – 10 - 15 мин.<br>Неявка – 0.<br>Критерии оценки:<br>1.Соответствие ответа заявленной тематике (0-5 баллов).<br>Максимальная сумма баллов - 5 баллов.<br>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 кадровой безопасности на предприятиях различной формы собственности.
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 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 «Кадровая безопасность» являются две текущие аттестации в виде тестов и одна итоговая аттестация в виде зачета с оценкой в устной форме.

| 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 |
|---|---|---|---|---|---|
| тестирование | УК-1, УК-5, ПК-5 | 25 вопросов | Компьютерное тестирование; время отведенное на процедуру - 30 минут | Результаты тестирования предоставляются в день проведения процедуры | Критерии оценки определяются процентным соотношением.<br>Не явка - 0<br>Удовлетворительно - от 51% правильных ответов.<br>Хорошо - от 70%.<br>Отлично – от 90%. |
| тестирование | УК-1, УК-5, ПК-5 | 25 вопросов | Компьютерное тестирование; время отведенное на процедуру – 30 минут | Результаты тестирования предоставляются в день проведения процедуры | Критерии оценки определяются процентным соотношением.<br>Не явка - 0<br>Удовлетворительно - от 51% правильных ответов.<br>Хорошо - от 70%.<br>Отлично – от 90%.<br>Максимальная оценка – 5 баллов. |
| Зачёт с оценкой | УК-1, УК-5, ПК-5 | 3 вопроса | Зачёт с оценкой проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут. | Результаты предоставляются в день проведения зачета с оценкой | Критерии оценки:<br>«**Отлично**»:<br>• знание основных понятий предмета;<br>• умение использовать и применять полученные знания на практике;<br>• работа на практических занятиях;<br>• знание основных научных теорий, изучаемых предметов;<br>• ответ на вопросы билета. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | «**Хорошо**»:<br>• знание основных понятий предмета;<br>• умение использовать и применять полученные знания на практике;<br>• работа на практических занятиях;<br>• знание основных научных теорий, изучаемых предметов;<br>• ответы на большинство вопросов билета<br>«У**довлетвори-тельно**»:<br>• демонстрирует частичные знания по темам дисциплин;<br>• незнание неумение использовать и применять полученные знания на практике;<br>• не работал на практических занятиях;<br>• ответил не на все вопросы билета<br><br>«**Неудовлетворительно**»:<br>• демонстрирует частичные знания по темам дисциплин;<br>• незнание основных понятий предмета;<br>• неумение использовать и применять полученные знания на практике;<br>• не работал на практических занятиях;<br>• не отвечает на вопросы. |

Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся, согласно приказу «О внедрении новой балльно-рейтинговой системы контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся» № 01-04/428 от 25 сентября 2020 г.

### 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. Что понимается под кадровой безопасностью предприятия (фирмы)?**

– это система правил и норм, приводящих человеческий ресурс в соответствие со стратегией предприятия (фирмы);

– это состояние, которое достигается посредством обеспечения и поддержания защищённости персонала предприятия (фирмы), а так же его жизненно важных интересов от внутренних и внешних угроз;

– это обеспечение охраны материальных и финансовых ресурсов предприятия (фирмы) от чрезвычайных обстоятельств и от несанкционированного проникновения на его территорию.

**2. Выберите мероприятия, которые относятся к кадровой политике предприятия (фирмы):**

– составление штатного расписания;

– отбор кадров;

– управление имуществом;

– аттестация персонала.

**4. 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.

**5. 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.

**6. 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;

**7. К какой категории информации относятся сами персональные данные?**

– к секретной информации;

– к открытой информации;

– к коммерческой информации;

– к конфиденциальной информации.

**8. 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;

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

– общедоступные;

– биометрические;

– секретные;

– специальные.

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

– Постановление Правительства РФ № 1119 от 2012 г;

– Приказ ФСТЭК РФ № 21 от 2013 г;

– Приказ ФСБ РФ № 86 от 2008 г;

– Госстандарт РФ.

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

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

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

– да;
– нет;

**13. 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.

**14. Какие виды дисциплинарной ответственности выделяют согласно Трудовому кодексу РФ?**

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

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

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

**16. Отличается ли материальная ответственность работника от гражданско-правовой?**

– да;
– нет;

**17. Какие виды материальной ответственности выделяют?**

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

**18. 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;

**19. 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.

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

– да;

– нет.

**21. 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;

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

– да;

– нет;

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

– да;

– нет.

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

– да;

– нет.

**25. 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.

**2-е тестирование по дисциплине**

**1. Предусмотрено ли создание электронного архива для хранения персональных данных?**

– да;

– нет.

**2. 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.

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

– да;
– нет.

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

– да;
– нет.

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

– внешняя;
– внутренняя;
– личная.
– универсальная.

**6. 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.

**7. 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.

**8. 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.

**9. 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.

**10. 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.

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

– да;

– нет.

**12. 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.

**13. Выберите приемлемые исходные данные для проведения классификации информационных систем обработки персональных данных согласно постановлению Правительства РФ № 1119 от 1.11.2012 г?**

– категория обрабатываемых персональных данных;

– гриф секретности обрабатываемых персональных данных;

– объём обрабатываемых персональных данных;

– степень защищённости персональных данных от НСД.

**14. 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.

**15. 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.

**16. 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;

**17. 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.

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

– да;

– нет.

**19. 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.

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

– до 10 м;

– до 100 м;

– до 300 м;

– до 500 м.

**21. 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.

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

– да;
– нет.

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

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

**24. 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).

**25. 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.

**26. 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.

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

– да;

– нет.

### 4.2. Типовые вопросы, выносимые на зачёт с оценкой

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

19. Характеристика категорий, обрабатываемых в информационных системах персональных данных и их объёмы.
20. Алгоритм проведения классификации информационных систем, связанных с обработкой персональных данных и порядок его построения.
21. Основные источники и классификация угроз безопасности при обработке персональных данных.
22. Содержание модели угроз верхнего уровня и характеристика её элементов.
23. Характеристика базовой модели угроз безопасности персональных данных при их обработке в информационных системах и порядок её формирования.
24. Характеристика первичных и вторичных носителей защищаемой речевой информации о персональных данных.
25. Потенциальные технические каналы утечки персональных данных и их характеристика.
26. Основные категории нарушителей при обработке персональных данных, и их характерные возможности.
27. Определение уровня исходной защищённости объектов обработки персональных данных.
28. Порядок определения вероятности реализации, коэффициентов реализуемости и показателей опасности угроз при обработке персональных данных.
29. Методика выявления актуальных угроз безопасности персональных данных при их обработке в информационных системах.
30. Методика по приведению информационных систем, связанных с обработкой персональных данных к требованиям законодательства.
31. Основные требования к построению системы защиты персональных данных в типовой организации и их характеристика.
32. Требования к локальному нормативному регулированию защиты персональных данных в организации и их характеристика.
33. Требования к назначению работников, ответственных за организацию обработки персональных данных в учреждениях, фирмах, на предприятиях.
34. Порядок построения и требования к информационной системе обработки персональных данных типовой организации.
35. Требования к защите персональных данных при неавтоматизированной обработке информации и их характеристика.
36. Особенности обработки и защиты персональных данных в государственных или муниципальных информационных системах.
37. 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.
38. Характеристика положений и требований основных методических документов ФСТЭК России в области обеспечения безопасности персональных данных при их обработке в информационных системах.

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

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

**Приложение 2**

*ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ*

*КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

# МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

# «КАДРОВАЯ БЕЗОПАСНОСТЬ»

**(Приложение 2 к рабочей программе)**

**Специальность: 38.05.01 «Экономическая безопасность»**
**Специализация: «Экономико-правовое обеспечение экономической безопасности»**
**Квалификация (степень) выпускника: экономист**
**Форма обучения: очная, заочная**

Королев
2023

## 1. Общие положения

**Цель дисциплины:**

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

– приобретение студентами теоретических сведений и практических навыков по применению законов и закономерностей функционирования и развития процессов обеспечения кадровой безопасности в современных политических и экономических отношениях, а так же по применению систем защиты персональных данных.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

**Универсальные компетенции**:

УК-1 - Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий;

УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия

**Профессиональные компетенции**

ПК-5 Способен принимать оптимальные управленческие решения, осуществлять управление кадровым составом, обеспечивать эффективные коммуникации, осуществлять мотивацию и контроль эффективности работы сотрудников и подразделений в сфере управления рисками.

**Основными задачами дисциплины являются:**

– 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 постав-
ленные задачи в области применения кадровой безопасности и 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 кадровой безопасности РФ.

**Практическое занятие 1**.

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

Тема и содержание практического занятия:

*Цель работы*: Получить знания и практические навыки по организации вопросов кадровой безопасности на предприятии.

*Основные положения темы занятия*:

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

2. Государственная политика в области кадровой безопасности и обеспечении 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: 2/1ч.

**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 знания и практические навыки 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: 2/1 ч.

**Тема: Характеристика угроз кадровой безопасности и 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 знания и практические навыки по определению перечня актуальных угроз кадровой безопасности и персональным данным.

*Основные положения темы занятия*:

1. Классификация угроз кадровой безопасности при обработке персональных данных.

2. Характеристика базовой модели угроз безопасности персональным данным 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: 2/1 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 знания и практические навыки 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 по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, введенного постановлением Правительства РФ № 1119.

3. Обзор методических документов ФСТЭК России в области обеспечения
безопасности персональных данных при их обработке в информационных системах.

Продолжительность занятия: 2/1 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 знания и практические навыки 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: 2/1 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 знания и практические навыки 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 кадровой 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: 2/1 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 знания и практические навыки по определению основных мероприятий кадровой безопасности и защиты 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: 2/1 ч.

**Тема: Перспективы развития кадровой безопасности и 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 знания и практические навыки 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: 2/1 ч.

## 3. Указания по проведению лабораторного практикума

Не предусмотрен учебным планом.

## 4. Указания по проведению самостоятельной работы студентов

*Цель самостоятельной работы*: подготовить обучаемых к самостоятельному научному творчеству.

*Задачи самостоятельной работы*:

– расширить представление в области кадровой безопасности и 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 / заочная форма обучения** |
|---|---|
| | **Всего академических часов** |
| Всего часов на самостоятельную работу | **76/96** |
| Вопросы, выносимые на самостоятельное изучение | 20/26 |
| Подготовка к практическим занятиям | 20/22 |
| Подготовка докладов | 20/24 |
| Выполнение практических заданий | 16/24 |

**Вопросы, выносимые на самостоятельное изучение:**

1. Характеристика программы действий по приведению вопросов кадровой безопасности 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 кадровой безопасности и 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 | 24/44 | Изучение открытых источников |
| 2. | Подготовка к практическим занятиям | 12/16 | Изучение открытых источников при подготовке доклада на выбранную тему. |
| 3. | Тематика докладов | 12/18 | 1. Обеспечение кадровой безопасности и защиты персональных данных в организациях банковской системы Российской Федерации.<br>2. Характеристика концепции защиты персональных данных в информационных системах оператора связи и анализ её основных положений.<br>3. Перспективы и пути интеграции информационных медицинских систем, особенности защиты персональных данных в них.<br>4. Обзор современных методов и технических средств кадровой безопасности и защиты персональных данных ведущих |

| | | | |
|---|---|---|---|
| | | | зарубежных стран, основные подходы по их использованию. |
| 4. | Выполнение практических заданий | 12/18 | 1. Характеристика способов перехвата конфиденциальной коммерческой информации, обрабатываемой техническими средствами.<br>2. Рейтинговый подход к защите коммерческой тайны и персональных данных, характеристика и особенности его применения.<br>3. Систематика ущерба информационным ресурсам организации, связанного с обработкой персональных данных.<br>4. Динамика обеспечения кадровой 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.
3. Анализ законодательной и нормативной базы обеспечения кадровой безопасности при использовании персональных данных.
4. Правовое исследование целесообразности создания и ведения автоматизированных баз данных при обработке персональных сведений.
5. Обзор и характеристика передовых методов организации защиты персональных данных в информационных системах.
6. 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 кадровую безопасность и защиту персональных данных.
8. Характеристика ключевых моментов типового порядка реализации программы построения систем защиты персональных данных.
8. 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 А4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

## 6. Перечень основной и дополнительной учебной литературы

**Основная литература:**

3. Кадровая безопасность компании : учеб. пособие / Т.О. Соломанидина, В.Г. Соломанидин. — 2-е изд., перераб. и доп. — М. : ИНФРА-М, 2021. — 559 с. + Доп. материалы [Электронный ресурс; Режим доступа http://www.znanium.com]. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/23580. http://znanium.com/bookread2.php?book=753429

4. Кадровая безопасность организации : учебник и практикум для академического бакалавриата / С. В. Духновский. — Москва : Издательство Юрайт, 2019. — 245 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-09266-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/427522

**Дополнительная литература:**

9. Карзаева Н.Н. Основы экономической безопасности : учебник / Н.Н. Карзаева. — М. : ИНФРА-М, 2017. — 275 с. — (Высшее образование: Специалитет). — www.dx.doi.org/10.12737/20854.http://znanium.com/bookread2.php?book=561349

10. Бабковская, В.Н. Розничный персонал от А до Я / В.Н. Бабковская. - 2-е изд. - Москва-Вологда : Инфра-Инженерия, 2016. - 352 с. : ил., табл., схем. - ISBN 978-5-9729-0129-6 ; То же [Электронный ресурс]. - URL://biblioclub.ru/index.php?page=book&id=444426

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

**Интернет-ресурсы**:

9. ЭБС «Университетская библиотека on-line»
10. www. consultant. ru
11. www.qarant. Ru
12. **www.biblioclub.ru**
13. **http://eup.ru/catalog/all-all.asp** – Научно-образовательный портал;
14. **www.wikIsec.ru** – Энциклопедия информационной безопасности. – Публикации, статьи;
15. **http://www.fsb.ru/** – Официальный сайт Федеральной службы безопасности РФ;
16. **http://www.fstec.ru/** – Официальный сайт Федеральной службы по техническому экспортному контролю РФ.

**1)Электронные ресурсы образовательной среды Университета.**

1.Учебный портал с электронно-методическими комплексами(do.kimes)

**2) Информационно-справочные системы:**

**СПС «Консультант Плюс»**

«Гарант» (**garantcenter.ru**);

«Кодекс» (**doskainfo.ru/advert/64804/**);

**3)Электронные ресурсы:**

*2.Университетская библиотека онлайн(www.biblioclub.ru).*

*3.Библиотека диссертаций РГБ(www.diss.ru)*

*4.Polpred.com(www.polpred.com)*

*5.Единое окно доступа(www.window.edu.ru).*

*6.Универсальная библиотека ИстВью(online.ebiblioteka.ru).*

*7.Издательский дом «Гребенников»(htth/grebennikon.ru)/*

## 8. Перечень информационных технологий

**Перечень программного обеспечения:** *MS Office.*

**Информационные справочные системы:**

1. Ресурсы информационно-образовательной среды Технологического Университета.

2. Рабочая программа и методическое обеспечение по дисциплине «Кадровая безопасность».

3. Информационно – справочные (правовые) системы:

– «Гарант» (**garantcenter.ru**);

– «Кодекс» (**doskainfo.ru/advert/64804/**);

– «Консультант +» (**artiks.ru**).