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**

# «СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКОВСКОЙ СФЕРЕ»

**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 Сухотерин А.И. Рабочая программа дисциплины: «Стандарты информационной безопасности в банковской сфере». – 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 фундаментальным проблемам информационной безопасности в условиях становления современного информационного общества.
2. Использование организационно-правовых механизмов обеспечения конституционных прав и свобод граждан в информационной сфере и регламентирующих создание и использование защищённых информационных технологий.
3. Получение первичных навыков в применении защищённых технологий при обеспечении информационной безопасности различных объектов.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

**Общекультурные компетенции:**

- ОК-5: способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики.

**Общепрофессиональные компетенции:**

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

**Профессиональные компетенции:**

- ПК-9: способность осуществлять подбор, изучение и обобщение научно- технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;
- ПК-10: способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности;
- ПК-12: способность организовывать работу малого коллектива исполнителей в профессиональной деятельности;

Основными **задачами** дисциплины являются:

- ознакомление студентов с процессами стандартизации компьютерных информационных систем с точки зрения информационной безопасности;
- ознакомление студентов с нормативно-правовым обеспечением компьютерных информационных систем по защите информации;
- формирование у студентов способности самостоятельно проводить классификацию автоматизированных систем и средств защиты информации по требованиям безопасности;
- формирование студентами предложений по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами.

После завершения освоения данной дисциплины студент должен:

**Знать:**

- законодательные акты в отношении средств защиты информации по требованиям безопасности;
- общепринятую классификацию стандартов в области информационной безопасности;
- международные и отечественные стандарты в области информационной безопасности;
- требования безопасности, предъявляемые к компьютерным информационным системам при обработке информации;
- организацию семейства протоколов TCP/IP технологии программирования распределенных систем, структуры и функции современных операционных систем.

**Уметь:**

- определять соответствие объектов оценки предъявляемым к ним требованиям безопасности;
- пользоваться краткой спецификацией объекта оценки, отвечающего требованиям безопасности;
- применять методы оценки системы ИТ для определения ее свойств безопасности;
- пользоваться методикой логического обоснования требований безопасности

**Владеть:**

- классификацией объектов информатизации по классам защищённости;

- анализом и оценкой уровня защищенности объектов информатизации;
- разработкой заданий по безопасности на основе стандартов информационной безопасности;
- оценкой защищаемой информации и необходимых средств защиты;
- рекомендациями по повышению надежности функционирования информационно-технических средств.

## 2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Стандарты информационной безопасности в банковской сфере» относится к базовой части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01«Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на знаниях школьной программы и ранее изученных дисциплинах: «Документоведение», «Организационное и правовое обеспечение информационной безопасности», «Основы информационной безопасности», «Налоговая система РФ», «Финансовые институты» и компетенциях: ОК-4,5,7, ОПК-4,5,7 и ПК-4,8,9,10,14,15.

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

## 3. Объем дисциплины и виды учебной работы

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

**Таблица1**

| Виды занятий | Всего часов | Семестр 8 | Семестр 9 | Семестр … | Семестр … |
|---|---|---|---|---|---|
| **Общая трудоемкость** | 144 | 144 | 144 | | |
| **ОЧНАЯ ФОРМА ОБУЧЕНИЯ** | | | | | |
| **Аудиторные занятия** | 48 | 48 | | | |
| Лекции (Л) | 12 | 12 | | | |
| Практические занятия (ПЗ) | 36 | 36 | | | |
| Лабораторные работы (ЛР) | - | - | | | |
| **Самостоятельная работа** | 96 | 96 | | | |
| **КСР** | - | - | | | |
| **Курсовые работы (проекты)** | - | - | | | |
| **Расчетно-графические работы** | - | - | | | |
| **Контрольная работа, домашнее задание** | +<br>- | +<br>- | | | |
| **Текущий контроль знаний (7 - 8, 15 - 16 недели)** -2ч | Т1;Т2 | Т1;Т2 | | | |
| **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 | Код компетенций |
|---|---|---|---|---|
| Тема 1. Введение в дисциплину. Общие сведения о стандартах в области информационной безопасности | 2 | 6 | 1 | ОК-5<br>ОПК-4<br>ПК-9<br>ПК-10<br>ПК-12 |
| Тема 2. Международные стандарты информационной безопасности | 2 | 6 | 1 | ОК-5<br>ОПК-4<br>ПК-9<br>ПК-10<br>ПК-12 |
| Тема 3. | 2 | 6 | 1 | ОК-5 |

| | | | | |
|---|---|---|---|---|
| Отечественные стандарты информационной безопасности | | | | ОПК-4<br>ПК-9<br>ПК-10<br>ПК-12 |
| Тема 4. Критерии оценки доверенных компьютерных систем («Оранжевая книга») | 2 | 6 | 1 | ОК-5<br>ОПК-4<br>ПК-9<br>ПК-10<br>ПК-12 |
| Тема 5. Руководящие документы Гостехкомиссии России (ФСТЭК). | 2 | 6 | 1 | ОК-5<br>ОПК-4<br>ПК-9<br>ПК-10<br>ПК-12 |
| Тема 6. Общие критерии | 2 | 6 | 1 | ОК-5<br>ОПК-4<br>ПК-9<br>ПК-10<br>ПК-12 |
| Итого: | 12 | 36 | 6 | |

## 4.2. Содержание тем дисциплины

**Тема 1. Введение в дисциплину**

Общие сведения о стандартах в области информационной безопасности.

Понятие стандарта в области информационной безопасности (ИБ). Обоснование необходимости использования стандартов ИБ. Классификация стандартов ИБ.

**Тема 2. Международные стандарты информационной безопасности**

Стандарты ISO/IEC 17799-2002 (BS 7799-2000). Стандарт ISO/IEC 27001:2005. Модель PDCA. Германский стандарт BSI. Общие критерии безопасности информационных технологий (стандарт ISO 15408-1999). Стандарты для беспроводных сетей. Стандарты в сети Internet.

**Тема 3. Отечественные стандарты информационной безопасности**

Нормативные документы по критериям оценки защищенности средств вычислительной техники (СВТ) и автоматизированных систем (АС). Документы, регулирующие информационную безопасность. Достоинства ГОСТ Р ИСО/МЭК 15408.

**Тема 4. Критерии оценки доверенных компьютерных систем**

(«Оранжевая книга»)

Назначение и структура требований. Группы классов защищенности и их характеристики.

**Тема 5. Руководящие документы ФСТЭК**

Основные положения концепции защиты СВТ и АС от НСД к информации. Защита от НСД к информации в СВТ и АС. Межсетевые экраны. Показатели защищенности. Классификация АС и требования по защите информации. Программное обеспечение средств защиты информации.

**Тема 6. Общие критерии**

Основные положения. Структура и содержание профиля защиты. Структура и содержание задания по безопасности. Функциональные требования безопасности. Требования доверия. Методы оценки. Оценочные уровни доверия.

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

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены 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 «Стандарты информационной безопасности в банковской сфере» приведена в Приложении 1.

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

**Основная литература:**

1. В.А. Галатенко Стандарты информационной безопасности: Учебное пособие .М.: ИНТУИТ,2006
2. Технические средства и методы защиты информации. Учебное пособие для вузов. А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.: под редакцией А.П. Зайцева и А.А. Шелуканова – 4-е издание исправленное и дополненное. - М.: Горячая линия – Телеком, 2012. - 616с.
3. Правовой режим лицензирования и сертификации в сфере информационной безопасности. Учебное пособие. Коваленко Ю.Ю. - М.: Горячая линия – Телеком, 2012. – 140с.
4. Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов. Вопросы управления информационной безопасностью кн. 5. Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия – Телеком, 2012. - 166с.

**Дополнительная литература:**

1. Государственная информационная политика в условиях информационно - психологической войны. – 3-е издание, стереотип. Манойло А.В., Петренко А.И.,

Фролов Д.Б.- М.: Горячая линия – Телеком, 2013. – 542с.

2. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. Учебное пособие. 2008 г. Москва, «Форум».

3. Введение в защиту информации в автоматизированных системах: Учебное пособие для вузов. – 4-е издание, стереотип. Малюк А.А., Пазизин С.В., Погожин Н.С. - М.: Горячая линия – Телеком, 2011. - 146с.

4. Тихонов В. А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты. Учебное пособие. 2006 г. М.: «Гелиос АРВ».

**Рекомендуемая литература:**

1. Указ Президента РФ «Об утверждении Концепции национальной безопасности Российской Федерации» №1300 от 17.12.1997г.

2. Доктрина информационной безопасности Российской Федерации № Пр-1895 от 9.09.2000г.

3. Федеральный закон «О безопасности» №15-ФЗ от 7.03.2005 г.

4. Федеральный закон «Об информации, информационных технологиях и защите информации» №149-ФЗ от 27.07.2006 г.

5. Родичев Ю. Информационная безопасность: нормативно-правовые аспекты. Учебное пособие. 2008 г. СПб, «Питер».

*6.* Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации. Учебное пособие. 2007 г. Москва, «Академия».

**Электронные книги:**

1. Иванов М.А., Чугунов И.В. криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие/ под редакцией М.А. Иванова .М.: НИЯУ МИФИ,2012.

**http://biblioclub.ru/index.php?page=book_view&book_id=231673**

2. В.А. Галатенко Стандарты информационной безопасности: Учебное пособие .М.: ИНТУИТ,2006

**http://www.intuit.ru/goods_store/ebooks/8172**

3. Д.С. Кулябов Защита информации в сетях. Уч. пос.ч1.2004.

**http://telesys.pfu.edu.ru/sites/telesys.pfu.edu.ru/files/imported/studies/book/net-sec-p1.pdf**

4. Международные стандарты по оценке безопасности информационных технологий. Гармонизированные критерии Европейских стран ITSEC.

**http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio/**

5. Андрианов В.В. Обеспечение информационной безопасности бизнеса. 2-е издание, переработанное и дополненное. 2011

**http://fanread.ru/book/8496757/?page=1**

6. Блинов А.М. Информационная безопасность:Учебное пособие. Часть1.-СПб.:Изд-во СПГУЭФ,2010.
**http://elibrary.unecon.ru/materials_files/341423666.pdf**
7. Скотт Бармен. Разработка правил информационной безопасности. Учебное пособи: Изд-во: Вильямс. 2002
**http://bookimir.ru/loads/kompyuteryiinternet/aznoe37/501266-razrabotka-pravil-informacionnoy-bezopasnosti-skott-barmen.html**

## 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. **http://informika.ru/** – образовательный портал.
3. **www.wikIsec.ru** - Энциклопедия информационной безопасности. – Публикации, статьи.
4. **www.biblioclub.ru** - Универсальная библиотека онлайн.
5. **www.rucont.ru** - ЭБС «Руконт».
6. **http://www.academy.it.ru/ –** академия АЙТИ.
7. **http://www.minfin.ru** - Официальный сайт Министерства финансов Российской Федерации
8. **http://www.gov.ru/** - Официальный сервер органов государственной власти Российской Федерации**.**
9. **http://www.fsb.ru/ -** Официальный сайт Федеральной Службы Безопасности
10. **http://www.fstec.ru/** - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

## 9. Методические указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины (модуля) приведены в Приложении 2 к настоящей рабочей программе.

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

- **Перечень программного обеспечения:** MSOffice.

- **Информационные справочные системы:**

1. Ресурсы информационно-образовательной среды МГОТУ.
2. Рабочая программа и методическое обеспечение по дисциплине: «Стандарты информационной безопасности в банковской сфере»

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

**Лекционные занятия**:

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

**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 MSOffice 7;
- 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

# «СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКОВСКОЙ СФЕРЕ»

**(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 компе-тенции | 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. | ОК-5 | способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики | Темы 1, 2,3, 4, 5,6 | законодательные акты в отношении средств защиты информации по требованиям безопасности; | определять соответствие объектов оценки предъявляемым к ним требованиям безопасности; | классификацией объектов информатизации по классам защищённости; |
| 2. | ОПК-4 | способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации | Темы 1,2,3, 4, 5,6 | общепринятую классификацию стандартов в области информационной безопасности; | пользоваться краткой спецификацией объекта оценки, отвечающего требованиям безопасности; | анализом и оценкой уровня защищенности объектов информатизации; |
| 3. | ПК-9 | способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор | Темы 1, 2,3, 4, 5,6 | международные и отечественные стандарты в области информационной безопасности; | применять методы оценки системы ИТ для определения ее свойств безопасности; | разработкой заданий по безопасности на основе стандартов информационной безопасности; |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности | | | | |
| 4. | ПК-10 | способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности | Темы 1, 2,3, 4, 5,6 | требования безопасности, предъявляемые к компьютерным информационным системам при обработке информации; | пользоваться методикой логического обоснования требований безопасности; | оценкой защищаемой информации и необходимых средств защиты; |
| 5. | ПК-12 | способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности | Темы 1, 2,3, 4, 5,6 | организацию семейства протоколов TCP/IP технологии программирования распределенных систем, структуры и функции современных операционных систем. | пользоваться краткой спецификацией объекта оценки, отвечающего требованиям безопасности; | рекомендациями по повышению надежности функционирования информационно-технических средств; |

## 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 |
|---|---|---|---|
| ОК-5 | Доклад в форме презентации | A) полностью сформирована<br>**5 баллов**<br>B) частично сформирована<br>**3-4 балла**<br>C) 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 непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал. |
| ОПК-4 | Доклад в форме презентации | A) полностью сформирована<br>**5 баллов**<br>B) частично сформирована<br>**3-4 балла**<br>C) 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). |

| | | | |
|---|---|---|---|
| | | | Максимальная сумма баллов - 5 баллов.<br>Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал. |
| ПК-9 | 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 непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал. |

| | | | |
|---|---|---|---|
| ПК-10 | Контрольная работа | А) полностью сформирована<br>**5 баллов**<br>В) частично сформирована<br>**3-4 балла**<br>С) не сформирована<br>**2 балла** | Проводится письменно 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 непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал. |
| ПК-12 | 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 непосредственно в день |

| | | | |
|---|---|---|---|
| | | | проведения презентации – 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. Предназначение стандартов информационной безопасности (ИБ), необходимость их использования.
2. Общие критерии безопасности информационных технологий (стандарт ISO 15408).
3. Взаимосвязь между общими критериями и общей методологией оценки.
4. Структура технического отчета об оценке.
5. Стандарты для беспроводных сетей.
6. Стандарты в сети Internet.
7. Отечественные стандарты безопасности информационных технологий.
8. Нормативные документы по критериям оценки защищенности средств вычислительной техники (СВТ) и автоматизированных систем (АС).
9. Документы, регулирующие информационную безопасность. Достоинства ГОСТ Р ИСО/МЭК 15408 - 2002.
10. Структура функционального класса.
11. Структура функционального семейства.
12. Общая схема представления класса.
13. Структура функционального компонента.
14. Критерии оценки доверенных компьютерных систем («Оранжевая книга»). Назначение и структура требований.
15. Группы классов защищенности и их характеристики.
16. Руководящие документы Гостехкомиссии России (ФСТЭК).
17. Межсетевые экраны. Показатели защищенности.
18. Классификация АС и требования по защите информации.
19. Программное обеспечение средств защиты информации.
20. Общие критерии. Основные положения.
21. Структура и содержание профиля защиты.
22. Структура и содержание задания по безопасности.
23. Функциональные требования безопасности.
24. Требования доверия. Методы оценки. Оценочные уровни доверия.
25. Основные положения концепции защиты СВТ и АС от НСД к информации
26. Средства вычислительной техники. Защита от НСД к информации. Показатели защищённости от НСД к информации

27. Автоматизированные системы. Защита от НСД к информации. Классификация. АС и требования по защите информации

28. ISO/IEC 17799:2005

29. ISO/IEC 27001:2005

30. BS 7799-3:2006

**Примерная тематика заданий на контрольную работу:**

1. Сформулировать функциональные требования по безопасности к СВТ типового выделенного помещения органа муниципального управления.
2. Сформулировать функциональные требования по безопасности к СВТ типового выделенного помещения высшего учебного заведения.
3. Сформулировать функциональные требования по безопасности к СВТ и АС типовой туристической фирмы.
4. Сформулировать функциональные требования по безопасности к СВТ и АС выделенного помещения типового машиностроительного предприятия.
5. Сформулировать функциональные требования по безопасности к СВТ выделенного помещения типового торгового предприятия.
6. Построить профиль защиты для объекта оценки типового органа муниципального управления.
7. Построить профиль защиты для объекта оценки типового высшего учебного заведения.
8. Построить профиль защиты для объекта оценки типовой туристической фирмы.
9. Построить профиль защиты для объекта оценки типового машиностроительного предприятия.
10. Построить профиль защиты для объекта оценки типового торгового предприятия.
11. Разработать задание по безопасности и меры доверия для объекта оценки типового органа муниципального управления.
12. Разработать задание по безопасности и меры доверия для объекта оценки типового высшего учебного заведения.
13. Разработать задание по безопасности и меры доверия для объекта оценки типовой туристической фирмы.
14. Разработать задание по безопасности и меры доверия для объекта оценки типового торгового предприятия.
15. Разработать задание по безопасности и меры доверия для объекта оценки типового машиностроительного предприятия.
16. Разработать требования доверия для объекта оценки типового органа муниципального управления.
17. Разработать требования доверия для объекта оценки типового высшего учебного заведения.
18. Разработать требования доверия для объекта оценки типовой туристической фирмы.

19. Разработать требования доверия для объекта оценки типового торгового предприятия.

20. Разработать требования доверия для объекта оценки типового машиностроительного предприятия.

21. Произвести оценку по классам защищённости СВТ и АС типового органа муниципального управления.

22. Произвести оценку по классам защищённости СВТ и АС типового высшего учебного заведения.

23. Произвести оценку по классам защищённости СВТ и АС типовой туристической фирмы.

24. Произвести оценку по классам защищённости СВТ и АС типового торгового предприятия.

25. Произвести оценку по классам защищённости СВТ и АС типового машиностроительного предприятия.

26. Разработать модель управления рисками типового органа муниципального управления.

27. Разработать модель управления рисками типового высшего учебного заведения.

28. Разработать модель управления рисками типовой туристической фирмы.

29. Разработать модель управления рисками типового торгового предприятия.

30. Разработать модель управления рисками типового машиностроительного предприятия.

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

Формой контроля знаний по дисциплине «Стандарты информационной безопасности в банковской сфере» являются две текущие аттестации в виде тестов и 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 | ОК-5<br>ОПК-4<br>ПК-9<br>ПК-10<br>ПК-12 | 20-40 вопросов | Компьютерное тестирование ; время отведенное на процедуру - 30 минут | Результаты тестирования предоставляются в день проведения процедуры | Критерии оценки определяются процентным соотношением.<br>Не явка -<br>Удовлетворительно - от 51% правильных ответов.<br>Хорошо - от 70%.<br>Отлично – от 90%. |
| Согласно учебному плану | тестирование | ОК-5<br>ОПК-4<br>ПК-9<br>ПК-10<br>ПК-12 | 20 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. |
| Согласно учебному плану | Экзамен | ОК-5<br>ОПК-4<br>ПК-9<br>ПК-10<br>ПК-12 | 3 теоретических вопроса + практическое задание | Экзамен проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 40 минут. | Результаты предоставляются в день проведения экзамена | 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; |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | • ответ на вопросы билета.<br>«**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 вопросы билета<br>• неправильно решено практическое задание<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><br>«**Неудовлетвори-тельно**»:<br>• демонстр |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | ирует 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. |

### 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 вариант ответа.

**1. Чем вызвана необходимость решения задачи стандартизации ИТ ?**

– правовыми аспектами

- совершенствованием процесса производства ИТ

– обеспечением совместимости продуктов и систем

**2. Какие стандарты ИБ относят к спецификации?**

– общие критерии

– управленческие стандарты

– руководящие документы ФСТЭК

**3. Какой стандарт является обязательным для применения в СЗИ ?**

– ГОСТ 28147-89

– ГОСТ Р ИСО/МЭК 15408-2002

– ISO 17799-2005

**4. Какие стандарты применяются при проведении сертификации средств защиты, предназначенных для работы с информацией, относящейся к гостайне ?**

– руководящие документы ФСТЭК

– ГОСТ 3411-2004

– ISO 27001-2005

**5. Чем должна определяться возможность доступа субъектов к объектам?**

– на основании распоряжений руководства организации

– на основании их идентификации и набора правил управления доступом

– на основании уровня конфиденциальности информации

**6. От чего должны быть защищены все средства защиты ?**

– сбоев в работе программного обеспечения

– от вирусов

– от несанкционированного вмешательства и отключения

**7. Требуемый уровень защищённости системы возрастает?**

– от группы **A** к группе **D**

– от группы **D** к группе **A**

– с уменьшением номера класса в пределах одной группы

**8. Что понимается под несанкционированным доступом (НСД) ?**

– доступ к информации, нарушающий установленные правила разграничения

– доступ к информации с использованием специальных программ

– доступ к информации с использованием нештатных СВТ

**9. Какой субъект рассматривается в качестве нарушителя согласно РД ФСТЭК?**

– не имеющий доступ к работе со штатными средствами АС и СВТ

– имеющий доступ к работе со штатными средствами АС и СВТ

– любой субъект, нарушающий правила разграничения доступа

**10. Какой документ оформляется по результатам успешных испытаний СВТ и АС ?**

– сертификат

– протокол проведения испытаний

– экспертное заключение

**11. Какое количество групп и классов защищённости СВТ от НСД устанавливается в соответствии с РД ФСТЭК ?**

– 8 классов защищённости, разбитые на 2 группы

– 3 группы, разбитые на 7 классов защищённости

– 7 классов защищённости, разбитые на 4 группы

**12. Какое количество групп и классов защищённости АС от НСД устанавливается в соответствии с РД ФСТЭК ?**

– 9 классов защищённости, разбитые на 3 группы

– 7 классов защищённости, разбитые на 5 групп

– 4 группы, разбитые на 6 классов защищённости

**13. С помощью чего осуществляется реализация СУИБ ?**

– на основании применения необходимых механизмов безопасности

– на основании политики безопасности

– на основании внедрения 4-х фазной модели PDCA

**14. В каком международном стандарте описывается процесс оценки рисков?**

– в Германском стандарте BSI

– в Британском стандарте BS 7799-3:2006

– в стандарте ISO/IEC 15408-1999

**15. Какой протокол используются для управления доступом в беспроводную сеть ?**

– IPSec

– SSL

– MAC

**16. Какой метод используется в качестве базовой технологии в стандарте IEEE 802.11b ?**

– метод частотного мультиплексирования OFDM

– метод распределённого спектра с прямой последовательностью DSSS

– алгоритм RC4

**17. Что представляет собой протокол WEP ?**

– протокол безопасных электронных транзакций

– протокол расширенной аутентификации

– протокол шифрования

**18. Что такое функциональный элемент ?**

– имя класса

– характеристика семейства

– наименьшее функциональное требование безопасности

**19. Что обозначает запись *FDP_IFF A.2* ?**

– спецификацию продукта

– идентификационный код

– краткую форму имени функционального элемента

**20. Что определяет краткая спецификация объекта ?**

– структуру и содержание задания по безопасности

– профиль защиты оцениваемого объекта

– отображение требований безопасности для объекта оценки

**21. Что такое «характеристика семейства» ?**

– оценка продукта или системы

– каталог функциональных требований

– описание функционального семейства, в котором излагаются его цели безопасности и общее описание функциональных требований

**22. Сколько семейств доверия содержит класс доверия?**

– не более шести

– по меньшей мере, одно семейство доверия

– не менее трёх

**23. Сколько оценочных уровней доверия определено ГОСТ Р ИСО/МЭК 15408-2002?**

– 6

– 4

– семь

## 4.2. Типовые вопросы, выносимые на экзамен

1. Предназначение стандартов информационной безопасности (ИБ), необходимость их использования.
2. Классификация стандартов ИБ.
3. Международные стандарты ИБ.
4. Стандарт ISO/IEC 27001:2005. Модель PDCA.
5. Стандарт ISO/IEC 17799:2002 (BS7799:2000). Модель управления рисками.
6. Германский стандарт BSI.
7. Общие критерии безопасности информационных технологий (стандарт ISO 15408).
8. Взаимосвязь между общими критериями и общей методологией оценки.
9. Структура технического отчета об оценке.
10. Стандарты для беспроводных сетей.
11. Стандарты в сети Internet.
12. Отечественные стандарты безопасности информационных технологий.
13. Нормативные документы по критериям оценки защищенности средств вычислительной техники (СВТ) и автоматизированных систем (АС).
14. Документы, регулирующие информационную безопасность. Достоинства ГОСТ Р ИСО/МЭК 15408 - 2002.
15. Структура функционального класса.
16. Структура функционального семейства.
17. Общая схема представления класса.
18. Структура функционального компонента.
19. Критерии оценки доверенных компьютерных систем («Оранжевая книга»). Назначение и структура требований.
20. Группы классов защищенности и их характеристики.
21. Руководящие документы Гостехкомиссии России (ФСТЭК).
22. Несанкционированный доступ (НСД). Способы НСД. Классификация нарушителей.
23. Межсетевые экраны. Показатели защищенности.
24. Классификация АС и требования по защите информации.
25. Программное обеспечение средств защиты информации.
26. Общие критерии. Основные положения.

27. Структура и содержание профиля защиты.
28. Структура и содержание задания по безопасности.
29. Функциональные требования безопасности.
30. Требования доверия. Методы оценки. Оценочные уровни доверия.

**Приложение 2**

*ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ*

*ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ*

*КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

# МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

# «СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКОВСКОЙ СФЕРЕ»

**(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

**Целью изучения дисциплины является:**

1. Формирование у студентов специализированной базы знаний по фундаментальным проблемам информационной безопасности в условиях становления современного информационного общества.
2. Использование организационно-правовых механизмов обеспечения конституционных прав и свобод граждан в информационной сфере и регламентирующих создание и использование защищённых информационных технологий.
3. Получение первичных навыков в применении защищённых технологий при обеспечении информационной безопасности различных объектов.

**Задачи дисциплины:**

- ознакомление студентов с процессами стандартизации компьютерных информационных систем с точки зрения информационной безопасности;
- ознакомление студентов с нормативно-правовым обеспечением компьютерных информационных систем по защите информации;
- формирование у студентов способности самостоятельно проводить классификацию автоматизированных систем и средств защиты информации по требованиям безопасности;
- формирование студентами предложений по совершенствованию, модернизации, унификации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами.

## 2. Указания по проведению практических занятий

### Тема 1: Введение в дисциплину. Общие сведения о стандартах в области информационной безопасности

**Практическое занятие 1**.

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

Тема и содержание практического занятия:

*Цель работы*: Ознакомиться с основными понятиями дисциплины и общими положениями о стандартах в области информационной безопасности

*Основные положения темы занятия*:

1. Общие сведения.
2. Классификация стандартов в области информационной безопасности.

*Вопросы для обсуждения:*

Основной доклад (реферат) по теме занятия.

1. Предназначение стандартов информационной безопасности (ИБ), необходимость их использования.

2. Взаимосвязь между общими критериями и общей методологией оценки.
3. Структура технического отчета об оценке.
Продолжительность занятия – 6 ч.

**Тема 2: Международные стандарты информационной безопасности**

**Практическое занятие 2.**

Вид практического занятия**:** *смешанная форма практического занятия.*
Тема и содержание практического занятия:
*Цель работы*: Ознакомиться с международными стандартами в области информационной безопасности

*Основные положения темы занятия*:
1. Перечень международных стандартов ИБ.
2. Функции международных стандартов ИБ.

*Вопросы для обсуждения:*
Основной доклад (реферат) по теме занятия.

1. ISO/IEC 17799:2005
2. ISO/IEC 27001:2005
3. BS 7799-3:2006

Продолжительность занятия – 6 ч.

**Тема 3: Отечественные стандарты информационной безопасности**

**Практическое занятие 3.**

Вид практического занятия**:** *смешанная форма практического занятия.*
Тема и содержание практического занятия:
*Цель работы*: Ознакомиться с российскими стандартами в области информационной безопасности.

*Основные положения темы занятия*:
1. Перечень российских стандартов ИБ.
2. Функции российских стандартов ИБ.

*Вопросы для обсуждения:*
Основной доклад (реферат) по теме занятия.
1.Основополагающий государственный стандарт Российской Федерации в области защиты информации.
2.Руководящие документы ФСТЭК России.
Продолжительность занятия – 6 ч.

**Тема 4: Критерии оценки доверенных компьютерных систем («Оранжевая книга»)**

**Практическое занятие 4.**

Вид практического занятия**:** *смешанная форма практического занятия.*
Тема и содержание практического занятия:

*Цель работы*: Получить базовые знания о стандарте **«Критерии оценки доверенных компьютерных систем».**

*Основные положения темы занятия*:

1. Общее понятие стандарта.
2. Требования и функции «Оранжевой книги».

*Вопросы для обсуждения:*

Основной доклад (реферат) по теме занятия.

1. Основные положения оранжевой книги
2. Механизмы безопасности
3. Классы безопасности

Продолжительность занятия – 6 ч.

## Тема 5: Руководящие документы Гостехкомиссии России (ФСТЭК)
## Практическое занятие 5.

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

Тема и содержание практического занятия:

*Цель работы*: Получить представление об основных документах ФСТЭК России.

*Основные положения темы занятия*:

1. Ознакомиться с классификацией автоматизированных систем по уровню защищенности от несанкционированного доступа
2. Ознакомиться с классификацией межсетевых экранов по уровню защищенности от несанкционированного доступа

*Вопросы для обсуждения:*

Основной доклад (реферат) по теме занятия.

1. Классификация автоматизированных систем по уровню защищенности от несанкционированного доступа
2. Классификация межсетевых экранов по уровню защищенности от несанкционированного доступа

Продолжительность занятия – 6 ч.

## Тема 6: Общие критерии безопасности информационных технологий
## Практическое занятие 6.

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

Тема и содержание практического занятия:

*Цель работы*: Получить практические навыки в формировании и построении защищенной системы электронного документооборота в кредитно-финансовой организации.

*Основные положения темы занятия*:

1. Общее понятие стандарта
2. Требования и функции Общих критериев.

*Вопросы для обсуждения:*

Основной доклад (реферат) по теме занятия.

1. Основные положения Общих критериев

2. Механизмы безопасности
3. Классы безопасности.
Продолжительность занятия – 6 ч.

## 4. Указания по проведению самостоятельной работы студентов

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

*Задачи самостоятельной работы*:

1) расширить представление в области стандартов информационной безопасности;

2) привить навыки самостоятельного решения задач в области стандартизации и следования стандартам систем информационной безопасности.

Объем 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 | 20 |
| Подготовка к практическим занятиям | 32 |
| Подготовка к лабораторным занятиям | - |
| Подготовка докладов | 12 |
| Выполнение практических заданий | 32 |

**Вопросы, выносимые на самостоятельное изучение:**

1. Предназначение стандартов информационной безопасности (ИБ), необходимость их использования.
2. Общие критерии безопасности информационных технологий (стандарт ISO 15408).
3. Взаимосвязь между общими критериями и общей методологией оценки.
4. Структура технического отчета об оценке.
5. Стандарты для беспроводных сетей.
6. Стандарты в сети Internet.
7. Отечественные стандарты безопасности информационных технологий.
8. Нормативные документы по критериям оценки защищенности средств вычислительной техники (СВТ) и автоматизированных систем (АС).
9. Документы, регулирующие информационную безопасность. Достоинства ГОСТ Р ИСО/МЭК 15408 - 2002.
10. Структура функционального класса.

11. Структура функционального семейства.
12. Общая схема представления класса.
13. Структура функционального компонента.
14. Критерии оценки доверенных компьютерных систем («Оранжевая книга»). Назначение и структура требований.
15. Группы классов защищенности и их характеристики.
16. Руководящие документы Гостехкомиссии России (ФСТЭК).
17. Межсетевые экраны. Показатели защищенности.
18. Классификация АС и требования по защите информации.
19. Программное обеспечение средств защиты информации.
20. Общие критерии. Основные положения.
21. Структура и содержание профиля защиты.
22. Структура и содержание задания по безопасности.
23. Функциональные требования безопасности.
24. Требования доверия. Методы оценки. Оценочные уровни доверия.
25. Основные положения концепции защиты СВТ и АС от НСД к информации
26. Средства вычислительной техники. Защита от НСД к информации. Показатели защищённости от НСД к информации
27. Автоматизированные системы. Защита от НСД к информации. Классификация. АС и требования по защите информации
28. ISO/IEC 17799:2005
29. ISO/IEC 27001:2005
30. BS 7799-3:2006

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 | 20 | Изучение открытых источников |
| 2. | Подготовка к практическим занятиям | 32 | Изучение открытых источников при подготовке доклада на выбранную тему. |
| 3. | Подготовка к лабораторным занятиям | - | Изучение открытых источников |
| 4. | Тематика докладов | 12 | см. примерные темы докладов |
| 5. | Выполнение практических заданий | 32 | |

## Примерные темы докладов

1. Предназначение стандартов информационной безопасности (ИБ), необходимость их использования.
2. Общие критерии безопасности информационных технологий (стандарт ISO 15408).
3. Взаимосвязь между общими критериями и общей методологией оценки.
4. Структура технического отчета об оценке.
5. Стандарты для беспроводных сетей.
6. Стандарты в сети Internet.
7. Отечественные стандарты безопасности информационных технологий.
8. Нормативные документы по критериям оценки защищенности средств вычислительной техники (СВТ) и автоматизированных систем (АС).
9. Документы, регулирующие информационную безопасность. Достоинства ГОСТ Р ИСО/МЭК 15408 - 2002.
10. Структура функционального класса.
11. Структура функционального семейства.
12. Общая схема представления класса.
13. Структура функционального компонента.
14. Критерии оценки доверенных компьютерных систем («Оранжевая книга»). Назначение и структура требований.
15. Группы классов защищенности и их характеристики.
16. Руководящие документы Гостехкомиссии России (ФСТЭК).
17. Межсетевые экраны. Показатели защищенности.
18. Классификация АС и требования по защите информации.
19. Программное обеспечение средств защиты информации.
20. Общие критерии. Основные положения.
21. Структура и содержание профиля защиты.
22. Структура и содержание задания по безопасности.
23. Функциональные требования безопасности.
24. Требования доверия. Методы оценки. Оценочные уровни доверия.
25. Основные положения концепции защиты СВТ и АС от НСД к информации
26. Средства вычислительной техники. Защита от НСД к информации. Показатели защищённости от НСД к информации
27. Автоматизированные системы. Защита от НСД к информации. Классификация. АС и требования по защите информации
28. ISO/IEC 17799:2005
29. ISO/IEC 27001:2005
30. BS 7799-3:2006

## 5. Указания по проведению контрольных работ для студентов факультета заочного обучения

Не предусмотрены учебным планом.

## 6. Перечень основной и дополнительной учебной литературы

**Основная литература:**

1. В.А. Галатенко Стандарты информационной безопасности: Учебное пособие .М.: ИНТУИТ,2006
2. Технические средства и методы защиты информации. Учебное пособие для вузов. А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.: под редакцией А.П. Зайцева и А.А. Шелуканова – 4-е издание исправленное и дополненное. - М.: Горячая линия – Телеком, 2012. - 616с.
3. Правовой режим лицензирования и сертификации в сфере информационной безопасности. Учебное пособие. Коваленко Ю.Ю. - М.: Горячая линия – Телеком, 2012. – 140с.
4. Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов. Вопросы управления информационной безопасностью кн. 5. Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия – Телеком, 2012. - 166с.

**Дополнительная литература:**

1. Государственная информационная политика в условиях информационно - психологической войны. – 3-е издание, стереотип. Манойло А.В., Петренко А.И., Фролов Д.Б.- М.: Горячая линия – Телеком, 2013. – 542с.
2. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. Учебное пособие. 2008 г. Москва, «Форум».
3. Введение в защиту информации в автоматизированных системах: Учебное пособие для вузов. – 4-е издание, стереотип. Малюк А.А., Пазизин С.В., Погожин Н.С. - М.: Горячая линия – Телеком, 2011. - 146с.
4. Тихонов В. А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты. Учебное пособие. 2006 г. М.: «Гелиос АРВ».

**Рекомендуемая литература:**

1. Указ Президента РФ «Об утверждении Концепции национальной безопасности Российской Федерации» №1300 от 17.12.1997г.
2. Доктрина информационной безопасности Российской Федерации № Пр-1895 от 9.09.2000г.
3. Федеральный закон «О безопасности» №15-ФЗ от 7.03.2005 г.

4. Федеральный закон «Об информации, информационных технологиях и защите информации» №149-ФЗ от 27.07.2006 г.
5. Родичев Ю. Информационная безопасность: нормативно-правовые аспекты. Учебное пособие. 2008 г. СПб, «Питер».
6. Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации. Учебное пособие. 2007 г. Москва, «Академия».

**Электронные книги:**

1. Иванов М.А., Чугунов И.В. криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие/ под редакцией М.А. Иванова .М.: НИЯУ МИФИ,2012.
**http://biblioclub.ru/index.php?page=book_view&book_id=231673**
2. В.А. Галатенко Стандарты информационной безопасности: Учебное пособие .М.: ИНТУИТ,2006
**http://www.intuit.ru/goods_store/ebooks/8172**
3. Д.С. Кулябов Защита информации в сетях. Уч. пос.ч1.2004.
**http://telesys.pfu.edu.ru/sites/telesys.pfu.edu.ru/files/imported/studies/book/net-sec-p1.pdf**
4. Международные стандарты по оценке безопасности информационных технологий. Гармонизированные критерии Европейских стран ITSEC.
**http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio/**
5. Андрианов В.В. Обеспечение информационной безопасности бизнеса. 2-е издание, переработанное и дополненное. 2011
**http://fanread.ru/book/8496757/?page=1**
6. Блинов А.М. Информационная безопасность:Учебное пособие. Часть1.-СПб.:Изд-во СПГУЭФ,2010.
**http://elibrary.unecon.ru/materials_files/341423666.pdf**
7. Скотт Бармен. Разработка правил информационной безопасности. Учебное пособи: Изд-во: Вильямс. 2002
**http://bookimir.ru/loads/kompyuteryiinternet/aznoe37/501266-razrabotka-pravil-informacionnoy-bezopasnosti-skott-barmen.html**

## 7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

**Интернет-ресурсы**:

1. http://eup.ru/catalog/all-all.asp – научно-образовательный портал.
2. http://informika.ru/ – образовательный портал.
3. www.wikIsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.
4. **www.biblioclub.ru** - Универсальная библиотека онлайн.

5. **www.rucont.ru** - ЭБС «Руконт».
6. http://www.academy.it.ru/ - академия АЙТИ.
7. http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации
8. http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации.
9. http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности
10. http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному контролю

## 8. Перечень информационных технологий

**Перечень программного обеспечения:** MSOffice, PowerPoint.
**Информационные справочные системы:**
1. Ресурсы информационно-образовательной среды «МГОТУ».
2. Рабочая программа и методическое обеспечение по дисциплине: «Стандарты информационной безопасности в банковской сфере».