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**

# «ЗАЩИЩЕННЫЕ ЭЛЕКТРОННЫЕ ТЕХНОЛОГИИ БАНКА»

**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: «Защищенные электронные технологии банка». – 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. Ускоренная адаптация студентов в предметную область информационная безопасность, опираясь на весь спектр научных воззрений, на развитие и защиту информационно - телекоммуникационной инфраструктуры и компьютерной информации в кредитно – финансовой сфере;
2. Повысить уровень специальных знаний, которые необходимых обучающимся для высоко профессиональной деятельности во всех сферах информационной безопасности с учетом требований высшей школы, для активизации их учебной и исследовательской деятельности;
3. Формирование у студентов специализированной базы знаний по основным понятиям в области информационной безопасности банковской деятельности;
4. Приобретение студентами первичных навыков по практическому формированию комплекса документов, составляющих правовую базу защиты информации в банковской сфере.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

**Общепрофессиональные компетенции**

- ОПК-2: способность применять соответствующий математический аппарат для решения профессиональных задач;
- ОПК-4: способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.

**Профессиональные компетенции**

- ПК-7: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений;
- ПК-11: способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов.

**Профессионально - специализированные компетенции:**

- ПСК-3: способность участвовать в разработке информационно-аналитических систем финансового мониторинга.

Основными **задачами** дисциплины являются:

- ознакомить студентов с задачами в области безопасности банковской деятельности на основе действующего российского законодательства;
- научить студентов самостоятельно решать поставленные задачи в области защиты информации в банках по базовым направлениям защиты банковской тайны и конфиденциальной информации;
- формировать систему знаний у обучающихся в области защиты информации в кредитно финансовой сфере деятельности.
- изучить основы организации противодействия угрозам информационной безопасности в кредитно – финансовой сфере;
- ознакомить с системным описанием внешних угроз безопасности кредитно – финансовой деятельности, правовых и организационных основ противодействия им, а также техники обеспечения безопасности кредитно – финансовой организации;
- ознакомить с методами и средствами защиты информации банковских инструментов и технологий функциональных и контролирующих подразделений финансово – кредитных организаций.

После завершения освоения данной дисциплины студент должен:

**Знать:**

- методику выявления и анализа потенциально существующих угроз безопасности информации в банке;
- методы анализа и оценки рисков в результате утечки сведений конфиденциального характера в банке;
- порядок организации работы по обеспечению сохранности сведений, составляющих конфиденциальный характер в банке;
- основные положения законодательства РФ по защите государственной и коммерческой тайны в банке;
- меры и условия по обеспечению охраны конфиденциальности информации в банке;
- основы применения специальных аналитических технологий для выявления и предупреждения противоправных посягательств в банке;
- алгоритм подготовки типовых рекомендации по сохранности сведений конфиденциального характера для руководства банком.

**Уметь:**

- использовать в практической деятельности знания по безопасности банковской деятельности;

- анализировать и составлять основные правовые акты и осуществлять правовую оценку информации, используемых в профессиональной деятельности, предпринимать необходимые меры по восстановлению нарушенных прав;
- пользоваться нормативными документами по защите информации в банковской сфере деятельности.

**Владеть:**

- правилами хранения и обращения с документами, содержащими сведения конфиденциального характера, описанием потенциально уязвимых мест со стороны криминальных угроз и иных рисков, системному представлению угроз в банке;
- основными понятиями, раскрывающими содержание предметной области;
- организацией информационной безопасности в банке;
- базовыми положениями по организации защиты информации в банке.

## 2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Защищенные электронные технологии банка» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность», профиль: «Информационно-аналитические системы финансового мониторинга».

Дисциплина реализуется кафедрой информационной безопасности.

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОК-5,6, ОПК-2,4,6 и ПК-4,14.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Мониторинг рынка страхования», 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 3 зачетные единицы, 108 часов.

**Таблица1**

| Виды занятий | Всего часов | Семестр 5 | Семестр 6 | 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) | - | - | | | |
| **Самостоятельная работа** | 76 | 76 | | | |
| **КСР** | - | - | | | |
| **Курсовые работы (проекты)** | - | - | | | |
| **Расчетно-графические работы** | - | - | | | |
| **Контрольная работа, домашнее задание** | + | + | | | |
| **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 |
|---|---|---|---|---|
| Раздел I. Основы информационной безопасности банковской деятельности | | | | |
| Тема 1. Концептуальные основы информационной безопасности банка | 1 | 1 | 1 | ОПК-2,4; ПК-7,11; ПСК-3 |
| Тема 2. Правовые основы информационной безопасности банка | 1 | 1 | 1 | ОПК-2,4; ПК-7,11; ПСК-3 |
| Тема 3. Стандарты информационной безопасности банка | 1 | 1 | 1 | ОПК-2,4; ПК-7,11; ПСК-3 |

| | | | | |
|---|---|---|---|---|
| Тема 4. Организационные основы информационной безопасности банка | 1 | 1 | 1 | ОПК-2,4; ПК-7,11; ПСК-3 |
| Тема 5. Техника обеспечения информационной безопасности банка | 2 | 2 | 1 | ОПК-2,4; ПК-7,11; ПСК-3 |
| Тема 6. Защита от информационных преступлений, посягающих на собственность банка | 2 | 2 | 1 | ОПК-2,4; ПК-7,11; ПСК-3 |
| Раздел II. Технологии защиты информации в банковской деятельности | | | | |
| Тема 7. Защита от хищения денежных средств и иного имущества с использованием векселей (информационный аспект) | 2 | 2 | 1 | ОПК-2,4; ПК-7,11; ПСК-3 |
| Тема 8. Защита от информационных преступлений, посягающих на информационную безопасность функционирования банка | 2 | 2 | 1 | ОПК-2,4; ПК-7,11; ПСК-3 |
| Тема 9. Организация противодействия отмыванию преступных доходов и финансированию терроризма (информационный аспект) | 2 | 2 | 2 | ОПК-2,4; ПК-7,11; ПСК-3 |
| Тема 10. Комплексное обеспечение информационной безопасности | 2 | 2 | 2 | ОПК-2,4; ПК-7,11; ПСК-3 |

| | | | | |
|---|---|---|---|---|
| банка | | | | |
| Итого: | 16 | 16 | 12 | |

## 4.2. Содержание тем дисциплины

### Раздел I. Основы информационной безопасности банковской деятельности

**Тема 1. Концептуальные основы безопасности банка**

Понятия и концепция безопасности банка. Банк как объект противоправных посягательств. Система угроз безопасности банка. Банк как субъект борьбы с противоправными посягательствами.

**Тема 2. Правовые основы информационной безопасности банка**

Система правового обеспечения безопасности банка. Правовые акты общего действия, обеспечивающие безопасность банков методами охранительного содержания. Банковское законодательство. Нормативные акты Банка России. Внутренние нормативные акты. Содержание аудита по ИБ технических средств обработки информации.

**Тема 3. Стандарты информационной безопасности банка**

О Стандарте Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения.

Основные цели и задачи стандарта Банка России при обеспечении информационной безопасности.

Основные направления работы по дальнейшему сопровождению и доработке Стандарта в рамках специально созданного Подкомитетом 3 “Защита информации в кредитно-финансовой сфере” Технического комитета 362 “Защита информации” Федерального агентства по техническому регулированию и метрологии.

Аудит информационной безопасности банка.

Преимущества и недостатки выполнения работ по защите ПДн в рамках Стандарт Банка России СТО БР ИББС 1.0-2006.

Система технических средств безопасности банка. Технические средства охраны. Технические средства охраны банковских операций и продуктов. Технико – криминалистические средства.

**Тема 4. Организационные основы информационной безопасности банка**

Организация системы безопасности банка. Субъекты обеспечения безопасности банка. Средства и методы обеспечения безопасности банка. Организация внутреннего контроля банка. Организация службы безопасности банка.

**Тема 5. Техника обеспечения информационной безопасности банка**

Система технических средств безопасности банка. Технические средства охраны. Технические средства охраны банковских операций и

продуктов. Технико – криминалистические средства.

**Тема 6. Защита от информационных преступлений, посягающих на собственность банка**

Хищения денежных средств, при совершении кредитных операций. Хищения денежных средств с незаконным использованием пластиковых карт. Хищения денежных средств с использованием аккредитивов. Хищение денежных средств с использованием чеков. Хищение денежных средств с использованием платежных поручений.

## Раздел II. Технологии защиты информации в банковской деятельности

**Тема 7. Защита от хищения денежных средств и иного имущества с использованием векселей (информационный аспект)**

Правовая характеристика векселя. Риски в сфере вексельного обращения. Преступления против собственности, в которых вексель является предметом посягательств. Преступления против собственности, в которых вексель является средством совершения преступления. Меры предупреждения преступлений в сфере вексельного обращения.

**Тема 8. Защита от информационных преступлений, посягающих на информационную безопасность функционирования банка**

Злоупотребления полномочиями. Коммерческий подкуп. Противоправные посягательства на сведения банка, составляющие банковскую, коммерческую и служебную тайну. Противоправные посягательства в сфере компьютерного обеспечения деятельности банка. Противоправные посягательства на кадровое обеспечение банка. Противоправные посягательства на нематериальные активы банка.

**Тема 9. Организация противодействия отмыванию преступных доходов и финансированию терроризма (информационный аспект)**

Понятие и правовая характеристика легализации (отмывания) доходов, полученных преступным путем. Криминалистическая характеристика легализации и отмывания преступных доходов. Система мер предупреждения легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма.

**Тема 10. Комплексное обеспечение информационной безопасности банка**

Информация, использующая в целях обеспечения безопасности банка, и ее источники. Бюро кредитных историй. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность банка

## 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 «Защищенные электронные технологии банка» приведена в Приложении 1.

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

**Основная литература:**

1. Гамза В.А., Ткачук И.Б.. Безопасность банковской деятельности: учебник.- 2 –е изд., перераб. и доп. – М.: Маркет ДС, 2010. (Универсететская серия).
2. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие.— М.:ИНФРА-М.,2008.-416 с.: ил.- (профессиональное образование) .
3. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. – М.: Горячая линия телеком, 2009 – 552 с.: ил.

**Дополнительная литература:**

1. Дик В.В. Банковские информационные системы: учебник. – М.: Маркет ДС, 2006.- 816 с. (Универсететская серия).
2. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М.: 2-е издание, 2007.
3. Тихонов В.А., Райх В.В., Информационная безопасность: концептуальные, правовые. Организационные и технические аспекты.: Учебное пособие. -М.: Гелиос АРВ, 2006. -528 с., ил. с.171.
4. Семененко В.А. Информационная безопасность: Учебное пособие. 3-е изд., стереотип. – М.: МГИУ, 2008. – 277 с.
5. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие. – М.: ФОРУМ, 2009. – 256 с.: ил – (Высшее образование).

**Рекомендуемая литература:**

1. Федеральный закон от 10 июля 2002 г. № 86-ФЗ «О центральном банке Российской федерации (Банке России)».
2. Стандарт Банка России СТО БР ИББС 1.0-2006

3. Федеральный закон от 27 июля 2006 г. №149 «Об информации, информационных технологиях и о защите информации».

4. Федеральный закон от 29 июля 2004 г. № 98-ФЗ (с изменениями и дополнениями от 2 февраля 2006 года № 19-ФЗ; от 24 июля 2007 года № 244 – ФЗ) « О Коммерческой тайне».

5. Федеральный закон от 27 июля 2006 г. № 152 – ФЗ «О персональных данных».

6. Указ Президента РФ от 09 сентября 2000 г. «Доктрина информационной безопасности Российской Федерации».

7. Указ Президента РФ от 16 августа 2004 г. № 1085 « Вопросы Федеральной Службы по техническому и экспортному контролю».

8. Указ Президента РФ от 06 марта 1997 г. № 188 « Об утверждении перечня сведений конфиденциального характера».

9. Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

10. Яковец Е.Н. Основы правовой защиты информации и интеллектуальной собственности: учебное пособие. – М.: Юрлитинформ, 2010. – 400 с.

11. Дединев М.А., Дыльнов Д.В. и др. Защита информации в банковском деле и электронном бизнесе. Учебно – справочное пособие – М.: КУДИЦ – ОБРАЗ, 2004. --512 с. (СКБ – специалиту по компьютерной безопасности).

**Электронные книги:**

1. Жарковская, Е. П. Финансовый анализ деятельности коммерческого банка [Электронный ресурс]: Учебник / Е.П. Жарковская. - М: Омега-Л, 2010. - 328 с. – Режим доступа:
**http://www.biblioclub.ru/book/54713/**

2. Бертунов, А.Э. Внедрение инновационных технологий в сфере банковского дела [Электронный ресурс] / А.Э. Бертунов. — М.: Лаборатория Книги, 2012. — 93 с.
**http://www.biblioclub.ru/book/140927/**

3. Исаев, Г. Н. Информационные системы в экономике[электронный ресурс]: Учебник.Доп. МО и науки РФ в кач-ве учебника для студентов вузов / Г.Н. Исаев.-3-е изд., стер. - Москва: Омега-Л, 2010. - 464 с.
**http://www.biblioclub.ru/book/54663/**

4. Шапкин, А. С. Математические методы и модели исследования операций [Электронный ресурс]: учебник / А. С. Шапкин, В. А. Шапкин. — 5-е изд. — М.: Дашков и К, 2012. — 400 с.
**http://www.biblioclub.ru/book/112204/**

5. Банковское дело [Электронный ресурс]: учебник / А.М. Тавасиева, В.А. Москвин, Н.Д. Эриашвили. - М.: ЮНИТИ-ДАНА, 2012. - 287 с.

**http://www.biblioclub.ru/book/116705/**

6. Чикида, А. Деятельность коммерческого банка в современных условиях [Электронный ресурс]: учебное пособие / А. Чикида. — М.: Лаборатория Книги, 2010. — 130 с.

**http://www.biblioclub.ru/book/100020/**

7. Николаева, И. П. Рынок ценных бумаг [Электронный ресурс]: учебник для студентов вузов, обучающихся по направлению «Экономика» / И. П. Николаева. — М.: ЮНИТИ - ДАНА , 2012. — 223 с.

**http://www.biblioclub.ru/book/118462/**

8. Кириллов, П. К. Основы менеджмента банковских услуг [Электронный ресурс] /П.К. Кириллов. - М: Лаборатория книги, 2010. - 158 с.

**http://www.biblioclub.ru/book/88353/**

9. Ковалев, П. П. Банковский риск-менеджмент [Электронный ресурс] / П.П. Ковалев. - : Финансы и статистика, 2009. - 303 с.

**http://www.biblioclub.ru/book/79604/**

10. Насреддинов, Х. Г. Учет определенных операций в банках (эмиссия пластиковых карт, учет счетов, банковские переводы) [электронный ресурс] / Х.Г. Насреддинов. - Саратов: Ай Пи Эр Медиа, 2010. - 72 с.

**http://www.biblioclub.ru/book/78803/**

11. Финансы организаций (предприятий) [Электронный ресурс]: учебник д л я студентов вузов / Н.В. Колчина [и д р . ] ; под ред. Н.В. Колчиной. — 5-е изд., перераб. и доп. — М.: ЮНИТИ-ДАНА, 2012. — 407 с.

**http://www.biblioclub.ru/book/118178/**

## 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 приведены в Приложении 2 к настоящей рабочей программе.

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

- **Перечень программного обеспечения:** MSOffice, PowerPoint.

- **Информационные справочные системы:**

1. Ресурсы информационно-образовательной среды МГОТУ.
2. Рабочая программа и методическое обеспечение по дисциплине: «Защищенные электронные технологии банка»

## 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

## «ЗАЩИЩЕННЫЕ ЭЛЕКТРОННЫЕ ТЕХНОЛОГИИ БАНКА»
**(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. | ОПК-2 | способность применять соответствующий математический аппарат для решения профессиональных задач | Тема :1,2,3,5,6,7,8,9, 10 | правовые основы обеспечения национальной безопасности Российской Федерации; | определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем | профессиональной терминологией в области информационной безопасности |
| 2. | ОПК-4 | способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации | Тема :1,2,3,4,8,9,10 | правовые основы обеспечения национальной безопасности Российской Федерации; | анализировать мировоззренческие, социально и личностно значимые философские проблемы, проводить исторический анализ событий, анализировать и оценивать социальную информацию, планировать и осуществлять свою деятельность с учетом результатов этого анализа; | навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; |
| 3. | ПК-7 | способность | Тема | основные | разрабатывать, | навыками, |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений | :1,2,3,4,6,7,8,10 | угрозы безопасности информации и модели нарушителя в автоматизированных системах | реализовывать, оценивать и корректировать процессы менеджмента информационной безопасности; | эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности |
| 4. | ПК-11 | 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 | Тема :3,4,5,7,8,9,10 | основные угрозы безопасности информации и модели нарушителя в автоматизированных системах | определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач; | навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; |
| 5. | ПСК-3 | способность проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов | Тема :3,6,7,8,9,10 | основные методы управления информационной безопасностью; | определять возможности применения теоретических положений и методов математических дисциплин для постановки и решения конкретных прикладных задач; | методиками оценки показателей качества и эффективности ЭВМ и вычислительных систем; |

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

| Код компетенции | Инструменты, оценивающие сформированность компетенции | Показатель оценивания компетенции | Критерии оценки |
|---|---|---|---|
| ОПК-2 | 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). |

| | | | |
|---|---|---|---|
| | | | 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-7 | 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-11 | 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). |

| | | | |
|---|---|---|---|
| | | | 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. |
| ПСК-3 | Контрольная работа | A) полностью сформирована<br>**5 баллов**<br>B) частично сформирована<br>**3-4 балла**<br>C) 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. |

## 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. Информационные технологии управления КБ и иные технологии оказания КБ услуги роль информационной безопасности при их применении.
2. Состав и свойства информационных объектов СБ (системы бюджетирования). Функциональность и алгоритмы СБ и ее инфомационная безопасность.
3. Информационная безопасность при оказании услуги и выполнении операций в кредитном учреждении.
4. Органические структуры. Управленческие функции и их разделение в банке. Информационное взаимодействие управленческой и аналитической служб. Организационная структура КБ. Подсистема ядра БИС. Роль и место службы информационной безопасности
5. Информационная безопасность подсистемы ведения индивидуальных счетов клиентов.
6. Информационная безопасность подсистемы работы с банковскими картами.
7. Информационная безопасность подсистемы кредитования и подсистема валютно – обменных операций.
8. Информационная безопасность подсистема операций с ценными бумагами.
9. Информационная безопасность подсистема инкассации и подсистемы межбанковского взаимодействия.
10. Информационная безопасность подсистемы управления ресурсами (дилинга).
11. Информационная безопасность в подсистеме обеспечения безопасности.
12. Информационная безопасность подсистемы генерации отчетов, планирования и анализа деятельности.
13. Информационная безопасность подсистема удаленного банковского обслуживания.
14. Информационная безопасность подсистема обеспечения внутренней деятельности банка как субъекта экономики.
15. Информационная безопасность системы электронного документооборота банка.
16. Информационная безопасность традиционных технологий расчетов.
17. Информационная безопасность и архитектура системы «Клиент – банк».

18. Информационная безопасность и способы передачи информации до компьютерной сети банка.
19. Информационная безопасность системы телефонного банкинга.
20. Информационная безопасность системы «Клиент – банк» на основе технологии «толстого клиента»

**Примерная тематика заданий на контрольную работу:**

1. Информационная безопасность модели Интернет - банкинга.
2. Информационная безопасность расчетов банковскими картами в Интернете.
3. Место ЭЦП в ряду криптографических механизмов. История возникновения ЭЦП в России. Общее правило создания ЭЦП. Общее правило верификации ЭЦП.
4. Схема защищенного информационного обмена при использовании симметричных методов защиты информации.
5. Схема защищенного информационного обмена при использовании криптографических алгоритмов с открытыми ключами.
6. Применение и информационная безопасность режима электронной кодовой книги. Режима сцепления блоков шифротекста. Режима обратной связи по шифротексту.
7. Режим счетчика (counter). Функция хеширования и асиметричные алгоритмы.
8. Информационная безопасность и защита электронных транзакций протокол (SSL). Схема работы протокола SET.
9. Информационная безопасность электронных платежуй с помощью цифровых денег.
10. Информационная безопасность расчетной функции банков и ее автоматизации. Схема обработки платежного документа клиентами.
11. Информационная безопасность и ключевые принципы для системно – значимых платежных систем. Определение количества ресурсов, которые банк будет держать на своих корсчетах.
12. Информационная безопасность и правила обмена электронными документами. Общие требования, предъявляемые к ЭД (пакетам ЭД).
13. Информационная безопасность при составление и направление ЭД участником – отправителем.
14. Информационная безопасность и порядок контроля ЭД, полученных от участников – отправителей. Порядок оформления ЭД, подтверждающих исполнение ЭД участников.
15. Информационная безопасность и порядок приема к исполнению ЭД участником – получателем. Порядок хранения и уничтожения ЭД.

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

Формой контроля знаний по дисциплине «Защищённые электронные технологии банка» 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 | ОПК-2<br>ОПК-4<br>ПК-7<br>ПК-11<br>ПСК-3 | 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 -<br>Удовлетворительно - от 51% правильных ответов.<br>Хорошо - от 70%.<br>Отлично – от 90%. |
| Согласно учебному плану | тестирование | ОПК-2<br>ОПК-4<br>ПК-7<br>ПК-11<br>ПСК-3 | 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 учебн | Экзамен | ОПК-2<br>ОПК-4<br>ПК-7 | 3 вопроса | Экзамен проводится в | Результаты предоставл | Критерии оценки:<br>«**Отлично**»: |

| | | | | | | |
|---|---|---|---|---|---|---|
| ому плану | | ПК-11 ПСК-3 | | письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут. | яются в день проведения экзамена | • 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.<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>• 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. |

### 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) Из какого материала производят банковские карточки?**
(!) бумажные;
(!) пластиковые;
(?) деревянные;
(!) металлические.

**2) В какое время появились карточки с магнитной полосой?**
(?) В 40-е гг XX столетия;
(?) в 50-е гг XX столетия;
(!) в 60-е гг XX столетия;
(?) в 70-е гг XX столетия.

**3) Какая операция проводится эмитентом в случае утери карты:**
(?) Держателю карты выносят штраф;
(!) Номер карты заносится в стоп-лист;
(?) Эмитент отказывается от сотрудничества с держателем карты.
(?) Все из вышеперечисленного.

**4) Какую операцию выполняет кассир (сотрудник предприятия торговли) при оплате картой в магазине:**
(!) Идентификацию;
(?)Аутентификацию;
(!) Авторизацию;
(?) Все эти операции.

**5) Под дебетной картой понимают?**
(!) карта позволяющая рассчитываться в пределах остатка на счете:
(?) карта позволяющая рассчитываться в пределах установленных лимитов:
(?) карта позволяющая рассчитываться в пределах как установленных лимитов так и в пределах остатка на счете:
(?) карта при выдаче которой записывается базовый остаток и дата его возобновления:

**6) «Защищенный остаток» памяти микропроцессора предназначен?**
(!) для хранения крупных денежных сумм и проведения расходных операций с предъявлением ПИНа:
(?) для хранения небольших денежных сумм :
(?) для пополнения счета карта без предъявления ПИНа:
(?) память микропроцессора не содержит «защищенный остаток»:

**7) Каким количеством способов может быть проведен этап авторизации при оплате заказных товаров у интернет-магазина?**

(!) 2
(?) 3
(?) 5
(!) 6

**8) Хранящиеся на сервере копии электронных документов по всем операциям доступны**

(!)продавцам и покупателям в любой момент времени
(?) только продавцам в течении 48часов после проведения операции расчета
(?)только покупателям в течении 48часов после проведения операции расчета
(?)продавцам в любой момент времени

**9) Платежная интернет-система ASSIST позволяет**

(!) в реальном времени проводить авторизацию и процессинг платежей, совершаемых при помощи кредитных карт с любого компьютера , подключенного к интернет
(?)в реальном времени проводить авторизацию при помощи кредитных карт с любого компьютера, подключенного к интернет
(?)в реальном времени проводить процессинг платежей, совершаемых при помощи кредитных карт с любого компьютера , подключенного к интернет
(?) верный ответ не представлен

**10) Что понимается под системой «Клиент-Банк»:**

(!) комплекс, используемый клиентами коммерческого банка и автоматизации документооборота между банком и его клиентами; (?)
(?) комплекс, используемый клиентами некоммерческого банка и автоматизации документооборота
(?) комплекс, не используемый клиентами банка
(?) нет верного варианта

**11) Основное назначение системы «Клиент-Банк»:**

(!)сократить число визитов клиента в офис банка и формализовать процесс обмена документами
(?) увеличить число визитов клиента в офис банка и формализовать процесс обмена документами
(?) формализовать процесс обмена документами
(?)увеличить количество клиентов

**12) Что имеет наибольшее значение для клиента банка в системе:**

(!) простота эксплуатации
(!)функциональная полнота системы
(?) простота внедрения
(?) защищенность от НСД

**13) Что имеет наибольшее значение для банка при функционировании системы**

(?) простота эксплуатации
(?)функциональная полнота системы
(!) простота внедрения
(!) защищенность от НСД

**14) Принципиальная особенность системы «Клиент-Банк» на основе технологии «тонкого клиента»:**

(!) вся информация передается в банк по мере её ввода клиентом
(?) информация не передаётся в банк по мере ввода клиентом
(?) клиент не вводит информацию в банк
(?) нет верного, вариант

**15) Что под собой подразумевает WAP-банкинг:**

(!) использование в качестве клиентской части системы мобильного протокола
(?)использование в качестве серверной части системы мобильного протокола
(?) использование в качестве клиентской части системы транспортного протокола
(?) нет правильного варианта

**16) Что такое WAP?**

(!) протокол, с помощью которого информация из Интернет передаётся на небольшой дисплей мобильного телефона
(?)протокол, с помощью которого информация из Интернет не передаётся на дисплей мобильного телефона
(?) устройство, с помощью которого информация из Интернет передаётся на небольшой дисплей мобильного телефона
(?) протокол, с помощью которого информация передаётся со стационарного телефона на небольшой дисплей мобильного телефона

**17) Выбор организации работы клиента с коммерческим банком зависит от факторов:**

(?)удаленность клиента от офиса банка
(?)наличие коммуникационных каналов
(?)удобство эксплуатации клиентской части системы
(!) количество клиентов банка

**18) Расшифруйте аббревиатуру WAP:**

(!)Wireless Application Protocol
(?)Wireless Application Prototype
(?)Wireless Application Protection
(?)Windows Application Protocol

**19) Что в общем случае подразумевается под интернет-банкингом:**

(!)оказание банковских услуг через интернет
(?)оказание банковских услуг через терминал
(?) оказание банковских услуг физическим лицам
(?)оказание банковских услуг юридическим лицам

**20) В системе «Клиент-Банк» возможно использование информационных технологий:**

(!)тонкий клиент
(!)толстый клиент
(?)умеренный клиент
(?)полный клиент

**21) Два основных типа каналов связи:**

(!)коммутируемый
(!) выделенный
(?) забронированный
(?)воздушный

**22) Типы уровней доступных операций взаимодействия клиента с банком:**

(!) информационный
(!)транзакционный
(?) биологический
(?)социальный

**23) Что подразумевается под SMS-банкингом:**

(!)возможность заказывать и получать информацию посредством SMS-сообщений одного из провайдеров мобильной связи
(?) возможность блокировать информацию посредством SMS-сообщений одного из провайдеров мобильной связи
(?) возможность только заказывать и получать денежные средства посредством SMS-сообщений одного из провайдеров мобильной связи
(?) нет правильного ответа

**24) Что подразумевается под переводом в валюты:**

(!)ввод формы для осуществления валютного перевода
(?)вывод формы для осуществления валютного перевода
(?)ввод формы для осуществления текстового перевода
(?) ввод формы для осуществления оплаты услуг ЖКХ

**25) Что подразумевается под обменными операциями:**

(!) операции по конвертации из одной валюты в другую
(?)операции по конвертации из одной валюты в ту же валюту
(?)операции по конвертации валового продукта
(?)нет правильного варианта

**26) Что подразумевается под регулярными платежами:**

(!) возможность заказа регулярных платежей со своего счёта на другие счета
(?) возможность заказа регулярных платежей с чужого счёта
(?) не возможность заказа регулярных платежей со своего счёта на другие
(?)возможность периодического пополнения своего счета

**27) Уровни поддержки решений для интернет - банкинга:**

(?) Базовый
(?)Расширенный
(?)Полная
(!)все варианты верны

**28) Суть классической системы «Клиент-Банк» с «толстым клиентом»:**

(!)на стороне клиента устанавливается специальное программное обеспечение, которое является частью БИС
(?) на стороне банка устанавливается специальное программное обеспечение, которое является частью БИС
(?)на стороне клиента устанавливается антивирусное программное обеспечение
(?)нет правильного варианта

**29) Расшифруйте аббревиатуру БИК:**

(!)банковский идентификационный код
(?) банковский интернет-клиент
(?) банковские, информационный коммуникации
(?) белорусский интернет-клиент

**30) Под расчётами, в рамках какой-либо коммерческой сделки, заключаемой в устрой или письменной форме понимается:**

(!)технология проведения оплаты.
(?)способ передачи денежных средств
(?)способ взаимодействия клиента с банком
(?)технология проведения расчётов

**31) Межбанковский расчёт отличается от межхозяйственных:**

(!)количественными и качественными характеристиками (?)
(?)формой проведения
(?)суммой денег, вовлечённых в расчёт
(?)участием банка в операции

**32) Безналичный расчёт осуществляется через:**

(!)Посредника
(?)Брокера
(?)Юриста
(?)Банк

**33) Безналичные расчёты бывают:**

(!)С платёжным поручением
(!)С платёжным требованием
(?)С платёжными транзакциями
(?)С платёжными рисками

**34) Телефонный банкинг выделяется за счёт:**

(!)Использования базовых телефонных функций
(?)Возможностью мобильного использования банка
(?)Использования базовых компьютерных функций

(?)Развития информационных технологий

**35) Система клиент-банк организует:**

(!)Электронный документооборот между банками и его клиентами
(?)Электронный документооборот между банками
(?)Электронный документооборот между клиентами
(?)Электронный документооборот между контрагентами

**36) Система клиент-банк основывается на технологии:**

(!)Тонкий клиент
(!)Толстый клиент
(?)Платёжный клиент
(?)Онлайн клиент

**37) Электронный чек отличается от бумажного:**

(!)Формой представления
(?)Информативностью
(?)Идентификаторами
(?)Всем вышеперечисленным

**38) Какие факторы в большей степени влияют на платёжные интернет-системы:**

(!)Экономические потребности
(?)Технологические возможности
(?)Правовая база
(?)Состоянием экономики

**39) В традиционных формах расчёта все формы безналичных расчётов выполняются через:**

(!)Финансового посредника
(?)Маклера
(?)Брокера
(?)Банк

**40) В основе внешних информационных взаимодействий коммерческого банка лежат:**

(!)Компьютерные сети
(?)Телефонные сети
(?)Банковские сети
(?)Телекоммуникационные сети

**41) Международные расчёты выполняются через систему:**

(!)SWIFT
(?)RINET
(?)EDIFER
(?)OEDIPE

**42) При разработке «Стандарты публикации финансовой отчётности коммерческих банков» в качестве начального стандарта была выбрана спецификация языка:**

(!)XBRL
(?)XLRB
(?)LBRL
(?)RBXL

### 4.2. Типовые вопросы, выносимые на экзамен

1. Понятия и концепция информационной безопасности банка.
2. Банк как объект защиты информации.
3. Система информационных угроз безопасности банка.
4. Банк как субъект борьбы с противоправными посягательствами (информационный аспект).
5. Система правового обеспечения информационной безопасности банка.
6. Правовые акты общего действия, обеспечивающие безопасность банков методами охранительного содержания.
7. Банковское законодательство: Нормативные акты Банка России и стандарт ИБ банка России.
8. Содержание аудита по ИБ технических средств обработки информации.
9. Организация системы информационной безопасности банка.
10. Субъекты обеспечения информационной безопасности банка.
11. Средства и методы обеспечения безопасности банка.
12. Организация внутреннего контроля банка (аспект ЗИ).
13. Организация службы информационной безопасности банка.
14. Система технических средств информационной безопасности банка.
15. Технические средства охраны банковских операций и продуктов.
16. Технико – криминалистические средства защиты информации банка.
17. Защита от хищения денежных средств при совершении кредитных операций.
18. Защита от хищения денежных средств с незаконным использованием пластиковых карт.
19. Защита от хищения денежных средств с использованием аккредитивов.
20. Защита от хищения денежных средств с использованием чеков.
21. Защита от хищения денежных средств с использованием платежных поручений.
22. Правовая характеристика векселя и особенности ее защиты.
23. Риски в сфере вексельного обращения и их информационная безопасность.
24. Преступления против собственности, в которых вексель является предметом посягательств (аспект ЗИ).
25. Меры предупреждения преступлений в сфере вексельного обращения (аспект ЗИ).
26. Злоупотребления полномочиями (аспект ЗИ).
27. Коммерческий подкуп (аспект ЗИ).

28. Противоправные посягательства на сведения банка, составляющие банковскую, коммерческую и служебную тайну (аспект ЗИ).

29. Противоправные посягательства в сфере компьютерного обеспечения деятельности банка (аспект ЗИ).

30. Противоправные посягательства на кадровое обеспечение банка. Противоправные посягательства на нематериальные активы банка (аспект ЗИ).

31. Понятие и правовая характеристика легализации (отмывания) доходов, полученных преступным путем (аспект ЗИ).

32. Криминалистическая характеристика легализации отмывания преступных доходов (аспект ЗИ).

33. Информационная безопасность и система мер предупреждения легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма.

34. Информация, использующая в целях обеспечения информационной безопасности банка, и ее источники.

35. Бюро кредитных историй (аспект ЗИ).

36. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на информационную безопасность банка.

**Приложение 2**

*ИНСТИТУТ ТЕХНИКИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ*

*ФАКУЛЬТЕТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ*

*КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ*

# МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

# «ЗАЩИЩЕННЫЕ ЭЛЕКТРОННЫЕ ТЕХНОЛОГИИ БАНКА»

**(Приложение 2 к рабочей программе)**

**Направление подготовки: 10.03.01 Информационная безопасность**

**Профиль: Информационно-аналитические системы финансового мониторинга**

**Квалификация (степень) выпускника: бакалавр**

**Форма обучения: очная**

Королев
2020

## 1. Общие положения

**Цель дисциплины:**

- Ускоренная адаптация студентов в предметную область информационная безопасность, опираясь на весь спектр научных воззрений, на развитие и защиту информационно - телекоммуникационной инфраструктуры и компьютерной информации в кредитно – финансовой сфере;
- Повысить уровень специальных знаний, которые необходимых обучающимся для высоко профессиональной деятельности во всех сферах информационной безопасности с учетом требований высшей школы, для активизации их учебной и исследовательской деятельности;
- Формирование у студентов специализированной базы знаний по основным понятиям в области информационной безопасности банковской деятельности;
- Приобретение студентами первичных навыков по практическому формированию комплекса документов, составляющих правовую базу защиты информации в банковской сфере.

**Задачи дисциплины:**

- ознакомить студентов с задачами в области безопасности банковской деятельности на основе действующего российского законодательства;
- научить студентов самостоятельно решать поставленные задачи в области защиты информации в банках по базовым направлениям защиты банковской тайны и конфиденциальной информации;
- формировать систему знаний у обучающихся в области защиты информации в кредитно финансовой сфере деятельности.
- изучить основы организации противодействия угрозам информационной безопасности в кредитно – финансовой сфере;
- ознакомить с системным описанием внешних угроз безопасности кредитно – финансовой деятельности, правовых и организационных основ противодействия им, а также техники обеспечения безопасности кредитно – финансовой организации;
- ознакомить с методами и средствами защиты информации банковских инструментов и технологий функциональных и контролирующих подразделений финансово – кредитных организаций.

## 2. Указания по проведению практических занятий

### Тема 1. Концептуальные основы информационной безопасности банка
### Практическое занятие 1.

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

Тема и содержание практического занятия:

*Цель работы*: Получить практические знания и навыки моделирования основных угроз безопасности банка.

*Основные положения темы занятия*:

1. базовые составляющие концепции информационной безопасности банка.

2. основные направления обеспечения информационной безопасности банковской деятельности.

*Вопросы для обсуждения:*

а) Основной доклад (реферат) по теме занятия.

1. Понятия и концепция информационной безопасности банка.
2. Банк как объект противоправных посягательств.
3. Система информационных угроз безопасности банка.
4. Банк как субъект борьбы с противоправными посягательствами.

Продолжительность занятия – 1 ч.

### Тема 2. Правовые основы информационной безопасности банка
### Практическое занятие 2.

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

Тема и содержание практического занятия:

*Цель работы*: Получить практические знания и навыки моделирования основных угроз безопасности банка в соответствии с требованиями законодательства.

*Основные положения темы занятия*:

1. базовые составляющие правого обеспечения информационной безопасности банка.

2. стратегия информационной безопасности типового банка.

*Вопросы для обсуждения:*

а) Основной доклад (реферат) по теме занятия.

1. Система правового обеспечения безопасности банка.
2. Правовые акты общего действия, обеспечивающие безопасность банков методами охранительного содержания.
3. Банковское законодательство.
4. Нормативные акты Банка России.
5. Внутренние нормативные акты.
6. Содержание аудита по информационной безопасности технических средств обработки информации.

Продолжительность занятия – 1 ч.

**Тема 3. Организационные основы информационной безопасности банка**

**Практическое занятие 3**.

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

Тема и содержание практического занятия:

*Цель работы*: Получить практические знания и навыки организации работы типовых структурных подразделений службы безопасности банка.

*Основные положения темы занятия*:

1. базовые составляющие организационного обеспечения информационной безопасности банка.

*Вопросы для обсуждения:*

а) Основной доклад (реферат) по теме занятия.

1. Организация системы безопасности банка.
2. Субъекты обеспечения безопасности банка.
3. Средства и методы обеспечения безопасности банка. Организация внутреннего контроля банка.
4. Организация службы безопасности банка.

Продолжительность занятия – 1 ч.

**Тема 4. Техника обеспечения информационной безопасности банка**

**Практическое занятие 4**.

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

Тема и содержание практического занятия:

*Цель работы*: Получить практические знания и навыки организации работы типовых структурных подразделений службы безопасности банка.

*Основные положения темы занятия*:

1. технические средства охраны банка.
2. безопасность банковских расчетов

*Вопросы для обсуждения:*

а) Основной доклад (реферат) по теме занятия.

1. Система технических средств информационной безопасности банка. Технические средства охраны.
2. Технические средства охраны банковских операций и продуктов.
3. Технико – криминалистические средства.

Продолжительность занятия – 1 ч.

**Тема 5. Защита от информационных преступлений, посягающих на собственность банка**

**Практическое занятие 5**.

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

Тема и содержание практического занятия:

*Цель работы*: Получить практические знания и навыки организации работы службы безопасности по проведению расследований инцидентов информационной безопасности.

*Основные положения темы занятия*:

1. Характеристика преступлений связанных с хищением денежных средств.
2. безопасность банковских расчетов

*Вопросы для обсуждения:*

а) Основной доклад (реферат) по теме занятия.

1. Хищения денежных средств при совершении кредитных операций.
2. Хищения денежных средств с незаконным использованием пластиковых карт.
3. Хищения денежных средств с использованием аккредитивов.
4. Хищение денежных средств с использованием чеков. Хищение денежных средств с использованием платежных поручений.

Продолжительность занятия – 2 ч.

## Тема 6. Стандарты информационной безопасности банка

### Практическое занятие 6.

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

Тема и содержание практического занятия:

*Цель работы*: Получить практические знания и навыки организации учета требований стандартов информационной безопасности банка.

*Основные положения темы занятия*:

1. Характеристика российских и международных стандартов банковской деятельности.

*Вопросы для обсуждения:*

а) Основной доклад (реферат) по теме занятия.

1. О Стандарте Банка России “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения.
2. Основные цели и задачи стандарта Банка России при обеспечении информационной безопасности.
3. Основные направления работы по дальнейшему сопровождению и доработке Стандарта в рамках специально созданного Подкомитетом 3 “Защита информации в кредитно-финансовой сфере” Технического комитета 362 “Защита информации” Федерального агентства по техническому регулированию и метрологии.
4. Аудит информационной безопасности банка.
5. Преимущества и недостатки выполнения работ по защите ПДн в рамках Стандарт Банка России СТО БР ИББС 1.0-2006.

Продолжительность занятия – 2 ч.

## Тема 7. Хищения денежных средств и иного имущества с использованием векселей (информационный аспект)

### Практическое занятие 7.

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

Тема и содержание практического занятия:

*Цель работы*: Получить практические знания и навыки в противодействии хищения денежных средств в сфере вексельного обращения.

*Основные положения темы занятия*:

1. Противодействие хищению денежных средств и иного имущества с использованием векселей.

*Вопросы для обсуждения:*

а) Основной доклад (реферат) по теме занятия.

1. Правовая характеристика векселя. Риски в сфере вексельного обращения.
2. Преступления против собственности, в которых вексель является предметом посягательств.
3. Преступления против собственности, в которых вексель является средством совершения преступления.
4. Меры предупреждения преступлений в сфере вексельного обращения.

Продолжительность занятия – 2 ч.

## Тема 8. Защита от информационных преступлений, посягающих на информационную безопасность функционирования банка

### Практическое занятие 8.

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

Тема и содержание практического занятия:

*Цель работы*: Получить практические знания и навыки в защите от информационных преступлений.

*Основные положения темы занятия*:

1. Противодействие преступлениям, посягающим на информационную безопасность банка.

*Вопросы для обсуждения:*

а) Основной доклад (реферат) по теме занятия.

1. Злоупотребления полномочиями.
2. Коммерческий подкуп.
3. Противоправные посягательства на сведения банка, составляющие банковскую, коммерческую и служебную тайну.
4. Противоправные посягательства в сфере компьютерного обеспечения деятельности банка.
5. Противоправные посягательства на кадровое обеспечение банка.
6. Противоправные посягательства на нематериальные активы банка.

Продолжительность занятия – 2 ч.

**Тема 9. Организация противодействия отмыванию преступных доходов и финансированию терроризма (информационный аспект)**

**Практическое занятие 9**.

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

Тема и содержание практического занятия:

*Цель работы*: Получить практические знания и навыки в противодействии отмыванию доходов полученных преступным путем.

*Основные положения темы занятия*:

1. Противодействие преступлениям, с вязанных с отмыванием доходов полученных преступным путем и финансированием терроризма.

*Вопросы для обсуждения:*

а) Основной доклад (реферат) по теме занятия.

1. Понятие и правовая характеристика легализации (отмывания) доходов, полученных преступным путем.
2. Криминалистическая характеристика легализации (отмывания преступных доходов).
3. Система мер предупреждения легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма.

Продолжительность занятия – 2 ч.

**Тема 10. Комплексное обеспечение информационной безопасности банка**

**Практическое занятие 10**.

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

Тема и содержание практического занятия:

*Цель работы*: Получить практические знания и навыки в формировании комплексной системы информационной безопасности банка.

*Основные положения темы занятия*:

1. Основные требования предъявляемые к системе обеспечения банковской деятельности.

*Вопросы для обсуждения:*

а) Основной доклад (реферат) по теме занятия.

1. Информация, использующая в целях обеспечения безопасности банка, и ее источники.
2. Бюро кредитных историй.
3. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность банка.

Продолжительность занятия – 2 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 существующих современных аппаратных средств вычислительной техники;

2) привить навыки самостоятельного решения нестандартных задач в области аппаратных средств вычислительной техники.

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 | **76** |
| Вопросы, выносимые на самостоятельное изучение | 34 |
| Подготовка к практическим занятиям | 16 |
| Подготовка к лабораторным занятиям | - |
| Подготовка докладов | 10 |
| Выполнение практических заданий | 16 |

**Вопросы, выносимые на самостоятельное изучение:**

**для очной формы обучения:**

1. Информационные технологии управления КБ и иные технологии оказания КБ услуги роль информационной безопасности при их применении.
2. Состав и свойства информационных объектов СБ (системы бюджетирования). Функциональность и алгоритмы СБ и ее инфомационная безопасность.
3. Информационная безопасность при оказании услуги и выполнении операций в кредитном учреждении.
4. Органические структуры. Управленческие функции и их разделение в банке. Информационное взаимодействие управленческой и аналитической служб. Организационная структура КБ. Подсистема ядра БИС. Роль и место службы информационной безопасности
5. Информационная безопасность подсистемы ведения индивидуальных счетов клиентов.
6. Информационная безопасность подсистемы работы с банковскими картами.
7. Информационная безопасность подсистемы кредитования и подсистема валютно – обменных операций.

8. Информационная безопасность подсистема операций с ценными бумагами.
9. Информационная безопасность подсистема инкассации и подсистемы межбанковского взаимодействия.
10. Информационная безопасность подсистемы управления ресурсами (дилинга).
11. Информационная безопасность в подсистеме обеспечения безопасности.
12. Информационная безопасность подсистемы генерации отчетов, планирования и анализа деятельности.
13. Информационная безопасность подсистема удаленного банковского обслуживания.
14. Информационная безопасность подсистема обеспечения внутренней деятельности банка как субъекта экономики.
15. Информационная безопасность системы электронного документооборота банка.
16. Информационная безопасность традиционных технологий расчетов.
17. Информационная безопасность и архитектура системы «Клиент – банк».
18. Информационная безопасность и способы передачи информации до компьютерной сети банка.
19. Информационная безопасность системы телефонного банкинга.

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 | 34 | Изучение открытых источников |
| 2. | Подготовка к практическим занятиям | 16 | Изучение открытых источников при подготовке доклада на выбранную тему. |
| 3. | Подготовка к лабораторным занятиям | - | |
| 4. | Тематика докладов | 10 | См. примерные темы докладов |
| 5. | Выполнение практических заданий | 16 | Информационная безопасность ДБО |

## Примерные темы докладов

1. Информационная безопасность подсистемы ведения индивидуальных счетов клиентов.
2. Информационная безопасность подсистемы работы с банковскими картами.
3. Информационная безопасность подсистемы кредитования и подсистема валютно – обменных операций.
4. Информационная безопасность подсистема операций с ценными бумагами.
5. Информационная безопасность подсистема инкассации и подсистемы межбанковского взаимодействия.
6. Информационная безопасность подсистемы управления ресурсами (дилинга).
7. Информационная безопасность в подсистеме обеспечения безопасности.
8. Информационная безопасность подсистемы генерации отчетов, планирования и анализа деятельности.
9. Информационная безопасность подсистема удаленного банковского обслуживания.
10. Информационная безопасность подсистема обеспечения внутренней деятельности банка как субъекта экономики.
11. Информационная безопасность системы электронного документооборота банка.
12. Информационная безопасность традиционных технологий расчетов.
13. Информационная безопасность и архитектура системы «Клиент – банк».
14. Информационная безопасность и способы передачи информации до компьютерной сети банка.
15. Информационная безопасность системы телефонного банкинга.
16. Информационная безопасность системы «Клиент – банк» на основе технологии «толстого клиента»
17. Информационная безопасность модели Интернет - банкинга.

## 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. Основная часть работы раскрывает процесс проектирования заданного аппаратного устройства и должна содержать соответствующие таблицы или временные диаграммы, которые должны формироваться разрабатываемым устройством, принципиальную схему устройства и описание его работы.

3. В процессе изложения материала необходимо давать ссылки на используемую литературу.

4. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

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

### 5.3. Требования к оформлению

Объём контрольной работы – 5-6 страниц формата А4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

## 6. Перечень основной и дополнительной учебной литературы

**Основная:**


1. Гамза В.А., Ткачук И.Б.. Безопасность банковской деятельности: учебник.- 2 –е изд., перераб. и доп. – М.: Маркет ДС, 2010. (Универсететская серия).
2. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие.— М.:ИНФРА-М.,2008.-416 с.: ил.- (профессиональное образование) .
3. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. – М.: Горячая линия телеком, 2009 – 552 с.: ил.


**Дополнительная:**


1. Дик В.В. Банковские информационные системы: учебник. – М.: Маркет ДС, 2006.- 816 с. (Универсететская серия).
2. Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. М.: 2-е издание, 2007.
3. Тихонов В.А., Райх В.В., Информационная безопасность: концептуальные, правовые. Организационные и технические аспекты.: Учебное пособие. -М.: Гелиос АРВ, 2006. -528 с., ил. с.171.
4. Семененко В.А. Информационная безопасность: Учебное пособие. 3-е изд., стереотип. – М.: МГИУ, 2008. – 277 с.
5. Ищейнов В.Я., Мецатунян М.В. Защита конфиденциальной информации: учебное пособие. – М.: ФОРУМ, 2009. – 256 с.: ил – (Высшее образование).

**Рекомендуемая:**


1. Федеральный закон от 10 июля 2002 г. № 86-ФЗ «О центральном банке Российской федерации (Банке России)».
2. Стандарт Банка России СТО БР ИББС 1.0-2006
3. Федеральный закон от 27 июля 2006 г. №149 «Об информации, информационных технологиях и о защите информации».
4. Федеральный закон от 29 июля 2004 г. № 98-ФЗ (с изменениями и дополнениями от 2 февраля 2006 года № 19-ФЗ; от 24 июля 2007 года № 244 – ФЗ) « О Коммерческой тайне».
5. Федеральный закон от 27 июля 2006 г. № 152 – ФЗ «О персональных данных».
6. Указ Президента РФ от 09 сентября 2000 г. «Доктрина информационной безопасности Российской Федерации».
7. Указ Президента РФ от 16 августа 2004 г. № 1085 « Вопросы Федеральной Службы по техническому и экспортному контролю».
8. Указ Президента РФ от 06 марта 1997 г. № 188 « Об утверждении перечня сведений конфиденциального характера».
9. Постановление Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".
10. Яковец Е.Н. Основы правовой защиты информации и интеллектуальной собственности: учебное пособие. – М.: Юрлитинформ, 2010. – 400 с.
11. Дединев М.А., Дыльнов Д.В. и др. Защита информации в банковском деле и электронном бизнесе. Учебно – справочное пособие – М.: КУДИЦ – ОБРАЗ, 2004. –512 с. (СКБ – специалиту по компьютерной безопасности).


**Электронные книги:**


1. Жарковская, Е. П. Финансовый анализ деятельности коммерческого банка [Электронный ресурс]: Учебник / Е.П. Жарковская. - М: Омега-Л, 2010. - 328 с. – Режим доступа: **http://www.biblioclub.ru/book/54713/**
2. Бертунов, А.Э. Внедрение инновационных технологий в сфере банковского дела [Электронный ресурс] / А.Э. Бертунов. — М.: Лаборатория Книги, 2012. — 93 с. **http://www.biblioclub.ru/book/140927/**
3. Исаев, Г. Н. Информационные системы в экономике[электронный ресурс]: Учебник.Доп. МО и науки РФ в кач-ве учебника для студентов вузов / Г.Н. Исаев.-3-е изд., стер. - Москва: Омега-Л, 2010. - 464 с. **http://www.biblioclub.ru/book/54663/**
4. Шапкин, А. С. Математические методы и модели исследования операций [Электронный ресурс]: учебник / А. С. Шапкин, В. А.

Шапкин. — 5-е изд. — М.: Дашков и К, 2012. — 400 с.
**http://www.biblioclub.ru/book/112204/**

5. Банковское дело [Электронный ресурс]: учебник / А.М. Тавасиева, В.А. Москвин, Н.Д. Эриашвили. - М.: ЮНИТИ-ДАНА, 2012. - 287 с.
**http://www.biblioclub.ru/book/116705/**
6. Чикида, А. Деятельность коммерческого банка в современных условиях [Электронный ресурс]: учебное пособие / А. Чикида. — М.: Лаборатория Книги, 2010. — 130 с.
**http://www.biblioclub.ru/book/100020/**
7. Николаева, И. П. Рынок ценных бумаг [Электронный ресурс]: учебник для студентов вузов, обучающихся по направлению «Экономика» / И. П. Николаева. — М.: ЮНИТИ - ДАНА , 2012. — 223 с.
**http://www.biblioclub.ru/book/118462/**
8. Кириллов, П. К. Основы менеджмента банковских услуг [Электронный ресурс] /П.К. Кириллов. - М: Лаборатория книги, 2010. - 158 с.
**http://www.biblioclub.ru/book/88353/**
9. Ковалев, П. П. Банковский риск-менеджмент [Электронный ресурс] / П.П. Ковалев. - : Финансы и статистика, 2009. - 303 с.
**http://www.biblioclub.ru/book/79604/**
10. Насреддинов, Х. Г. Учет определенных операций в банках (эмиссия пластиковых карт, учет счетов, банковские переводы) [электронный ресурс] / Х.Г. Насреддинов. - Саратов: Ай Пи Эр Медиа, 2010. - 72 с.
**http://www.biblioclub.ru/book/78803/**
11. Финансы организаций (предприятий) [Электронный ресурс]: учебник д л я студентов вузов / Н.В. Колчина [и д р . ] ; под ред. Н.В. Колчиной. — 5-е изд., перераб. и доп. — М.: ЮНИТИ-ДАНА, 2012. — 407 с.
**http://www.biblioclub.ru/book/118178/**

## 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, Multisim.*

**Информационные справочные системы:**

1. Ресурсы информационно-образовательной среды МГОТУ
2. Рабочая программа и методическое обеспечение по дисциплине «Защищенные электронные технологии банка».